WILEY

КИБЕР БЕЗОПАСНОСТЬ

ГЛАВНЫЕ ПРИНЦИПЫ

РИК ХОВАРД

Обновленные стратегии и тактики

the cyberwire

Cybersecurity First Principles

A Reboot of Strategy and Tactics

Presented by the cyberwire

Rick Howard

WILEY

Кибербезопасность главные принципы

Обновленные стратегии и тактики

Рик Ховард

ПИТЕР®
Санкт-Петербург • Москва • Минск
2024

Рик Ховард

Кибербезопасность: главные принципы

Серия «Библиотека программиста»

Перевел с английского С. Черников

Руководитель дивизиона	*Ю. Сергиенко*
Руководитель проекта	*А. Питиримов*
Ведущий редактор	*Н. Гринчик*
Научный редактор	*Д. Старков*
Литературный редактор	*Н. Рощина*
Художественный редактор	*В. Мостипан*
Корректоры	*Е. Павлович, Н. Терех*
Верстка	*Г. Блинов*

ББК 32.988.02-018-07
УДК 004.056.53

Ховард Рик

Х68 Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-2201-1

С 1970-х годов InfoSec-специалисты постепенно совершенствовали безопасность, даже не задумываясь, в правильном ли направлении со стратегической точки зрения они движутся. Рик Ховард утверждает, что нет. Общее направление само по себе было ошибочным, но идейные лидеры в этой области так и не смогли докопаться до корня проблемы. Идя по стопам таких авторитетов, как Декарт и Илон Маск, автор обосновывает главный принцип кибербезопасности и определяет стратегии и тактики его реализации.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ISBN 978-1394173082 англ.
ISBN 978-5-4461-2201-1

Изготовлено в России. Изготовитель: ООО «Прогресс книга». Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург, Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 05.2024. Наименование: книжная продукция. Срок годности: не ограничен.

Налоговая льгота — общероссийский классификатор продукции ОК 034-2014, 58.11.12 — Книги печатные профессиональные, технические и научные.

Импортер в Беларусь: ООО «ПИТЕР М», 220020, РБ, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс: 208 80 01.

Подписано в печать 22.03.24. Формат 70×100/16. Бумага офсетная. Усл. п. л. 25,800. Тираж 700. Заказ 0000.

Краткое содержание

Оглавление

Посвящается людям, о которых никто не имеет представления и которым предстоит делать то, что никто не может себе представить. Пришло время сделать шаг вперед.

Рик Ховард, автор книги

Посвящается Сенеке, сказавшему, что «самая короткая и беспокойная жизнь бывает у людей, которые не помнят прошлого, пренебрегают настоящим и боятся будущего». Я бы посвятил эту книгу своей семье, но они никогда ее не прочтут.

Стив Винтерфельд, научный редактор

Посвящается специалистам по кибербезопасности, а также хакерам и киберпреступникам, без которых у нас не было бы работы.

Брендон Карпф, научный редактор

Об авторе

Рик Ховард и Стив Винтерфельд крепко дружат уже более 20 лет и все это время спорят обо всем на свете, в том числе о кибербезопасности. Брендон Карпф — коллега Рика по The CyberWire, где одна из его самых обременительных задач сводится к тому, чтобы заставлять Рика придерживаться фактов и выражаться предельно ясно. Памятуя слова Стивена Кинга, эти ребята не дают Рику превратиться в литературного пустозвона.

Рик является главным аналитиком и старшим научным сотрудником крупнейшей в мире сети подкастов, посвященных кибербезопасности в сфере B2B, — The CyberWire, а также руководителем отдела безопасности N2K (материнской компании The CyberWire). Ранее он возглавлял отдел безопасности в компании Palo Alto Networks (коммерческий поставщик услуг в сфере кибербезопасности), работал директором по информационной безопасности в TASC (оборонный подрядчик), генеральным директором iDefense (коммерческая служба анализа киберугроз компании VeriSign), директором глобального SOC-центра компании Counterpane (один из первых поставщиков управляемых услуг по обеспечению безопасности) и командиром группы реагирования на инциденты компьютерной безопасности армии США (отвечает за координацию операций по защите сети, сетевой разведке и реализации атак в глобальной армейской сети). Один из основателей Cyber Threat Alliance (центр обмена информацией и ее анализа для поставщиков систем безопасности) и Cybersecurity Canon Project (Зал славы книг по кибербезопасности). На протяжении многих лет Рик занимался построением организаций с нуля и повышением продуктивности существующих организаций путем разработки стратегий и тактик, соответствующих требованиям высшего руководства. В течение пяти лет он преподавал информатику в Военной академии США и, несмотря на множество ролей, которые ему довелось играть на протяжении своей сорокалетней карьеры, он считает себя прежде всего учителем.

О научных редакторах

Стив Винтерфельд — консультирующий директор по информационной безопасности (ИБ) компании Akamai, где он сотрудничает с клиентами по вопросам стратегии, учит сотрудников службы безопасности и отдела продаж обдумывать актуальные проблемы безопасности и помогает формировать видение продуктовой линейки. До прихода в Akamai он занимался разработкой программ обеспечения безопасности в качестве директора по ИБ банка Nordstrom, директора по кибербезопасности в Nordstrom Corp., а также был руководителем отдела реагирования на инциденты и анализа угроз компании Charles Schwab. Стив познакомился с Риком, когда работал старшим техническим директором и руководителем группы по кибербезопасности компании Northrop Grumman, где создал RCERT South — Южноамериканскую группу реагирования на инциденты компьютерной безопасности армии США. Имеет богатый опыт работы в сфере розничной торговли, финансов, разведки и исполнения государственных контрактов и при этом отлично понимает, как создавать программы обеспечения оперативной обороны, соответствующие нормативным требованиям и способные противостоять как хакерам, так и аудиторам. Стив опубликовал две книги о кибервойнах (одна из них является кандидатом на попадание в Зал славы Cybersecurity Canon), имеет сертификаты CISSP, ITIL и PMP. Стив — постоянный участник группы The CyberWire Hash Table, делится своими экспертными знаниями в нескольких подкастах Рика.

Брендон Карпф — исполнительный директор по развитию новых рынков компании N2K Networks. Ранее он работал техническим редактором и руководителем отдела стратегического планирования в CyberWire, был офицером Центра подготовки к информационным войнам ВМС США. Во время службы в ВМС Брендон занимал должность старшего вахтенного офицера и начальника отделения в отделе обеспечения работы компьютерных сетей Агентства национальной безопасности, в киберкомандовании США — начальника оперативного отдела, в Военно-морской академии США был адъюнкт-профессором в сфере кибернауки. Служил начальником отдела подготовки к информационным войнам на корабле USS Boxer, где являлся экспертом в области криптологии, радиоэлектронной разведки,

электронной войны и информационных операций. Брендон с отличием окончил Военно-морскую академию США по специальности «Робототехника и проектирование систем управления», получил степень магистра наук в Массачусетском технологическом институте. Кроме того, он написал множество статей и докладов в области национальной безопасности и политики обеспечения кибербезопасности, кибервойн и операций, технологических рисков и соответствия нормативным требованиям, передовых сетевых архитектур и экосистем оборонных технологий. Он является преподавателем и одним из активнейших слушателей подкастов.

Благодарности

Писать книгу оказалось гораздо сложнее, чем я думал. Мне понравился этот процесс, но надо признать, что на протяжении всего пути мне помогало множество людей. Я бы ни за что не справился с этой задачей в одиночку.

Прежде всего хочу поблагодарить свою замечательную супругу Кэти. Пока я писал книгу, она следила за своевременным выполнением домашних дел, отвлекала меня от потенциальных катастроф и мирилась с моими резкими ответами на важные семейные вопросы. Спасибо, дорогая. Ты самая лучшая жена в мире.

Особую благодарность хочу выразить бывшему начальнику Марку Маклафлину. Я имел честь и удовольствие сотрудничать с ним дважды на протяжении своей карьеры — в VeriSign и Palo Alto Networks. Он — лучший руководитель из всех, на кого я когда-либо работал (как в военном, так и в коммерческом секторе), а также потрясающий человек. Спасибо, Марк. Если вам что-нибудь понадобится, просто позвоните.

Хочу выразить признательность своему нынешнему начальнику Питеру Килпу — генеральному директору компании N2K Networks. Когда в начале 2022 года я пришел к нему и сказал: «Я думаю, что у меня достаточно материала для книги, публикацию которой может спонсировать компания», он не посмеялся надо мной и не выгнал из кабинета. Он даже связался со своими приятелями в издательстве Wiley и убедил их в том, что это хорошая идея. Питер, я бесконечно вам благодарен.

Также хочу поблагодарить своего лучшего друга Стива Винтерфельда — одного из редакторов этой книги. Именно ему я звоню, когда мне нужно уехать из страны по той или иной причине. Это тот человек, который делает все без лишних вопросов. Кроме того, это один из умнейших людей на планете в том, что касается кибербезопасности. Многолетняя дружба с ним и бурные обсуждения вопросов кибербезопасности (и посвященных этой теме фильмов) сильно повлияли на мое собственное видение этой области. Помимо прочего, он способен указать на мои глупые ошибки как в жизни, так и при написании книги. Я люблю тебя, дружище.

Хочу сказать спасибо коллегам по The CyberWire Джону Петрику, Элиоту Пельтцману и Брендону Карпфу. Большое количество материала в этой книге взято из статей, которые я писал для своего подкаста *CSO Perspectives*. Джон отредактировал все эти материалы и сделал так, чтобы я не выглядел полным идиотом. Он весьма плодовитый писатель, чье мастерство и зоркий взгляд помогли мне улучшить свои навыки как автора. Отдельные неудачные моменты — это результат того, что я не прислушался к его советам. Элиот с самого начала был моим звукорежиссером в The CyberWire. Его понимание того, что звучит хорошо, а что — нет, сделало из меня гораздо лучшего рассказчика. Наконец, Брендон, один из редакторов книги и относительный новичок по сравнению с остальными старожилами, способен впитывать информацию как губка и быстро указывать на речевые и логические ошибки, которые я никогда бы не обнаружил самостоятельно. Спасибо вам всем.

Я также хочу поблагодарить своего друга и коллегу Джека Фройнда за рецензирование главы, посвященной прогнозированию рисков. Чтение книги Джека *Measuring and Managing Information Risk: A Fair Approach*, написанной в соавторстве с Джеком Джонсом и включенной в Зал славы Cybersecurity Canon, стало моим первым шагом на пути к пониманию темы прогнозирования рисков. Когда я обращался к Джеку за помощью, он всегда откликался. Спасибо вам, сэр.

Благодарю своего друга Джорджа Финни, который любезно отрецензировал главу, посвященную стратегии нулевого доверия. Он сам написал книгу *Project Zero Trust: A Story about a Strategy for Aligning Security and the Business*, которую я очень рекомендую. Мы с Джорджем познакомились много лет назад благодаря интересу к книгам и кибербезопасности. Спасибо за помощь, Джордж. Твоя рецензия успокоила меня и убедила в том, что я живу не в сумасшедшем мире.

Благодарю свою давнюю коллегу и подругу Джорджиану (Джорджи) Ши. Я не раз обращался к ней за помощью в ходе работы над своими проектами (Cybersecurity Canon и The CyberWire Hash Table), она здорово помогла мне и в этот раз, отрецензировав главу, посвященную киберустойчивости. Джорджи, ты лучше всех.

Я также хочу сказать спасибо Адаму Барлоу и Шридеви Джоши, которые часами сидели со мной у доски в поисках простого способа оценки риска. С каждой нашей встречей я на шаг приближался к цели. Их рецензия на главу о прогнозировании риска была бесценной.

Выражаю признательность своему новому другу и коллеге Джону Эйбену, который превратил мои заметки, сделанные мелками и скотчем, в прекрасные иллюстрации. Благодаря его работе я даже стал гораздо лучше понимать собственные идеи. Благодарю тебя, Джон.

Наконец, я хочу сказать спасибо своим коллегам из издательства Wiley за помощь в редактировании книги. Именно их надежные руки помогли мне, автору-новичку, не сбиться с пути. Особую благодарность выражаю Джиму Минателу, Дебиану Уизерспуну, Питу Гогану, Мелиссе Берлок, Магешу Элановану и Киму Вимпсету.

Предисловие. Кто мы такие

> Я не хотел писать книгу, даже такую короткую, как эта, из-за которой я чувствовал бы себя литературным пустозвоном или трансцендентальным кретином. Благо таких книг и таких писателей на рынке предостаточно.
>
> *Стивен Кинг, писатель*

За мою карьеру мне довелось поработать генеральным директором в двух замечательных компаниях — VeriSign и Palo Alto Networks. С некоторыми выдающимися людьми мне посчастливилось работать в обеих компаниях, и Рик Ховард был одним из таких специалистов. В те времена, когда компания VeriSign была не только ведущим поставщиком интернет-инфраструктуры, но и значимым игроком в сфере безопасности, Рик руководил бизнесом под названием iDefense. Именно тогда я впервые увидел его в качестве практикующего специалиста по ИБ, евангелиста, лидера и рассказчика, что является редким сочетанием в любой сфере, тем более в области безопасности. Мне посчастливилось поучиться у него, в том числе умению объяснять очень сложные вещи доступно и понятно.

Рик умеет воспринимать общую картину, не упуская из виду сиюминутных потребностей, с которыми сталкиваются специалисты по кибербезопасности. Как оказалось, этот навык очень полезен в сфере, которая развивается с огромной скоростью и на переднем крае которой находятся злоумышленники. Поэтому неудивительно, что вскоре после прихода в Palo Alto Networks в 2011 году я попытался привлечь Рика к работе в качестве нашего первого руководителя отдела безопасности (CSO). Несмотря на то что в то время эта компания была довольно небольшой и я не смог четко описать ему роль CSO, Рик присоединился к нам, разделив наши видение и миссию, направленную на защиту цифрового образа жизни. Он быстро стал неотъемлемой частью команды и пользовался большим авторитетом у наших клиентов, потенциальных заказчиков и в отрасли в целом.

Рик сыграл важную роль в создании и успешной работе таких организаций, как Unit 42 (первая в компании публичная группа киберразведки), Cyber Threat Alliance (первый центр обмена информацией и ее анализа для поставщиков систем безопасности), CyberSecurity Canon Project и Joint Service Academy Cyber Summit. На этом пути он продемонстрировал свою удивительную способность обобщать всю историю кибербезопасности, делать ее актуальной для конкретного слушателя, а также давать советы и рекомендации относительно вероятного будущего этой сферы. Учитывая его способности и увлеченность, совсем не удивительно, что в настоящее время Рик является директором по безопасности, старшим научным сотрудником и главным аналитиком компании The CyberWire, а его статьи и подкасты пользуются огромной популярностью. Я часто советую послушать Рика новичкам в сфере кибербезопасности, желающим понять, что в ней происходит. И когда люди пишут такие книги, как *The Perfect Weapon* и *This Is How They Tell Me The World Ends*, они в первую очередь упоминают людей вроде Рика. В своей новой книге, которую вы держите в руках, он поделился мудростью, опытом и актуальными советами, а главное — объяснил важность основополагающих принципов обеспечения кибербезопасности. Я уверен, что она вам понравится и принесет пользу.

И не забудьте ознакомиться со всеми подкастами Рика на сайте CyberWire. Они все замечательные. Однако если вы намерены прослушать только один из них, то пусть это будет *A CSO's 9/11 Story: CSO Perspective*. Из него вы узнаете все, что нужно знать о Рике. В Вест-Пойнте, нашей общей альма-матер, говорили, что лидеры — это те, кто бежит на звук выстрела, а не прочь от него. Именно таким лидером и является Рик.

Приятного чтения!

Марк Маклафлин, бывший президент,
генеральный директор и председатель совета
директоров компании Palo Alto Networks,
председатель совета директоров компании
Qualcomm, Inc., член и бывший председатель
Консультативного совета национальной
безопасности США в сфере телекоммуникаций

Введение

Наметьте свое будущее, но сделайте это карандашом. Дорога впереди будет настолько длинной, насколько вы захотите. Сделайте так, чтобы путешествие оказалось стоящим.

Джон Бон Джови, американский певец, автор песен, гитарист и актер

Для кого предназначена книга

Эта книга посвящена переосмыслению темы кибербезопасности с использованием идеи *базовых принципов*. Я подробно объясню, что имею в виду, в главе 3 «Нулевое доверие», но по сути речь идет о фундаментальных истинах, лежащих в основе построения любой программы обеспечения кибербезопасности. Таким образом, при написании книги я ориентировался на широкий круг специалистов по ИБ, относящихся к трем группам.

Первая группа состоит из *руководителей отделов безопасности*. Это мои коллеги и люди, которые работают на них, обеспечивая кибербезопасность коммерческого сектора, правительственных (как политических, так и технических) и научных кругов. С помощью идеи базовых принципов я собираюсь бросить вызов тому, как представляют себе кибербезопасность ветераны сферы сетевой защиты. Я хочу доказать, что на протяжении последних 25 лет мы делали это неверно, и рассмотрение основных принципов поможет вернуться на правильный путь и изменить нынешний образ мышления, чтобы занять оборонительные позиции, обеспечивающие более высокую вероятность успеха.

Вторая группа — *новички в сфере кибербезопасности*. Это молодые свеженспеченные выпускники вузов, государственные служащие, перешедшие

в коммерческий сектор, а также люди, уставшие от прежней работы и рассматривающие построение карьеры в области кибербезопасности как более интересное и прибыльное занятие. Я дам этим людям базовые знания, основанные на фундаментальных принципах, а также познакомлю их с историей сферы кибербезопасности, чтобы они понимали, каковы текущее положение дел и потенциальные направления развития.

К последней группе относятся *преподаватели и студенты начальных и старших курсов*. В рамках дисциплины «Кибербезопасность» возможно множество важных и увлекательных направлений, которые, по мнению многих студентов и преподавателей, слабо связаны между собой и из-за большого объема материала кажутся непосильными для изучения. Описанные в этой книге базовые принципы кибербезопасности станут основой вашей учебной программы. Я покажу, как можно все свести к основным принципам, что позволит студентам справиться с тем объемом материала, который им предстоит изучить.

При этом специалисты по защите сетей, как правило, работают в организациях трех типов: коммерческих, государственных и научных. Я могу привести аргументы в пользу существования двух категорий защитников правительственных сетей: традиционных защитников (делающих то же, что и их коллеги из коммерческих и научных организаций) и специалистов по наступательным операциям, занимающихся шпионажем и низкоуровневыми киберконфликтами (кибервойнами). В книге речь пойдет только о первой категории.

Наконец, с самых первых дней существования Интернета в плане сетевой защиты организации находились в промежутке между «имущими» и «неимущими», и их место в нем обычно, но не всегда зависело от размера организации. «Неимущими», как правило, оказываются небольшие организации (например, стартапы и органы власти городского/окружного уровня), у которых едва хватает средств на оплату счетов за электричество. К «имущим» в основном относятся крупные организации (например, компании из списка Fortune 500), обладающие большим количеством свободных ресурсов. Я опишу основанные на базовых принципах кибербезопасности стратегии и тактики, которые должна учитывать любая организация, реализующая программу информационной безопасности, независимо от ее размера. Полноценное внедрение всех этих стратегий и концепций требует больших затрат, что по силам лишь крупным компаниям. Тем не менее их нельзя считать некими

чек-листами. Это способы, позволяющие снизить вероятность нанесения существенного ущерба. В зависимости от условий, в которых вы находитесь, одни из них будут работать лучше, чем другие. Специально для «неимущих» я по возможности постараюсь описать способы реализации этих идей при ограниченном бюджете.

О чем пойдет речь

Базовые принципы той или иной проблемной области настолько фундаментальны, что являются самоочевидными; настолько элементарны, что ни один специалист в данной области не может их оспорить; настолько важны для ее понимания, что без них инфраструктура, на которой держится наша передовая практика, рассыпалась бы как песчаный замок во время прилива. Они атомарны. Эксперты используют их как строительные блоки для получения всего остального, что известно в выбранной проблемной области. Все новые знания, полученные в ней, зависят от ранее сформулированных основных принципов. Это означает, что существует некий абсолютный первичный принцип, дающий начало всему.

В научных кругах, правительстве и коммерческом секторе начали осознавать пользу Интернета в начале 1990-х годов. Примерно в то же время киберзлодеи открыли возможности использования Сети для совершения преступлений, шпионажа, хактивизма[1], военных действий и проведения операций влияния. Организации стали нанимать сетевых защитников вроде меня, чтобы противостоять разрушительной деятельности этих «черных шляп». На первых порах сообщество сетевых защитников делало множество предположений о том, как можно достичь этой цели. Двадцать пять лет спустя оказалось, что многие из них вовсе не являлись базовыми принципами — в основном это были простые предположения. Настало время пересмотреть свой образ мышления и определить, каковы главные принципы кибербезопасности и какой из них является абсолютным.

В книге я привожу аргументы в пользу атомарного принципа кибербезопасности, объясняю стратегии, необходимые для его воплощения, и рассматриваю тактики, техники и процедуры, позволяющие реализовать каждую из них.

[1] Хакерство во имя политических, гуманитарных или религиозных целей. — *Примеч. ред.*

Значения используемых терминов

Далее приведены определения нескольких используемых в этой книге терминов, облегчающие понимание изложенного материала.

Кибербезопасность

Я использую термин «кибербезопасность» в качестве всеобъемлющего обозначения работы, которую выполняют специалисты-практики. За прошедшие годы в сообществе появилось множество синонимов, имеющих то же значение. Вот лишь некоторые из них:

- цифровая безопасность;
- безопасность информационных технологий (ИТ);
- ИТ-безопасность;
- информационная безопасность (InfoSec).

Для моих целей все они обозначают одно и то же, поэтому используются как взаимозаменяемые.

Профессионалы в области кибербезопасности

То же самое можно сказать об определениях, которыми мы описываем друг друга:

- практикующие специалисты в области информационной безопасности;
- защитники сети;
- специалисты по безопасности;
- профессионалы в области безопасности.

Эти понятия я также использую как синонимы.

Организации

Как правило, существует три типа организаций, инвестирующих в триаду «люди — процессы — технологии» в сфере кибербезопасности: коммерческие компании, правительственные и научные учреждения. Если я упоминаю один из этих типов организаций, считайте, что говорю обо всех сразу. Когда это не так, я прямо на это указываю.

Проект Cybersecurity Canon Project

Проект Canon (cybersecuritycanon.com) — это попытка сообщества специалистов по кибербезопасности выделить книги, которые следует прочесть профессионалам в этой области. Я основал данный проект в 2013 году, а на момент написания книги его спонсором является Университет штата Огайо. Я ссылаюсь на многие полезные книги, как уже вошедшие в этот Зал славы, так и на те, что являются кандидатами на попадание в него. Обзоры этих и многих других книг можно найти на веб-странице проекта.

Военные истории Рика

Я работаю в сфере кибербезопасности уже более 30 лет. За это время я сталкивался с ситуациями, о которых некоторые читатели, вероятно, захотели бы узнать. Я называю их *военными историями*. Многие из них очень далеки от рассматриваемой темы, а некоторые вообще не имеют к ней отношения (они мне просто нравятся). Часть из них я пересказал в книге. При этом я понимаю, что некоторые читатели могут захотеть ознакомиться только с основным ее содержанием (как, например, один из моих редакторов, Стив Винтерфельд, который стремится пропускать подобные истории). Чтобы облегчить задачу таким читателям, я выделил текст моих военных историй серым цветом.

Сайт книги

В ходе предварительного исследования я подготовил дополнительные материалы, которые помогли мне организовать мыслительный процесс. К ним относятся:

- манифест гибкой разработки программного обеспечения (Agile-манифест);
- истории успеха Байеса (взяты из книги Шэрона Макгрейна *The Theory That Would Not Die*);
- историческая хронология развития хаос-инженерии;
- книги, вошедшие в Зал славы Cybersecurity Canon;

- историческая хронология развития сферы кибербезопасности;
- исторические этапы становления разведки в области кибербезопасности;
- историческая хронология развития сферы шифрования;
- хронология взлома Equifax;
- исторические этапы становления сферы идентификации и аутентификации;
- девять правил нулевого доверия, предложенные Киндервагом;
- историческая хронология появления «красной» и «синей» команд;
- хронология взлома системы безопасности RSA;
- историческая хронология развития парадигмы программно-определяемого периметра (Software Defined Perimeter, SDP);
- резюме исследования того, почему тепловые карты — плохое средство передачи информации о рисках (Why Heat Maps Are Poor Vehicles for Conveying Risk).

Чтобы понять мои основные тезисы, вам не обязательно обращаться к этим материалам, однако некоторые из них могут оказаться полезными или по крайней мере интересными.

Дополнительную информацию вы можете найти на сайте thecyberwire.com/CybersecurityFirstPrinciplesBook.

Дорожная карта

Данная книга охватывает довольно большой объем материала. Если вы запутались в круговороте идей и не можете понять, где находитесь по отношению к главному тезису, обратитесь к схеме, изображенной на рис. B.1. Читайте ее снизу вверх. Первая строка — это основа, абсолютный, базовый принцип кибербезопасности (см. главу 1). Следующие две строки указывают на стратегии, которые можно использовать для реализации этого первичного принципа: нулевое доверие (см. главу 2), предотвращение реализации убийственной цепочки вторжения (kill chain) (см. главу 4), обеспечение устойчивости (см. главу 5), прогнозирование рисков (см. главу 6) и автоматизация (см. главу 7). В остальных блоках указаны тактические приемы, которые можно использовать для реализации каждой из названных

стратегий. Им посвящены разделы соответствующих глав. Серые линии отражают связи между стратегиями и тактиками. Обратите внимание на то, что стратегия автоматизации и тактика соблюдения нормативных требований связаны со всеми остальными элементами. В главе 7 вы узнаете почему.

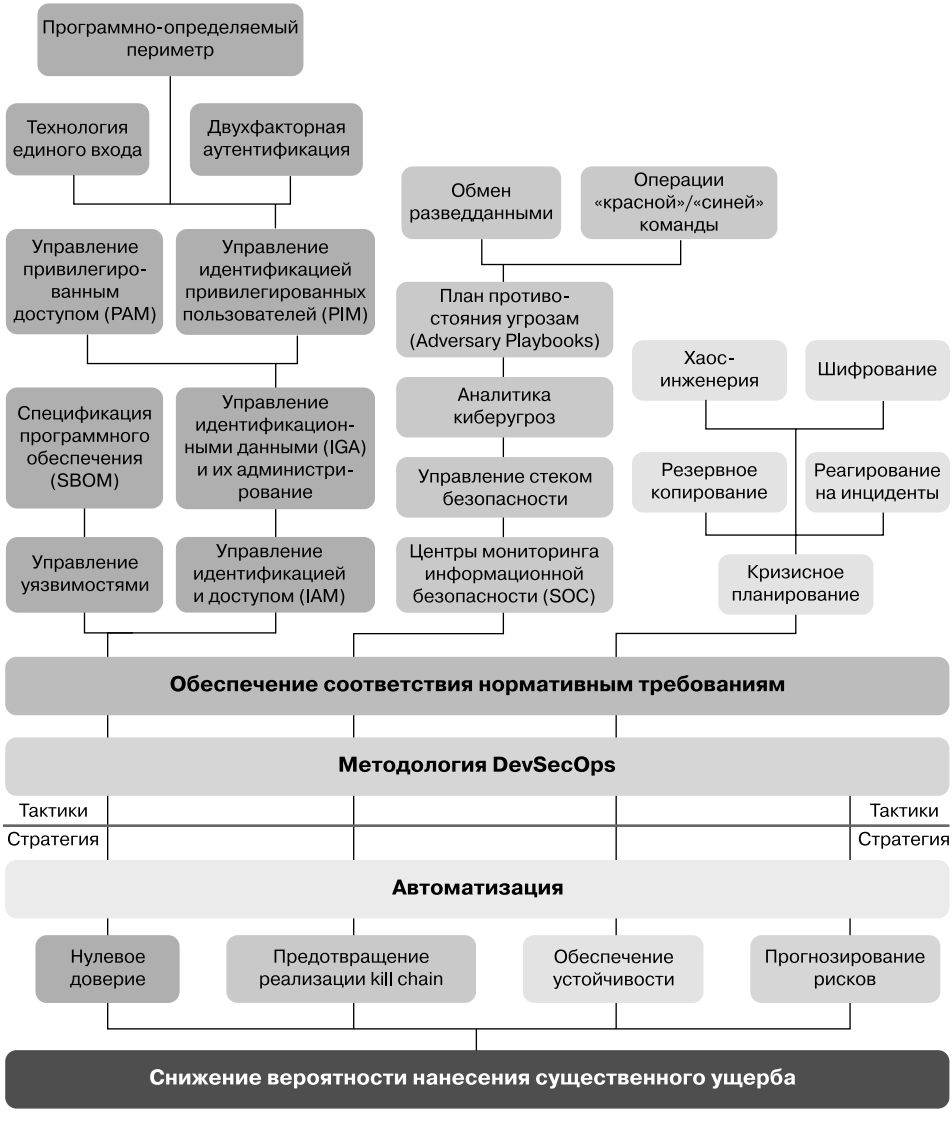


Рис. В.1. Дорожная карта основных принципов кибербезопасности

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства www.piter.com вы найдете подробную информацию о наших книгах.

01 Базовые принципы

Образ мышления, основанный на базовых принципах, предполагает, что все ваши действия опираются на основополагающие убеждения, или базовые принципы.

Рид Хастингс,
генеральный директор Netflix

...Чтобы изучить процесс приобретения [знаний], мы должны начать с исследования тех основных причин, которые называются принципами.

Рене Декарт, философ

Я считаю, что при рассуждении важно руководствоваться базовыми принципами, а не аналогиями... [При их использовании] вы сводите все к фундаментальным истинам... и затем рассуждаете, опираясь на них.

Илон Маск,
основатель компании SpaceX

Обзор главы

Эта глава предназначена для тех читателей, кто не знаком с такой общепринятой передовой научной практикой, как концепция базовых принципов. Это не просто мем, о котором можно услышать в Twitter. Ученые издавна используют ее, чтобы открывать тайны природы и общества. Данная книга представляет собой мое исследование этой концепции применительно

к кибербезопасности. Разумеется, основы кибербезопасности широко обсуждались, но, как будет показано далее, уже в начале 1970–1980-х годов исследователи считали, что основным принципом обеспечения кибербезопасности является создание полностью защищенного компьютера. К началу 2020-х годов большинство практиков отказались от этой идеи, сочтя ее непрактичной. При этом сообщество специалистов по ИБ не заменило ее ничем существенным, если не считать концепции триады «конфиденциальность, целостность и доступность» (КЦД). Однако даже сторонники этой триады не возводят ее в ранг базового принципа и говорят о ней просто как об одной из лучших практик. В этой главе я объясняю, почему триада КЦД, равно как и другие общепринятые лучшие практики: соблюдение правил кибергигиены (исправление ошибок), предотвращение заражения вредоносным ПО, реагирование на инциденты, следование контрольным спискам ИБ-фреймворков и соблюдение требований международного законодательства — не могут считаться абсолютным базовым принципом. В конце главы я предлагаю свое видение того, каким должен быть настоящий атомарный первичный принцип кибербезопасности.

Что такое базовые принципы

Идея базовых принципов была предложена великим философом Аристотелем (384–322 годы до н. э.) в его труде «Физика» [12] (опубликован примерно в 340 году до н. э.), где он изложил свои представления о натурфилософии — способе изучения природы (physis). Однако прежде, чем приступить к изложению своего основного тезиса, он указал на то, что невозможно полностью понять какую-либо концепцию до тех пор, пока не разберешься в ее сущности: «Ибо мы не считаем вещь познанной до тех пор, пока не познакомимся с ее первичными причинами, или первичными принципами, и не проанализируем ее простейшие элементы». Далее Аристотель описал свой метод нахождения этих причин: для этого мы берем то, что нам известно из наблюдений, и доходим до самой сути. Он сказал: «Естественный способ это сделать — двигаться от вещей, которые более понятны и очевидны для нас, к тем, которые являются более явными и понятными по природе» [12]. При этом он уточнил, что эти известные природе атомарные идеи являются уникальными строительными блоками, с которых начинается любое исследование: «Ибо первичные принципы не должны выводиться ни друг из друга, ни из чего-либо другого, тогда как все должно выводиться из них» [12]. После нахождения этих важнейших понятий они становятся

«большим взрывом» для всей гипотезы. «Первичные принципы вечны и не имеют скрытых причин» [13, 14, 122, 126].

Евклид, знаменитый греческий математик и учитель, ни разу не упомянул о первичных принципах в своей основополагающей книге «Начала» (около 300 года до н. э.), однако его краткое изложение 23 определений, пяти постулатов, или аксиом, и пяти общих понятий на протяжении более чем 23 веков являлось основой геометрии и других математических дисциплин [75]. Не существует более убедительного доказательства того, что образ мышления, основанный на базовых принципах, способен привести нас к пониманию истинной природы окружающего мира [6, 301, 311].

В 1644 году величайший философ и скептик всех времен, отец современной философии Рене Декарт опубликовал свой труд «Начала философии» [66, 67]. В нем он начинает «с самых общих вопросов, например с того, что слово “философия” обозначает занятие мудростью, под которой понимается не только благоразумие в делах, но и совершенное знание всего, что может познать человек; это же знание направляет нашу жизнь, служит сохранению здоровья, а также открытиям во всех искусствах». Это весьма масштабная цель, не правда ли? Как же ее можно достичь? По словам Декарта, для получения этого понимания мы должны вывести его из первичных источников: «А чтобы оно стало таковым, оно обязательно должно быть выведено из первичных причин так, чтобы тот, кто старается овладеть им (а это и значит, собственно, философствовать), начинал с исследования этих первичных причин, именуемых началами». Далее он говорит о том, что эти начала должны отвечать двум требованиям: «Во-первых, они должны быть столь ясны и самоочевидны, чтобы при внимательном рассмотрении человеческий ум не мог усомниться в их истинности; во-вторых, познание всего остального должно зависеть от них, тогда как сами эти принципы должны быть познаваемы помимо познания прочих вещей». Под этим он подразумевает то, что все знание о предмете исходит из этих первичных принципов: «Затем надо попытаться вывести знание о вещах из тех начал, от которых они зависят, таким образом, чтобы во всем ряду выводов не встречалось ничего, что не было бы совершенно очевидным».

Следует отметить, что нахождение базовых принципов любого предмета — очень сложная задача. Своей книгой Декарт полностью перевернул сложившийся на тот момент философский образ мышления, заявив, что Аристотель и его современники (Платон и Сократ) так и не смогли найти первичный

принцип философии. Подход Декарта, предполагающий сомнение во всем, установил абсолютный первичный принцип философии: «Я мыслю, следовательно, существую» (Cogito, ergo sum) [312].

В 1910 году два британских математика, Альфред Уайтхед и Бертран Рассел, опубликовали книгу *Principia Mathematica*, в которой попытались с нуля перестроить язык математики на основе небольшого набора базовых принципов [314]. Они обнаружили некоторые несоответствия в существующем на тот момент наборе правил, используемых математическим сообществом. С помощью одних и тех же правил можно было получить два разных и абсолютно правильных результата. Это открытие получило название парадокса Рассела [120]. Для мира точной инженерии это означало потенциальную катастрофу. Поэтому они вернулись к чертежной доске и начали с нуля. Их математическое доказательство того, что 1 + 1 = 2, заняло 80 страниц. В одной из сносок Уайтхед и Рассел написали: «Приведенное ранее утверждение иногда бывает полезным». А вы думали, что математики не умеют шутить.

Отвечая на вопрос о том, как он подошел к созданию концепции экономичных космических полетов, Илон Маск не сказал, что он опирался на то, что агентство НАСА и компания Boeing делали в 1960-х годах в рамках программ «Аполлон» и «Спейс шаттл». Он отбросил все эти наработки и начал с чистого листа. Это, безусловно, очень смелый шаг, и, возможно, именно поэтому он является мультимиллионером, а я — нет [56, 186, 308].

Аристотель, Евклид, Декарт, Уайтхед, Рассел и Маск говорят о том, что для решения любой сложной проблемы практик должен свести ее к первичной сущности.

Базовые принципы той или иной проблемной области настолько фундаментальны, что являются самоочевидными, настолько элементарны, что ни один специалист в данной области не может их оспорить, настолько важны для того, чтобы мы хорошо ее поняли, что без них инфраструктура, на которой держится наша передовая практика, рассыпалась бы как песчаный замок во время прилива. Они атомарны. Эксперты используют их как строительные блоки для получения всего остального, что известно в выбранной проблемной области. Все новые знания, полученные в ней, зависят от ранее сформулированных базовых принципов.

Если это правда, а я считаю, что так и есть, то отсюда следует логичный вопрос: каковы первичные принципы кибербезопасности?

Предыдущие исследования базовых принципов кибербезопасности

Компьютерная эра началась тогда, когда мейнфреймы стали использоваться правительством, университетами и коммерческими организациями (примерно в 1960–1981 годах). Прошло около десяти лет, прежде чем пользователи мейнфреймов осознали вероятность возникновения проблемы компьютерной безопасности, и первыми это поняли американские военные. Начало этому процессу положила работа Уиллиса Уэра *Security Controls For Computer Systems* [309], которую он опубликовал в 1970 году, будучи сотрудником корпорации Rand. Эта работа представляла собой не столько определение понятия кибербезопасности, сколько перечисление и описание всех проблем, которые могут возникнуть в будущем, когда компьютеры будут объединены в сеть и начнут совместно использовать ресурсы. Я бы отнес этот документ к категории «первый шаг в решении любой проблемы — это признание ее наличия». Он намекает на то, что сообщество специалистов по безопасности должно найти способ построения защищенной системы. Эта идея находилась в центре внимания исследователей на протяжении 1990-х годов. В опубликованной в 2021 году книге *A Vulnerable System: The History of Information Security in the Computer Age* [296], попавшей в Зал славы Cybersecurity Canon, ее автор Эндрю Стюарт сетует на то, что с самого начала цифровой эры никто так и не смог построить защищенную систему. От этого отказались практически все.

В статье *Computer Security Technology Planning Study* [8], написанной Джеймсом Андерсоном в 1972 году, были развиты идеи, изложенные в работе Уиллиса Уэра. Вероятно, в ней была впервые высказана мысль о том, что о безопасности нужно думать не после создания системы, о чем специалисты говорят и сегодня, когда обсуждают концепцию сдвига влево или принцип конструктивной безопасности. Она подразумевает, что создание безопасной системы является конечной целью, но при этом предполагает, что любая безопасная система нуждается в способе ее мониторинга на предмет наличия дефектов и вторжений.

Годом позже Дэвид Белл и Лен Лападула, на тот момент работавшие в организации MITRE, опубликовали работу *Secure Computer Systems: Mathematical Foundations* [26], в которой привели арифметическое доказательство, гарантирующее безопасность компьютерной системы. При этом они сразу признали, что даже при возможности построения системы, соответствующей этому доказательству, ее создатели не могли бы гарантировать правильность

ее реализации. Теоретически это возможно, но как можно поручиться за правильность практически? И эта проблема остается актуальной для такого рода исследований на протяжении 30 лет.

В 1975 году Джером Зальтцер и Майкл Шредер опубликовали труд под названием *The Protection of Information in Computer Systems* в журнале *Proceedings of the IEEE* [192]. В нем они изложили первые зачатки триады КЦД, хотя и не использовали эту терминологию. Они также впервые доказали, что комбинация «имя пользователя — пароль» — это слабая форма защиты и однажды возникнет потребность в двухфакторной аутентификации. Кроме того, они одними из первых выступили за снижение сложности во всем, что связано с разработкой системы безопасности, и за то, чтобы ее разработка не скрывалась от посторонних глаз. Другими словами, это, вероятно, первые исследователи, публично высказавшиеся против применения принципа «безопасность через неясность». Наконец, они продвигали идею использования *безопасных умолчаний* (fail-safe defaults), которая предполагает изначальный запрет всего с последующим разрешением в виде исключения. Эта идея, вероятно, является первым зародышем концепции защиты периметра, то есть создания внешнего барьера, позволяющего контролировать доступ к сети. Она была высказана примерно за десять лет до появления соответствующих технологий (межсетевых экранов).

В 1991 и 1992 годах доктор Фред Коэн опубликовал первые работы, в которых для описания общей модели обеспечения кибербезопасности в сообществе сетевых защитников использовалась концепция эшелонированной защиты [51–53]. Не он придумал этот термин, но, скорее всего, именно он первым описал соответствующую концепцию в своей работе. Эшелонированная защита предполагает возведение электронного барьера между Сетью и цифровыми активами организации. Чтобы преодолеть этот барьер со стороны Интернета, необходимо было пройти через контрольный пункт, которым обычно служил межсетевой экран, а в первые годы иногда еще и маршрутизатор. Начиная с 1990-х годов и по сей день общепринятой практикой является добавление дополнительных средств контроля позади межсетевого экрана для обеспечения более гибких функций. В первые годы это были системы обнаружения вторжений и антивирусные системы. Все вместе эти средства образовывали так называемый *стек безопасности*, принцип работы которого заключается в том, что если один из инструментов стека не сможет предотвратить доступ злоумышленника, то это сделает следующий. Если и он не справится с задачей, его место займет следующий. В этом и заключается суть концепции эшелонированной защиты.

В 1998 году Донн Паркер опубликовал книгу *Fighting Computer Crime: A New Framework for Protecting Information*, в которой резко осудил элементы триады КЦД, назвав их неадекватными [172]. При этом словосочетание «триада КЦД» не упоминалось. Он предложил добавить еще три элемента — владение или контроль, аутентичность и полезность, результатом чего стала модель под названием «гексада Паркера». Но она не получила широкого распространения по причинам, которые, вероятно, может объяснить лишь маркетолог.

В этот период большинство специалистов по ИБ в той или иной форме занимались совершенствованием стека безопасности. Однако с появлением облачных окружений, возникших примерно в 2006 году, количество нуждающихся в защите цифровых сред многократно увеличилось. Организации начали хранить и обрабатывать данные в различных местах, которые я называю *островами данных* (к ним относятся традиционные центры обработки данных, мобильные устройства, облачные среды и SaaS-приложения). Идея стека безопасности стала более абстрактной. Речь шла уже не об одном наборе инструментов, физически развернутом за межсетевым экраном, — это была целая серия стеков безопасности, развернутых для каждого отдельного острова данных. Стек безопасности превратился в набор всех развернутых инструментов, укрепляющих оборонительную позицию организации вне зависимости от места их расположения, иными словами, концепция эшелонированной защиты стала применяться абстрактно ко всем средам. Большая часть проводимых в этот период исследований была направлена на улучшение возможностей триады КЦД путем создания более совершенных инструментов для стека безопасности, таких как межсетевые экраны уровня приложений, системы управления идентификацией и доступом, средства для расширенного обнаружения и реагирования (XDR) и т. д., и более совершенных моделей для противодействия противнику (работа Киндервага о стратегии нулевого доверия *No More Chewy Centers*, 2010 [133]; модель убийственной цепочки Lockheed Martin, 2010 [115]; модель Diamond Министерства обороны США, 2011 [39]; база знаний компании Mitre ATT&CK Framework, 2013 [299]).

Точно не помню, когда услышал о работе Уайтхеда и Рассела, но размышлять и писать о базовых принципах кибербезопасности я начал еще в 2016 году. Тогда мои мысли еще не были полностью сформулированы, но я уже понимал, что сообщество специалистов по информационной безопасности движется в неправильном направлении. Почему-то все мы полагали, что защита отдельных систем с помощью триады КЦД — верное решение. Тем не менее количество сообщений о взломах продолжало расти. Уже тогда

я понимал, что триада КЦД недостаточно элементарна. Нам не нужно было защищать отдельные компьютерные системы. Следовало предотвращать причинение существенного ущерба нашим организациям. Тогда я осознал необходимость возвращения к базовым принципам.

Примерно в это же время научное сообщество впервые задумалось о способах применения идеи базовых принципов к области кибербезопасности. Сотрудники Университета Буффало Чарльз Арбутина и Сарбани Банерджи связали то, что они называют *основополагающими утверждениями*, с контрольным списком Агентства национальной безопасности США (АНБ), содержащим критерии, которым должны соответствовать защищенные системы [195]. Однако в этой работе предполагается, что создание защищенной системы является абсолютным базовым принципом кибербезопасности, не подлежащим обсуждению. Идея следовать первичным принципам кибербезопасности правильная, но недостаточно атомарная: она не позволяет понять, что же на самом деле является базовым принципом. Некоторые из предложенных задач, в том числе разделение доменов, изоляция процессов и сокрытие информации, могут и должны использоваться в качестве тактик, однако в своей работе авторы не иллюстрируют того, что именно они пытаются сделать. Они не доходят до сути проблемы.

В 2017 году доктор Мэтью Хейл, доктор Робин Ганди и доктор Бриана Моррисон в своей работе *Introduction to Cybersecurity First Principles*, предназначенной для учащихся начальной школы, предложили аналогичный подход с использованием контрольного списка АНБ [95]. А в 2021 году доктор Джон Сэндс, Сьюзан Сэндс и Джейми Махони из Общественного колледжа Брукдейла осветили эту тему более подробно, но опять же не привели никаких аргументов в пользу того, почему указанные ими принципы являются первичными [193].

В 2020 году на 7-м семинаре ACM по защите движущихся целей Шоухуай Сюй опубликовал свою работу *The Cybersecurity Dynamics Way of Thinking and Landscape* [319]. В ней он представил трехмерную ось, включающую такие базовые принципы, как анализ методом моделирования, основанный на предположениях, анализ данных, основанный на экспериментах, и метрики, зависящие от применения и семантики. Однако он также не привел аргументов в пользу элементарности предложенных принципов.

В 2021 году в Университете Айдахо Николас Сили опубликовал магистерскую диссертацию *Finding the Beginning to Discover the End: Power System Protection as a Means to Find the First Principles of Cybersecurity* [199]. Из всех упомянутых здесь работ эта наиболее полная с точки зрения осмыс-

ления первичных принципов. Сили также проанализировал большинство из них, прежде чем сделать выводы, и утверждает, что основные идеи, вытекающие из этих работ, вращаются вокруг проблемы доверия. Затем он задается вопросом о том, является ли концепция доверия достаточно фундаментальной для того, чтобы быть базовым принципом. Он цитирует Джеймса Коулмана — автора книги *The Foundations of Social Theory*, в которой говорится о том, что «ситуации, предполагающие проявление доверия, относятся к подмножеству ситуаций, связанных с риском». Или, как говорит Сили, «при отсутствии риска в доверии нет необходимости». Сили утверждает, что риск — это функция вероятности, мера неопределенности. Он считает неопределенность более фундаментальной концепцией по сравнению с триадой КЦД и любыми другими контрольными списками, предложенными вышеупомянутыми авторами. Интересно то, что в своей книге *The Foundations of Decision Analysis Revisited* отец теории анализа решений доктор Рон Ховард утверждает то же самое.

Из книги Лумана, Кинга и Моргнера *Trust and Power* Сили заимствует идею о том, что доверие позволяет нам уменьшить сложность своей жизни [144]. Затем, подобно Евклиду, он предлагает набор допущений (постулатов или аксиом) в качестве базовых принципов кибербезопасности.

- Полное знание о системе недостижимо, поэтому в нашем понимании этой системы всегда будет некоторая доля неопределенности.
- Принципал системы вынужден доверять одному или нескольким агентам.
- Известные риски могут быть уменьшены посредством их контроля, передачи и избегания, в противном случае они должны быть приняты.
- Неизвестные риски проявляются через сложность.

Затем он останавливается на определении абсолютного первичного принципа кибербезопасности и использует свои аксиомы для разработки лучшего, чем у Белла и Лападулы, доказательства того, что один дизайн системы более безопасен по сравнению с другим, анализируя собственные значения соответствующих графов. Другими словами, он возвращается к традиционному способу проектирования безопасных систем.

Концепция образа мышления, основанного на представлении о базовых принципах, существует практически с момента зарождения просвещенной научной мысли. Однако ее применение к сфере кибербезопасности — относительно новая идея.

Хотя отцы-основатели кибербезопасности (Уэр, Андерсон, Белл и Лападула, Зальтцер и Шредер, Кларк и Уилсон) никогда не упоминали о первичных принципах, они сформулировали две основные концепции, которые, по сути, и были положены в основу этой дисциплины. Первая заключается в том, что мы все пытаемся формализовать безопасность систем. Исследовательское сообщество в конце концов отказалось от этой идеи в 1990-х годах, сочтя ее нерабочей. Мы обнаружили, что чем более защищенными становятся машины, тем менее полезными они оказываются для решения распространенных задач. Защищенные системы могут применяться в специфических случаях, например связанных с государственной тайной, но рядовому пользователю Интернета они не очень полезны. Второй была концепция триады КЦД. Несмотря на жалобы критиков на ее неадекватность и попытки улучшения, ее общий смысл оставался неизменным с момента публикации работы Зальтцера и Шредера. Учитывая то, что в 2020 году ее признавали даже такие организации, как Национальный институт стандартов и технологий (NIST), триада КЦД фактически является первым принципом кибербезопасности.

В следующем разделе я постараюсь доказать, что она не подходит на эту роль, и предложу более надежный базовый принцип.

Атомарный базовый принцип кибербезопасности

В предыдущем разделе я говорил о том, что сообщество специалистов по ИБ обеспечило постепенный прогресс в плане цифровой защиты наших организаций. Очевидно, что мы прошли долгий путь. Однако, ознакомившись с работой Уайтхеда и Рассела, я подумал о том, что мы столкнулись с парадоксом, аналогичным описанному в ней. Мы продолжаем добавлять к уже сделанному множество разных вещей, не задумываясь о правильности выдвинутых ранее предположений. Наши защитные системы были значительно усовершенствованы, но складывается впечатление, будто это никак не повысило эффективность предотвращения кибератак. Более того, учитывая количество успешных атак, ежедневно попадающих в заголовки прессы, можно сделать вывод о том, что защита ухудшилась. Это относится не ко всем. Некоторые справляются с задачей довольно успешно. Я говорю о сообществе ИБ-специалистов в целом. Как и в случае с Уайтхедом и Расселом, разные группы, входящие в это сообщество, используя одни и те же передовые методы, получают разные результаты.

Я пришел к следующему выводу: все, что мы делаем как сообщество в плане защитной триады «люди — процессы — технологии», с помощью которой пытаемся обеспечить безопасность своих организаций, вероятно, не является настолько фундаментальным, чтобы оказывать существенное влияние. Разумеется, все это дает определенный эффект. Но проблема в том, что даже полноценная реализация этой триады оказывается недостаточной либо слишком сложной или дорогостоящей и поэтому не приводит к успеху.

И я не согласен с мнением, что обеспечение кибербезопасности чем-то отличается от остальных мировых проблем и является настолько уникальной проблемой, что ее невозможно решить. В конце концов, мы высадили людей на Луну, приручили атомную энергию и изобрели Интернет. Я считаю, что обеспечение кибербезопасности представляет собой гораздо менее масштабную задачу по сравнению с этими и многими другими. Проблема, как мне кажется, заключается в том, что у нас нет единого понимания термина «обеспечение кибербезопасности». Если вы попросите трех специалистов в сфере защиты сети описать, что именно они пытаются сделать с помощью своей программы по обеспечению ИБ, то получите три принципиально разных ответа.

Если сообщество не может договориться о том, что именно мы пытаемся сделать, значит, пора вернуться к первичным принципам. Более того, пришло время определить абсолютный принцип, способный послужить базовым определением кибербезопасности. До сих пор сообщество использовало набор терминов и фраз для обозначения кибербезопасности или ее компонентов. Некоторые его представители говорят:

- о реализации триады КЦД;
- создании надежной программы исправления ошибок;
- защите от вредоносных программ;
- быстром обнаружении и эффективном устранении угроз (реагировании на инциденты);
- развертывании NIST Cybersecurity Framework или другого фреймворка;
- поддержании работы программы обеспечения соответствия нормативным требованиям.

Существует и множество других направлений, некоторые весьма хороши. Но ни одно из них не кажется достаточно фундаментальным. Ни одно не дотягивает до статуса того основополагающего элемента, на базе которого мы могли бы строить свои программы. Как же вышло, что за 30 лет работы в со-

обществе так и не сформировалось единого мнения о том, к чему именно мы все стремимся? Это и является основным тезисом данной книги.

Как я уже говорил в начале главы, создание набора первичных принципов кибербезопасности предполагает сведение концепции защиты сети к ее основной сути. Перечисленные ранее идеи могут присутствовать в нашем списке в качестве потенциальных тактик, но они недостаточно атомарны. Мы не можем использовать их как строительные блоки для выведения всего, что известно в данной проблемной области, уподобившись Уайтхеду и Расселу, которым потребовалось 80 страниц для доказательства простой математической концепции.

Итак, первым делом я объясню, почему перечисленные идеи не являются главными принципами кибербезопасности.

Является ли триада КЦД абсолютным первичным принципом?

С момента своего возникновения в 1970-е годы и до начала 2020-х годов триада КЦД оставалась основополагающей философией обеспечения информационной безопасности. В документе *NIST Special Publication 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, опубликованном в 2020 году Национальным институтом стандартов и технологий США (NIST), говорилось о том, что «триада КЦД описывает три столпа информационной безопасности». Другими словами, именно она лежит в основе стратегии защиты государственных систем [43].

В августе 2022 года в ходе беседы со мной Дженнифер Рид, специалист в области безопасности и технологий с 20-летним стажем, привела доводы в пользу того, что статья Зальтцера и Шредера является первым публичным упоминанием о триаде КЦД — концепции того, что для обеспечения безопасности системы архитекторам необходимо позаботиться о конфиденциальности, целостности и доступности. По ее словам, несмотря на то что Зальтцер и Шредер не использовали словосочетание «триада КЦД» и не упоминали такие термины, как «конфиденциальность», «целостность» и «доступность», они «с точки зрения специалистов по безопасности говорили о трех типах вторжений, известных как: а) несанкционированный доступ к информации (конфиденциальность); б) несанкционированная модификация информации (целостность); в) несанкционированный отказ в использовании (доступность)».

Не вполне ясно, когда триада КЦД сформировалась в целостную концепцию. Во многих ранних работах (работы Уэра, Андерсона, Белла и Лападулы, Зальтцера и Шредера, Кларка и Уилсона [317, 29, 82] «Оранжевая книга» Министерства обороны США [65, 188], работы Бранстада [34] и Липнера [141]) обсуждаются один или несколько элементов триады КЦД, но лишь как пункты списка того, что необходимо сделать, или в рамках описания потенциальных проблем, а не в качестве единого фундаментального принципа обеспечения безопасности. Это различие может показаться незначительным, но я считаю его важным. В те давние времена каждый элемент того, что впоследствии стало известно как триада КЦД, представлял собой просто пункт контрольного списка задач, которые необходимо было решить для построения защищенной системы. Они были объединены со многими другими вещами. Триада КЦД еще не оформилась в фундаментальную концепцию, поэтому специалисты по ИБ еще не оперировали соответствующим термином.

По словам Йеруна ван дер Хама, сотрудника Национального центра кибербезопасности Нидерландов и Университета Твенте, термин, связавший все воедино, был предложен Стивом Липнером в 1986 году [307]. Однако в беседе со мной в августе 2022 года Липнер сказал, что его предложил не он [112].

> Липнера вполне можно поставить в один ряд с такими отцами-основателями кибербезопасности, как Уэр, Андерсон, Белл и Лападула, Зальтцер и Шредер, Кларк и Уилсон. Он один из авторов «Оранжевой книги» Министерства обороны США (1985 год) и один из архитекторов инициативы компании Microsoft по созданию доверенных вычислительных систем, реализованной в 2000-е годы.

Даже Паркер в своей книге, в которой он описывает эти три элемента в качестве отдельного набора неадекватных идей, не называет их триадой. В какой-то момент между публикацией статьи Зальтцера и Шредера 1975 года и книги Паркера 1998 года сообщество ИБ-специалистов начало рассматривать три элемента триады КЦД вместе в виде фундаментального принципа кибербезопасности, или, если хотите, ее первичного принципа. Однако как концепция триада сформировалась лишь после выхода книги Паркера, причем точную дату этого события назвать нельзя. Однако странно то, что никто до сих пор так и не заявил свои права на эту основополагающую доктрину, столь широко признанную и так долго просуществовавшую в сообществе специалистов-практиков. Это еще одно доказательство того,

что ИБ-сообщество действительно верит в тот «грубый консенсус», о котором говорил Дэвид Кларк.

При этом уже на ранних этапах исследователи признавали, что триада КЦД имеет определенные проблемы. Подробнее о них вы можете почитать в книге Паркера.

Однако лично я сомневаюсь в том, что конфиденциальность, целостность и доступность являются первичными принципами. Достаточно ли они фундаментальны? Атомарны ли они? Не возникает ли у вас уточняющих вопросов при размышлении о каждом из этих трех элементов? Применяете ли вы эти стратегии ко всем данным и системам, даже несущественным? Всегда ли применяете эти принципы? Другими словами, защищаете ли вы все системы и все данные на протяжении всего времени? Это кажется крайностью. Данная триада ничего не говорит по этому поводу. Следующий вопрос заключается в том, хотим ли мы ограничиться универсальными средствами защиты, не задумываясь о фактических действиях противника. Я имею в виду то, что мы не можем активно защититься от убийственной цепочки вторжения, опираясь лишь на пассивные средства обеспечения конфиденциальности, целостности и доступности. Третья проблема подробно описана в книге Паркера и заключается в том, что эта триада не учитывает вероятность нецелевого использования системы. Например, сотрудники, имеющие законный доступ к конфиденциальной информации компании, могут не разглашать ее, не изменять и не делать недоступной для клиентов, но при этом манипулировать ею с выгодой для себя каким-либо мошенническим способом. Это не нарушает правил данной триады.

Учитывая сказанное, триада КЦД не может считаться атомарным первичным принципом кибербезопасности.

Является ли патчинг абсолютным базовым принципом?

В начале 1990-х годов одной из первых лучших практик, сформировавшихся в ИБ-сообществе, было исправление ошибок программного обеспечения, или патчинг. Идея заключалась в том, что если мы сможем устранять уязвимости в программном обеспечении по мере их обнаружения и до того, как злоумышленники смогут ими воспользоваться, то нам удастся не допустить в свои сети ни преступников, ни шпионов, ни хактивистов. По сей день многие специалисты по кибербезопасности тратят значительную часть своих ограниченных ресурсов на это мероприятие, называя его лучшей практикой

сообщества. Однако, по мнению Кэролайн Вонг, автора книги *Security Metrics, A Beginner's Guide*, попавшей в Зал славы Cybersecurity Canon, большинство защитников сетей употребляют словосочетание «лучшая практика» неправильно [318]. Она говорит: «Под лучшей практикой следует понимать подход или методику, которые являются более эффективными для достижения определенного результата, чем любые другие методы, применяемые в конкретной ситуации». По ее словам, многие общепринятые передовые методы обеспечения кибербезопасности, хотя и являются хорошими идеями, не способствуют достижению этих результатов.

Я по собственному опыту знаю, что исправление ошибок программного обеспечения — это одна из таких лучших практик. Не поймите меня неправильно. Систематическое обновление всех программных компонентов, независимо от того, написали ли мы их сами, приобрели у коммерческого поставщика или позаимствовали у сообщества разработчиков ПО с открытым исходным кодом, — важная задача. Злоумышленники постоянно ищут бреши в нашей защитной броне. Их эксплуатация — это один из наиболее эффективных типов атак, поскольку уязвимостей в ПО очень много и, похоже, с каждым годом их количество растет в геометрической прогрессии. Однако вопрос заключается в том, действительно ли устранение программных ошибок настолько важно, чтобы претендовать на звание основного принципа кибербезопасности, на основе которого мы должны выстраивать все свои стратегии. Я утверждаю, что это не так.

Это значимая тактика, которую мы можем использовать для предотвращения причинения ущерба своей организации, но не важнейшая. Существует миллион других тактических приемов, способных дать такой же или даже больший эффект, в частности создание надежной системы идентификации и авторизации, предоставляющей сотрудникам доступ лишь к тем ресурсам, которые необходимы им для работы, развертывание в стеке безопасности максимального количества средств предотвращения для каждого из известных этапов реализуемых противником атак или внедрение процедур, позволяющих организации быстро восстановиться после разрушительной кибератаки.

Кроме того, хакеры эксплуатируют ошибки в коде менее чем в 10 % случаев известных взломов [121, 152]. Этот показатель приблизительный и основан на отчетах британской консалтинговой компании IT Governance и данных проекта Валерия Марчука *Zero-Day Tracking Project*, но даже если этот процент значительно выше, вероятность эксплуатации ошибок все равно довольно мала по сравнению с количеством прочих действий, которые ха-

керы предпринимают для компрометации своих жертв. Иными словами, предположение о том, что защита от эксплойтов — это лучшая практика, на которой следует основывать программу обеспечения информационной безопасности, является ложным. ИБ-сообщество придерживается этой стратегии уже более двух десятилетий, но это не привело к уменьшению количества успешных кибервзломов. Кэролайн Вонг права. Патчинг как передовая практика не дал тех результатов, на которые мы рассчитывали. Поэтому, с моей точки зрения, нельзя рассматривать его в качестве принципа, на котором может быть основана программа обеспечения информационной безопасности.

Является ли защита от вредоносного ПО абсолютным первичным принципом?

Разница между эксплойтами и вредоносными программами заключается в том, что эксплойты используются хакерами для получения доступа к системе, а вредоносные программы — для всего остального, например для поиска в системе данных, которые они намерены украсть или уничтожить, повышения привилегий, перемещения по сети жертвы для выполнения дальнейшего поиска, обеспечения утечки данных по командно-контрольному каналу и т. д. Иногда хакерские вредоносные программы включают в себя эксплойты в качестве компонентов. Это кажется важным. Если бы мы могли защититься от всех вредоносных программ, то лишили бы хакеров шанса на успешное проникновение в наши сети. Не следует ли положить эту стратегию в основу программы обеспечения кибербезопасности?

И тут я снова могу ответить отрицательно, сославшись на Кэролайн Вонг. Возведение защиты от вредоносного ПО в ранг лучшей практики привело ИБ-сообщество к таким же неблагоприятным последствиям, как и в случае с патчингом. Антивирусные инструменты, появившиеся в начале 1990-х годов, к середине 2010-х трансформировались в средства обнаружения угроз для конечной точки (endpoint detection and response, EDR) и реагирования на них. Эти современные средства значительно превосходят старые инструменты, и большинство организаций считают передовой практикой их использование в своих сетях. Однако количество успешных кибератак остается довольно стабильным на протяжении последних шести лет. По данным Identity Theft Resource Center, в период с 2015-го по 2021-й среднегодовое число атак на публичные ресурсы составляло 1259 и оставалось в диапазоне

между 1000 и 2000 [60]. Если решения для защиты от вредоносного ПО дают такие хорошие результаты и большинство ИБ-специалистов применяют те или иные их версии, не должно ли число таких атак быть близко к нулю?

Опять же я не утверждаю, что использование средств защиты от вредоносного ПО — это плохая идея. Всем нам следует рассматривать их установку как тактику снижения вероятности компрометации систем. Однако их применение, вероятно, не самая важная стратегия из всех существующих и, подобно патчингу, не основополагающая. Это не то, на чем следует выстраивать всю программу обеспечения ИБ. Поэтому, с моей точки зрения, мы не можем рассматривать защиту от вредоносного ПО в качестве базового принципа кибербезопасности.

Является ли реагирование на инциденты абсолютным первичным принципом?

В 2010-х годах в сообществе специалистов по информационной безопасности начало распространяться мнение, что киберзащита — слишком сложная задача, поэтому от нее следует отказаться в пользу реагирования на инциденты, иными словами, отказаться от механизмов предотвращения в пользу механизмов раннего обнаружения угроз и эффективных систем их устранения. Оказалось, что это так же сложно и дорого, как и реализация традиционного оборонительного подхода. Инструменты, необходимые для предотвращения атак, аналогичны тем, которые задействуются в первой части этой стратегии — при их обнаружении. Для реализации ее второй части (реагирования) требуется высококвалифицированная команда специалистов, способных справляться со сложными техническими аспектами современных кибератак, понимающих цифровую архитектуру организации лучше, чем ее разработчики, и обладающих коммуникативными навыками, позволяющими доносить информацию до руководства по мере превращения потенциальных угроз в реальные. Если вам кажется, что все это очень дорого, вы не ошибаетесь. Вне зависимости от того, обладаете ли вы техническими и социальными навыками, необходимыми для выполнения этих задач, одна только стоимость делает эту передовую практику недоступной для организаций небольшого и среднего размера. Для тех групп, которые могут себе это позволить, реагирование на инциденты может стать ключевой и необходимой функцией. Для остальных же эта практика остается нереализуемой и, следовательно, не может являться первичным принципом кибербезопасности.

Когда меня спрашивают о том, как распределить ресурсы (людей, процессы и технологии) между решениями для защиты и реагирования, я вспоминаю о различии между пожарными инспекторами и пожарными, о котором говорит Стив Винтерфельд (редактор этой книги). Инспекторы проверяют, соответствует ли здание нормам пожарной безопасности, функционирует ли система пожаротушения, надлежащим ли образом хранятся пожароопасные предметы, имеются ли в здании необходимые знаки и огнетушители и т. д. Однако иногда пожары все равно случаются, и тогда вам необходимо вызывать пожарных. Чем эффективнее будут предпринятые вами меры по предотвращению возгорания, тем меньше вероятность того, что пожарным придется на него реагировать. Однако вероятность этого не равна нулю. Это не вопрос «или — или». Вам нужно и то и другое.

Является ли соблюдение правил фреймворков безопасности абсолютным первичным принципом?

Одним из удивительнейших феноменов, наблюдаемых со времен появления Интернета, является готовность сетевых инженеров и инженеров по безопасности добровольно тратить свое время на разработку стандартов и фреймворков, приносящих пользу всему сообществу. Одним из примеров такой деятельности являются усилия Инженерного совета Интернета (Internet Engineering Task Force, IETF). На сайте этой организации написано, что ее миссия заключается в «улучшении работы Интернета через создание высококачественных, значимых технических документов, которые оказывают влияние на то, как люди разрабатывают что-либо для Интернета, пользуются и управляют Интернетом» [278]. Другие стандарты и фреймворки иногда определяются нормативными требованиями, бизнес-моделями, отраслевым передовым опытом, правительствами, нуждающимися в рекомендациях, и аналитическими исследованиями. Среди наиболее известных можно назвать следующие.

- Нормативное регулирование:
  - Федеральный совет по проверке финансовых институтов (FFIEC), регулирующий деятельность банков в США;
  - Генеральный регламент ЕС о защите персональных данных;
  - закон КНР о защите данных и личной информации.

- Бизнес-модели:
  - HiTrust (руководство по реализации закона о преемственности и подотчетности медицинского страхования) и ISO 27000;
  - ISO 27001 (стандарт Международной организации по стандартизации, устанавливающий требования по внедрению мер управления информационной безопасностью);
  - SOC 2 (отчет Service Organization Control о соблюдении поставщиками услуг мер по защите данных клиентов).
- Лучшие отраслевые практики:
  - триада КЦД (конфиденциальность, целостность и доступность);
  - открытый проект по обеспечению безопасности веб-приложений (OWASP);
  - критические элементы управления безопасностью, определяемые Центром интернет-безопасности (CIS);
  - задачи управления для информационных и смежных технологий (COBIT), разработанные Ассоциацией аудита и контроля информационных систем (ISACA);
  - убийственная цепочка компании Lockheed Martin (см. главу 4);
  - стандарт безопасности данных индустрии платежных карт (PCI DSS);
  - технология защиты критической инфраструктуры Североамериканской корпорации по обеспечению надежности электросистем.
- Спонсируемые государством:
  - модель Diamond (см. главу 4);
  - MITRE ATT&CK® (см. главу 4);
  - NIST Cybersecurity Framework (Национальный институт стандартов и технологий США).
- Разработанные аналитическими фирмами:
  - Forrester (Zero Trust; см. главу 3);
  - Gartner (SASE; см. главу 4).

Существует и множество других стандартов. Некоторые из них представляют собой обширные списки того, что необходимо учесть при развертывании программы обеспечения информационной безопасности. ИБ-специалисты

часто просят меня порекомендовать один из них. С практической точки зрения (то есть в плане обеспечения наилучшей безопасности) это не имеет особого значения. Выберите стандарт, который подходит именно вам, и следуйте ему. По большому счету, все хорошие стандарты охватывают одни и те же области. Однако с точки зрения бизнеса один из них может оказаться более предпочтительным в зависимости от страны, в которой работает ваша организация.

И все же можно ли считать рассмотрение любого набора средств управления безопасностью или концепций в этой области образом мышления, предполагающим существование базовых принципов кибербезопасности? Возможно, авторы не представляют их в таком свете. Они говорят о «дорожных картах» или моделях зрелости, которые ИБ-специалисты могут использовать для демонстрации руководству и аудиторам того, что в организации действительно существует программа обеспечения информационной безопасности, соответствующая своду лучших практик, признанному сообществом. Прохождение сертификации по одному или нескольким из этих направлений представляет собой весьма дорогостоящее и длительное мероприятие. Причем результатом всех этих трудов является не рабочая программа, основанная на базовых принципах кибербезопасности, а моментальный снимок, фиксирующий то, что было сделано для прохождения сертификации. Я по своему опыту знаю, что обычно эти снимки распечатывают, помещают в папки, которые ставят куда-нибудь на книжную полку и забывают навсегда.

Но даже если руководство службы информационной безопасности решит не проходить сертификацию, а просто следовать общим концепциям, результатом, скорее всего, станет организация, которая будет гораздо лучше защищена в цифровом мире по сравнению с организацией, не придерживающейся никаких стандартов.

Однако вопрос в том, чего именно вы пытаетесь достичь всеми этими усилиями. Когда вы достигаете стопроцентного соответствия тем или иным требованиям, чего вы добиваетесь и как оцениваете эффективность проделанной работы? Ответы на этот вопрос, как правило, бывают самыми разными.

Это вполне понятно. Одной организации соответствие стандартам может понадобиться для решения одной бизнес-задачи, а другой организации — для решения другой. Такой подход имеет смысл, но не является образом мышления, предполагающим существование базовых принципов

кибербезопасности. Программа кибербезопасности, основанная на первичном принципе, может предполагать соблюдение правил тех или иных фреймворков, но это не настолько атомарно, чтобы лежать в основе каждой программы по обеспечению информационной безопасности.

Таким образом, соблюдение правил фреймворков безопасности также не может считаться первичным принципом кибербезопасности.

Является ли соблюдение нормативных требований абсолютным первичным принципом?

С первых дней существования Интернета законодатели и поставщики коммерческих услуг всего мира пытались как-то регулировать сферы, связанные с цифровыми преступлениями, конфиденциальностью и стандартами информационной безопасности. Наиболее известными попытками в этом направлении являются:

- Генеральный регламент о защите персональных данных (GDPR), принятый Европейским парламентом;
- Федеральный совет по проверке финансовых институтов (FFIEC);
- стандарты Североамериканской корпорации по обеспечению надежности электросистем (NERC);
- стандарт безопасности данных индустрии платежных карт (PCI DSS);
- закон США о борьбе с компьютерным мошенничеством и злоупотреблениями (CFAA);
- принятый в США закон Грэмма — Лича — Блайли (GLBA);
- федеральный закон США об управлении информационной безопасностью (FISMA);
- федеральная программа США по управлению рисками и авторизацией (FEDRAMP);
- закон США о преемственности и подотчетности медицинского страхования (HIPAA).

Изначально многие ИБ-специалисты видели в нормативных требованиях попытку либо установить стандарты для базовых программ обеспечения безопасности/конфиденциальности, либо провести различие между преступной деятельностью в цифровой сфере и активностью обычных интер-

нет-пользователей. Они рассматривали их как необходимое зло, позволяющее избежать штрафов (например, GDPR), или как цену ведения бизнеса (например, FEDRAMP), но не как необходимое условие для защиты своих организаций в интернет-пространстве. ИБ-специалисты понимают, что эти требования законодательства нужно соблюдать, но большинство не рассматривают их в качестве основы для своих программ обеспечения информационной безопасности. Кроме того, некоторым организациям проще платить штрафы и смириться с ними как с издержками ведения бизнеса. Таким образом, соблюдение нормативных требований тоже не может претендовать на роль первичного принципа кибербезопасности.

Атомарный первичный принцип кибербезопасности

В результате этого анализа я убедился в том, что все описанные ранее кандидаты на роль первичного принципа либо слишком упрощенные, либо слишком тактические. Они связаны с такими техническими задачами, как предотвращение программных эксплойтов, защита от вредоносного ПО, обнаружение и уничтожение инструментов злоумышленников, следование контрольным спискам и соблюдение нормативных требований. Однако они не позволяют достичь главной цели любой программы обеспечения информационной безопасности. Глядя на них, вы можете сказать: «Это хорошая цель, но как быть со всеми остальными вопросами? Решит ли это все мои проблемы, связанные с обеспечением кибербезопасности?» Другими словами, они недостаточно фундаментальны. Кроме того, они носят технический характер и их сложно объяснить высшему руководству на понятном ему языке. К тому же эти принципы являются дискретными: вы либо придерживаетесь их, либо нет. Они не допускают никаких нюансов, жизненно необходимых в условиях быстро меняющегося ландшафта угроз и бизнеса.

Вместо бинарных показателей нам нужна шкала, отражающая что-то вроде степени вероятности. Мы должны создать программу, соответствующую риск-аппетиту руководства. Наша программа, основанная на первичных принципах, должна снижать вероятность успешной реализации атаки со стороны киберпротивника. Это дает определенное пространство для планирования. Например, мы можем сказать руководству о том, что, потратив *X* долларов на новый защитный инструмент или функцию, снизили вероятность того, что группа противников проведет успешную киберкампанию против нас, с 20 до 15 %. Если программа обеспечения информационной

безопасности будет представлена в таком свете, руководство сможет оценить оправданность затрат на этот проект.

И даже если противнику удастся украсть нашу интеллектуальную собственность или зашифровать наши данные, эта программа все равно не будет считаться провальной. Мы ведь не говорили совету директоров, что она позволит предотвратить все атаки, — лишь обещали снизить вероятность их успешной реализации.

Вот это уже ближе к абсолютному первичному принципу. Это уже не бинарный вопрос, поскольку мы сформулировали его в терминах вероятностей, которые может учесть руководство. Однако здесь по-прежнему чего-то не хватает. Эта задача все еще слишком обширна и предполагает трату ресурсов на что-то неважное.

Чего нам не хватает, так это обсуждения темы существенности. Согласитесь, что не все сведения в вашей сети существенные. Если злоумышленники скомпрометируют ноутбук Луиджи и украдут меню с фирменными блюдами, подаваемыми в корпоративном кафетерии, вы вряд ли обратитесь в ФБР. Возможно, вам будет немного неприятно, но утечка меню на некий командно-контрольный сервер в Таджикистане не создаст для компании особых проблем. Так зачем тратить ресурсы на его защиту?

Не знаю, как у вас, но в моей практике объем ресурсов, выделяемых на обеспечение кибербезопасности, никогда не был бесконечным. Если попытаться распределить эти ресурсы на все без исключения, то они закончатся раньше, чем список запланированных дел. Проекты, на которые выделяются средства, скорее всего, не будут профинансированы в достаточной мере для того, чтобы решить проблему целиком. Это все равно что пытаться накормить ораву соседских детей одной ложкой арахисового масла и куском хлеба. В результате сыт не будет никто. Другими словами, следует сконцентрировать усилия на том, что существенно для бизнеса. Все остальное — мелочи.

Специалисты по управлению рисками компании Datamaran определяют существенность следующим образом: «Существенная проблема может оказать значительное влияние на финансовые, экономические, репутационные и юридические аспекты деятельности компании, а также на систему ее внутренних и внешних заинтересованных сторон» [153]. В финансовом мире существуют более конкретные определения, касающиеся раскрытия информации перед инвестированием, однако в мире кибербезопасности определение существенности, предложенное компанией Datamaran, является самым лучшим и наиболее лаконичным из тех, что мне удалось найти.

Дело в том, что для разных организаций существенными и несущественными могут быть разные вещи. Это зависит от многих факторов, в том числе от приемлемого уровня риска, размера организации, ее типа (коммерческая, научная или государственная) и т. д. И с течением времени это может меняться. То, что сегодня существенно для стартапа, перестанет быть таковым, когда он превратится в гиганта Кремниевой долины. При этом руководители компаний знают, что существенно для их бизнеса. Специалисты по безопасности тоже должны это понимать. Я хочу тратить свои ограниченные ресурсы на защиту существенных вещей, а не обеденного меню Луиджи.

Таким образом, на данный момент мы считаем базовым принципом кибербезопасности снижение вероятности нанесения нам существенного ущерба вследствие киберинцидента, но ему чего-то не хватает, он недостаточно конкретен. Последний необходимый элемент — привязка ко времени. Расчет вероятности причинения существенного ущерба организации в любой момент в будущем (скажем, в ближайшие 100 лет) значительно отличается от расчета этой вероятности на следующие три года. Смогут ли злоумышленники проникнуть в нашу цифровую среду в будущем? Это вполне вероятно, если вопрос задан в открытой форме, без указания конечной даты. Но смогут ли они добиться успеха в ближайшие три года? Вероятность этого резко снизится, если вопрос будет привязан к времени. Дополнительным преимуществом является то, что высшему руководству будет на чем сосредоточиться. Вместо того чтобы для получения финансирования программы по информационной безопасности использовать страх, неопределенность и сомнения, употребляя фразы наподобие: «О боже, все так ужасно! Мне надо гигантское количество денег на то, чтобы все исправить», вы могли бы проинформировать высшее руководство о потенциальных рисках, актуальных для следующего этапа развития бизнеса, и не пытаться вскипятить океан.

Учитывая все сказанное ранее, основополагающий первичный принцип, краеугольный камень кибербезопасности, на котором мы будем строить всю программу обеспечения информационной безопасности, должен учитывать три элемента: вероятность, существенность и время. Таким образом, предлагаемый мною вариант абсолютного базового принципа кибербезопасности, а также главный тезис этой книги звучит так: «Снижение вероятности существенного ущерба вследствие киберинцидента в течение ближайших трех лет».

Вот и все. Остальное не имеет значения. Количество лет может быть другим — один год, три года, пять лет. Просто выберите период, актуальный для

вашей организации. Но само утверждение атомарно. После его прочтения вы не говорите себе: «Мне все нравится, но нужно сделать еще три вещи». По сравнению с другими рассмотренными ранее кандидатами на роль базового принципа этот однозначно указывает на то, чего мы пытаемся достичь, а также предоставляет способ оценки вашей программы. Если вы тратите ресурсы на проекты, которые напрямую не способствуют реализации этого принципа, значит, вы тратите их впустую.

Заключение

При написании этой главы я исходил из того, что вы не знакомы с концепцией базовых принципов. Я объяснил, что это такое, и рассказал о некоторых крупных мыслителях, таких как Евклид, Аристотель, Декарт, Уайтхед, Рассел, а также Илон Маск, которые использовали их для решения сложнейших проблем человечества. Затем отметил, что в начале цифровой эры многие крупные ученые-компьютерщики, такие как Джеймс Андерсон, Уиллис Уэр, Белл и Лападула, Зальтцер и Шредер, доктор Фред Коэн и Донн Паркер, пытались сформулировать первичный принцип кибербезопасности, но так и не смогли этого сделать. Ближе всего к этой цели подошли авторы триады КЦД, которая, однако, тоже не является концепцией базовых принципов. Затем я привел аргументы в пользу того, что другие кандидаты на роль первичного принципа кибербезопасности также не подходят. Эффективное исправление ошибок, защита от вредоносных программ, быстрое обнаружение и устранение угроз, следование контрольным спискам, например предлагаемым организацией NIST или ISO, и даже соответствие нормативным требованиям не может считаться первичным принципом. Это хорошие тактические приемы, которые могут быть полезны, но они не представляют собой последовательную стратегию, базирующуюся на первичном принципе.

Затем я привел аргументы в пользу того, что абсолютным первичным принципом кибербезопасности является следующий: «Снижение вероятности существенного ущерба вследствие киберинцидента в течение ближайших трех лет».

Вот и все. Я обдумывал эту идею, обсуждал ее и писал о ней на протяжении почти десяти лет, в течение которых она неоднократно пересматривалась. Но мне кажется, что нынешний ее вариант как никогда близок к четкой формулировке того, чего все мы пытаемся достичь с помощью программ по обеспечению информационной безопасности.

В связи с этим возникает вопрос: что же дальше? Если все мы стремимся снизить вероятность нанесения существенного ущерба своим организациям вследствие киберинцидента в течение некоторого периода времени, то с помощью каких строительных блоков можно это сделать? Какие основные концепции позволят нам, подобно Уайтхеду и Расселу, однозначно доказать эквивалент утверждения 1 + 1 = 2 в мире сетевых защитников?

Дальнейший материал посвящен обсуждению стратегий и тактик, базирующихся на первичном принципе кибербезопасности и позволяющих снизить вероятность существенного ущерба вследствие киберинцидента в течение определенного времени. В следующей главе вы найдете обзор стратегий, логически вытекающих из предложенного мной первичного принципа кибербезопасности.

02 Стратегии

Без цели [маневрирование] бессмысленно.
Вы можете быть виртуозным тактиком, но у вас
не будет чувства стратегии.

Гарри Каспаров,
чемпион мира по шахматам

Какой бы красивой ни была стратегия, вам следует
время от времени оценивать результаты.

Сэр Уинстон Черчилль,
премьер-министр Великобритании
во время Второй мировой войны

Обзор главы

Эта глава представляет собой резюме остальной части книги, то есть глав 3–8. В главе 1 я объяснил понятие первичного принципа и привел аргументы в пользу того, что базовым принципом кибербезопасности является снижение вероятности причинения существенного ущерба вследствие киберинцидента в течение определенного периода времени. В этой главе описаны пять стратегий, которые логически вытекают из этой концепции. Можете рассматривать эту главу как введение, знакомящее с концепциями, тактиками и стратегиями, которым посвящены последующие главы. Прежде чем мы погрузимся в детали, я хочу дать здесь представление о том, что ждет вас впереди. Эти стратегии и тактики довольно сложны. Если вы не будете внимательны при чтении книги, то легко можете потерять нить

повествования. Используйте эту и первую главы для того, чтобы напомнить себе о том, где вы находитесь и зачем отправились в это путешествие.

И еще одно замечание: я не утверждаю, что сетевые защитники всех организаций (правительственных, коммерческих и научных) должны реализовать каждую из описанных далее стратегий для того, чтобы внедрить программу обеспечения кибербезопасности, базирующуюся на первичном принципе. Я лишь утверждаю, что эти стратегии логически вытекают из предложенного мной абсолютного первичного принципа. Если мы пытаемся снизить вероятность нанесения нам существенного ущерба, то рассматривать нужно именно эти стратегии, а не другие, вытекающие из кандидатов на роль атомарного первичного принципа, о которых я говорил и которые отверг в предыдущей главе.

Специалисты по безопасности могут реализовывать каждую из этих стратегий по отдельности, полностью или частично, а могут комбинировать их. Используемая при этом тактика позволяет до некоторой степени снизить вероятность существенного ущерба. Выбор той или иной стратегии зависит от размера организации, склонности высшего руководства к риску и имеющихся в вашем распоряжении ресурсов в виде людей, процессов и технологий. Кроме того, это зависит от вашей способности измерять эту вероятность с достаточной точностью для того, чтобы вести с руководством содержательный диалог. Эта задача настолько важна, что ей целиком посвящена глава 6.

Разница между стратегиями и тактиками

В главе 1 я привел аргументы в пользу того, что атомарным первичным принципом кибербезопасности, которого все мы должны придерживаться, является снижение вероятности нанесения нам существенного ущерба вследствие киберинцидента в течение определенного периода времени. Это краткое изложение того, что мы пытаемся сделать. Другими словами, это стратегия. В нашем случае это базирующаяся на первичном принципе, то есть самая важная, стратегия. Но она не говорит о том, как это сделать. Ответом на вопрос «как?» является набор тактик, или отдельных шагов, которые мы можем предпринять, чтобы приблизиться к целям, определяемым нашей стратегией.

В своей книге *Cyber War: The Next Threat to National Security and What to Do about It*, попавшей в Зал славы Cybersecurity Canon, Ричард Кларк и Роберт Кнаке называют безрассудством применение тактик без хорошо разработанной стратегии [49]. В качестве примера тактики они приводят создание киберкомандования США в 2009 году. Они критикуют правительство страны за то, что оно создало целую организацию, не имея полного представления о стратегии, которую ей предстоит реализовать. Я написал книгу о первичных принципах кибербезопасности в том числе и потому, что многие представители ИБ-сообщества поступают точно так же — используют набор тактических приемов, не имея всеобъемлющей стратегии.

В своей книге *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* Джейсон Андресс и Стив Винтерфельд описывают средний уровень — уровень оперативных промежуточных целей, соединяющий стратегию («что?») с тактикой («как?») [9]. Например, стратегия, базирующаяся на первичном принципе, может заключаться в пресечении всех действий известного противника. Промежуточной целью может быть выявление в нашей сети любой активности хактивистов из группы Killnet. Тактика может заключаться в развертывании всех средств предотвращения и обнаружения, связанных с тактиками, методами и процедурами Killnet, перечисленными в базе знаний MITRE ATT&CK [283].

Суть в том, что стратегия и тактика неразрывно связаны друг с другом. Стратегия без тактики означает, что вы хорошо ставите цели, но не имеете представления о том, как их достигать. Тактика без стратегии означает, что вы совершаете беспорядочные действия, не имея четкой цели и направления.

Основные стратегии реализации программы защиты информации, базирующейся на первичном принципе

Если к этому моменту вы еще не захлопнули книгу, сочтя ее абсурдной, значит, вам по крайней мере интересно узнать о том, какими могут быть стратегии, основанные на первичных принципах кибербезопасности. Как было сказано в главе 1, первичные принципы любой проблемной области атомарны и используются в качестве строительных блоков для выведения всего остального. Если нашей стратегией, базирующейся на первичном принципе, является снижение вероятности существенного ущерба в ре-

зультате киберинцидента, то вспомогательные стратегии должны логически вытекать из нее. Они не самостоятельные, то есть не существуют в вакууме. Исходя из этого, я считаю, что мы должны использовать некую комбинацию из пяти подстратегий («что?»), которые могут непосредственно способствовать достижению поставленной цели, и набора тактик для реализации каждой из них («как?»).

В следующих главах я подробно опишу каждую из подстратегий и сопутствующих им тактик, а здесь приведу лишь краткий их обзор. Две из пяти подстратегий непосредственно вытекают из нашего абсолютного базового принципа. Мы можем укрепить свою оборонительную позицию с помощью пассивной кибергигиены — тактик общего назначения, позволяющих помешать деятельности любого противника (о стратегии нулевого доверия речь пойдет в главе 3). Также можем создать более активные средства защиты на основе известных последовательностей этапов атак, разрабатывая защитные кампании с учетом специфики киберпротивника (стратегия предотвращения реализации kill chain рассматривается в главе 4). Третья подстратегия заключается в обеспечении устойчивости (глава 5), позволяющей снизить вероятность существенного ущерба, даже если киберпротивнику удастся прорвать нашу оборону. Это позволяет ограничить ущерб от наступившего события. Четвертая подстратегия состоит в прогнозировании рисков (глава 6). Если наша программа обеспечения информационной безопасности основана на снижении вероятности нанесения нам существенного ущерба, то как мы можем вычислить эту вероятность и размер ущерба? Наконец, последней подстратегией является автоматизация (глава 7). В мире, где властвует концепция «инфраструктура как код», автоматизация тактик, базирующихся на первичном принципе, становится просто необходимой.

Обзор стратегии нулевого доверия

До 2010 года самой распространенной оборонительной стратегией являлась так называемая *защита периметра (perimeter defense)*. Суть ее заключалась в возведении вокруг цифровых активов надежного электронного барьера, за который допускались лишь авторизованные пользователи и устройства. Проблема этой стратегии в том, что она отлично работает лишь до тех пор, пока какой-нибудь злоумышленник не проникнет за это ограждение. Попав внутрь, он получает доступ ко всему (см. пример с Эдвардом Сноуденом в главе 3). Наше отношение к этой стратегии начало меняться после

публикации статьи Джона Киндервага *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security* в 2010 году [133]. В ней он предлагает сетевым архитекторам исходить из того, что киберпротивники уже действуют в их цифровой среде. Если это так, то какие проектные решения они должны принять, чтобы снизить вероятность существенного ущерба вследствие кибератаки?

Первый шаг заключается в том, чтобы закрыть все окна и двери в цифровую среду, затруднив деятельность киберпротивников. Кто-то может назвать это *кибергигиеной*, концепцию которой Винт Серф предложил еще в 2000 году [44], но на самом деле это нечто гораздо большее. Мы также должны знать, у кого (сотрудники и подрядчики) и чего (устройства и программные модули) есть право доступа к нашим цифровым средам, какими полномочиями они обладают, а также обеспечить мониторинг соблюдения установленных правил. Здесь на ум приходят такие очевидные тактики, как управление уязвимостями и управление идентификацией и доступом (IAM), однако существует и множество других потенциально полезных тактик (см. главу 3).

В своей статье Киндерваг пишет: «В режиме нулевого доверия весь сетевой трафик является недоверенным. Таким образом, специалисты по безопасности должны проверять и защищать все ресурсы, ограничивать и строго контролировать доступ, а также проверять и регистрировать весь сетевой трафик». Согласно принципам NIST нулевое доверие «предполагает отсутствие неявного доверия к активам или учетным записям пользователей, основанного исключительно на их физическом или сетевом расположении (например, локальные сети или Интернет) или на принадлежности активов (корпоративные или личные)» [187].

Когда я занимал должность директора по безопасности в компании Palo Alto Networks (поставщик решений для обеспечения безопасности, наиболее известный своими межсетевыми экранами прикладного уровня, или брандмауэрами), руководство хотело найти способ продемонстрировать внешним заказчикам то, как внутренняя служба безопасности компании использует межсетевой экран для реализации принципа нулевого доверия. Оказалось, что межсетевые экраны прикладного уровня (а их версии есть у всех производителей,

не только у Palo Alto Networks) отлично подходят для решения этой задачи. Их администраторы устанавливают правила для запущенных приложений, привязанных к аутентифицированным пользователям. В этом мире приложением является все, начиная с использования любого SaaS-сервиса и интернет-серфинга и заканчивая подключением к сетевому принтеру и пингованием хоста. Буквально все, что делает пользователь, устройство или программный компонент, генерирующий сетевой трафик, проходящий через сетевой экран, является контролируемым приложением. Мы быстро обнаружили, что, используя имеющийся у нас инструмент обеспечения безопасности (собственный межсетевой экран прикладного уровня), можем реализовать стратегию нулевого доверия и нам не требуется покупать и развертывать дополнительный набор технологий. Нужны были только люди и процессы. А поскольку мы применяли один и тот же брандмауэр для всех своих островов данных, включая облако, SaaS, мобильные устройства и центр обработки данных, достаточно было единожды создать набор правил в виде политики, который система могла самостоятельно распространить на все острова данных. В результате у нас сформировался новый образ мышления, основанный на принципе нулевого доверия.

Это весьма важные идеи. В книге нулевое доверие преподносится не только как стратегия кибербезопасности, основанная на базовом принципе, но и как образ мышления или философия. Вы не создаете среду с нулевым уровнем доверия, а приближаетесь к этой цели шаг за шагом, принимая сотни и тысячи повседневных проектных решений, укрепляющих вашу оборонительную позицию. Это путешествие, не имеющее пункта назначения. В главе 3 я подробно опишу ряд тактик, которые необходимо рассмотреть для реализации стратегии нулевого доверия.

Однако стратегия нулевого доверия является пассивной, то есть реализуемые параметры проектирования представляют собой конфигурационные решения и лучшие практики, которым должны следовать все вне зависимости от актуальных угроз. Для более активной обороны, то есть для развертывания средств предотвращения атак, основанных на поведении известного противника, необходима другая стратегия, направленная на то, чтобы не была реализована убийственная цепочка вторжения.

Обзор стратегии предотвращения реализации убийственной цепочки вторжения

Из опыта нам известно, что, атакуя своих жертв, киберпротивники не ограничиваются каким-то одним действием. Для достижения своих целей они должны провести ряд мероприятий. Но мы узнали об этом лишь в 2010 году благодаря исследовательской группе компании Lockheed Martin. В оригинальном техническом документе *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, подготовленном Хатчинсом, Клоппертом и Амином, говорится: «Защита компьютерных сетей на основе разведданных — это стратегия управления рисками, направленная на связанные с ними угрозы, предусматривающая анализ противников, их возможностей, целей, доктрин и ограничений. Она требует нового понимания самих вторжений, причем не как единичных событий, а как последовательностей действий» [115].

ИБ-сообщество отслеживало поведение киберпротивников практически с самого начала развития сферы инфобезопасности. Еще в 1998 году Агентство оборонных информационных систем выявило активность российских хакеров в нескольких правительственных сетях США (эта серия кибератак получила кодовое название Moonlight Maze) [211]. В настоящее время фреймворк MITRE ATT&CK представляет собой, пожалуй, наиболее полную и бесплатную коллекцию тактик, техник и процедур, используемых известными противниками.

Мы также на собственном опыте убедились в том, что киберпротивники не разрабатывают совершенно новые кампании для каждой отдельной жертвы. Они используют одни и те же последовательности действий снова и снова до тех пор, пока какой-нибудь защитник сети их не остановит. Но даже в этом случае они не отказываются от всей кампании — просто заменяют конкретный ее этап, который был заблокирован. Учитывая то, что нам известно большинство последовательностей шагов злоумышленников, вполне логичными являются разработка и внедрение средств их предотвращения и обнаружения для любого стека безопасности, развернутого на основе этих разведданных. Даже самый младший аналитик по кибербезопасности слышал фразу: «Защитник должен делать все правильно в 100 % случаев. Атакующему достаточно сделать все правильно хотя бы один раз». Так вот, стратегия предотвращения реализации убийственной цепочки вторжения перевернула эту идею с ног на голову. Теперь атакующий должен безоши-

бочно выполнять каждый шаг, тогда как защитнику достаточно сделать все правильно лишь один раз. Мышление в терминах убийственной цепочки смещает баланс сил в пользу защитника.

Однажды, будучи директором по безопасности в Palo Alto Networks, я отправился во Францию, чтобы посетить клиентов и потенциальных заказчиков компании. В ходе поездки я встретился с полковником, возглавляющим подразделение французской жандармерии по борьбе с киберпреступностью (C3N). Он сразу же отмахнулся от меня, препоручив работу со мной одному из капитанов, который был явно раздражен тем, что начальник заставил его нянчиться с американцем. Уже через пять минут разговора я понял, что он меня почти не слушает (его английский был довольно хорош, а я совсем не говорю по-французски, что, вероятно, раздражало его еще больше). Примерно через 30 минут он резко прервал разговор и заявил, что ему нужна оперативная информация, касающаяся французской киберпреступности, а не пространное описание межсетевых экранов нового поколения. Ему нужна возможность арестовывать преступников, а не просто блокировать трафик злоумышленников. Пока сопровождавший меня сотрудник отдела продаж пытался успокоить капитана, я написал своему директору службы разведки и попросил предоставить мне французские IP-адреса, связанные с командно-контрольными узлами, используемыми киберпреступниками (см. главу 4 и схему убийственной цепочки компании Lockheed Martin). Спустя десять минут мой директор прислал мне четыре IP-адреса. Когда я передал капитану этот список, его глаза загорелись и он выбежал из комнаты. Я понял, что встреча окончена. Через несколько дней от того же сотрудника отдела продаж я узнал о том, что капитан немедленно получил разрешение на поиск физических адресов, связанных с IP-адресами этих французских командно-контрольных узлов, и остановил их работу.

Как я уже говорил, в отличие от пассивной стратегии нулевого доверия стратегия предотвращения реализации убийственной цепочки вторжения является активной. Обе эти стратегии вытекают непосредственно из первичного принципа кибербезопасности. Сначала вы максимально ограничиваете доступ к среде в рамках стратегии нулевого доверия, а затем развертываете средства для обнаружения и предотвращения всех известных

последовательностей действий противника. В главе 4 я подробно опишу некоторые тактические приемы, которые следует рассмотреть для организации защиты от убийственной цепочки вторжения.

С помощью этих двух стратегий можно значительно снизить вероятность существенного ущерба. Но что делать, если киберпротивник все же проникнет в нашу систему? Мы ведь всего лишь снизили вероятность, а не полностью предотвратили все успешные атаки. Здесь нам может пригодиться стратегия обеспечения устойчивости.

Обзор стратегии обеспечения устойчивости

Организация ASIS International ввела термин *«устойчивость» (resilience)* в обиход в 2009 году, по сути, сама концепция обозначает то, что называется непрерывностью бизнеса. В 2012 году на Всемирном экономическом форуме это понятие было определено как «...способность систем и организаций противостоять киберинцидентам...» [302].

С тех пор другие лидеры мнений доработали это определение. В 2013 году президент США Барак Обама даже подписал директиву, предписывающую обеспечить устойчивость критической инфраструктуры страны.

В 2017 году Международная организация по стандартизации (ISO) определила устойчивость как «...способность организации воспринимать изменяющиеся условия и адаптироваться к ним, позволяющая ей достигать поставленных целей, выживать и процветать» [17].

Однако больше всего мне нравится определение, данное Стокгольмским университетом в 2015 году. В своей работе *Cyber Resilience — Fundamentals for a Definition* Фредрик Бьек, Мартин Хенкель, Янис Стирна и Елена Здравкович определяют устойчивость как «...способность постоянно достигать поставленных целей, несмотря на неблагоприятные киберинциденты» [32].

Другими словами, вам следует допустить то, что злоумышленникам в какой-то момент удастся реализовать свою убийственную цепочку, найти брешь в вашей броне нулевого доверия или когда-нибудь в будущем произойдет масштабный сбой. Один из моих армейских начальников всегда говорил, что плохой парень получает право голоса и активно пытается разрушить вашу

стратегию и тактику. На этот случай вам следует разработать стратегию, которая обеспечит функционирование основных служб вашей организации. В этом и заключается суть устойчивости.

С этой задачей довольно успешно справляются такие крупные облачные провайдеры, как Google, Amazon и Microsoft. Как вы знаете, работа их внутренней инфраструктуры обеспечивается тысячами, а то и миллионами компьютеров. Если среднее время наработки до отказа (MTTF) для каждого отдельного устройства составляет от трех до пяти лет, то можно предположить, что у каждого из этих поставщиков всегда есть машины, выходящие из строя. Это становится очевидно, если учесть огромное количество используемых ими компьютеров и выполнить ряд простых математических вычислений с переменными MTTF. Однако замечаете ли вы как потребитель сбои в работе этих служб? Нет, не замечаете, поскольку каждый из этих поставщиков создал отказоустойчивые системы, способные продолжать предоставлять услуги даже во время подобных сбоев.

В главе 5 мы подробно обсудим различия и пересечения таких понятий, как непрерывность бизнеса, аварийное восстановление и устойчивость. Рассмотрим также ряд тактик, которые необходимо учитывать при развертывании стратегии обеспечения устойчивости, такие как соблюдение нормативных требований, кризисное планирование, резервное копирование и восстановление, шифрование данных в состоянии покоя и в движении, а также реагирование на инциденты.

Обзор стратегии прогнозирования рисков

Поскольку атомарный базовый принцип кибербезопасности заключается в снижении вероятности существенного ущерба, то очевидная стратегия, вытекающая непосредственно из него (более очевидная, чем нулевое доверие, предотвращение реализации убийственной цепочки вторжения и обеспечение устойчивости), заключается в нахождении эффективного способа оценки вероятностей. Если мы не можем измерить сиюминутную вероятность существенного ущерба в результате какого-либо киберинцидента в ближайшем будущем, то определенно не сможем измерить степень снижения этой вероятности в результате реализации одной или нескольких стратегий, базирующихся на первичном принципе.

По правде говоря, сетевые защитники испытывают трудности при решении этой задачи. Если быть до конца честными, то мы просто не знаем, как это сделать. До недавнего времени я и сам относился к этой категории. Я прочитал все книги по этой теме, попавшие в Зал славы Cybersecurity Canon (а их немало), и даже представил доклад на ежегодной конференции RSA вместе с Ричардом Сирсеном (одним из соавторов книги «Как оценить риски в кибербезопасности») [334]. Но в ходе всех этих попыток я, по сути, лишь нащупывал очертания проблемы. Читая книги, я все время ожидал, что обнаружу главу с четким описанием пошагового алгоритма реализации этой стратегии, но так и не находил ее. В итоге понял, что должен разобраться в этом сам. После нескольких лет я наконец-то нашел ответ.

Проблема, как мне кажется, заключается в чрезмерном усложнении поставленной задачи. Мы думали: поскольку она связана с математикой, необходимо выполнять высокоточные вычисления, предусматривающие подсчет всех элементов в наших сетях, учет всех известных и неизвестных переменных и прогон всего этого через некий алгоритм Монте-Карло. Через несколько лет после множества попыток я понял, что это неправильный подход. Специалистам по безопасности не нужны точные ответы для принятия решений о выделении таких ресурсов, как люди, процессы и технологии. Нам нужны довольно точные, но приблизительные ответы, позволяющие быстро принимать решения, практически мгновенно оценивать текущую ситуацию и доносить информацию о ней до высшего руководства.

Прогнозирование рисков предполагает использование комбинации методов суперпрогнозирования (популяризованы доктором Филипом Тетлоком и Дэном Гарднером) [332], оценок Ферми (названы в честь всемирно известного физика Энрико Ферми), правила Байеса (изобретено статистиком Томасом Байесом), приблизительных расчетов «извне внутрь» с помощью общедоступных данных и приблизительных расчетов «изнутри наружу» с задействованием результатов применения наших стратегий, основанных на базовом принципе кибербезопасности.

Знаю, что все это кажется трудновыполнимым, однако я объясню каждую из этих вещей в главе 6 и, что еще важнее, покажу, как их можно совместить, на двух примерах. Другими словами, в этой книге есть та самая глава с пошаговым алгоритмом, которой мне так не хватало в свое время.

Итак, мы переходим к последней стратегии, основанной на базовом принципе кибербезопасности, которая заключается в автоматизации.

Обзор стратегии автоматизации

Автоматизация стала играть ключевую роль в начале 1990-х годов, когда Интернет начали использовать широкие слои населения. В те времена мы создавали программы для выполнения простых задач, облегчающие нам жизнь: текстовые редакторы, антивирусы и приложения для работы с электронной почтой, а также игры наподобие Doom, Half-Life и Golden-Eye 007. Но уже тогда будущие гиганты Кремниевой долины, такие как Amazon и Google, начали осознавать возможность автоматизации целых экосистем для обеспечения стабильности их работы, масштабирования, быстрого восстановления и централизации ошибок. В конечном итоге это привело к появлению сервисов AWS и Google Cloud, в основе которых лежат принцип «инфраструктура как код» и философии разработки программного обеспечения Agile и DevOps. Как говорят авторы книги «Site Reliability Engineering», попавшей в Зал славы Cybersecurity Canon, «автоматизируйте ВСЕ!» [321].

Мир информационных технологий довольно быстро принял эту концепцию, но ИБ-сообщество не спешило этого делать. И это было ошибкой. Если мы хотим получить хоть какое-то преимущество в предотвращении успешных атак на наши цифровые среды со стороны киберпротивников, то мы как группа должны быть более гибкими, чем они. Неважно, насколько надежны ваши реализации стратегий нулевого доверия, защиты от убийственной цепочки вторжения и обеспечения устойчивости. Если вашей организации требуются дни или недели на то, чтобы модифицировать свою инфраструктуру, основанную на базовом принципе кибербезопасности, при изменении ландшафта угроз, потому что приходится делать все вручную, то вероятность нанесения вам существенного ущерба все равно будет довольно высока. Мы знаем, что противники автоматизировали свою инфраструктуру. Для ИБ-сообщества работать в ручном режиме — это все равно что прийти с ножом на перестрелку, как сказал Шон Коннери в фильме «Неприкасаемые» (1987). Рассматриваемая с этой точки зрения автоматизация — не просто полезная функция, которую мы можем внедрить в свободное время, а стержень для развертывания всей нашей стратегии, основанной на базовом принципе.

В главе 7 я описываю историю автоматизации, начиная с каскадной модели разработки ПО и заканчивая методологиями Agile и DevOps. В ней рассказывается также о способах защиты кода, разработанного внутри организации, и настоятельно рекомендуется внедрить SRE-подход (Site Reliability Engineering — обеспечение надежности сайта). В заключение я высказываю

сожаление по поводу того, что представители ИБ-сообщества очень медленно вовлекаются в процесс DevOps в своих организациях с целью его трансформирования в DevSecOps, и показываю, как это сделать, на примере Chaos Monkey компании Netflix.

Заключение

Итак, в этой главе вы познакомились с кратким описанием стратегий, вытекающих из атомарного первичного принципа кибербезопасности. Подробнее о каждой из них поговорим в следующих главах. Помните, что стратегии описывают то, чего мы хотим достичь. Набор тактик, которым посвящена остальная часть книги, определяет то, как именно можно достичь каждой из поставленных стратегических целей. В этой главе я привел высокоуровневое описание таких стратегий, как:

- нулевое доверие;
- предотвращение реализации убийственной цепочки вторжения (kill chain);
- обеспечение устойчивости;
- прогнозирование рисков;
- автоматизация.

Я также объяснил, что сетевым защитникам не обязательно реализовывать каждую стратегию в полном объеме, чтобы внедрить программу обеспечения информационной безопасности, основанную на базовом принципе. Целью нашей программы является снижение вероятности существенного ущерба. Каждая из рассмотренных стратегий будет способствовать ее снижению. Однако степень ее влияния будет зависеть от эффективности применения тактик. Выбор стратегии зависит от размера организации, ее культуры производства и пожеланий высшего руководства.

Теперь, когда вы познакомились с кратким обзором, пришло время подробно рассмотреть основанную на первичном принципе кибербезопасности стратегию нулевого доверия.

03 Нулевое доверие

Нулевое доверие — это не проект, а новый взгляд на обеспечение информационной безопасности.

Джон Киндерваг,
автор основополагающей работы
о стратегии нулевого доверия
No More Chewy Centers

Переход к ZTA (архитектуре нулевого доверия) — это путь, связанный с тем, как организация оценивает риски в рамках реализации своей миссии, и он не может быть осуществлен простой заменой технологий.

Специальная публикация 800-207
Национального института
стандартов и технологий

Обзор главы

Как вы помните из главы 2, разница между стратегией и тактикой заключается в том, что стратегия определяет то, чего мы хотим добиться, а тактика отвечает на вопрос, как можно это сделать. В этой главе поговорим о стратегии нулевого доверия и рассмотрим несколько тактик ее реализации. На примере случая с Эдвардом Сноуденом я покажу важность стратегии нулевого доверия и объясню, почему ее реализация представляет собой скорее непрерывный путь, нежели конечную цель. Я расскажу о том, как

вы можете следовать по этому пути, используя уже имеющиеся инструменты и оборудование, и объясню, почему управление уязвимостями — это важная тактика нулевого доверия, но не самостоятельная стратегия. Также приведу аргументы в пользу того, что вам следует уже сейчас организовывать свои внутренние системы с использованием спецификаций программного обеспечения (SBOM) и что программно-определяемый периметр (SDP) — более предпочтительная архитектура безопасности с нулевым доверием по сравнению с существующими моделями. В заключение я опишу текущее положение дел в сфере управления идентификацией и доступом (IAM), технологии единого входа (SSO) и многофакторной аутентификации (MFA).

Актуальность стратегии нулевого доверия: случай с Эдвардом Сноуденом

Когда речь заходит об актуальности применения стратегии нулевого доверия, в первую очередь, как правило, вспоминают об инсайдерских угрозах, которые исходят не от какой-то продвинутой хакерской группировки национального масштаба, а изнутри. Их источником являются ваши сотрудники и подрядчики, которым вы доверяете управление бизнесом или взаимодействие с государственными органами. Некоторые из тех, кто имеет доступ к конфиденциальной информации, по разным причинам иногда решают причинить вред организации, в которой работают.

За прошедшие годы в новостях освещалось множество подобных примеров. Вот три наиболее печально известных.

- *2010 год:* Челси Мэннинг, военнослужащая армии США, передала сайту WikiLeaks 500 000 правительственных документов.
- *2018 год:* недовольный сотрудник компании Tesla повысил свои привилегии, внес изменения в код производственной операционной системы и передал большое количество конфиденциальных данных компании неизвестным третьим лицам.
- *2019 год:* недовольный сотрудник компании Capital One опубликовал на GitHub данные о 100 млн клиентских счетов и заявок на получение кредитных карт.

Можно вспомнить множество подобных событий, однако наиболее показательным примером инсайдерской угрозы, демонстрирующим важность стратегии нулевого доверия, является случай с бывшим сотрудником Агентства национальной безопасности Эдвардом Сноуденом. Работая системным администратором, поддерживающим работу секретных сетей АНБ, Сноуден начал собирать документы, которые, по его мнению, доказывали превышение правительством своих полномочий в области сбора внутренних разведданных и секретных программ слежения. В 2013 году он опубликовал в прессе около 1 млн таких секретных документов [132].

Вне зависимости от того, считаете ли вы этого человека предателем или героем, именно его имеют в виду представители индустрии кибербезопасности, когда говорят об инсайдерских угрозах. Будучи системным администратором, он мог войти в любую из сетей АНБ и получить доступ практически ко всем хранящимся там данным. Правительство США использует несколько сетей, не имеющих прямого подключения к Интернету. Большинство из нас слышали о таких сетях, как NIPRNET (Non-classified Internet Protocol — сеть маршрутизации неконфиденциального IP-трафика, которая, по сути, представляет собой Интернет правительства США), SIPRNET (Secret Internet Protocol Router Network — система взаимосвязанных компьютерных сетей для передачи секретной информации) и JWICS (Joint Worldwide Intelligence Communications System, также называемая *high-side network*, — объединенная глобальная сеть разведывательных коммуникаций, в которой хранятся сверхсекретные разведданные).

Сноуден приобрел в даркнете веб-краулер примерно за 100 долларов и запустил его в сеть JWICS. Он собрал более 1 млн особо секретных документов, вышел с ними за дверь и, скажем так, вызвал своими дальнейшими действиями международный резонанс. Чтобы получить доступ к JWICS, он не произвел взлом уровня Марка Цукерберга, показанный в фильме «Социальная сеть». По сути, он просто прогулялся по Интернету, чтобы посмотреть, что ему удастся найти. Правда, полномочия системного администратора тоже оказались нелишними [182].

В то время сетевые инженеры JWICS не имели понятия о сети с нулевым уровнем доверия, поскольку эта концепция еще не получила своего распространения. Но мне видится некая ирония в том, что Джон Киндерваг основывал свой тезис о нулевом доверии (см. следующий раздел) на способах, с помощью которых разведывательное сообщество обычно разделяет свои секреты, то есть на принципе минимальной необходимой осведомленности.

Сотрудники не получают доступа к информации, работа с которой не входит в их обязанности, за исключением системных администраторов, обеспечивающих работу системы, верно? Справедливости ради следует отметить, что в 2013 году никто не предполагал, что проверенный подрядчик будет делать подобные вещи в сверхсекретной сети. Если оглянуться назад, такая вероятность кажется вполне очевидной, но в то время меры контроля, которые применяло АНБ для проверки таких сотрудников, казались адекватными и превосходили все то, что большинство из нас использует сегодня.

Концепция нулевого доверия переоценена рынком, но...

Прежде всего позвольте мне объяснить разницу между маркетинговым ажиотажем на рынке, вызванным поставщиками систем безопасности, и потребностью в применении стратегии, основанной на первичном принципе, внутри организации. Я знаю, что слова «нулевое доверие» уже набили оскомину большинству сетевых защитников. В 2022 году поставщики использовали их так часто, что они начали утрачивать свой изначальный смысл. Специалисты-практики уже устали слышать о нулевом доверии, а некоторые из них даже отвергают саму идею, вызвавшую всю эту шумиху, считая ее просто маркетинговым ходом. Однако это вполне обычное явление в сфере технологий, причем так бывает с любой перспективной концепцией.

Все начинается с того, что у кого-то появляется хорошая идея, как было с Джоном Киндервагом, опубликовавшим в 2010 году основополагающую работу о принципе нулевого доверия *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*. Медленно, но верно все воодушевляются ею как панацеей от всех бед и способом достижения мира во всем мире. Однако в какой-то момент люди отказываются от этой замечательной идеи, осознав, что найти практический способ ее реализации очень сложно, а коммерческие продукты, производители которых утверждают, что они решили эту задачу, не дотягивают до заявленного уровня.

Эти изменения в уровне ожиданий прекрасно отражает знаменитая *кривая зрелости* технологии Gartner — *Hype Cycle* [171]. Как сообщается на сайте Challenging Coder, эта концепция была разработана в 1995 году сотрудницей компании Gartner Джеки Фенн, которая обратила внимание на повторяющиеся закономерности в ожиданиях потребителей в отношении инноваци-

онных технологических товаров и услуг, появляющихся на рынке средств обеспечения безопасности. После представления продукта наблюдается пик завышенных ожиданий, когда потребители осознают потенциал новой идеи. Затем уровень ожиданий снижается, достигая впадины разочарования, когда те же самые люди начинают понимать, что новая технология еще не совсем готова к прайм-тайму. Потом этот уровень вновь повышается, следуя по более пологому склону просветления. Наконец, в результате наступления зрелости продукт достигает плато продуктивности. В 2008 году Фенн опубликовала книгу, посвященную этой концепции [78].

Несмотря на то что многие сетевые защитники определили бы место концепции нулевого доверия ближе к впадине разочарования, в период написания этой книги (2022 год) аналитики Gartner наблюдали некоторые изменения. Согласно отчету Gartner Hype Cycle за сентябрь 2021 года (рис. 3.1), продукты, реализующие эту концепцию, выбрались из впадины разочарования и начали медленное восхождение по склону просветления.

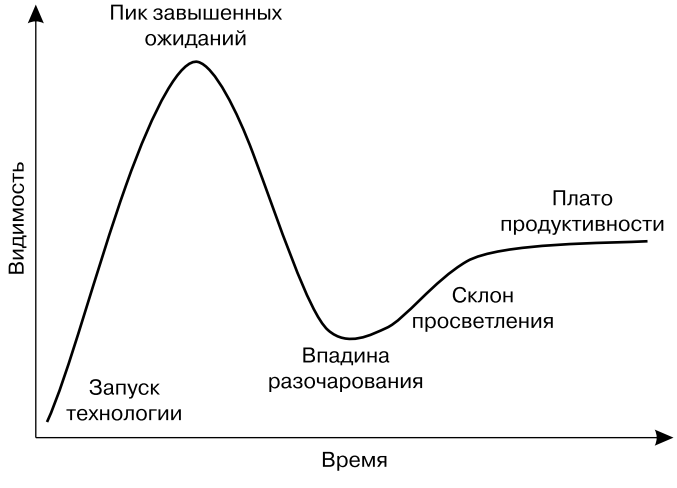


Рис. 3.1. Пример кривой зрелости технологии Gartner Hype Cycle

Я бы сказал, что соответствующие функции этих продуктов в основном сводятся к ограничению доступа к тем или иным ресурсам на основе принципа минимальной необходимой осведомленности. И это хорошо. Однако хочу немного сместить угол зрения и рассмотреть нулевое доверие в качестве стратегии, базирующейся на первичном принципе, а не на функции того или иного инструмента обеспечения безопасности.

Кибергигиена, эшелонированная защита и защита периметра: нулевое доверие до появления одноименной концепции

Понятие *кибергигиены* ввел в обиход отец Интернета Винт Серф. По крайней мере, он озвучил эту фразу в ходе выступления перед Объединенным экономическим комитетом Конгресса США в 2000 году [44]. Серф является одним из создателей стека протоколов TCP/IP, разработанного в 1970-х годах, и именно он придумал название для передовой практики кибергигиены, которой большинство сетевых защитников придерживалось на протяжении более десяти лет.

Изначально мы просто пытались исправлять все ошибки в программном обеспечении. Это можно уподобить попытке защитить свой дом от воров. Вы можете потратить много денег и времени на установку, обслуживание и мониторинг дорогостоящего оборудования для видеонаблюдения. Однако если забудете запереть двери и окна, уходя на весь вечер, то ворам будет гораздо проще проникнуть в дом, чем в случае, когда вы это сделали. В данном случае запирание окон и дверей — это метафора исправления ошибок в коде программы.

Однако со временем стратегия кибергигиены трансформировалась в модель защиты периметра, предусматривающую возведение надежных электронных барьеров, обычно с помощью брандмауэров, которые отделяли внутреннюю зону, в которой мы работали, от остального Интернета. Первые коммерческие межсетевые экраны с контролем состояния появились примерно в 1994 году [48, 102, 116]. За ними находились важные активы организации и работали системы и люди.

Постепенно защита периметра переросла в потребность в средствах, предназначенных для решения конкретных задач, связанных с обнаружением и предотвращением атак. Стали появляться системы обнаружения вторжений (IDS) и антивирусы. Дороти Деннинг изобрела современную IDS в 1986 году [63], примерно в то же время появились первые антивирусы [245]. В итоге мы стали называть феномен использования нескольких инструментов в стеке безопасности *эшелонированной защитой*. Этот термин вошел в обиход благодаря статье Фреда Коэна, опубликованной

в 1992 году [51–53]. Мы также стали именовать набор развернутых защитных средств *стеком безопасности*.

Суть его заключалась в том, что если первый инструмент не сможет предотвратить вторжение злоумышленника, это сделает второй. Если и тот не справится с задачей, будет задействован третий и т. д. Как сказала математику Бертрану Расселу старушка, объясняя существование Бога: «[Все знают, что] черепахи там до самого низа!» Количество черепах в стеке безопасности зависело от размера бюджета. В 2023 году, когда предприятия работают с множеством островов данных (центры обработки данных, мобильные устройства, SaaS-сервисы и многочисленные облачные среды), их стеки безопасности нередко насчитывают от 15 до 300 инструментов в зависимости от размера организации.

На практике защита периметра и эшелонированная защита сводились к соблюдению правил кибергигиены. Другими словами, после создания периметра нужно было следить за тем, чтобы в системах были установлены самые последние патчи, а в средствах стека безопасности — актуальные сигнатуры.

Рождение концепции нулевого доверия

Защита периметра и эшелонированная защита оставались доминирующими моделями безопасности на протяжении 2000-х годов. В 2010 году по Интернету одновременно прокатились три гигантские шоковые волны, которые изменили все представления об обеспечении кибербезопасности. Первым из этих событий стала публикация статьи сотрудников Lockheed Martin с описанием модели kill chain [115]. Вторым событием была известная китайская кибератака на Google (операция Aurora) [196]. Наконец, третьим стала публикация технического документа компании Forrester, посвященного концепции нулевого доверия [133]. Модель убийственной цепочки никак не связана с концепцией нулевого доверия, но то, что исследователи Lockheed Martin обнародовали ее в тот же самый год, когда исследователи из Forrester опубликовали документ о принципе нулевого доверия, весьма примечательно. Этим двум концепциям в основном и посвящена данная книга (в частности, эта и следующая главы).

Связь между атаками на Google и техническим документом Forrester состоит лишь в том, что в статье Forrester была изложена стратегия нулевого доверия, а атаки китайцев заставили инженеров Google перепроектировать свои внутренние сети и развернуть одну из первых работоспособных реализаций этой стратегии. В дальнейшем это привело к появлению коммерческого продукта под названием Beyond Trust. В отрасли сложилось мнение, что если такой гигант Кремниевой долины, как Google, решил взять на вооружение концепцию нулевого доверия, значит, это не просто очередная теория какой-нибудь аналитической компании наподобие Forrester.

Идеи, связанные с концепцией нулевого доверия, витали в воздухе с начала 2000-х годов. Но как философия она была окончательно сформулирована Джоном Киндервагом в работе *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*. Название оказалось довольно неудачным, потому что, не изучив документ, можно подумать, что это оксюморон. Как можно управлять сетью, не доверяя ничему и никому? Однако Киндерваг говорил не об этом.

Он основывает свой тезис на том, что военные и разведывательные сообщества защищают секретную информацию, руководствуясь принципом минимальной необходимой осведомленности. Другими словами, если какая-то информация не нужна вам для выполнения работы, вы не должны иметь к ней доступа. Таким образом, при реализации стратегии нулевого доверия сетевые архитекторы исходят из того, что их цифровые среды уже скомпрометированы, и проектируют их таким образом, чтобы снизить вероятность причинения существенного ущерба в случае реального рискового события.

Эта мощная концепция казалась довольно радикальной по сравнению с господствовавшей в то время идеей защиты периметра.

Защита периметра предполагает возведение мощного внешнего барьера. Однако в случае проникновения внутрь злоумышленники получают доступ ко всему. Все внутренние транзакции автоматически становятся доверенными, как в случае с Эдвардом Сноуденом. Судя по содержанию статьи, Джон считает эту идею смехотворной. Просто взгляните на ее заголовок: *No More Chewy Centers* («Больше никаких жевательных начинок»). Я называю защиту периметра «дао сетевого дизайна M&M», имея в виду твердую оболочку драже снаружи и аппетитную шоколадную начинку внутри.

Инцидент со Сноуденом заставил АНБ и многих сетевых защитников переосмыслить свои подходы к дизайну сетей. В результате для ИБ-сообщества теоретическая статья Киндервага превратилась из интересной идеи в ключевой принцип проектирования, которого все мы решили придерживаться. Именно так мы собирались строить сети в дальнейшем. А потом... ничего существенного не произошло. Большинство из нас их так и не построило. Хотя тезисы Киндервага блестящи, мы с трудом представляем, как подойти к их практической реализации. Именно поэтому спустя десять с лишним лет мы все еще говорим о том, как подступиться к решению этой задачи. Ответу на вопрос «как?» и посвящена оставшаяся часть этой главы.

Нулевое доверие — это философия, а не продукт

Как указывал Киндерваг, нулевое доверие — это не продукт, а философия, стратегия, способ размышления о безопасности, который всегда можно улучшить. Таким образом, это не пункт назначения. Вы никогда не достигнете конечной цели. Никогда не представите своему начальнику отчет со словами: «Ну вот, мы это сделали. Мы обеспечили нулевой уровень доверия». Речь идет скорее о пути.

Стратегия нулевого доверия предполагает, что, даже если человек, устройство или программный компонент (для краткости назовем их *сетевыми сущностями*) работают в нашей цифровой среде на законных основаниях, мы не обязательно доверяем им во всем, что они делают. А раз так, то следует ограничить их полномочия до абсолютного минимума, необходимого для того, чтобы они могли выполнить свою задачу. Другими словами, зачем нам давать повару Луиджи, работающему в кафетерии, разрешение на доступ к базе данных компании, содержащей сведения о слияниях и поглощениях? Нам нужно, чтобы он заказывал продукты на следующий день, а не взаимодействовал с информацией о потенциальных приобретениях компании. Зачем администратору Сноудену предоставили доступ к системам, за которые он не отвечал? И мы должны пристально следить за всеми сетевыми сущностями, чтобы убедиться в том, что они не превышают своих четко определенных полномочий. Кроме того, мы должны постоянно проверять, действительно ли эти сетевые сущности являются теми, за кого себя выдают. Зачем давать Луиджи права администратора на доступ к POS-системе

кафетерия? Он не должен, введя пароль в понедельник, иметь доступ к системе каждый день без дополнительного подтверждения, пока не перезагрузит ее. Мы будем проверять его на каждом шагу, в каждой системе, к которой ему приходится подключаться, и всегда, когда он инициирует какую-либо транзакцию. Как говорит Киндерваг, каждый раз, подтверждая личность Луиджи, мы повышаем свою уверенность в том, что он является именно тем, за кого себя выдает.

Мы стремимся уменьшить поверхность атаки на компоненты своего цифрового пространства, ограничив доступ к рабочим нагрузкам (сервисам и данным) для сетевых сущностей на всех наших островах данных, включая мобильные устройства, дата-центры, SaaS-приложения и облачные среды. Этот подход противоположен тому, который мы привыкли использовать при защите периметра и обеспечении эшелонированной защиты. Эти модели предполагают, что, попав внутрь, вы получаете доступ к большинству содержимого.

Сегодня никакого периметра в традиционном понимании этого слова уже не существует. У нас больше нет единого периметра, так как наши данные и автоматизированные процессы разбросаны по множеству островов. Обеспечить защиту периметра было довольно сложно даже тогда, когда он был только один. Теперь при наличии множества островов данных задача обеспечения нулевого уровня доверия кажется еще более сложной.

Однако стратегия нулевого доверия говорит нам о том, что мы хотим сделать, вне зависимости от того, насколько это трудно. То, как мы это делаем, то есть тактику, мы можем постоянно корректировать, начав с использования средств, уже развернутых в стеке безопасности. Вы можете приобрести дополнительные продукты, способные в этом помочь, однако стратегия нулевого доверия представляет собой образ мышления, который вы можете начать применять тактически, используя уже имеющиеся в вашей сети системы. Да, вы все правильно поняли. Скорее всего, в вашей системе уже есть инструменты, позволяющие существенно продвинуться по пути реализации стратегии нулевого доверия.

Существует миллион вещей, которые можно сделать технически и технологически, чтобы усилить свою защиту, закрыть цифровые двери и окна и гарантировать, что никто из тех, кто бродит по цифровым коридорам наших сетей, не обнаружит приоткрытую дверь и не найдет то, к чему не должен иметь доступа, а если это и произойдет, то не окажет существенного влияния на компанию. Я называю это *базовой реализацией стратегии нулевого доверия*.

Базовая реализация стратегии нулевого доверия

Межсетевые экраны нового поколения появились на рынке в 2007 году, и в настоящее время продукты всех основных производителей межсетевых экранов имеют соответствующий функционал [116]. Если ваша организация относится к категории среднего или крупного бизнеса, то, скорее всего, в ее сетях уже развернуто множество таких средств.

С момента появления первых коммерческих продуктов в начале 1990-х годов брандмауэр стал неотъемлемой частью стандартного стека безопасности. Но когда я говорю о брандмауэре, большинство читателей вспоминают старые межсетевые экраны с контролем состояния, изобретенные примерно в то же время. По сути, они представляли собой причудливые маршрутизаторы, позволяющие блокировать входящий и исходящий трафик на основе портов, протоколов и IP-адресов. Мы устанавливали их на границе между своими цифровыми средами и Интернетом, обеспечивая с их помощью защиту периметра.

Однако межсетевые экраны нового поколения представляют собой нечто совсем иное. Архитекторы безопасности используют их для блокирования сетевого трафика на основе приложений, привязанных к аутентифицированному пользователю, а не на основе IP-адресов. Задумайтесь об этом на секунду.

Вместо того чтобы работать на третьем уровне с портами, протоколами и IP-адресами, этот межсетевой экран работает на седьмом уровне с приложениями. Если вы обеспокоены тем, что ваши сотрудники используют некую соцсеть в течение рабочего дня, можете попытаться заблокировать их доступ к множеству IP-адресов, которые задействует эта соцсеть и которые постоянно меняются, на третьем уровне. Кстати, эта задача практически невыполнима. В качестве альтернативы можете написать правило брандмауэра нового поколения, работающего на седьмом уровне, согласно которому заходить в соцсеть разрешается только сотрудникам отдела маркетинга. После этого можете больше никогда не возвращаться к этому вопросу.

В мире межсетевых экранов нового поколения приложением является все, начиная с использования платформы Salesforce и внутреннего сервера Exchange и заканчивая получением доступа к библиотеке кода, пингованием хоста в вашей сети и чтением газеты Washington Post. Возможность

блокировать приложения на основе групп их пользователей позволяет ИБ-специалистам приступить к реализации стратегии нулевого доверия, не перепроектируя сеть. Возможно, им придется внести в нее некоторые дополнения, но не нужно будет начинать все с нуля.

Логическая и микросегментация

Существует два подхода: логическая сегментация и микросегментация. Логическая сегментация является чуть более простой.

> Мне нравится, когда люди обещают, что все будет легко. Один из моих армейских начальников любил повторять латинскую фразу, которую помещал на всех мемориальных досках: «Nihil facile est». В переводе это означает: «Ничто не дается легко». Этими словами следует руководствоваться и в жизни.

Логическая сегментация предполагает создание правил брандмауэра седьмого уровня для сотрудников основных подразделений компании, таких как отдел маркетинга, юридическая служба, отдел разработки программного обеспечения и т. д. Именно на этом этапе многие защитники сетей и спотыкаются. Поскольку мы создаем правила межсетевого экрана нового поколения, привязывая приложения к аутентифицированным пользователям, возникает соблазн разработать правила для отдельных сотрудников. Например, Кевин может заходить в соцсеть, а Луиджи — нет. В любой крупной организации такой подход быстро превращается в управленческий кошмар. Попытка руководить неизбежными изменениями, связанными с ротацией отдельных сотрудников, быстро приведет к тому, что система рухнет под собственным весом. Вместо этого сосредоточьтесь на 10–15 крупных функциональных отделах. Создание правил, определяющих, какие приложения они могут использовать, а какие — нет, позволит существенно продвинуться по пути реализации стратегии нулевого доверия. Вам по-прежнему придется управлять перемещением сотрудников, однако их права будут не индивидуальными, а основанными на нескольких важных функциях компании.

Более сложным подходом является микросегментация. Он тоже предполагает создание функциональных групп и написание правил для них, но

основное внимание уделяется устройствам, используемым этими функциональными группами. Сотрудники отдела маркетинга могут зайти на сайт корпоративного кафетерия со своего смартфона, чтобы заказать обед, но у этой группы нет доступа к серверу базы данных финансового отдела, содержащей сведения о слияниях и поглощениях. Сложность этого подхода заключается в том, что служба информационной безопасности должна проделать дополнительную работу по созданию инфраструктуры открытых ключей на каждом устройстве в организации, которое может быть опрошено межсетевым экраном нового поколения. Для малых и средних компаний эта задача может оказаться слишком сложной. Однако в крупных организациях подобная система, скорее всего, уже есть. Им достаточно лишь начать использовать ее по максимуму.

Короче говоря, в тех организациях, где уже есть межсетевые экраны нового поколения, сетевые защитники могут использовать их для реализации стратегии нулевого доверия.

Управление уязвимостями: тактика нулевого доверия

В начале 1990-х годов управление уязвимостями в основном сводилось к пониманию эксплойтов и ошибок, обнаруженных в используемом нами программном обеспечении, и последующему их исправлению. В те времена эксплойты использовались не так часто, и армии различных государств, преступники, дети и хактивисты не атаковали нас круглосуточно, как происходит сегодня. Поэтому мы устраняли проблемы тогда, когда было удобно.

В то время большинство из нас использовало ту или иную версию ОС Windows на настольных компьютерах и некую разновидность ОС Unix на серверах. Когда возникали проблемы, мы больше думали о расстановке приоритетов. Мы могли выбирать между установкой нового принтера в лаборатории и выкатыванием исправления для системы Digital UNIX 4.0, которое не позволяет локальным пользователям получать root-привилегии с помощью длинного аргумента командной строки (переполнения буфера).

В 1995 году Дэн Фармер создал первый сканер уязвимостей Security Administrator Tool for Analyzing Networks (SATAN), который использовал сеть для сканирования Unix-хостов в поисках известных уязвимостей [72].

Однако он требовал очень много сетевых и процессорных ресурсов и при неосторожном обращении мог вывести сеть из строя.

Тогда у нас даже не было общепринятого языка для обсуждения уязвимостей и эксплойтов с коллегами и экспертами. Согласно Tripwire, в то время каждый производитель программного обеспечения использовал собственный метод отслеживания уязвимостей в своих продуктах [243]. Специалисты по безопасности не могли выяснить, является ли уязвимость у производителя А той же самой, что и у производителя Б, или это две разные проблемы. Нам приходилось действовать в одиночку. Назовем этот первый этап управления уязвимостями (начало 1990-х годов) фазой растерянности.

Ситуация начала меняться в 1999 году, когда сотрудники организации MITRE Дэвид Манн и Стивен Кристи опубликовали технический документ *Towards a Common Enumeration of Vulnerabilities* [151]. В том же году отдел компьютерной безопасности NIST создал инструмент интернет-категоризации атак (Internet-Categorization of Attacks Toolkit, ICAT) — первый интегрированный список уязвимостей и эксплойтов [284]. По иронии судьбы, попытка уменьшить сложность и путаницу привела к появлению еще большего количества аббревиатур: NIST, CVE, ICAT, NVD, CVSS, SCAP и E-I-E-I-O.

> Признаюсь, аббревиатуру E-I-E-I-O я выдумал, но мне кажется, что после прочтения этого списка аббревиатур вы можете захотеть пропеть «E-I-E-I-O» на мотив классической песенки «У старого Макдональда была ферма».

Манн и Кристи предложили создать список известных уязвимостей CVE (Common Vulnerabilities and Exposures), которым могло бы пользоваться все сообщество, и эта идея быстро получила распространение. Первый опубликованный ими список CVE содержал сведения о 321 уязвимости, отобранной после тщательного анализа и изучения дубликатов. К 2002 году список CVE содержал уже более 2000 уязвимостей программного обеспечения, и организация NIST рекомендовала правительству США использовать только ПО с идентификаторами CVE.

К 2005 году инструмент ICAT превратился в Национальную базу данных уязвимостей (National Vulnerability Database, NVD), предназначенную для дополнения списка CVE оценками риска и воздействия с использованием

Общей системы оценки уязвимостей (Common Vulnerability Scoring System, CVSS) и предоставления других сведений, таких как информация о патчах, затронутых продуктах и соответствии стандарту SCAP (Security Content Automation Protocol) [265]. Сканер SCAP сравнивает конфигурацию и/или версию патчей целевого компьютера или приложения с базовым уровнем, указанным в базе данных SCAP. В настоящее время спонсорами NVD являются организации CISA и NIST.

Я знаю, что все это кажется сложным, но это была лишь вторая фаза. Назовем ее легкой фазой (1999–2005), поскольку по сравнению со следующей она была относительно простой. Ее простота объясняется тем, что в то время немногие использовали личные ноутбуки и мобильные устройства для работы, облачные технологии еще не изменили индустрию, так как самого понятия «облако» не существовало, а управление уязвимостями распространялось лишь на устройства, находящиеся за периметром.

Когда в 2005 году компания Concur презентовала первый SaaS-сервис [304], а в 2006-м компания Amazon представила AWS [276, 160], ситуация начала меняться. Теперь мы имели дело с информацией, хранящейся на островах данных, а не в традиционных дата-центрах, находящихся за периметром. Примерно в 2014 году организации начали разрешать своим сотрудникам использовать для работы личные устройства — телефоны, планшеты и ноутбуки. Но это не точная дата. Некоторые организации стали делать это раньше, чем другие. Правительства пришли к этому гораздо позже, а часть из них до сих пор этого не сделала. Однако после перехода со второго этапа на третий, который мы назовем фазой сложности (с 2005 года по сегодняшний день), сложность управления уязвимостями многократно возросла. Например, в 2021 году организация NIST опубликовала список, содержащий 18 378 вновь обнаруженных уязвимостей, причем этот показатель бил рекорд пятый год подряд [93]. Если учесть, что эти уязвимости разбросаны по множеству островов данных, то неудивительно, что многие директора по информационной безопасности, будучи молодыми людьми, выглядят на 107 лет. Это сильно их старит.

Как обычно бывает в сфере безопасности, из-за роста сложности сетевые защитники уже не могли управлять уязвимостями организационного ПО с помощью электронных таблиц. Эта задача стала слишком трудной и ресурсоемкой, а большинство организаций постоянно отстают в этом вопросе. Их можно сравнить с малярами, которые работают на мосту «Золотые ворота» в Сан-Франциско. Они красят мост с одного конца до другого и тут же возвращаются и начинают все сначала. Эта работа никогда не заканчивается.

Управление уязвимостями как разведывательная задача

Согласно книге Эндрю Магнуссона *Practical Vulnerability Management*, вошедшей в Зал славы Cybersecurity Canon, управление уязвимостями не ограничивается управлением патчами. Управление патчами в организации — важная задача, но это еще не все. На момент написания данной книги Агентство по кибербезопасности и защите инфраструктуры США (CISA) зафиксировало использование только 812 из 18 378 уязвимостей, обнаруженных в 2021 году [282]. По данным проекта Project Zero компании Google, в 2021-м было зарегистрировано 58 эксплойтов нулевого дня, что более чем в два раза превысило аналогичный показатель предыдущего года, и все же 58 — это немного по сравнению с 18 000 обнаруженных на тот момент уязвимостей [298].

Много лет назад один продавец поделился со мной своей аналогией, помогающей понять разницу между уязвимостями, эксплойтами и вредоносными программами, которая показалась мне блестящей. Он предложил рассмотреть свой дом с точки зрения его защиты от грабителей. У вас есть некие стандартные средства защиты: двери, которые запираются, и окна, которые защелкиваются. Но в этой системе могут быть уязвимые места. Например, вы установили дешевый замок на входную дверь, оконной защелкой можно легко манипулировать снаружи, а в кухонной двери, ведущей на задний двор, предусмотрен лаз для собаки. Пока ничего страшного не произошло, но это потенциальные пути, которыми взломщики могут проникнуть в ваш дом. То же самое можно сказать и о программном обеспечении. Когда вы слышите об уязвимости ПО, это означает, что кто-то обнаружил потенциальный недостаток в коде, которым может воспользоваться хакер. Если грабители заявляются в ваш дом вечером, пока вас нет, и взламывают замок входной двери, манипулируют оконной защелкой или пролезают через собачий лаз, это можно уподобить эксплойту. Взломщики воспользовались обнаруженной уязвимостью в системе, чтобы получить доступ в ваш дом. То же самое бывает и с кодом. Хакеры пишут собственный код (эксплойт), чтобы воспользоваться обнаруженной программной уязвимостью, позволяющей получить доступ к компьютеру. В качестве примера можно привести печально известный эксплойт EternalBlue, разра-

ботанный АНБ, похищенный и опубликованный группой хактивистов Shadow Brokers, использованный северокорейцами в рамках атаки WannaCry и российскими хакерами — в ходе атаки NotPetya. Попав в дом, грабители забирают столовое серебро из кухни, ювелирные украшения с тумбочки и уходят через входную дверь. Это сродни вредоносному ПО. Как только хакеры получают доступ к вашему компьютеру, код, который они применяют для автоматизации последовательности этапов атаки в рамках kill chain (см. главу 4), становится вредоносным ПО.

Если смотреть с этой точки зрения, то управление патчами ради него самого не кажется правильным способом распределения ресурсов. Другими словами, внесение всех возможных исправлений — это не самая лучшая стратегия. Подход к решению этой задачи необходимо тщательно продумать. Существует целый ряд действий, которые требуется выполнить до того, как мы сможем хотя бы задуматься о применении патчей.

- Непрерывно мониторьте все программные активы, работающие в сети, в плане контроля версий, вложенных библиотек для пакетов с открытым исходным кодом, текущей конфигурации (кто и что может получить доступ к активу, к чему может получить доступ сам актив), истории обращений к активу, а также вероятности того, что на него могут воздействовать посредством вновь обнаруженных уязвимостей и эксплойтов.
- Опираясь на стратегию нулевого доверия, регулярно проверяйте, чтобы все программные активы имели доступ только к тому, что им абсолютно необходимо для выполнения своей работы.
- Отдавайте приоритет наиболее существенным программным активам, то есть ПО, которое может разрушить ваш бизнес, если хотя бы на секунду перестанет функционировать или приведет к утечке данных клиентов.

При выявлении новых уязвимостей и эксплойтов сделайте следующее.

- Определите, подвергается ли ваша организация соответствующей опасности.
- Оцените вероятность того, что какой-нибудь злоумышленник воспользуется этой уязвимостью.
- Оцените вероятность того, что в случае такой атаки ущерб будет существенным.

- Выясните, существует ли исправление или другой обходной путь, позволяющий устранить проблему.
- Решите, какие действия необходимо предпринять для снижения риска (в зависимости от вашего прогноза это может быть множество действий или ни одного).

После выполнения перечисленных действий необходимо реализовать принятое решение, то есть план мероприятий по снижению рисков. Каждый из приведенных пунктов предполагает получение критически важной информации, необходимой для принятия решения в отношении вновь обнаруженной уязвимости или эксплойта. Со временем собранные разведданные позволят вам добиться определенных успехов в реализации программы управления уязвимостями.

Я специально упомянул о сборе разведданных. Более подробно о киберразведке расскажу в главе 4, однако это идеальная задача для вашей разведгруппы вне зависимости от того, идет ли речь о специальной команде, двух парнях и собаке в чулане, работающих на полставки, подрядчике, выполняющем эту работу за вас, или о чем-то еще. Данная задача является частью жизненного цикла разведки (см. главу 4).

Однако для стартапов, малых и даже некоторых предприятий среднего размера эта задача может оказаться слишком сложной. Таким организациям может не хватать средств даже на поддержание работоспособности принтеров и кофейных аппаратов, не говоря уже об управлении патчами. Более актуальными для них могут оказаться другие стратегии нулевого доверия (см. далее). Тем не менее по мере роста организации и появления у нее дополнительных ресурсов автоматизация крупных фрагментов программы управления уязвимостями может стать для нее выгодной в долгосрочной перспективе (см. главу 7).

Нулевое доверие — это ключевая стратегия для снижения вероятности существенного ущерба. С тактической точки зрения существует множество способов ее реализации, большая часть которых связана с идентификацией и авторизацией. Косвенной тактикой является управление уязвимостями. У большинства из нас оно не ассоциируется с нулевым доверием, но в моем понимании это именно так. Управление уязвимостями — это не некий независимый набор действий, выполнение которых предписано всем сетевым защитникам. Я не рассматриваю его в качестве стратегии, так как для этого оно недостаточно атомарно. Тем не менее оно представляет собой важную тактику, основанную на первичном принципе кибербезопасности и способствующую реализации принципа нулевого доверия.

Использование спецификаций программного обеспечения: тактика нулевого доверия

Прежде чем объяснить, что такое спецификация программного обеспечения (Software Bill of Materials, SBOM), расскажу о том, почему она необходима. В случае со стратегией нулевого доверия ярким примером была история Сноудена, в случае с SBOM весьма показательной является история Log4j.

Модуль Log4j появился в 1999 году в качестве фреймворка для ведения журналов. В июле 2014-го организация Apache Software Foundation выпустила модуль Log4j версии 1. В следующем году комитет по управлению проектом Apache Logging Services выпустил ему на замену модуль Log4j 2 [191]. Шесть лет спустя, в ноябре 2021-го, сотрудник службы безопасности Alibaba Cloud Чэнь Чжао Чжин сообщил в Apache Software Foundation об уязвимости, обнаруженной в этом модуле [94]. Девятого декабря организация Apache объявила об эксплуатации данной уязвимости и назвала ее Log4shell. На следующий день организация NIST внесла эту уязвимость в Национальную базу данных уязвимостей (NVD), классифицировав ее как критическую [103].

Причина такой классификации заключается в повсеместной распространенности модуля Log4j и простоте кода для эксплуатации уязвимости Log4shell. Повсеместное распространение этого модуля было обусловлено тем, что код кросс-платформенного веб-сервера Apache — это открытое и самое популярное веб-серверное ПО в мире. Если вы используете какие-то веб-сервисы, то, скорее всего, задействуете Apache и модуль Log4j. Простота эксплуатации уязвимости была обусловлена тем, что в то время любой неаутентифицированный пользователь сервиса Log4j мог получить контроль над сервером, отправив 12-символьный фрагмент кода.

На момент написания этой книги уязвимость Log4shell относилась к третьему по значимости типу уязвимостей программного обеспечения из списка OWASP Top 10 (справочного документа, описывающего наиболее критичные риски безопасности веб-приложений) — в данном случае к инъекциям [285]. Это значит, что неисправленный модуль Log4j не изолирует свой код от данных. Он интерпретирует сообщения журнала (данные) как инструкции (код). Когда хакеры посылают модулю URL-адрес, сервис захватывает его, извлекает хранящиеся по этому адресу данные и запускает исполняемую полезную нагрузку с полными привилегиями основной программы Log4j.

И не стоит думать, что ситуация с Log4j уникальна. Речь идет о крошечном программном модуле в целой галактике повторно используемого ПО с открытым исходным кодом. По словам Джона Дугласа из компании Microsoft, в ноябре 2021 года доля публичных репозиториев программного обеспечения, использующих открытое ПО, составляла более 80 % [70]. Согласно отчету компании Synopsys за 2022 год 97 % коммерческого ПО содержит компоненты с открытым исходным кодом. При этом основная часть этой кодовой базы (78 из 97 %) приходится на открытое ПО [22]. По словам Дугласа, это означает, что «тысячи посторонних людей могут вносить изменения непосредственно в ваш производственный код. Таким образом, через цепочку поставок ПО на ваш продукт могут влиять непропатченные уязвимости, невинные ошибки или даже злонамеренные атаки». Большинство ИБ-специалистов не имеют ни малейшего представления о том, какие библиотеки кода использует их организация и какие библиотеки вложили в свое открытое программное обеспечение его разработчики.

Сходство автомобильного производства с методологией DevOps

Авторы романа «Проект “Феникс”» [323], посвященного методологии DevOps и попавшего в Зал славы Cybersecurity Canon, говорят о том, что современный процесс разработки программного обеспечения должен быть похож на знаменитую производственную систему TPS компании Toyota, ставшую результатом переосмысления процесса производства автомобилей после Второй мировой войны. Это замечательная метафора, но у меня есть одна претензия к ней: хотя разработку программного обеспечения можно сравнить с производством автомобилей на макроуровне, на микроуровне это сравнение перестает работать. Я имею в виду то, что аналогом производственной системы Toyota в сфере разработки ПО является методология DevOps и я всячески ратую за принятие ее философии (см. главу 7). Она позволяет отбросить прежний каскадный метод разработки программного обеспечения, при котором новые рабочие фрагменты кода выпускались раз в два года, а то и реже, в пользу внедрения методологии Agile, позволяющей развертывать изменения по нескольку раз в день. Это макроуровень, и на нем данная метафора работает.

Однако на микроуровне, то есть на уровне повседневных операций, метафора TPS перестает работать. Каждая деталь (имеются в виду аппаратные, а не программные компоненты) поставляется одним и тем же надежным

подрядчиком или изготавливается самостоятельно. После сборки эти детали практически не меняются. Конечно, бывают исключения, но обычно это так. Суть в том, что каждый раз, когда вы делаете заказ, эти детали оборудования поставляются из одного и того же места. Вы более или менее знаете своих поставщиков и особенности их работы. Но с разработкой программного обеспечения дело обстоит иначе.

Коммерческое ПО — это ПО с открытым исходным кодом

Почти все коммерческое программное обеспечение более чем на три четверти состоит из компонентов с открытым исходным кодом. Это означает, что в отличие от деталей оборудования, подпитывающих производственную систему Toyota, мы не знаем, откуда берутся наши программные компоненты, кто их создал и продолжают ли разработчики их поддерживать. И эта проблема даже более коварна, чем кажется на первый взгляд. Если большинство разработчиков программного обеспечения используют открытое ПО, то велика вероятность, что создатель одного из таких компонентов задействовал для его создания другой модуль с открытым исходным кодом. Вся эта идея развивается по экспоненциальной спирали, подобно фракталу. И это еще не говоря о том, что производителям оборудования не приходится бороться с армиями злоумышленников, которые регулярно находят способы применять произведенные ими компоненты в криминальных, шпионских и прочих противоправных целях. Использование ПО с открытым исходным кодом дает этим группам злоумышленников широкие возможности для атак в рамках того, что мы называем *цепочкой поставок программного обеспечения*. DevOps-специалисты вынуждены работать на совершенно ином уровне, чем производители автомобилей.

Цепочка поставок ПО и первичные принципы кибербезопасности

За последние 20 лет мы были свидетелями нескольких атак на цепочки поставок ПО, однако в период с 2010 по 2020 год злоумышленники заново открыли для себя эту стратегию и удвоили свои усилия в этом направлении. В период с 2015 по 2020 год весьма мощным атакам подверглись несколько сторонних поставщиков, включая MEDoc, Solarwinds, Asus, CCleaner,

Kaseya, Accellion и Codecov [185, 266]. Подобные атаки более хитроумны по сравнению с прямым нападением на наши средства киберзащиты, которые мы разработали, развернули и на которые потратили значительные ресурсы. При атаке на цепочки поставок зрелость этих программ не имеет значения. Первый этап последовательности атаки хакеры реализуют через широко открытую заднюю дверь в средствах защиты наших островов данных, подпертую стулом для еще более легкого проникновения. По сути, мы устанавливаем вредоносное ПО за злоумышленников. Наши киберпротивники знают об этом и, как говорит Дмитрий Рейдман (технический директор компании Cybeats), «охотятся за уязвимыми компонентами цепочки поставок открытого программного обеспечения, чтобы получить возможность заразить троянами другие коммерческие продукты и ПО с открытым исходным кодом» [181]. Однако, когда возникают проблемы, как в случае с Log4j, 80 % работы по их устранению (помимо внесения исправлений) сводится к поиску всех запущенных экземпляров соответствующей программы.

Удивительно то, что мы как сообщество, рассматривая нулевое доверие как одну из стратегий, базирующихся на первичных принципах кибербезопасности, до сих пор не решили вопрос защиты цепочек поставок. Мы изо всех сил стараемся идентифицировать всех своих сотрудников, подрядчиков и устройства, а затем предоставить им доступ к определенным рабочим нагрузкам. При этом практически не следим за новым программным обеспечением, которое используется для обновления наших производственных систем. Даже руководители служб кибербезопасности, которые следят за данной ситуацией, используют для этого ручные, самодельные и недостаточно полные инструментальные средства.

Одним из решений этой проблемы является использование спецификации программного обеспечения (SBOM) — формальной записи, содержащей сведения о различных компонентах, применяемых при создании ПО, и взаимосвязях между ними в цепочке поставок. SBOM представляют собой списки вложенных друг в друга программных компонентов, предназначенные для обеспечения прозрачности цепочки поставок. Таким образом, если моя компания использует приложение Fortnite, то в SBOM будут перечислены все его компоненты: весь оригинальный код, написанный разработчиками компании Epic (владеющей Fortnite), все компоненты с открытым исходным кодом, которые они использовали, а также все подкомпоненты, созданные другими разработчиками открытого ПО.

По мнению Дмитрия, при рассмотрении этого вопроса целесообразно отличать *производителей* SBOM (вышестоящие поставщики, ориентированные на свои продукты) от *потребителей* SBOM (нижестоящие поставщики, ориентированные на продукты вышестоящего поставщика). И те и другие будут использовать инструменты, соответствующие формальной спецификации стандарта. К сожалению, на момент написания этой книги стандартной SBOM-платформы еще не существует. Зато у нас есть множество разрабатываемых стандартов и требований к инструментам, предназначенных для снижения рисков, связанных с атаками на цепочки поставок ПО. Несмотря на то что некоторые поставщики уже начинают продавать SBOM-платформы, сама идея SBOM в данный момент по-прежнему находится на уровне концепции.

Актуальные стандарты SBOM

В августе 2021 года стандарт SPDX (Software Package Data Exchange), также известный как ISO/IEC 5962 и разработанный по инициативе Linux Foundation в 2010-м, стал международным открытым стандартом безопасности, соблюдения лицензионных требований и других параметров цепочки поставок ПО [250]. Другими словами, он превратился в официальный орган по стандартизации SBOM. Несмотря на то что стандарт SPDX получил международное признание совсем недавно, компании Intel, Microsoft, Sony и VMware уже используют его для передачи информации SBOM. Однако SPDX не стал сенсацией в одночасье. Это результат десятилетнего сотрудничества поставщиков в области анализа состава программного обеспечения (Software Composition Analysis, SCA), разрабатывающих инструменты для оценки открытого ПО, библиотек кода и контейнеров, дающих единое представление о рисках и мерах по их устранению, а также предлагающих стратегии для поддержания такого ПО в актуальном состоянии [117, 230, 252].

В 2015 году Международная организация по стандартизации (ISO) выпустила стандарт ISO/IEC 19770-2 для идентификационных меток программного обеспечения (SWID) [250]. Этот стандарт предполагает создание шаблона в формате XML для идентификации и описания компонентов программного обеспечения и соответствующих патчей. Затем в 2017 году сообщество Open Web Application Security Project Foundation (OWASP) разработало CycloneDX — облегченный стандарт, объединяющий функции SPDX и SWID [261].

Директива президента

Как уже было сказано, сейчас SBOM представляет собой набор еще не вполне готовых стандартов, однако сообщество уже близко к тому, чтобы получить нечто пригодное для использования. Концепция SBOM получила большой толчок к развитию в 2021 году, когда президент США Джо Байден подписал указ об усилении кибербезопасности (EO 14028) [247], согласно которому все агентства федеральной гражданской исполнительной власти (FCEB) и ключевые игроки должны соответствовать определенным требованиям к обеспечению кибербезопасности, включающим разработку SBOM-программы, или превосходить их.

Доктор Джорджиана Ши, один из мировых экспертов в области внедрения SBOM, отслеживает работу FCEB, направленную на выполнение президентской директивы, и утверждает, что в целом правительство укладывается в отведенные сроки. Однако при этом она поясняет: «Эти требования не задумывались как оперативно исполняемые. Таким образом, выполнить фактические требования было легко. Директива президента содержала два конкретных требования относительно SBOM: определить минимальные элементы и предоставить руководство по внедрению SBOM» [107, 201]. Правительство выполнило их оба. Таким образом, все FCEB находятся в процессе реализации директивы, однако впереди еще много работы.

Три инструмента для снижения рисков, связанных с цепочкой поставок

SBOM — это не единственный необходимый нам инструмент. Помимо возможности получить представление обо всех программных компонентах, было бы неплохо иметь авторитетный источник сведений, отвечающий за автоматическое обнаружение в них уязвимостей и эксплойтов. Такой источник стал бы модернизированной версией общей системы оценки уязвимостей (CVSS). Вместо того чтобы читать отчеты об уязвимостях ПО и пытаться определить, применимы ли они к данным в моей спецификации SBOM, я мог бы использовать машиночитаемую версию CVSS, позволяющую другой системе — системе управления активами — просматривать информацию в моей спецификации SBOM и сравнивать ее с собственным содержимым. Пока у нас нет такой возможности.

Однако у нас есть стандартный способ формулирования информации об уязвимостях в компонентном ПО, который называется VEX-документом (Vulnerability Exploitability Exchange) [128, 135, 136]. По словам Дмитрия, VEX является результатом деятельности рабочей группы NTIA, создавшей стандарт SBOM, и управляется CISA. NTIA (National Telecommunications and Information Administration) — это Национальная администрация США по телекоммуникациям и информации, чья рабочая группа создала данный формат для хранения сведений об уязвимостях и эксплойтах в программных компонентах. Консорциум OASIS опубликовал проект стандарта CSAF (Common Security Advisory Framework) для описания VEX-документа в машиночитаемом формате, аналогичном CycloneDX. В настоящее время и CSAF, и CycloneDX поддерживают инкапсуляцию VEX-информации в своей объектной структуре.

А вот чем VEX не является, так это системой, хранящей эту информацию неким автоматизированным способом. Таким образом, если мы хотим снизить риск, связанный с цепочками поставок ПО, нам необходимы система SBOM и система управления активами, которая сверяет информацию SBOM с содержимым системы CVSS, хранящей данные в формате VEX.

Светлое будущее SBOM

Справедливости ради следует отметить, что концепция SBOM существует уже много лет, но стимулов для ее массового внедрения пока не было. Некоторые стандарты в этой области разрабатывались добровольцами под эгидой NTIA, Linux Foundation, OWASP и других организаций. В последние несколько лет, когда участились атаки на цепочки поставок ПО, ряд которых имел серьезные последствия (Solarwinds, MeDoc и Accellion), кто-то убедил президента Байдена включить требования, касающиеся использования SBOM, в президентскую директиву. И это хорошая новость.

Прогресс в разработке SBOM есть. В частности, этому способствует высокая вероятность того, что в определенный момент правительство США обяжет всех поставщиков программного обеспечения предоставлять информацию SBOM в рамках своего контракта. Я считаю, что это подвигнет всех остальных представителей отрасли последовать их примеру. Однако, по моему мнению, переход SBOM из разряда концепций в разряд реальных вещей займет еще не менее пяти лет. Дмитрий с этим не согласен и настроен более оптимистично. Он говорит о том, что наблюдает активную работу

организаций «от стартапов до компаний из списка Fortune 500, большинство из которых уже нашли способ генерации SBOM». По его словам, они оценили потенциальную отдачу от инвестиций в управление этими спецификациями.

Управление идентификацией: тактика нулевого доверия

Концепция идентичности чрезвычайно интересна. Какие из наших особенностей позволяют другим людям понять, что мы собой представляем? Имя, адрес, профессия, хакерский псевдоним, принадлежность к политической партии, участие в волонтерских организациях, предпочтительные варианты отдыха, любимые персонажи игры Dungeons & Dragons и многие другие виды деятельности и вещи, которые мы поддерживаем, составляют нашу идентичность. И это не считая различных масок. Например, у меня есть маски для работы, семьи, общения с соседями и участия в играх. Каждая из них предназначена для взаимодействия с разными сообществами, в которых я состою. Например, я, скорее всего, не захочу демонстрировать свою игровую маску в виде хаотично-нейтрального тифлингского мага 20-го уровня по имени Абигейл генеральному директору своей компании, так как он может этого не понять.

Однако в мире транзакций нам необходимо привязать к своей личности что-то, что позволило бы подтвердить ее подлинность. Благодаря этому принимающая сторона сделки может убедиться в том, что мы имеем право в ней участвовать. Например, вы можете зайти в Twitter и рассказать всему миру о том, как сильно любите конкретную бейсбольную команду. Однако любовь к бейсболу не позволит вам получить деньги в банкомате. Именно поэтому мы ищем способы доказать своим партнерам по сделкам, что являемся теми, за кого себя выдаем, а не какими-то ботами с искусственным интеллектом.

В 1850-х годах в Великобритании начали использовать свидетельства о рождении для подтверждения гражданства [177]. Например, люди могли предъявить свидетельство о рождении в банке для получения кредита. В 1903 году Миссури и Массачусетс стали первыми штатами США, где для управления автомобилем требовалось водительское удостоверение [167]. После Первой мировой войны Лига наций выступила за использование паспортов для международных поездок. В 1935 году Конгресс США при-

нял закон о социальном страховании, в соответствии с которым гражданам присваивались уникальные номера [290]. Номера социального страхования превратились в атрибут, позволяющий однозначно отличить Джона Смита, живущего в Альбукерке, от Джона Смита из Фресно.

В 1960-х годах, когда компьютеры стали важным инструментом деятельности крупного бизнеса и правительственных структур, великий Фернандо Корбато, один из отцов-основателей сферы компьютерных вычислений, предложил идею использования паролей для получения доступа к компьютерным системам [157]. Сам того не подозревая, он предоставил киберзлоумышленникам бесконечный вектор атаки для взлома этих систем. Справедливости ради следует отметить, что система парольной аутентификации начала рушиться лишь в середине 1990-х годов, когда Интернет стал использоваться для проведения онлайн-транзакций. Из-за роста масштабов Всемирной паутины пароли просто перестали справляться со своей задачей. Удивительно, но большинство людей до сих пор используют пароли для аутентификации, хотя этой технологии уже более 50 лет.

Забавный факт: Корбато хранил пароли в текстовом файле, что, вероятно, спровоцировало один из первых в истории компьютерных взломов. Алан Шерр, работавший в то время над докторской диссертацией, обнаружил этот незащищенный текстовый файл и украл пароли других студентов, чтобы получить возможность подольше поработать за компьютером. Ну как можно не любить этих ботаников из Массачусетского технологического института?

В 1993 году Тим Хоус, Стив Килле и Венджик Йонг изобрели протокол LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам) [277]. По словам Джульет Кемп из ServerWatch, LDAP позволяет администраторам организовывать информацию в сети и предоставлять пользователям доступ к ней. Хоус и его команда разработали его для упрощения аутентификации в распределенной сети TCP/IP [130]. К 2000 году компания Microsoft включила этот протокол в свою базовую систему аутентификации Active Directory, которая для поиска пользователей использует LDAP, а для их аутентификации — протокол Kerberos [37], разработанный в 1988 году в Массачусетском технологическом институте в рамках проекта Athena.

В 2002 году Конгресс США принял знаменитый закон Сарбейнса — Оксли, который, помимо прочего, предусматривал ответственность компаний за некачественное управление доступом. К началу 2006 года появились первые управляемые сервисы для управления идентификацией, а к началу 2010 года — первые SaaS-сервисы для управления идентификацией [173]. В 2014 году организации начали распределять свою информацию по множеству островов данных, среди которых были традиционные периметры, частные дата-центры, персональные устройства, SaaS-провайдеры и поставщики облачных услуг (IaaS и PaaS). Стало ясно, что локальные решения для идентификации уходят в прошлое, уступая место соответствующим SaaS-сервисам.

Одна из проблем цифровой идентификации и аутентификации заключается в том, что нынешние системы ориентированы на конкретные сайты. Пользователям приходится предоставлять учетные данные множеству цифровых платформ, таких как Amazon, Netflix, eBay и т. д., которые по большей части не взаимодействуют друг с другом. Технология единого входа, о которой я расскажу в разделе «Единый вход: тактика нулевого доверия», близка к решению этой проблемы, так как позволяет пользователю авторизоваться сразу в нескольких приложениях с помощью одного набора учетных данных.

Если считать, что в 1960-х годах Фернандо Корбато создал бета-версию системы идентификации и аутентификации, то, согласно Дику Хардту, активному сторонникy идеи сетевой идентичности, к середине 2000-х годов мы наконец получили версию 1.0 в виде наших сайтоцентрированных систем. Разработанная спустя некоторое время концепция федерации удостоверений, вероятно, способствовала появлению системы идентификации и аутентификации версии 1.5 [140].

По словам Хелен Паттон, бывшего директора по информационной безопасности Университета штата Огайо, концепция федерации удостоверений — это идея, согласно которой если два партнера друг другу доверяют, то они доверяют и пользователям друг друга. Если Хелен отправится в университетский городок своего доверенного партнера, скажем Мичиганского университета, то она сможет без каких-либо координационных проблем войти в сеть Wi-Fi на территории этого учебного заведения. С моей точки зрения, федерация удостоверений представляет собой ассоциативное свойство доверия. Если Мичиганский университет доверяет Университету штата Огайо, а Университет штата Огайо доверяет Хелен, то Мичиганский университет тоже доверяет Хелен. Это не означает, что Мичиганский

университет разрешает Хелен совершать множество действий. Для этого ей необходимо было бы пройти авторизацию. Однако федерация удостоверений упрощает процесс аутентификации в случае разовых партнерских взаимодействий [106].

Это хорошее, но не идеальное решение. Разовые партнерские взаимодействия между Университетом штата Огайо и Университетом штата Мичиган не очень хорошо масштабируются. Опять же механизмы единого входа таких компаний, как Google, Apple, и ряда других предусматривают масштабирование, но при этом требуют, чтобы партнеры по сделке доверяли третьей стороне как истинному источнику учетных данных для одной или обеих сторон сделки.

Нам необходима версия системы идентификации и аутентификации 2.0, чтобы перейти от сайтоцентрированных решений к решениям, ориентированным на пользователя. В этом случае я сам становлюсь брокером. Когда я вхожу в систему Netflix или Amazon, эти компании запрашивают учетные данные, хранящиеся на моем мобильном устройстве. Учетные данные принадлежат мне, а не компании Amazon. То есть она приходит ко мне, а не наоборот.

В начале 2000-х годов появились две технологии, приближающие нас к этой цели: SAML и OpenID/OAuth. SAML (Security Assertion Markup Language — язык разметки декларации безопасности) представляет собой тяжеловесный вариант языка XML, позволяющий одному компьютеру выполнять аутентификацию и авторизацию от имени других компьютеров. OpenID/OAuth представляет собой пару конкурирующих с SAML технологий, имеющих драматическую запутанную историю [212].

Не волнуйтесь, если все это кажется непонятным. Так оно и есть. Например, OAuth означает открытую аутентификацию (open authentication). Самое интересное, что протокол OAuth ничего не аутентифицирует. Он просто разрешает одной машине войти в систему другой машины от имени человека. За аутентификацию отвечает технология OpenID. К 2014 году ситуация более или менее прояснилась. В настоящее время, по данным журнала CSO Magazine, большинство сетевых операторов используют протокол SAML для корпоративных приложений и технологию OAuth для ситуаций в открытом Интернете [36, 38].

На данный момент благодаря технологиям SAML и OpenID/OAuth мы, вероятно, имеем версию системы идентификации и аутентификации 1.7, которая превосходит версию 1.5, полученную благодаря концепции федерации

удостоверений, но все еще не дотягивает до версии 2.0. Чтобы перейти к версии 2.0, то есть к решению, ориентированному на пользователя, я бы предложил начать с чтения статьи Кима Камерона *The Laws of Identity*, написанной в 2005 году [40]. В ней он перечисляет семь характеристик, которыми должна обладать любая современная система идентификации.

1. *Контроль и согласие пользователя* — пользователь отвечает за все.
2. *Минимальное раскрытие информации для ограниченного использования* — нулевое доверие к обмениваемым данным.
3. *Обоснованное участие сторон* — нулевое доверие к обменивающимся данными сторонам.
4. *Направленная идентификация* — однонаправленная и направленная во все стороны.
5. *Плюрализм операторов и технологий* — возможность работы с несколькими технологиями и несколькими сущностями.
6. *Интеграция человека* — система должна способствовать безопасному человеческому взаимодействию.
7. *Согласованный опыт в разных контекстах* — как говорил великий главный редактор Marvel Comics Стэн Ли, «довольно слов».

Можно сказать, что концепция идентичности имеет наибольшую важность для будущего транзакционного интернет-бизнеса. Мы можем реализовать любые стратегии, базирующиеся на первичном принципе кибербезопасности, однако возможность точно установить, что хаотично-нейтральный тифлингский маг 20-го уровня Эбигейл — это Рик Ховард, а не координатор какой-нибудь российской операции влияния из Новосибирска, является ключом ко всему. Без этого мы не сможем быть уверены ни в одной из будущих систем, например предназначенных для проведения онлайн-голосования, переписи населения или осуществления любых других взаимодействий с нашими правительствами, коммерческими предприятиями или научными учреждениями.

Вы будете правы, если скажете, что описанная мной версия системы идентификации и аутентификации 1.7 работает довольно неплохо. И это действительно так. Я могу без особых проблем смотреть Netflix, покупать книги на Amazon и заказывать гамбургеры в местном ресторане Five Guys. Однако эти сайтоцентрированные системы были разработаны коммерческими фирмами для получения прибыли. Я не имею ничего против этого, но, думаю, ИБ-сообществу стоило бы преследовать более высокие цели. Возможно, нам

следует разрабатывать системы идентификации и аутентификации таким образом, чтобы пользователи сами контролировали свои учетные данные.

При этом если речь идет о корпоративной безопасности, то стратегию нулевого доверия не удастся реализовать до тех пор, пока не будет создана надежная система управления идентификацией. Это просто невозможно. Если вам точно не известны все люди, подключающиеся к вашей сети, все аппаратные устройства, запрашивающие доступ к ресурсам, и все программные компоненты, начиная от собственных разработок и заканчивая коммерческими инструментами и программными модулями с открытым исходным кодом, то вы не сможете ограничить доступ на основе принципа минимальной необходимой осведомленности. Важность этого обусловлена тем, как именно большинство киберпротивников проникают в сети своих жертв и маневрируют в них.

В главе 4 я подробно опишу концепцию kill chain, но если вкратце, то, скомпрометировав нулевую жертву, хакеры пытаются передвигаться по сети в поисках данных, которые хотят украсть или уничтожить. При этом они стремятся повысить свои привилегии там, где это возможно. В качестве примера можно привести атаку хакерской группировки Cozy Bear на продукт SolarWinds Orion, произошедшую в конце 2020 года [19].

Сначала хакеры из Cozy Bear взломали сеть SolarWinds и внедрили бэкдор в пакет обновления для программы Orion. После того как пользователи Orion установили этот пакет, команда Cozy Bear получила возможность удаленного входа в систему. С этого исходного плацдарма они двинулись дальше по сети жертвы в поисках учетных записей администраторов. По данным Центра реагирования на угрозы компании Microsoft, хакеры из Cozy Bear воспользовались системой SAML, о которой мы говорили ранее: «Попав в сеть, злоумышленник использует полномочия администратора, полученные в результате компрометации локальной сети, для получения доступа к учетной записи глобального администратора организации и/или доверенному сертификату, используемому для подписи токенов SAML. Это позволяет злоумышленнику подделать SAML-токены, выдав себя за любого из существующих в организации пользователей, включая высокопривилегированных».

Атаки Cozy Bear на платформу SolarWinds Orion подчеркивают один ключевой момент. В нынешнюю эпоху инфраструктуры как кода для запуска определенных легитимных DevOps-механизмов в коде, например создания SAML-токенов, должны требоваться дополнительные разрешения. Другими словами, мы не хотим, чтобы Луиджи, который каждый день обновляет меню

на сайте кафетерия компании, имел право создавать токены SAML. Это противоречит самой сути стратегии нулевого доверия. Мы также не хотим, чтобы какой-нибудь случайный программный модуль, за которым никто не следит, имел право повышать свои привилегии и вносить изменения в систему.

При этом я не придираюсь конкретно к SAML. Вероятно, ваша среда предусматривает сотни инфраструктурных транзакций, для выполнения которых требуются повышенные привилегии. Я просто хочу сказать, что нам, как специалистам по безопасности, следует выяснить, что представляет собой каждая из них, и установить специальные правила, определяющие, какие именно сетевые сущности могут выполнять соответствующие функции.

Согласно Gartner, «управление идентификацией и доступом (IAM) — это дисциплина, которая позволяет правильным людям получать доступ к правильным ресурсам в правильное время и по правильным причинам» [272]. Аналогичное определение дает и организация NIST: «[Процесс и технологии, необходимые] для обеспечения доступа правильных людей и вещей к правильным ресурсам в правильное время» [90].

Компоненты IAM: IGA, PIM и PAM

Если размышлять в терминах первичных принципов вообще и стратегии нулевого доверия в частности, то можно сказать, что программа IAM состоит из трех компонентов [206, 279].

- *Управление и администрирование идентификационных данных* (identity governance & administration, IGA) — внутренняя группа руководителей ИТ-служб, служб информационной безопасности и бизнес-лидеров, определяющих политику.
- *Управление идентификацией привилегированных пользователей* (privileged identity management, PIM) — система, которая динамически управляет всеми идентичностями и определяет, к чему они имеют доступ.
- *Управление привилегированным доступом* (privileged access management, PAM) — система, обеспечивающая выполнение правил, созданных IGA, в отношении идентичностей в PIM.

Сетевые защитники могут покупать эти услуги у поставщиков, создавать и развертывать их своими силами или использовать комбинацию этих способов. IGA может быть формальным или неформальным, для PIM может использоваться электронная таблица или огромная база данных, а PAM может

осуществляться с помощью ручных средств управления, которые администраторы настраивают в своих средах Microsoft Active Directory, или в рамках схемы программно-определяемого периметра (см. раздел «Программно-определяемый периметр: тактика нулевого доверия» далее). Так или иначе, любая программа IAM должна предусматривать некоторую совокупность подобных тактик для реализации всех трех перечисленных компонентов.

Наконец, следует учитывать, что системы и данные внутри программы IAM являются своеобразными ключами от города. Другими словами, система IAM с нулевым доверием, которую сетевые защитники проектируют и развертывают для снижения вероятности нанесения организации существенного ущерба, сама по себе становится существенной из-за содержащейся в ней информации и поэтому должна быть защищена таким же образом, как и все остальные важные для бизнеса системы. Как вам такая рекурсивная логика обеспечения безопасности? Если хакеры получат контроль над такой IAM-системой, они смогут обойти все средства безопасности с нулевым уровнем доверия. Таким образом, для защиты IAM-системы мы должны использовать те же стратегии, что и для защиты всей организации, а именно нулевое доверие, предотвращение реализации убийственной цепочки вторжения, обеспечение устойчивости, прогнозирование рисков и автоматизацию.

Единый вход: тактика нулевого доверия

До появления технологии единого входа (single sign-on, SSO), разработанной ближе к началу 2000-х годов, управление идентификацией и доступом представляло собой простой процесс рукопожатия, при котором пользователь или приложение отправляли учетные данные некой рабочей нагрузке для получения доступа к нужному ресурсу. Эта рабочая нагрузка сравнивала хранящиеся локально идентификатор пользователя и пароль с данными, полученными от сетевой сущности, и в случае их совпадения предоставляла ей доступ. Пользователи повторяли этот процесс для получения доступа к каждому нужному им приложению и сети, поэтому должны были хранить множество различных паролей. Руководство службы безопасности осуждало их, если они не могли придумать надежный пароль или использовали один и тот же пароль многократно. Мы до сих пор публично высмеиваем таких пользователей в ежегодных отчетах о наиболее распространенных и ненадежных паролях, используемых в Интернете, примерами которых являются «12345» и «password». Это все равно что обвинять жертву и упрекать людей

в том, что они исключительно плохо пользуются системой идентификации, которая была изобретена в начале 1960-х годов в качестве временного решения. Такой подход кажется неправильным.

На концептуальном уровне суть SSO заключается в том, что пользователь или приложение могут подтвердить свою идентичность перед доверенным источником один раз, а когда этому же пользователю потребуется доступ к другой рабочей нагрузке в другом месте, доверенный источник сможет оценить действительность этого запроса. Хорошая новость заключается в том, что при таком подходе пользователям достаточно запомнить лишь один пароль. Плохой новостью является то, что пользователи по-прежнему могут применить легко угадываемый пароль вроде «12345». Улучшить эту ситуацию может двухфакторная аутентификация, которую мы обсудим в следующем разделе. Тем не менее технология SSO значительно упрощает процесс управления идентификацией и доступом, правда, для того, чтобы прийти к ней, потребовалось 50 лет, прошедших с момента разработки доктором Корбато идеи использования паролей в начале 1960-х годов.

Процесс OAuth

Единый вход в систему организуется с помощью наших старых знакомых OAuth и SAML. Напомню, что протокол OAuth, как правило, применяется для авторизации обычных интернет-пользователей. По словам Майкла Бисселла [31] из NWEA, в этом процессе участвуют три стороны: пользователь (например, интернет-тролль raceBannon99), провайдер идентификации (авторитетный источник идентификационных данных и ролей пользователя, например Google) и поставщик услуг (приложение, к которому raceBannon99 пытается получить доступ, например Twitter). raceBannon99 — рядовой пользователь продуктов компании Google (Gmail, Google Drive и пр.) и заходит в систему Google каждый день. Но теперь он хочет потроллить людей в Twitter. Вместо того чтобы войти в Twitter, используя другой набор учетных данных, raceBannon99 переходит на сайт Twitter и начинает процесс входа в систему, изображенный на рис. 3.2.

1. raceBannon99 спрашивает у системы Twitter, может ли он использовать технологию единого входа для авторизации в ней.
2. Twitter предлагает ему получить асимметричный ключ у провайдера идентификации (Google).
3. raceBannon99 запрашивает у Google ключ, позволяющий системе Twitter проверить действительность его учетных данных.

4. Google упаковывает и отправляет ему ключ.
5. raceBannon99 отправляет этот ключ в Twitter.
6. Twitter отправляет ключ в Google и спрашивает: «Этот парень тот, за кого себя выдает?»
7. Google отвечает: «Да, это raceBannon99» (только, скорее всего, он делает это на языке, который понимают только компьютеры).

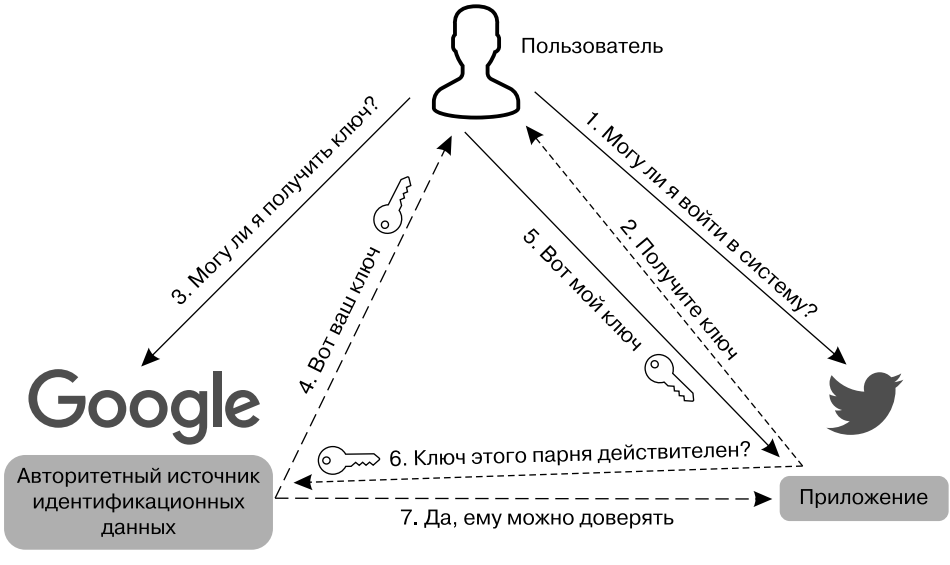


Рис. 3.2. Реализация единого входа в систему с помощью протокола OAuth

В рамках данной транзакции OAuth ни одна из трех сторон не обменивалась паролями. Они просто передавали друг другу асимметричные ключи.

По словам Бена Луткевича из компании TechTarget, Google — это не единственный технологический гигант, выступающий в качестве такого авторитетного источника [147]. На момент написания этой книги наиболее популярными провайдерами идентификации являлись:

- Google;
- Facebook[1];
- Apple;

[1] Деятельность компании Meta, которой принадлежит Facebook, запрещена в России. — *Примеч. ред.*

- Fitbit;
- Microsoft;
- Box;
- Amazon Web Services (AWS).

Итак, для выполнения обычных интернет-транзакций пользователи выбирают компанию, которой доверяют, разрешают ей хранить свои учетные данные, а затем задействуют ее в качестве авторитетного источника этих данных для получения доступа к другим интернет-ресурсам.

Процесс SAML

Процесс использования протокола SAML аналогичен рассмотренному ранее, но более надежен. Как вы помните, SAML обычно применяется для корпоративных приложений вроде Quest Enterprises, и вместо того, чтобы просто передавать асимметричные ключи, как это делает OAuth, он позволяет провайдеру идентификации (в данном случае это Google, поскольку Quest Enterprises работает с GSuite) упаковывать и шифровать такую информацию о пользователе, как персональные данные (personally identifiable information, PII), группы безопасности, роли и другие полезные сведения, которые могут задействоваться для входа в систему (рис. 3.3). Мы можем с помощью этой информации обеспечивать соблюдение правил нулевого доверия, например проверять, имеет ли право директор по безопасности компании Quest Enterprises Рейс Бэннон использовать приложение Slack.

1. Рейс Бэннон заходит в официальное приложение Slack компании Quest Enterprises и начинает процесс авторизации.
2. Slack сообщает Рейсу о необходимости получить пакет персональных данных (PII) у провайдера идентификации (Google).
3. Рейс запрашивает у Google свой PII-пакет для Slack.
4. Для проверки того, что Slack является именно тем, за кого себя выдает, провайдер идентификации (Google) запрашивает у Slack его ключ.
5. Slack отправляет Google свой открытый ключ.
6. Google шифрует персональные данные Рейса с помощью ключа Slack и отправляет их Бэннону.
7. Рейс отправляет зашифрованный PII-пакет приложению Slack.
8. Slack открывает PII-пакет Рейса своим закрытым ключом.

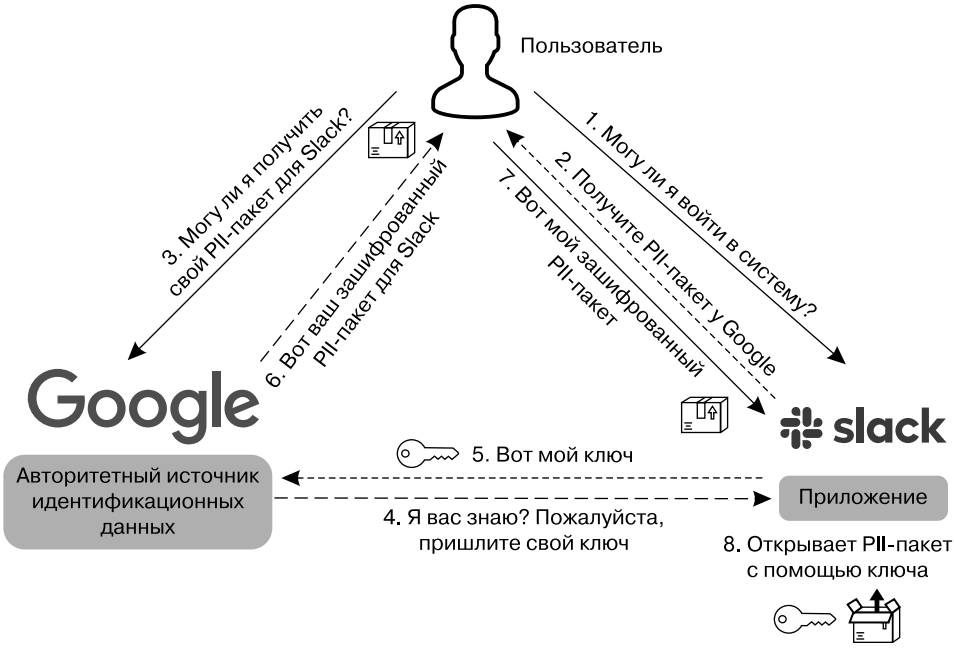


Рис. 3.3. Реализация единого входа в систему с помощью протокола SAML

Здесь следует отметить два момента. Во-первых, Рейс не может просмотреть содержимое своего PII-пакета, поскольку Google зашифровал его с помощью открытого ключа Slack. Во-вторых, после открытия этого пакета Slack может решить, к каким частям приложения Рейс может получить доступ.

Как и в случае с OAuth, провайдер идентификации SAML играет важную роль и реализовать его можно множеством способов. Бисселл приводит следующие распространенные системы, которые могут использоваться в программах управления идентификацией и доступом (существует и множество других):

- Active Directory;
- Lightweight Directory Access Protocol;
- PingFederate;
- SharePoint.

По меркам Интернета технологии SSO потребовалось много времени, чтобы приблизиться к чему-то более или менее пригодному для использования.

Однако по обычным меркам этот переход был феноменально быстрым. Я имею в виду то, что в интернет-пространстве время летит стремительно. Например, с момента выхода на рынок первого iPhone (2007 год) до появления возможности смотреть на нем сериал «Лунный рыцарь» от Disney+ прошло 15 лет. По меркам Интернета это целая вечность. Однако по человеческим меркам это далеко не так. Потребовалось всего 15 лет, чтобы у меня появилась возможность смотреть кинофраншизу мирового класса на телефоне. Это потрясающе. То же самое касается и технологии SSO. Благодаря появлению языка SAML в 2002 году и протокола OAuth в 2010-м рядовые интернет-пользователи сегодня могут пользоваться преимуществами технологии единого входа, а специалисты по обеспечению корпоративной безопасности — создавать надежные системы с нулевым уровнем доверия. Впереди еще много работы, но основа уже заложена. Технология SSO — это отличная идея, и нам всем следует способствовать ее дальнейшему развитию.

Двухфакторная аутентификация: тактика нулевого доверия

В те давние времена, когда доктор Корбато работал с мейнфреймами, парольная аутентификация была довольно слабой, но это не вызывало серьезных проблем. Тогда компьютеры использовались в основном для реализации правительственных проектов и проведения научных исследований. В то время мало кто имел доступ к компьютерам, объединенным в сеть. Однако к началу 1980-х годов, когда сеть ARPANet постепенно превратилась в Интернет, количество пользователей компьютеров стало стремительно расти и сообществу потребовались более надежные методы аутентификации в критически важных для бизнеса системах.

В середине 1980-х годов компания Security Dynamics Technologies разработала первый аппаратный токен, генерирующий одноразовые пароли (OTP) для аутентификации [237]. К 1995 году компания AT&T запатентовала идею двухфакторной аутентификации [62]. Согласно ей для идентификации авторизованного пользователя система должна проверять как минимум два из трех факторов: то, что у него есть, например смартфон, то, что является его биометрическим параметром, например отпечаток пальца, или то, что он знает, например пароль. Однако первые такие системы были неуклюжи-

ми, сложными в управлении и использовались лишь там, где требовалась максимальная безопасность. Но с распространением смартфонов в середине 2000-х годов ситуация начала меняться. Внезапно у каждого человека в кармане появился второй фактор аутентификации, что способствовало возникновению всевозможных инноваций.

Виды двухфакторной аутентификации

В 2017 году Крис Хоффман написал для сайта How-To Geek отличную статью о различных формах двухфакторной аутентификации [104]. Далее я кратко опишу принцип их работы, а затем мы поговорим о том, насколько они безопасны.

Верификация с помощью СМС. Интернет-тролль raceBannon99 хочет зайти на сайт Audible.com. Сайт отправляет ему текстовое сообщение с кодом, позволяющим получить доступ к своей учетной записи.

Верификация с помощью электронной почты. Этот способ аналогичен методу СМС-верификации, за исключением того, что в качестве второго фактора выступает электронная почта, а не система обмена текстовыми сообщениями.

Программные токены аутентификаторов (например, Google Authenticator, ID.me, Battlenet компании Blizzard и LastPass). Аутентификаторы используют алгоритм IETF (Internet Engineering Task Force — Инженерный совет Интернета) для генерации одноразовых кодов, называемых *одноразовыми паролями на основе времени* (time-based one-time password, TOTP). Рейс Бэннон, директор по информационной безопасности компании Quest Enterprises, хочет войти в свою учетную запись Google G-Suite. G-Suite запрашивает одноразовый код. Рейс открывает приложение Google Authenticator на смартфоне и ищет в перечне Google. У него есть несколько вариантов на выбор, например LastPass и HR-приложение Quest Enterprise. Алгоритм стандартный, поэтому Google Authenticator можно использовать для входа в приложения других компаний, например Microsoft или Amazon. Он обращает внимание на обратный отсчет времени рядом с каждым из вариантов. Каждые 30 с приложение Google Authenticator генерирует новый код. Рейс запоминает шестизначный код и вводит его на экране входа в систему Google до того, как на таймере закончится время.

Аутентификация с помощью push-уведомлений (от Google, Apple, Microsoft и Twitter). В отличие от СМС-верификации система push-аутентификации Google не использует коды. Теща Рейса Бэннона попросила его приехать и устранить какую-то техническую проблему с ее iPad. Там у него возникает необходимость войти в свою учетную запись Gmail, чтобы получить некоторую информацию. Google не распознает iPad тещи Рейса в качестве зарегистрированного устройства и отправляет на его iPhone уведомление через свое приложение. Рейс открывает приложение Google на своем смартфоне и нажимает кнопку с надписью: «Да, я Рейс Бэннон». На объяснение этих действий требуется гораздо больше времени, чем на их выполнение, но в итоге Рейс получает доступ к своей учетной записи Gmail с планшета тещи. Версия Apple работает подобным образом, но она не привязана к приложению, а использует операционную систему.

Универсальная двухфакторная аутентификация. Универсальная двухфакторная аутентификация (Universal 2nd Factor, U2F) — это открытый стандарт, призванный улучшить и упростить процесс двухфакторной аутентификации за счет использования устройств с USB (universal serial bus — универсальная последовательная шина) или технологией NFC (near-field communication — коммуникация ближнего поля). Рейс Бэннон хочет войти в менеджер паролей LastPass, чтобы получить доступ к корпоративным паролям. Он вводит свой идентификатор пользователя и пароль, после чего LastPass просит его вставить в ноутбук физический USB-ключ аутентификации (в данном случае Yubikey от Yubico). Он нажимает кнопку на внешней стороне физического ключа, и приложение LastPass предоставляет ему доступ.

Принцип работы заключается в том, что USB-ключ создает пару, состоящую из открытого и закрытого ключей, для каждого сайта, например LastPass. Браузер пользователя проверяет эти ключи, после чего предоставляет ему доступ. Благодаря этому исключается вероятность кражи учетных данных с помощью поддельных сайтов.

Существуют версии этого стандарта, работающие на базе беспроводных технологий Bluetooth или NFC. NFC — это протокол, который позволяет двум устройствам осуществлять беспроводную связь, когда они находятся рядом друг с другом (радиус действия — около 10 см). Пример — использование мобильного устройства для проверки посадочного талона в аэропортах. Устройства, оснащенные технологией NFC, могут устанавливать связь с аналогичными устройствами, а также с NFC-метками, которые представляют собой пассивные NFC-чипы, получающие питание от расположенных рядом устройств с поддержкой NFC (рис. 3.4).

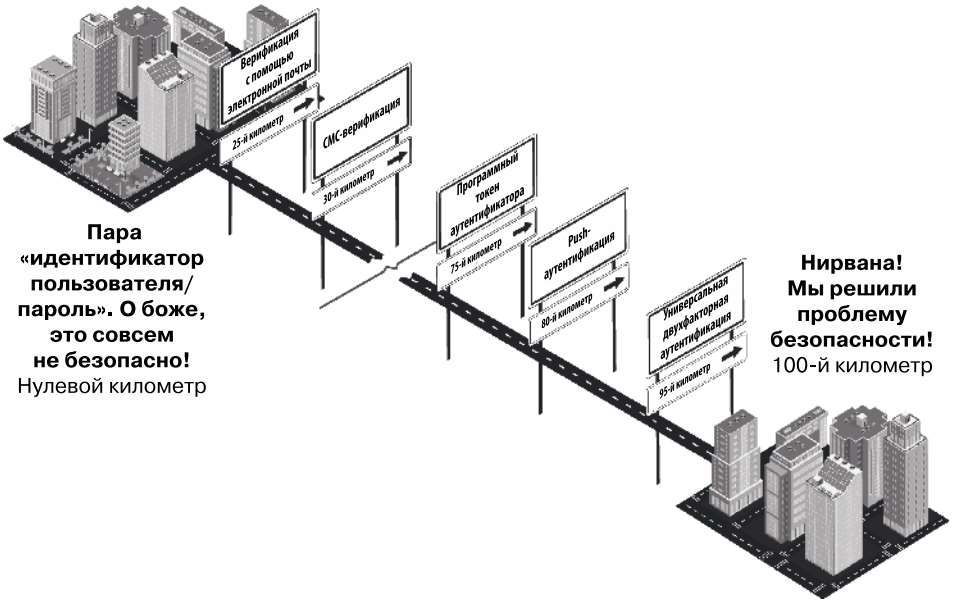


Рис. 3.4. Средства двухфакторной аутентификации на пути к нирване

Насколько безопасна двухфакторная аутентификация

На простой линейной шкале двухфакторная аутентификация намного превосходит использование пары «идентификатор пользователя/пароль». Если расположить все описанные в этом разделе методы аутентификации вдоль 160-километрового пути между двумя великими городами «О боже, это совсем не безопасно» и «Нирвана! Мы решили проблему безопасности», то остановка, соответствующая использованию пары «идентификатор пользователя/пароль», окажется всего в полутора километрах от первого города, а значит, это лишь слегка превосходит полное отсутствие учетных данных. Все остальные методы представляют собой остановки на пути к «Нирване».

Остановка, соответствующая верификации с помощью электронной почты, находится примерно в 40 км от исходной точки и в 120 км от «Нирваны», поскольку электронная почта не вполне подходит на роль второго фактора. Ее учетная запись уникальна, как и пароль, но доступ к ней можно получить

из любого места. Это не то, что всегда находится при вас, и не какой-то биометрический параметр. Таким образом, два паролеподобных фактора — это лучше, чем один, но ненамного.

Остановка, соответствующая СМС-верификации, находится примерно в 50 км от места старта. Этот метод слегка превосходит верификацию по электронной почте, поскольку привязан ко второму фактору, однако злоумышленники из реального мира продемонстрировали три различных способа перехвата этих кодов. Первый способ называется *подменой SIM-карты*. С помощью социальной инженерии злоумышленники заставляют телефонную компанию перенести ваш номер на свой телефон, этот же процесс вы сами будете использовать в следующем году при покупке новой модели iPhone. После этого при каждой попытке войти в систему СМС-код будет отправляться не на ваш, а на телефон злоумышленника, и он сможет использовать его для входа в вашу учетную запись. Второй способ, продемонстрированный на практике, предполагает перехват СМС-кодов некоторыми недобросовестными правительствами в процессе сбора разведывательной информации, то есть шпионажа. Третий способ заключается во взломе телефонной сети SS7 жертвы и перенаправлении кода на телефон злоумышленника. SS7 (Signaling System 7 — система сигнализации № 7) — это стандарт, определяющий порядок обмена управляющими сигналами в коммутируемых телефонных сетях общего пользования (ТСОП). Тем не менее СМС-верификация значительно превосходит применение пары «идентификатор пользователя/пароль», хоть и тоже далека от «Нирваны». Она вполне подходит для обычных случаев использования Интернета, например для получения доступа к библиотеке. Однако если вы хотите защитить важную информацию или занимаетесь шпионажем, избегайте СМС-верификации.

Остановка, соответствующая применению программных токенов аутентификатора, расположена примерно в 120 км от точки старта. Она находится довольно далеко от исходного города и достаточно близко к «Нирване», для того чтобы этот великий город можно было из нее увидеть. Данный способ аутентификации по-прежнему подвержен атакам типа «человек посередине», в ходе которых пользователя обманом заставляют ввести код на фишинговом сайте, находящемся под контролем злоумышленников. Реализовать такую атаку проще, чем скомпрометировать сеть SS7 жертвы, и она, безусловно, входит в набор навыков современного киберпреступника. Чтобы добиться успеха, злоумышленник должен получить код и войти в учетную запись до того, как аутентификатор его изменит. Временной фактор в дан-

ном случае имеет решающее значение, но он не делает атаку невозможной, а лишь усложняет ее реализацию.

Остановка, соответствующая push-аутентификации, находится на отметке 130 км и расположена чуть ближе к «Нирване», чем предыдущая. Тем не менее злоумышленники нашли способ обойти и эту защиту путем отправки множества уведомлений на телефоны жертв. Если потенциальная жертва занята или недостаточно внимательна, она может нажать на кнопку подтверждения своей личности, просто чтобы убрать сообщение, так и не поняв, что своим действием разрешила злоумышленнику войти в одну из своих учетных записей.

Остановка, соответствующая универсальной двухфакторной аутентификации, находится на отметке 150 км, она последняя на пути к «Нирване». Если вы предъявляете серьезные требования к безопасности, а не просто блуждаете по просторам Интернета, стоит воспользоваться именно этим способом. Однако недостатком применения USB-ключа безопасности является высокая вероятность его потери. Лично я возлагаю гораздо бóльшие надежды на будущие NFC-решения, поскольку потеряю телефон с меньшей вероятностью, чем USB-ключ. Однако проблема в том, что такие решения еще не получили широкого распространения и все еще находятся на стадии становления. В настоящее время технологии U2F продвигает организация Fast Identity Online (FIDO). Согласно диаграмме Hype Cycle 2021 для технологий управления идентификацией и доступом, подготовленной компанией Gartner, усилия FIDO Alliance все еще находятся во впадине разочарования, а до достижения плато продуктивности пройдет от двух до пяти лет.

Будущее двухфакторной аутентификации

Можете считать меня сумасшедшим, но не думаю, что в ближайшее десятилетие у меня уменьшится количество паролей, находящихся под управлением LastPass. В условиях бурного развития Интернета вещей и распространения сетей 5G число учетных записей, которыми нам придется управлять в личной и профессиональной жизни, будет только расти. Программные токены аутентификаторов, push-аутентификация и технология U2F не уйдут из нашей жизни в обозримом будущем. И возможно, где-то на пути между «О боже!» и «Нирваной» мы сможем полностью избавиться от временной меры, предложенной доктором Корбато в 1960-х годах.

Программно-определяемый периметр: тактика нулевого доверия

Как я уже говорил, в первое время (в середине 1990-х годов) основными моделями обеспечения безопасности были защита периметра и эшелонированная защита. С помощью стека безопасности мы создавали барьер между Диким Западом, которым тогда являлся Интернет, и бастионом нашей коммерческой и личной активности (рис. 3.5). И этот подход замечательно работал, если вы целыми днями находились внутри периметра и вам не нужно было зачем-то выходить в Интернет. Однако тут же появились всевозможные исключения. Наша политика безопасности предполагала блокировку всего, чему мы не доверяли, с помощью межсетевого экрана. Но по разным связанным с бизнесом причинам пришлось пробивать дыры в этом экране, чтобы позволить подрядчикам, партнерам и сотрудникам, работающим за пределами охраняемого периметра, получить доступ к тому, что находилось внутри. Иногда мы просто поднимали межсетевой экран, устанавливая специальные правила для каждого исключения. А в 2000-х годах начали предоставлять им доступ к нужным ресурсам через виртуальную частную сеть (VPN).

Разница между непосредственным прохождением через брандмауэр и использованием VPN лежит на третьем (сетевом) уровне стека TCP/IP. При использовании VPN клиент создает на третьем уровне защищенный туннель (зашифрованное соединение), ведущий к VPN-серверу, находящемуся внутри периметра. Прохождение через межсетевой экран можно уподобить входу в офисное здание через парадную дверь. Когда вы проходите через контрольно-пропускной пункт со считывателем карт, все видят, что вы делаете. В случае использования VPN вы, словно герой телесериала «Звездный путь», входите в телепортационную комнату с внешней стороны брандмауэра и выходите с внутренней, минуя все системы безопасности.

Это очень удобно для пользователя VPN, поскольку ни один посредник, включая межсетевой экран, не может наблюдать за данными, которыми обмениваются стороны. Все они зашифрованы. Однако плохая новость для службы безопасности заключается в том, что она не может отслеживать трафик на предмет вредоносной активности. Даже если весь этот трафик проходит через стек безопасности (например, через брандмауэр и систему обнаружения вторжений), это ничего не значит. Волшебства, которое предусмотрено вашим стеком безопасности, не происходит, поскольку он просто не видит этих данных.

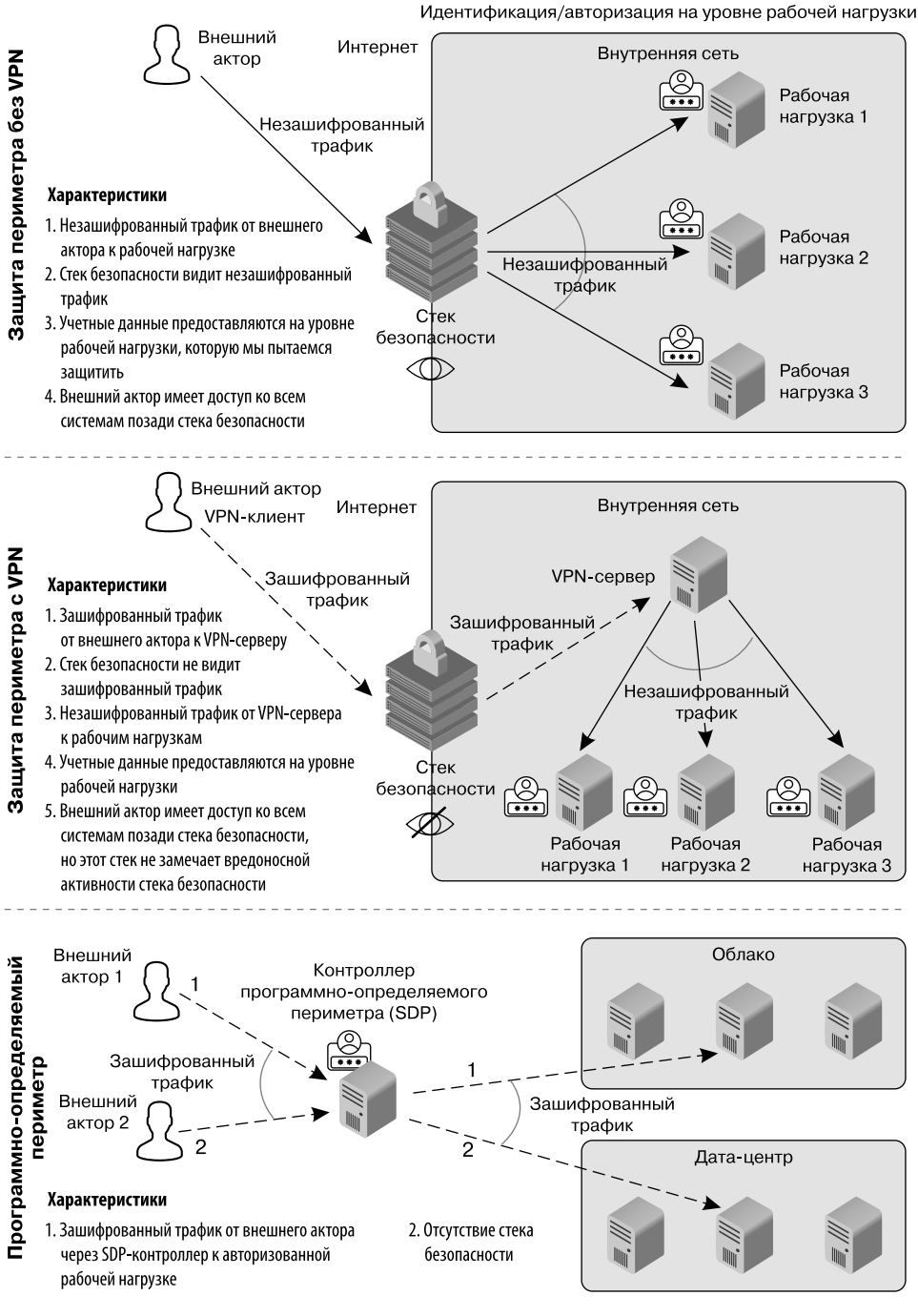


Рис. 3.5. Сравнение методов получения доступа внешними акторами

Обе архитектуры — прохождение через брандмауэр и использование VPN — неудачны. Оставляя дыры в межсетевом экране для сотрудников, вы открываете такие же возможности и для злоумышленников. Если им удастся пробраться через одну из таких дыр, они получат доступ ко всему, что находится внутри периметра. Недостаток VPN заключается в том, что туннель позволяет полностью обойти стек безопасности.

Современные межсетевые экраны способны взламывать VPN-шифрование на границе, проверять трафик, повторно его зашифровывать и отправлять дальше. В этом случае межсетевой экран становится устройством-посредником. Однако данный подход непросто реализовать, а в некоторых странах приняты законы о конфиденциальности, которые это запрещают.

Программно-определяемый периметр становится новой моделью

В начале 2000-х годов американские военные начали экспериментировать с архитектурой, названной *депериметризацией*, в рамках проекта Jericho Forum [213]. Суть ее заключалась в том, чтобы отделить функции идентификации и авторизации от важной рабочей нагрузки. Другими словами, вместо того, чтобы пытаться войти в систему через брандмауэр или VPN-туннель, вы подключаетесь к отдельной системе — контроллеру программно-определяемого периметра (SDP), находящемуся за пределами брандмауэра, который проверяет вашу личность и необходимость в получении доступа к запрашиваемому ресурсу. В случае прохождения проверки SDP-контроллер устанавливает VPN-подобное туннельное соединение между вами и конкретной рабочей нагрузкой. Такая система скрывает эту и все остальные рабочие нагрузки в своеобразном «черном облаке», как это назвали в Министерстве обороны. Иначе говоря, ни один случайный злоумышленник из Интернета не может увидеть или обнаружить важные рабочие нагрузки, защищенные периметром. Они видят лишь SDP-контроллер, выполняющий функции идентификации и авторизации. Кроме того, даже если злоумышленникам удастся получить доступ к этой рабочей нагрузке, они не смогут добраться до остальных. В этом и заключается суть стратегии нулевого доверия — сократить поверхность атаки до минимума. К сожалению, Министерство обороны так и не разработало такую систему.

В 2010 году компания Google и несколько коммерческих и оборонных подрядчиков объявили о том, что они подверглись массированной кибератаке со

стороны китайских хакеров, ставшей известной как операция Aurora [175]. В последующие недели выяснилось, что в сети Google действовала не одна китайская правительственная структура, а две: Народно-освободительная армия Китая (НОАК), которая похищала интеллектуальную собственность, в частности исходный код технологических компаний, и Министерство государственной безопасности (МГБ), которое преследовало таких политических диссидентов, как далай-лама, уйгуры и тибетские этнические меньшинства. И что довольно характерно для правительственных бюрократий, ни одна из этих организаций не знала о действиях другой, пока Google не обнародовала эту информацию.

> Интересный факт: на заре отслеживания кибершпионов (то есть в 2000-е годы) одним из признаков причастности китайского правительства было время проведения атак — в основном они происходили с 09:00 до 17:00 по шанхайскому времени. Создавалось впечатление, будто китайские хакеры работают по часам, как обычные люди. Я помню, что в те времена мы все придавали большую важность часовым поясам. Если атаки происходили с 09:00 до 17:00 по московскому времени, то, очевидно, за ними стояли русские. Оглядываясь назад, становится понятно, что это было весьма наивно. Если бы я планировал наступательную кибероперацию сегодня, то обязательно запутал бы следы, чтобы имитировать действия известного противника в соответствии с его часовым поясом. Это просто к слову.

В ответ на атаку Aurora SRE-инженеры компании Google полностью переделали свою внутреннюю архитектуру безопасности, используя концепции депериметризации и нулевого доверия [321]. Спустя несколько лет они выпустили коммерческий продукт под названием BeyondCorp, в котором были реализованы многие из идей, разработанных внутри компании.

В 2013 году некоммерческая организация Cloud Security Alliance объявила о запуске своей инициативы SDP Initiative, а годом позже выпустила спецификацию 1.0 [222]. В 2020-м организация NIST опубликовала документ с описанием архитектуры нулевого доверия, в котором были изложены некоторые тезисы относительно программно-определяемого периметра [187]. Наконец, в 2022 году организация Cloud Security Alliance анонсировала версию 2.0 своей спецификации [263].

Где-то между реализацией проекта Министерства обороны Jericho Forum и SDP организации Cloud Security Alliance концепция деперимetризации стала известна в отрасли как программно-определяемый периметр (SDP). Это довольно неудачное название, поскольку она не имеет абсолютно никакого отношения к защите периметра. Она полностью отделяет процесс входа в систему от рабочей нагрузки и, по сути, ликвидирует привычный периметр в том виде, в котором мы его знали в 1990-е годы.

Если бы я занимался маркетингом, то предложил бы для деперимetризованной архитектуры одно из следующих названий:

- программно-определяемая червоточина;
- идентификация и авторизация в черной дыре;
- каналы идентификации и авторизации;
- идентификация и авторизация с помощью телепортационной комнаты (для поклонников «Звездного пути»).

Хотя, может быть, мне стоит заниматься только кибербезопасностью.

На мой взгляд, SDP является более совершенной тактикой, базирующейся на первичном принципе обеспечения кибербезопасности, и лучше подходит для реализации стратегии нулевого доверия. Она предусматривает встроенные функции идентификации и авторизации и ограничивает доступ к рабочим нагрузкам на основе принципа минимальной необходимой осведомленности. К сожалению, несмотря на все усилия организаций Cloud Security Alliance и NIST, эта архитектура до сих пор не получила широкого распространения. Согласно результатам опроса, проведенного Cloud Security Alliance в 2020 году, лишь четверть респондентов слышали о ней [236]. В качестве главной причины, препятствующей ее внедрению, эти люди назвали сложность замены существующих технологий обеспечения безопасности. Это весьма печально. Если нулевое доверие действительно представляет собой первичный принцип кибербезопасности, то SDP, скорее всего, самый верный путь к достижению этой цели.

Однако следует сделать одно замечание: SDP отлично вписывается в программу IAM, о чем было сказано в разделе «Управление идентификацией: тактика нулевого доверия». Она заменяет другие архитектуры или улучшает уже существующие. Это напоминает нам о том, что любая развернутая

программа SDP по своей природе является существенной для организации системой и должна быть защищена как таковая с помощью стратегий, основанных на первичном принципе кибербезопасности. Если злоумышленникам удастся скомпрометировать SDP, игра будет проиграна.

Причины провала проектов с нулевым доверием

Когда в 2010 году Киндерваг опубликовал фундаментальный труд, посвященный концепции нулевого доверия, большая часть ИБ-сообщества сочла ее хорошей идеей — одной из миллиона идей, до реализации которых мы, вероятно, никогда не дойдем. Однако после инцидента со Сноуденом, выявившего слабые места в модели защиты периметра, способные причинить серьезный ущерб, она стала более актуальной. Случай со Сноуденом и более поздние громкие киберинциденты с участием инсайдеров (Челси Мэннинг, Tesla, Capital One и др.) дали повод для перемен. Однако многие до сих пор не встали на этот путь.

Причина в том, что большинство из нас ставит перед собой непосильную задачу. Мы считаем, что для обеспечения нулевого доверия нужно вскипятить океан, отказаться от всего, что у нас есть, и начать с нуля. Чтобы понять, о чем я говорю, взгляните на проект архитектуры нулевого доверия, опубликованный организацией NIST в феврале 2020 года (рис. 3.6) [187].

Несмотря на то что в этом документе абсолютно правильно изложены идея нулевого доверия и технические требования, необходимые для ее реализации, NIST предлагает систему систем — архитектуру черных ящиков, которая на первый взгляд кажется отсутствующей у всех нас, недоступной в коммерческом секторе и слишком большой для того, чтобы создавать ее самостоятельно. Но это не так.

Проекты нулевого доверия проваливаются не по причине отсутствия технологий, позволяющих их реализовать. Межсетевые экраны нового поколения существуют с 2007 года и были разработаны именно для этого. Причина провала таких проектов заключается в том, что сетевые защитники не выделяют достаточно ресурсов в виде людей и процессов для управления ими. А некоторые даже думают, что можно просто щелкнуть выключателем, чтобы система сама о себе позаботилась. Знаете, сколько раз за мою жизнь эта стратегия срабатывала? Ни одного.

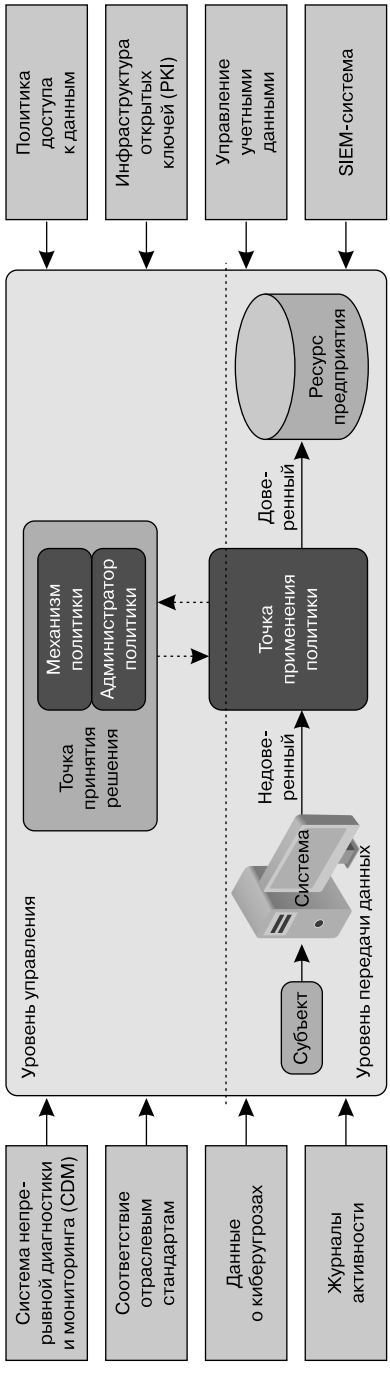


Рис. 3.6. Логические компоненты архитектуры нулевого доверия NIST

В лучшем случае у нас есть пара парней и собака, составляющие команду ИТ-экспертов, которые управляют нашими маршрутизаторами, стеком безопасности, принтерами, помогают Джорджу из отдела продаж подключить монитор к своему ноутбуку, а также приносят кофе генеральному директору по утрам. Теперь мы хотим, чтобы они еще и реализовывали стратегию нулевого доверия с помощью межсетевых экранов нового поколения. Они едва успевают проверять электронную почту перед работой, а мы собираемся поручить им еще одну задачу. Но это только увеличивает технический долг, который мы никогда не погасим. Кроме того, решение о том, кто из сотрудников получает доступ к тем или иным ресурсам компании, не должно приниматься командой из двух парней и собаки. Оно должно приниматься в рамках разработки политики на высшем уровне управления организацией. Даже если вы работаете в небольшой или средней компании, определение политики доступа — это решение, связанное с бизнес-процессами, а не с ИТ.

Всякий раз, когда я принимаю участие в реализации чьей-либо новой идеи, обещающей улучшить нашу жизнь с помощью очередной фантастической технологии, я раздражаю команду надоедливыми вопросами о людях и процессах. Однажды я работал на человека, который был очарован новой системой предотвращения утечек данных (DLP), которую предлагал его любимый поставщик. Она обещала автоматизировать очень многие действия, которые мы в то время выполняли вручную. Но пока я слушал, как представитель компании рассказывает о возможностях продукта (надо сказать, они были просто великолепны), я подсчитывал, сколько людей потребуется для управления этой системой и, что еще важнее, кто из руководства будет утверждать политики, внедряемые этой командой. Мне казалось, что я обнаружил гигантское несоответствие. А однажды я устроился на работу и узнал, что мой предшественник приобрел все новейшие средства обеспечения кибербезопасности, а затем покинул организацию, заняв более высокооплачиваемую должность (я рад за него). У нас было все, что только можно было пожелать в плане инструментов обеспечения безопасности. Однако у моего предшественника деньги закончились прежде, чем он нанял людей для управления этими инструментами. Моя проблема заключалась в том, что в SOC-центре работала команда новичков, пытавшихся управлять целым парком «Феррари», составляющим стек безопасности. И бóльшую часть времени эти машины простаивали, пока я пытался убедить босса нанять дополнительных специалистов.

Если нулевое доверие является важнейшим элементом философии, базирующейся на первичном принципе, то оно достаточно важно для того, чтобы создать специальную команду для реализации соответствующей стратегии. Как было показано в этой главе, обеспечение нулевого уровня доверия не ограничивается управлением идентификацией. Нужна команда, создающая процессы интеграции новых сотрудников и принимающая решения о том, к каким функциональным отделам они будут относиться изначально. Эта команда должна изменять уровень доступа сотрудников при их перемещении внутри организации на новые должности с новыми обязанностями, а также закрывать им доступ к системе при увольнении. И наконец, потребуется отдельная команда, занимающаяся автоматизацией этих процедур, чтобы управляющая команда по ошибке не внесла изменения в конфигурацию, оставив цифровые окна и двери открытыми для злоумышленников. Для всего этого нужны люди, процессы и технологии. Скорее всего, у вас уже есть необходимые ресурсы для того, чтобы приступить к разработке этих процессов.

Заключение

Оглядываясь на много лет назад, сетевые защитники склонны критиковать АНБ за то, что оно не создало сеть с нулевым уровнем доверия, предназначенную для снижения последствий реализации инсайдерских угроз наподобие случая с Эдвардом Сноуденом. Поразительная правда заключается в том, что большинство из нас в то время тоже не имели такой сети. Еще более печально то, что многие до сих пор не создали такую сеть, хотя все мы знаем, что она должна быть реализована, даже если считаем, что термин «нулевое доверие» затерт до дыр поставщиками систем безопасности.

На первый взгляд, задача преобразования наших старых сетей M&M (с твердой оболочкой и мягкой вкусной начинкой) в сети с нулевым уровнем доверия кажется пугающей и дорогостоящей. Вместо того чтобы воспринимать концепцию нулевого доверия в качестве пункта назначения, думайте о ней как о путешествии по бесконечному пути совершенствования, то есть как о стратегии, которой мы должны следовать каждый день. На этом пути мы можем сделать миллион разных вещей. Но есть то, что можно сделать прямо сейчас, — использовать уже имеющиеся технологии, чтобы начать закрывать цифровые двери и окна. И даже если мы по ошибке оставим какие-то из них приоткрытыми, обнаруженные злоумышленником данные не окажут существенного влияния на организацию. Киндерваг многократно дорабатывал

свои тезисы с момента написания основополагающей статьи в 2010 году. У него есть определенные мысли по поводу реализации этой стратегии в большинстве сред. Его «Девять правил» — хорошая отправная точка для этого.

По моему мнению, вам в первую очередь следует задействовать тактики, способные сильнее всего повлиять на вашу организацию, такие как логическая и микросегментация, управление уязвимостями, использование спецификаций программного обеспечения и управление активами в целом. Начните совершенствовать программу управления идентификацией уже сейчас и, если еще этого не сделали, включите в дорожную карту задачи внедрения технологии единого входа, двухфакторной аутентификации и программно-определяемого периметра. В процессе работы помните: проекты нулевого доверия проваливаются из-за того, что покупка новых инструментов для реализации той или иной тактики не сопровождается соответствующим увеличением численности сотрудников.

И не забывайте, что нулевое доверие — это философия и бесконечный путь, а не продукт. Это образ жизни, стратегия, которая напрямую поддерживает наш первичный принцип кибербезопасности, сводящийся к снижению вероятности существенного ущерба. Это не единственная стратегия, которой следует придерживаться, но это то, что должно стать частью ДНК и культуры каждой организации, причем не только ИБ-отдела, но и всех остальных ее подразделений.

Наконец, имейте в виду, что нулевое доверие представляет собой пассивную защитную стратегию общего назначения. Она совершенно не зависит от конкретных угроз, с которыми вы сталкиваетесь. Если же хотите сконцентрироваться на борьбе с конкретным известным противником, то вам потребуется более активная стратегия защиты, о которой мы поговорим в следующей главе.

04 Предотвращение реализации убийственной цепочки вторжения (kill chain)

Анализ убийственной цепочки показывает, что противник должен успешно пройти все ее этапы, чтобы достичь своей цели, ослабление всего лишь одного звена способно нарушить цепочку и планы противника.

Хатчинс, Клопперт и Амин, статья компании Lockheed Martin, посвященная концепции убийственной цепочки, 2010 год

Модель Diamond интегрирует... и дополняет анализ убийственной цепочки, расширяя перспективу, что обеспечивает необходимую детализацию и выражение сложных взаимосвязей между действиями злоумышленника в ходе вторжения.

Кальтаджироне, Пендергаст и Бетц, статья, посвященная модели Diamond, 2011 год

При отслеживании угроз «группы определяются как именованные наборы вторжений, группы угроз, группы акторов или кампании, которые обычно представляют собой целенаправленную, постоянную угрожающую активность».

Стром, Эпплбаум, Миллер, Пеннингтон и Томас, ATT&CK: Design and Philosophy, март 2020 года

Обзор главы

В этой главе я расскажу о том, почему считаю предотвращение реализации убийственной цепочки вторжения (kill chain) стратегией обеспечения кибербезопасности, базирующейся на первичном принципе. С момента своего появления в 2010 году она полностью изменила подход ИБ-специалистов к защите своих организаций в киберпространстве. Согласно данной стратегии цель сетевого защитника заключается не в блокировке технических средств, используемых хакерами, а в победе над противником, который стоит за этими средствами. Эта идея оказалась весьма радикальной. Ее развитию способствовали три исследовательские работы. Первой из них был оригинальный документ компании Lockheed Martin с описанием данной стратегии. Второй стала модель Diamond Министерства обороны США, в которой работа команды кибербразведки (CTI) была пересмотрена в соответствии с идеей убийственной цепочки. Третьей была база знаний ATT&CK компании MITRE — лучшая в мире коллекция описаний известных тактик и методов кибератак.

Я расскажу о том, как команда кибербразведки атрибутирует атаки и подсчитывает количество активных интернет-кампаний в каждый конкретный день. Затем опишу несколько тактик, которые могут оказаться полезными для предотвращения реализации убийственной цепочки вторжения, в частности:

- создание центров мониторинга информационной безопасности (SOC-центров);
- оркестрацию стека безопасности;
- анализ киберугроз (кибербразведка);
- операции «фиолетовой» команды;
- обмен разведданными.

Зарождение новой идеи

Во время первой войны в Персидском заливе в 1991 году иракские ракеты мобильного базирования SCUD доставили летчикам ВВС и ВМС США немало хлопот. Иракские солдаты успевали выпустить ракеты и переместить пусковые установки задолго до того, как американские самолеты могли их обнаружить и уничтожить. После войны, примерно в 2000 году, генерал

Джон Джампер изменил доктрину ведения воздушного боя, чтобы решить эту проблему, формализовав методы, позволяющие сократить время поиска и уничтожения противника на поле боя. В ВВС цикл поражения цели обозначается аббревиатурой F2T2EA (find — «найти», fix — «захватить», track — «сопроводить», target — «навести», engage — «поразить», assess — «оценить»). Хорошо известно, что военные любят аббревиатуры даже больше, чем представители киберсообщества. На простом языке это называется *убийственной цепочкой*. Джампер поставил перед ВВС задачу сократить длительность реализации этой убийственной цепочки с нескольких часов или дней до десяти минут [99]. Модель ВВС F2T2EA имеет значение для нашего повествования, поскольку десять лет спустя исследователи из компании Lockheed Martin применили эту же концепцию к обеспечению киберзащиты, результатом чего стала идея убийственной цепочки вторжения.

Документ компании Lockheed Martin, посвященный концепции убийственной цепочки

Две тысячи десятый год оказался богат на значительные события и революционные идеи в области кибербезопасности. Компания Google шокировала общественность, объявив о том, что подверглась атакам со стороны китайского правительства [175]. Джон Киндерваг опубликовал фундаментальную работу *No More Chewy Centers*, посвященную стратегии нулевого доверия [133]. Миру также стало известно об американо-израильской киберкампании Olympic Games, часто называемой Stuxnet, призванной замедлить развитие или подорвать потенциал Ирана в сфере производства ядерного оружия, которая продемонстрировала всю сложность разработки атаки для трудных киберцелей [320]. Наконец, компания Lockheed Martin опубликовала документ *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, авторами которого были Эрик Хатчинс, Майкл Клопперт и Рохан Амин [115]. Именно эта работа послужила символическим выстрелом из стартового пистолета для написания данной главы. В общем, год оказался чрезвычайно насыщенным.

Публикация документа Lockheed Martin вызвала настоящий сейсмический сдвиг в представлениях о киберзащите. До его выхода большинство сете-

вых защитников придерживалось таких моделей, как *защита периметра* и *эшелонированная защита* (см. главу 3). В то время мы искали способы сдерживания наступательных технических средств, таких как вредоносное ПО, эксплойты нулевого дня и небезопасные URL-ссылки. Тогда считалось, что для достижения успеха злоумышленнику достаточно сделать все правильно, например использовать эксплойт нулевого дня, лишь один раз, а защитник должен действовать безошибочно все время, то есть обеспечивать защиту от всех возможных эксплойтов нулевого дня. Именно поэтому сетевые защитники в те времена (а некоторые и сегодня) старались внести все возможные исправления во все системы. Однако работа, опубликованная компанией Lockheed Martin, перевернула эту идею с ног на голову. Ее авторы продемонстрировали, что для достижения успеха злоумышленнику необходимо правильно выполнить целую последовательность действий. Защитнику же достаточно нарушить эту последовательность на любом из этапов этой убийственной цепочки.

Ключевая идея данной статьи заключается в том, что сетевым защитникам не следует концентрироваться на таких пассивных вопросах кибергигиены, как внесение исправлений и защита от известных киберугроз. По мнению исследователей из Lockheed Martin, не менее важно активное развертывание средств предотвращения всех известных киберкампаний. Другими словами, защита периметра представляет собой универсальную оборонительную стратегию, аналогичную запиранию дверей и окон в доме. Развернутые средства защиты не являются специфическими для какого-либо из известных методов атаки. Они работают против всех преступников. Однако согласно концепции убийственной цепочки сетевым защитникам следует целенаправленно противодействовать известному поведению противника. Если вы знаете, что в вашем районе орудует дикая банда Буча Кэссиди, которая обычно использует собачий лаз для проникновения в дом, то можете предусмотреть дополнительную защиту лаза, чтобы противостоять атаке, характерной для этой шайки.

По мнению авторов документа, посвященного концепции убийственной цепочки, «методы защиты сети, опирающиеся на знания о противниках, могут создать петлю обратной связи, позволяющую защитникам достичь такого информационного превосходства, которое будет снижать вероятность успеха противника при каждой последующей попытке вторжения». Обратите внимание на слова «снижать вероятность успеха противника». Они прекрасно согласуются с нашей стратегией, базирующейся на первичном принципе кибербезопасности и заключающейся в снижении

вероятности существенного ущерба вследствие киберинцидента. Согласно этому документу, «защита компьютерных сетей на основе разведданных — это стратегия управления рисками, которая... требует нового понимания самих вторжений не как единичных событий, а скорее как последовательностей действий». Иными словами, эта простая и элегантная стратегия формулируется так: знай своего врага.

Модель убийственной цепочки

Концептуально документ Lockheed Martin разбивает кампанию противника на несколько этапов или звеньев цепи (рис. 4.1), таких как:

- *разведка (reconnaissance)* — исследование, идентификация и выбор целей;
- *вооружение (weaponization)* — создание инструментов для реализации атаки на выбранные цели;
- *доставка (delivery)* — перенос разработанных средств в целевую среду;
- *эксплуатация (exploitation)* — запуск вредоносных средств;
- *инсталляция (installation)* — установка средств для закрепления в атакованной среде;
- *получение контроля (command and control, C2)* — налаживание связи с внешним миром;
- *выполнение действий (actions on objectives)* — перемещение внутри сети и кража данных.

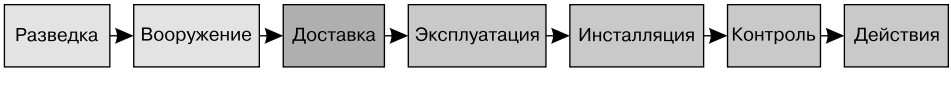


Рис. 4.1. Последовательность реализации атаки из оригинальной статьи 2010 года

Рассматривайте каждое звено этой цепи в качестве возможности сорвать известную хакерскую кампанию. Например, известная последовательность атаки, которую многие сетевые защитники регулярно наблюдали в 2010-х годах, носит название Fancy Bear («Модный медведь»). (Об именовании противников я расскажу чуть позже в этой главе.)

Если мы хотим защититься от кампании Fancy Bear, то должны разработать и внедрить специальные средства контроля, позволяющие противостоять тому, как реализующие ее хакеры изучают слабые места жертв, вредоносному ПО, которое они создают и развертывают (то есть их вооружению), методам доставки этого вредоносного ПО жертвам, коду эксплуатации, который они используют для компрометации нулевой жертвы, процессу загрузки и установки дополнительных инструментов, помогающих им в достижении цели, а также средства для блокировки их канала связи и предотвращения их перемещения по сети жертвы в поисках данных, которые они намерены украсть или уничтожить. (О том, где искать такие средства контроля, я расскажу далее в этой главе.)

И вот в чем заключается гениальность идеи убийственной цепочки Lockheed Martin. На момент написания данной книги база знаний MITRE ATT&CK Framework (см. одноименный раздел далее в главе) отслеживала около 90 методов, используемых в рамках типичной кампании Fancy Bear. Предположим, что хакеры из этой группировки разработали новый эксплойт нулевого дня и начали применять его на этапе эксплуатации. Поскольку эксплойт нулевого дня новый, ни один защитник не обладает уже развернутыми средствами, позволяющими ему противодействовать. Но если защитники уже развернули средства предотвращения и обнаружения для остальных 90 методов или хотя бы для некоторых из них, то разработка нового эксплойта хакерам ничего не даст, так как цепочка будет разорвана. Из-за нарушения последовательности действий кампания Fancy Bear не сработает даже с новым эксплойтом нулевого дня.

В то время как защита периметра и эшелонированная защита являются пассивными стратегиями, предназначенными для противодействия типичному хакеру, стратегия предотвращения реализации убийственной цепочки вторжения активная и нацелена на поражение конкретных киберпротивников. Главная идея авторов документа, посвященного данной концепции, заключается в том, что вне зависимости от мотивации противников (будь то преступная деятельность, шпионаж, развязывание войн или низкоуровневых киберконфликтов, хактивизм, пропаганда или простое вредительство) и инструментов, которые они используют для достижения своих целей (вредоносное ПО, код эксплойта, фишинг и пр.), всем им приходится произвести целый ряд действий для выполнения своей миссии (рис. 4.2). Они называют такие последовательности *атакующими кампаниями* (attack campaign). Сегодня в зависимости от сложности и зрелости кампания может включать в себя и 30 этапов, и 300, и более.

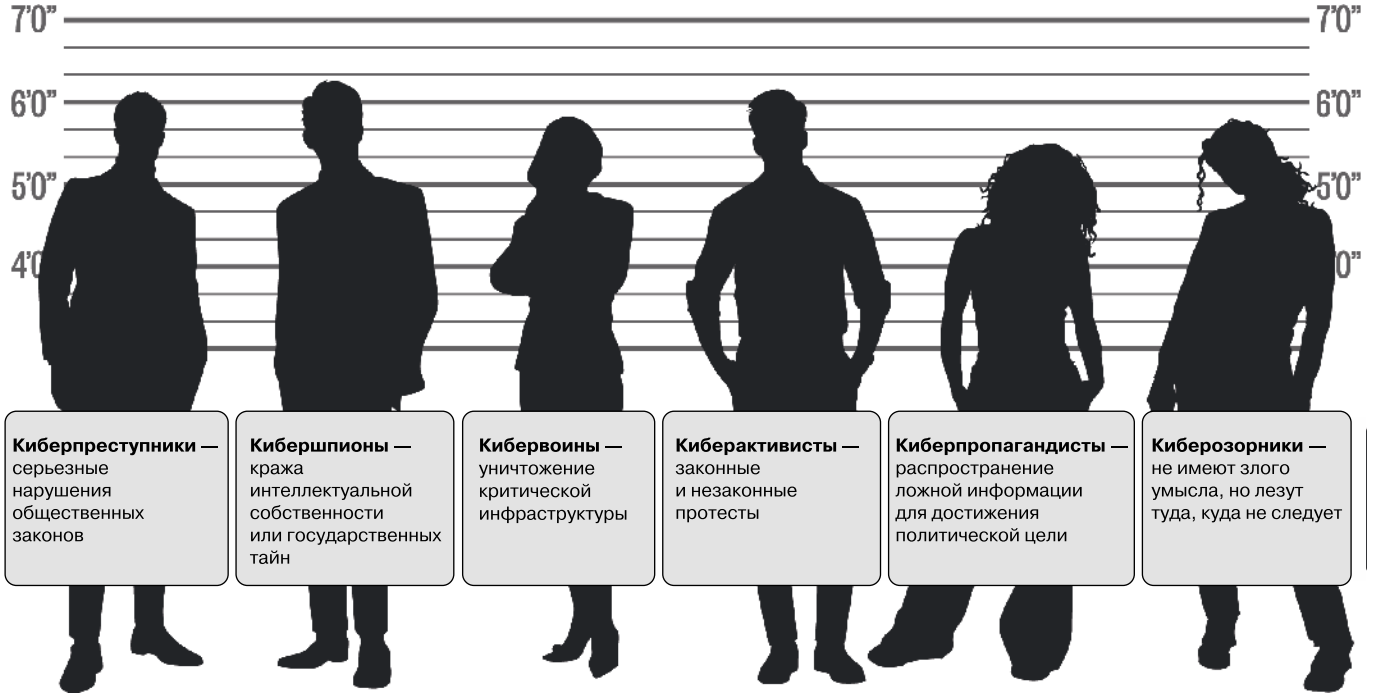


Рис. 4.2. Необычные подозреваемые: мотивы киберпротивников (модифицированный и обновленный вариант диаграммы, созданной компанией BAE Systems [291])

С 2013 по 2019 год я возглавлял отдел информационной безопасности компании Palo Alto Networks. В то время я только начал увлекаться концепцией убийственной цепочки. Как и многих других CSO и CISO, меня приглашали выступать на различных конференциях по всему миру, на которых я с упоением рассказывал о том, как мы используем продукты Palo Alto Networks для реализации своей внутренней стратегии предотвращения вторжений, основанной на этой концепции. Однако наши юристы быстро поставили на этом крест. Оказалось, что руководство Lockheed Martin осознало революционность своей идеи и решило закрепить авторство. В 2012 году они подали заявку на регистрацию в качестве товарного знака фразы CYBER KILL CHAIN («убийственная цепочка»), которую Патентное ведомство США удовлетворило в 2019 году. А до этого момента компания Lockheed Martin запретила любое публичное использование этого словосочетания без упоминания о процессе получения патента. Другими словами, поставщики систем безопасности не могли обсуждать новую интересную идею, не указывая на одного из своих потенциальных конкурентов. Поэтому они этого и не делали. Маркетинговые команды производителей систем безопасности, включая Palo Alto Networks, создавали собственные, слегка отличающиеся друг от друга версии с едва заметными изменениями формулировок, в результате чего изначальная идея распалась на мелкие кусочки, не имеющие достаточного веса. В итоге вместо всеобщего обсуждения новой революционной концепции идея убийственной цепочки затерялась в шуме. Постепенно индустрия преодолела свой страх перед признанием заслуг компании Lockheed Martin, но на это ушли годы.

Мотивация противника: преобразование кибервойны в низкоуровневый киберконфликт

Здесь я хочу сделать небольшое отступление, чтобы обсудить эволюцию взглядов сообщества на кибервойны. Это именно отступление, поскольку тема кибервойн напрямую не связана со стратегией предотвращения реализации убийственной цепочки вторжения. Тема кибервойны связана скорее с тем, как различные государства и другие международные акторы применяют концепцию убийственной цепочки для достижения тех или иных политических целей. Сами тактики ее использования значительно изменились с начала 2000-х годов.

Раньше специалисты по кибербезопасности считали возможным ведение войны исключительно в киберпространстве, полагая, что враждующие государства будут устраивать массированные кибератаки, не задействуя физические средства, такие как истребители, бомбардировщики, авианосцы, артиллерия, танки и пехота. Изначально я и сам так думал. Но эта теория потеряла свою популярность, когда все поняли, что она сродни вере в возможность ведения войны одной лишь артиллерией. Рассмотрев эту идею в таком контексте, мы осознали, насколько безумной она была. Мы поняли, что противодействующие стороны будут использовать наступательные кибероперации в качестве поддержки более масштабной боевой миссии, что в ходе войны кибероперации будут применяться в сочетании со всеми остальными боевыми средствами для достижения определенной цели.

Однако вскоре некоторые государства осознали, что они могут добиваться некоторых политических целей на международной арене, проводя наступательные кибероперации, не дотягивающие до настоящей войны. Другими словами, они могут добиться многого с помощью кибероперациий, подходя вплотную, но не переходя ту черту, за которой государство-жертва будет вынуждено начать войну в физическом пространстве с использованием своих вооруженных сил. Таким образом можно было уравнять шансы богатых и бедных государств на успешное проведение определенных операций.

Китайские военные отстаивали концепцию асимметричной войны в 1990-х годах [146, 179], а русские опубликовали аналогичную военную доктрину в начале 2010-х годов [91]. Граница между приемлемыми кибероперациями (кампаниями, не приводящими к началу реальной войны) и неприемлемыми (теми, которые приводят к началу такой войны) несколько размыта. До сегодняшнего дня ни одна киберкампания не стала причиной реальной войны, поэтому различные государства продолжают сдвигать границы, тщательно просчитывая, что допустимо, а что — нет.

Пожалуй, наиболее известными примерами в данном случае являются совместная операция США и Израиля под названием Operation Olympic Games (Stuxnet) 2010 года и российские атаки на Украину, произошедшие в 2014 году (NotPetya, Sandworm). Результатом этих двух печально известных кибератак стало разрушение физической инфраструктуры — типичной цели традиционных вооруженных сил. Однако государства-жертвы не стали применять в ответ традиционные военные средства. Эти кибератаки не спровоцировали начало реальной войны.

Такие государства, как Индия, Иран, Северная Корея, Пакистан, Вьетнам и некоторые другие, проводят асимметричные кибероперации настолько

часто, что известный журналист Дэвид Сэнгер окрестил их *непрерывными низкоуровневыми киберконфликтами* [194]. Несмотря на громоздкость этого выражения, оно довольно точно описывает то, что происходит в действительности.

Непрерывный низкоуровневый киберконфликт включает в себя множество киберкампаний по всей убийственной цепочке, направленных на достижение различных целей, в том числе традиционный шпионаж (кража государственных секретов), промышленный шпионаж (кража интеллектуальной собственности), разрушение критической инфраструктуры, операции влияния и т. д. У нас нет кибервойны в том виде, в котором мы ее представляли в начале 2000-х годов, но каждый год общественность узнает о международных субъектах, проводящих киберкампании в рамках непрерывных низкоуровневых киберконфликтов для достижения тех или иных политических целей.

Убийственная цепочка Lockheed Martin — это здорово, но...

Как я уже говорил, концепция убийственной цепочки Lockheed Martin представляет собой новаторскую идею, побудившую отрасль переосмыслить способы защиты предприятия. Это хорошая новость. Плохая новость заключается в том, что, несмотря на все достоинства, в этой концептуальной модели отсутствует такой важный аспект, как операции. Оригинальный документ содержит слишком мало подробностей о том, как реализовать эту концепцию на практике. Такие действия, как сбор разведданных о тактиках противника, их анализ, принятие взвешенных решений относительно противодействия противнику и развертывание плана по минимизации ущерба, оставлены на усмотрение читателя. Однако это придирки, поскольку статья этого и не обещала. Авторы заставили отрасль пересмотреть общепринятую лучшую практику, предложив стратегию, которая лучше подходит для предотвращения нанесения существенного ущерба нашим организациям. Пустоту в области оперативных аспектов предстояло заполнить другим крупным мыслителям.

Наш основополагающий принцип заключается в снижении вероятности нанесения организации существенного ущерба вследствие киберинцидента. Мы можем целыми днями заниматься блокировкой технических средств и, вероятно, добьемся определенного эффекта. Но если решим победить людей, которые стоят за этими инструментами, то результат

может оказаться гораздо более значительным. Вместо того чтобы блокировать отдельные инструменты в отрыве от стоящих за ними хакеров, мы должны блокировать каждый инструмент, используемый злоумышленниками на каждом этапе убийственной цепочки. В рамках стратегии предотвращения реализации убийственной цепочки мы разрабатываем защитные кампании, направленные на то, чтобы помешать конкретной хакерской группировке достичь поставленной цели, а не на поражение используемых ею средств.

Модели убийственной цепочки

В плейбуке (сценарии или наборе действий) противника содержатся все известные данные о последовательности атак хакерской группы, включая тактики, техники, индикаторы компрометации, временные рамки атаки, контекст, касающийся мотивации и атрибуции.

В работе *Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks*, которую мы с моим давним коллегой Райаном Олсоном опубликовали в 2020 году, была представлена стандартная схема, призванная облегчить задачу сбора разведданных и обмена ими с другими сетевыми защитниками [113]. Она упрощает им процесс написания кода для систематического усвоения этой информации и предоставляет средства для автоматического развертывания новых и обновленных средств защиты с целью укрепления уже существующей оборонительной позиции в рамках инфраструктуры DevSecOps.

В качестве лучших инструментов для моделирования разведданных при создании плейбуков противника были выбраны следующие три:

- парадигма kill chain, разработанная компанией Lockheed Martin;
- фреймворк ATT&CK компании MITRE [299];
- модель Diamond Министерства обороны США [39].

Когда в сообществе говорят о плейбуках противника, возникает ощущение, что все эти модели представляют собой разные подходы к одному и тому же. Но это не так. Одна из них представляет собой документ с описанием стратегии (Lockheed Martin), другая — схему оперативных защитных действий (MITRE), а третья — методологию для групп киберразведки (Diamond). Для создания плейбуков противника нельзя выбирать какую-то одну модель, поскольку все они работают в связке друг с другом. Если метафорой

для предотвращения успеха киберпротивников является слон, то каждая из этих моделей представляет собой различные его части. Давайте рассмотрим их все по очереди.

Фреймворк MITRE ATT&CK

Компания MITRE выпустила первую версию фреймворка ATT&CK в 2013 году, через три года после публикации оригинального документа компании Lockheed Martin. Данная аббревиатура расшифровывается как adversarial tactics, techniques, and common knowledge («тактики, техники и общеизвестные факты о злоумышленниках»). На первый взгляд может показаться, что этот фреймворк является небольшим улучшением оригинальной модели Lockheed Martin. Он расширяет исходные этапы и корректирует некоторые ограничения, а также исключает этап разведки и содержит более четкое и подробное описание действий на этапе достижения цели. Все это действительно так.

Существенным его новшеством стало расширение списка требований к информации, собираемой специалистами по разведке для плейбуков противников. В него были добавлены тактики, техники и процедуры (ТТП) (tactics, techniques, procedures, TTP). До появления этого фреймворка мы собирали индикаторы компрометации, в частности плохие IP- или URL-адреса, не связывая их с известным поведением противника. Это были просто списки плохих вещей. Сами по себе эти списки не абсолютно бесполезны, но они эфемерны, и хакеры могут легко изменить свое поведение в любой момент задолго до того, как службы информационной безопасности введут контрмеры.

Расширение модели убийственной цепочки, разработанное компанией MITRE, предполагает группировку тактик («почему»), используемых техник («как») и конкретных процедур, проводимых противником для реализации своей тактики («что»). Такая информация уже не столь эфемерна, привязана к известному поведению конкретного противника и позволяет разрабатывать эффективные контрмеры. Если модель убийственной цепочки Lockheed Martin концептуальная, то модель MITRE ATT&CK оперативная. Сетевые защитники могут использовать предоставленные ТТП для выявления и предотвращения реализации наблюдавшихся ранее киберкампаний.

Организация MITRE делится с общественностью данными, собранными собственными группами, а также синтезирует информацию, полученную

от членов оборонной промышленной базы (Defense Industrial Base, DIB). По данным Агентства кибербезопасности и защиты инфраструктуры США (CISA), DIB представляет собой всемирный промышленный комплекс, включающий более 100 тыс. компаний и их субподрядчиков, которые поставляют товары и услуги американским вооруженным силам. Все они являются основными мишенями для кибероперациий, проводимых различными государствами. Группы разведки MITRE обрабатывают информацию, собранную компаниями, входящими в DIB, публикуют ее в общедоступной базе знаний ATT&CK, после чего ею может воспользоваться любой желающий.

Несмотря на то что данная база знаний отслеживает деятельность нескольких преступных групп, основное внимание уделяется не этому, а тому, как группы, реализующие продолжительные атаки повышенной сложности (advanced persistent threat, APT), отыгрывают собственные сценарии. Другими словами, речь идет об отслеживании действий различных государств. Однако самое главное заключается в том, что данный фреймворк стандартизирует словарь таксономии, которым пользуются сетевые защитники для описания как наступательных, так и оборонительных мероприятий. До появления этого фреймворка каждый поставщик и правительственная организация пользовались собственным языком, поэтому собранные ими разведданные не могли быть переданы другим людям без их трудоемкого преобразования. Мы все наблюдали за одной и той же деятельностью, но не могли осмысленно обсуждать ее всем коллективом. Фреймворк MITRE ATT&CK исправил эту ситуацию, став в итоге фактическим отраслевым стандартом представления разведданных о сценариях действий противника. Другими словами, он помог нам разделить процесс разведки киберугроз на операции.

Тем не менее впереди еще много работы. Пользователям базы знаний ATT&CK необходимо автоматизировать процесс сбора данных и их использования для повышения уровня внутренней защиты. Они также могут оптимизировать процесс применения этих данных «красными» командами и командами, осуществляющими тестирование на проникновение. Наконец, сбор и распространение информации компанией MITRE происходит не в режиме реального времени. Она обновляет базу знаний лишь раз в несколько месяцев. Однако, поскольку злоумышленники не очень часто вносят изменения в свои последовательности атак, в настоящее время это не является серьезной проблемой.

Разработка атакующих кампаний, направленных против нескольких операционных систем и регулярно обходящих средства, составляющие стек без-

опасности, — это дело непростое и недешевое. Как правило, злоумышленники не отказываются от целых последовательностей атак при необходимости внести какие-то изменения. Если один из элементов последовательности перестает работать или нуждается в обновлении, они меняют этот элемент, а не всю последовательность. Такой подход более экономичен. Да им и не приходилось прибегать к другим методам. Большинство сетевых защитников пытаются справиться с отдельными инструментами безотносительно к последовательности действий, которые противник обычно выполняет для достижения успеха. Прелесть философии убийственной цепочки заключается в том, что при развертывании защитных механизмов, предназначенных для поражения противника, а не отдельных не связанных между собой инструментов мы имеем множество средств предотвращения и обнаружения, направленных на выявление известных специфических действий злоумышленников. Если противник изменит что-то в своей последовательности действий для обхода одного из этих средств, ему придется обойти и все остальные. Поэтому то, что MITRE не обновляет свою базу знаний в режиме реального времени, не становится препятствием. Тем не менее было бы здорово, если бы у всех сетевых защитников появился открытый источник информации о сценариях действий противника, которая бы регулярно обновлялась, автоматически потреблялась, обрабатывалась, подстраивалась под средства обнаружения и предотвращения в имеющемся стеке безопасности, а также автоматически применялась в режиме реального времени (см. главу 7).

Наконец, было бы здорово, если бы, помимо хакерских кампаний, проводимых государственными структурами, организация MITRE отслеживала также действия обычных преступников (criminals), активистов (activists) и простых озорников (mischief makers). Назовем их CAMM-кампаниями. База знаний MITRE ATT&CK практически не содержит информации о них. И на данный момент аналога базы MITRE ATT&CK для CAMM-кампаний не существует. Вы можете приобрести соответствующие сведения у коммерческих компаний, занимающихся киберразведкой, но эквивалентного открытого источника не найдете.

Тем не менее с 2010 года мы проделали большой путь. Исследовательская группа Lockheed Martin предложила нам новую стратегию, а организация MITRE помогла реализовать ее на практике. Остается решить задачу сбора достаточно точной информации о сценариях действий злоумышленников. Другими словами, нам нужно формализовать этот процесс, чтобы все группы киберразведки использовали одни и те же базовые процедуры и могли легко обмениваться собранными данными с коллегами. В этом нам может помочь модель Diamond.

Модель Diamond Министерства обороны США

Примерно тогда же, когда исследовательская группа из Lockheed Martin разрабатывала модель убийственной цепочки (2006 год), трое исследователей, работавших на Министерство обороны США, приблизились к аналогичным выводам, но в несколько ином контексте. Они пытались создать формальный математический метод разведки киберугроз, который можно было бы применить к «теории игр, графов и классификации/кластеризации для улучшения процесса анализа и принятия решений».

Как и исследователи из Lockheed Martin, авторы модели Diamond придерживались образа мышления, базирующегося на основополагающем принципе кибербезопасности. Они задались вопросом: «Что является основным атомарным элементом любой активности, направленной на вторжение?» К моменту публикации революционной статьи *The Diamond Model of Intrusion Analysis* [20] в 2011 году Серджио Кальтаджироне, Эндрю Пендергаст и Кристофер Бетц уже знали ответ на этот вопрос, который они назвали *событием*, состоящим из четырех основных компонентов, расположенных в вершинах ромба (рис. 4.3). В 2019 году Пендергаст, на тот момент работавший в коммерческой аналитической компании (ThreatConnect), представил диаграмму с дополнительной вертикальной линией, соединяющей верхнюю и нижнюю вершины [20].

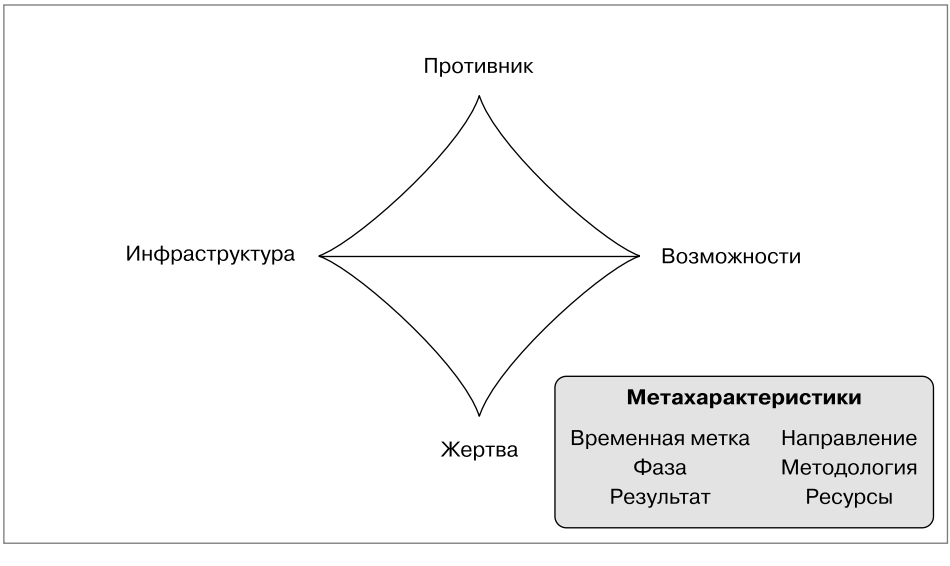


Рис. 4.3. Исходная модель Diamond из работы 2011 года

В статье говорилось: «Основные характеристики связаны между собой ребрами, отражающими фундаментальные взаимосвязи между этими характеристиками, которые могут использоваться аналитически для дальнейшего обнаружения и развития знания о вредоносной деятельности». Другими словами, противники (верхняя вершина) развивают атакующие возможности (правая вершина) и применяют их для эксплуатации инфраструктуры (левая вершина). Кроме того, противники (верхняя вершина) создают и поддерживают собственную инфраструктуру (левая вершина). Жертвы (нижняя вершина) создают и поддерживают инфраструктуру (левая вершина) и являются точкой приложения атакующих возможностей (правая вершина). Наконец, противники (верхняя вершина) эксплуатируют жертв (нижняя вершина). Суть заключается в том, что при описании киберинцидентов группы разведки заполняют пробелы в этих парах связей. Как отмечается в документе, «это позволяет представить весь объем знаний, не ограничиваясь наблюдаемыми индикаторами активности» [20].

Авторы пересмотрели так называемые *деревья атак*, концепция которых была предложена Брюсом Шнайером, лауреатом премии Cybersecurity Canon Lifetime Achievement и моим первым начальником в гражданском мире после ухода в отставку из армии США. Идея Шнайера заключалась в том, что графы атак «призваны отразить все возможные пути атаки и уязвимости для заданного набора защищаемых ресурсов, чтобы определить наиболее экономически эффективный способ обороны и наибольшую степень защиты» [20]. Это потрясающая идея, но в то время она плохо поддавалась масштабированию. Количество перестановок росло в геометрической прогрессии. Попытка авторов модели Diamond формализовать язык описания киберинцидентов стала первым шагом к улучшению ситуации. В рамках своей модели они строят «потоки активности», которые сводят воедино разведданные и традиционные графы атак в графы активности — атаки путем объединения «традиционного анализа уязвимостей со знаниями об активности противника» [20]. Именно это отчетливо демонстрирует то, что модель Diamond не альтернатива модели убийственной цепочки Lockheed Martin и фреймворка MITRE ATT&CK, а их усовершенствование. Атомарный элемент модели Diamond — событие, обладающее четырьмя основными характеристиками, — присутствует на каждом этапе убийственной цепочки (рис. 4.4).

В документе, посвященном модели Diamond, говорится: «Убийственная цепочка представляет собой высокоэффективную и влиятельную модель операций противника, на основе которой принимаются решения, направленные на предотвращение вторжений. Наша модель интегрирует этот поэтапный подход и дополняет анализ убийственной цепочки, расширяя перспективу,

что обеспечивает необходимую детализацию и выражение сложных взаимосвязей между действиями злоумышленника в ходе вторжения» [20].

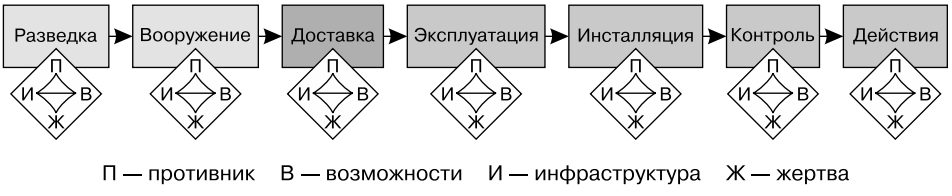


Рис. 4.4. Модель Diamond, наложенная на модель убийственной цепочки

На практике ваша разведгруппа может анализировать несколько инцидентов, как связанных, так и не связанных друг с другом. Используя стратегию Lockheed Martin, вы отслеживаете активность противника на всех этапах убийственной цепочки, реализуемой в рамках каждого из инцидентов. Вы собираете разведданные, заполняя пробелы в четырех парах характеристик (события) из модели Diamond, и стандартизируете язык описания тактик, техник и процедур с помощью словаря, предлагаемого фреймворком MITRE. Со временем ваши знания об убийственной цепочке противника становятся все более полными, обогащаясь данными обо всех инцидентах.

В определенный момент можно заметить, что события модели Diamond, случающиеся на этапах доставки и контроля в рамках инцидента 1, удивительным образом напоминают события, зафиксированные в ходе инцидента 2. Эти потоки активности, связывающие два инцидента, могут указывать на то, что атаки осуществляются одним и тем же противником и свидетельствуют о гораздо более масштабной кампании, направленной против вашей сети. В статье сказано: «События модели Diamond могут быть соотнесены с потоками активности для выявления кампаний противника, а также объединены в группы активности для выявления событий и угроз, имеющих общие черты». Результатом именно этого процесса становятся громкие заголовки новостей о кибербезопасности наподобие следующих:

- «Китайские хакеры из группировки APT10 используют эксплойты Zerologon для атаки на японские организации»;
- «Группировка Ferocious Kitten: шестилетняя слежка в Иране»;
- «За атаками на европейские объекты в 2019 году может стоять группировка Lazarus Group».

Когда группы разведки более или менее уверены в том, что они наблюдают схожие потоки активности в ходе нескольких инцидентов, обращенных

на одну и ту же жертву или описанных в других потоках активности, направленных против других жертв, они присваивают группе красочное название — своего рода ярлык для читателей новостей и разведывательных отчетов, указывающий на то, что все эти данные связаны между собой.

Некоторые соображения по поводу атрибуции

Названия берутся из разных источников. Поставщики систем безопасности придумывают большую часть имен, публикуя в блогах описания того, что они обнаружили с помощью своих продуктов и сервисов. Одна из причин выбора броских названий заключается в стремлении привлечь внимание участников рынка. Некоторые поставщики стали известны благодаря своим схемам именования.

- Компания Mandiant использует цифры, как в случае APT1.
- Компания Crowdstrike применяет названия животных, например Fancy Bear («Модный медведь»).
- Компания Microsoft использует в названиях химические элементы, например гафний.

Существует и множество других схем. Правительственные группы реагирования на инциденты компьютерной безопасности (CERT) и правоохранительные органы по всему миру тоже публикуют разведывательные отчеты. Большинство из них хоть и интересны, но не особенно полезны с оперативной точки зрения. Аналитики публикуют их в блогах, что заставляет читателя потратить время на вычленение наиболее важных фрагментов информации. Хотя многие поставщики и правительственные аналитики стараются использовать стандартизированную лексику, предлагаемую фреймворком MITRE ATT&CK, они еще не полностью приняли концепцию убийственной цепочки и по большому счету игнорируют модель Diamond.

Одна из возможных причин нежелания принимать эти модели заключается в том, что не все организации нуждаются в одинаковых разведывательных отчетах. Чуть позже я подробно расскажу о разведке киберугроз, а пока имейте в виду то, что вид необходимых разведывательных отчетов зависит от характера организации. Правоохранительным органам, правительственным шпионским агентствам, военным, коммерческим и научным организациям требуются разные виды разведданных. Правоохранительные органы стремятся задержать преступников, шпионские агентства преследуют национальные политические интересы, военные ищут наземные цели,

а коммерческие и научные организации пытаются предотвратить существенный ущерб от киберинцидентов.

В базе знаний MITRE ATT&CK можно найти информацию о таких известных хакерских кампаниях, освещавшихся в новостях, как APT1, Lazarus Group и Sandworm. Есть и другие менее известные кампании с интересными кодовыми названиями: Ferocious Kitten, Nomadic Octopus и Wizard Spider. Особенность этих кодовых названий заключается в том, что они не атрибутируют конкретные группы реальных киберзлодеев, которые стоят за активностью, например Nomadic Octopus. Мы используем названия группировок для обозначения неоднократно наблюдавшихся уникальных моделей поведения противника на разных этапах убийственной цепочки.

Я имею в виду, что, когда в базе MITRE ATT&CK публикуются сведения об активности Ferocious Kitten, они обычно не содержат информации о том, что за этими атаками стоит хакер по имени Кевин, днем работающий зазывалой в Walmart. В этой базе описывается лишь набор наблюдаемых в реальных условиях техник и специфических процедур, которые аналитики сгруппировали в единый плейбук противника.

Иногда аналитики спецслужб могут с уверенностью связать паттерны активности, например APT1, с конкретными правительствами или CAMM-группировками. В случае с APT1 компания Mandiant, поставщик средств обеспечения безопасности, фактически взломала компьютер одного из злоумышленников, получила доступ к его камере и наблюдала за работой хакеров в режиме реального времени [150]. Вы можете просмотреть некоторые из таких видео на YouTube. После той операции аналитики Mandiant могли с большой долей уверенности сказать, что хакеры, реализовавшие кампанию APT1, состоят в китайской военной хакерской группе, входящей во 2-е бюро Народно-освободительной армии, известное как подразделение 61398. Однако подобная атрибуция является скорее исключением из правил, когда речь идет о коммерческом пространстве. В отношении остальных групп, таких как Nomadic Octopus, у аналитиков могут быть некоторые подозрения, например, на то, что данная группировка действует из России, но они редко имеют столь же неопровержимые доказательства, как в случае с APT1.

Дело в том, что для большинства из нас не имеет значения, какое именно правительство стоит за атаками. Если вы знаете, что на вас нападает Северная Корея, что это меняет? Если вы не работаете в шпионской организации, занимающейся агентурной разведкой, или в правоохранительных органах,

стремящихся предъявить обвинение конкретным людям, это знание ничем вам не поможет. Вам важно убедиться лишь в том, что в случае выявления в вашей сети паттернов атак, характерных для Lazarus Group, ваша команда развернула необходимые средства, позволяющие защититься от них на каждом этапе убийственной цепочки.

Еще более запутанной ситуацию с кодовыми названиями делает отсутствие отраслевого стандарта именования паттернов атак. Каждый производитель и каждая государственная спецслужба пользуется собственной системой. В некоторых случаях мы получаем множество названий для одних и тех же паттернов. Например, организация MITRE присвоила название APT29 одной из отслеживаемых ею группировок. Но в ходе простого поиска в Google я обнаружил 14 названий, которые другие организации используют для описания той же самой активности, в частности Cozy Bear, the Dukes и Office Monkeys.

Кроме того, в новостях и разведывательных сводках можно прочитать о том, что группировка Cozy Bear связана с российской Службой внешней разведки (СВР, ранее КГБ). Однако мы никак не можем это проверить, поскольку отслеживаем сетевой трафик, а не действия конкретных людей в реальном мире. Правительственные шпионские агентства могут атрибутировать активность на этом уровне, но они вряд ли скажут вам, что им известно, за исключением некоторых особых случаев. Чаще всего они стараются защитить свои источники и методы.

Подобная атрибуция может объясняться тем, что какая-то другая разведгруппа в прошлом связала группу Cozy Bear с СВР и эта информация была просто включена в новый отчет, который вы читаете, без указания источника. Таким образом, большинство атрибуций, содержащихся в публичных разведывательных отчетах, не подкреплены убедительными доказательствами.

В то же время степень уверенности в наличии связи между Cozy Bear и определенными ТТП, перечисленными в базе знаний MITRE ATT&CK, довольно высока, что приводит к путанице. Публичные команды киберразведки, особенно работающие в компаниях — поставщиках защитных средств, продукты которых развернуты по всему миру и собирают телеметрические показатели безопасности 24 часа в сутки семь дней в неделю, могут точно определить последовательность атаки Cozy Bear в сетях своих клиентов. Благодаря уверенности в отношении ТТП при упоминании связи Cozy Bear с российской СВР читатели воспринимают оба утверждения как одинаково точные.

Короче говоря, не зацикливайтесь на названиях и атрибуции. Если не считать возможности посмеяться на совещании, сказав что-то вроде: «По нашим данным, группировка Office Monkeys (“Офисные обезьянки”) атаковала наших конкурентов с помощью вредоносного ПО BananaPeel (“Банановая кожура”)» (название не имеет значения). Когда я говорю об атрибуции ТТП, то стараюсь избежать путаницы, используя выражения наподобие: «Плейбук противника, связанный с последовательностью атак Cozy Bear». Я стараюсь не говорить: «Хакерская группировка под названием Cozy Bear». Это тонкое различие, но его стоит усвоить, чтобы избежать недоразумений.

Количество плейбуков активных противников

Рассказывая о плейбуках противников и предотвращении реализации убийственных цепочек вторжения в ходе своих выступлений на конференциях, я обычно делаю паузу и задаю аудитории вопрос: «Сколько активных сценариев действий противников реализуется в Интернете в любой момент времени? Другими словами, сколько кампаний проводят хакеры прямо сейчас?» Большинство присутствующих не имеет об этом ни малейшего представления, поэтому я начинаю задавать наводящие вопросы. «Кто из вас считает, что их больше миллиона?» — обычно после этого руки поднимает примерно половина аудитории. «А кто думает, что больше 1000?» — поднимается еще больше рук. «А сколько из вас полагают, что их меньше 1000?» — многие опускают руки. «Кто думает, что меньше 500?» — после этого вопроса поднятыми, как правило, остается всего лишь пара рук. «А что, если я скажу вам, что их количество, скорее всего, находится в диапазоне от 231 до 281?» — за этим обычно следует ошеломленное молчание.

На момент написания данной книги база знаний MITRE ATT&CK отслеживала около 125 кампаний, реализуемых различными государствами, на всех этапах убийственной цепочки. Другими словами, аналитики MITRE располагали сведениями о ТТП из 125 плейбуков противника. Предположим, что сколько-то сценариев, скажем 25 %, еще не было обнаружено. Это еще примерно 31 кампания, итого 156. А как быть с CAMM-кампаниями, которые MITRE не отслеживает? Если просто подсчитать число CAMM-кампаний, освещавшихся в СМИ в 2021 и 2022 годах, то окажется, что около

80 группировок постоянно проводят операции. Допустим, что 25 % таких кампаний не освещалось в новостях в последние два года. Тогда их число увеличится примерно до 100.

Это означает, что общее количество кампаний противников (к которым относятся разные государства и CAMM-группировки), реализуемых в Интернете в любой день, составляет примерно 256. Расчеты приблизительные (см. главу 6), так что это не точный показатель, а лишь результат обоснованного предположения. Если добавим 10%-ную погрешность для получения диапазона, то я готов поставить 100 долларов на то, что число активных кампаний в Интернете в любой день составляет от 231 до 281.

Эта цифра не кажется большой, не правда ли? Читая новости, легко прийти к мысли, что в мире действуют миллионы киберзлоумышленников. Складывается впечатление, будто каждый день происходит какая-то новая апокалиптическая атака. Из-за частоты публикации таких новостей их количество может показаться пугающе огромным и не поддающимся отслеживанию. Но это не так. Их всего около 250. При желании их можно было бы отслеживать в одной электронной таблице. Я не хочу сказать, что сбор информации обо всех известных действиях противников на всех этапах убийственной цепочки, ее обработка с целью создания средств обнаружения и предотвращения атак для стека безопасности и автоматическое развертывание этих средств в рамках инфраструктуры DevSecOps — простая задача. Это не так (см. главу 7). Однако масштаб проблемы гораздо меньше, чем нам кажется.

Три кита киберразведки: концепция убийственной цепочки, база знаний ATT&CK и модель Diamond

Для снижения вероятности нанесения нашей организации существенного ущерба вследствие киберинцидента мы можем использовать такие базирующиеся на первичных принципах кибербезопасности стратегии, как прогнозирование рисков, нулевое доверие, обеспечение устойчивости, автоматизация и предотвращение реализации убийственной цепочки вторжения. Из всех этих стратегий лично мне больше всего нравится последняя. Остальные тоже хороши и необходимы, но они являются пассивными. Их использование сродни употреблению овощей или замене масла в автомобиле. Делать это нужно, но неинтересно. А вот предотвращение реализации убийственной цепочки вторжения — совсем другое дело. Оно напоминает

сражение с противником на ринге. И сообществу сетевых защитников потребовалось более десяти лет для разработки необходимых для этого стратегий, операций и лучших практик киберразведки.

Выдающиеся мыслители из Lockheed Martin (убийственная цепочка), Министерства обороны США (модель Diamond) и организации MITRE (фреймворк ATT&CK) указали нам путь более десяти лет назад. Именно столько времени потребовалось остальным участникам сообщества на то, чтобы разобраться в этих ключевых концепциях. Теперь мы создаем плейбуки противника для автоматического сбора разведданных о фактических действиях злоумышленников на всех этапах убийственной цепочки Lockheed Martin. Мы реализуем этот процесс, используя стандартный словарь для описания тактик, техник и процедур противника, предлагаемый фреймворком MITRE ATT&CK. Мы ставим перед командами киберразведки задачу заполнения пробелов в парах событий, выявления похожих потоков активности в ходе нескольких инцидентов и создания групп активности для описания общих паттернов поведения в рамках модели Diamond. И наконец, автоматизируем процесс развертывания нашего плана по минимизации рисков в стеке безопасности. И во всем этом нам помогают три кита киберразведки: концепция убийственной цепочки, база знаний ATT&CK и модель Diamond.

Развертывание SOC-центров: тактика предотвращения реализации убийственной цепочки вторжения

Идея операционных центров существует уже на протяжении тысячелетий. В книге *A History of Western Technology* Фридрих Клемм утверждает, что эта концепция возникла примерно в 5000 году до н. э. [134]. По его словам, когда организация становится достаточно большой в плане численности сотрудников или количества выполняемых функций, то есть когда одна небольшая команда уже не может делать все, что от нее требуется, руководители создают такие центры для управления рабочим процессом и состоянием различных групп, а также координации их действий. Некоторые организации стали обретать черты современных SOC-центров еще на заре технологической революции — в начале 1900-х годов.

С появлением телефонных сетей в начале 1920-х годов такие телефонные компании, как AT&T, начали создавать специальные бюро управления трафиком для решения проблем с междугородной связью. К началу 1960-х годов

AT&T осуществляла большую часть телефонной коммутации с помощью механических устройств и организовала специальный центр управления сетью (network operations center, NOC). Историки AT&T считают, что этот NOC-центр был первым в своем роде [220]. К 1977 году компания Bell Systems создала первый национальный NOC-центр в Бедминстере, штат Нью-Джерси, который был очень похож на современные NOC. Если кто-то и занимался обеспечением безопасности в те годы, то это были именно операторы NOC-центров.

Американское разведывательное сообщество в 1960-е годы было вынуждено иметь дело со следующими международными инцидентами:

- 1962-й — Карибский кризис;
- 1967-й — Шестидневная арабо-израильская война;
- 1968-й — захват судна U.S.S. Pueblo;
- 1968-й — Пражская весна в Чехословакии;
- 1969-й — кризис, вызванный атакой на самолет-разведчик EC-121.

Агентство национальной безопасности решило, что ему необходим операционный центр для координации своих действий на международном уровне. В 2007 году в ответ на запрос, основанный на законе о свободе информации, АНБ опубликовало документ, в котором было описано создание первого Национального оперативного центра радиоэлектронной разведки (National SIGINT Operations Center, NSOC) в 1973 году [214]. По словам Чарльза Берлина, бывшего директора NSOC, АНБ постепенно расширяло круг его функций, кульминацией чего стало решение сосредоточить наступательные (радиоэлектронная разведка, SIGINT) и оборонительные (коммуникационная безопасность, COMSEC) операции в одном месте. В итоге аббревиатура SIGINT в названии была заменена на Security (безопасность). Так появился Операционный центр национальной безопасности. По словам Берлина, несколько лет спустя, когда возникла потребность обеспечить кибербезопасность, общая задача NSOC-центра стала слишком масштабной, поэтому АНБ создало отдельный Национальный операционный центр противодействия киберугрозам (National Cyber Threat Operations Center, NCTOC) [111]. Однако после постановки задачи обеспечения коммуникационной безопасности деятельность этих операционных центров стала мигрировать в сторону обороны. Сегодня в АНБ существует множество операционных центров, отвечающих за различные компоненты миссии этого ведомства, но NSOC-центр по-прежнему остается краеугольным камнем его деятельности.

Что касается правительственных организаций общего назначения, то после появления червя Морриса [231] (первого разрушительного интернет-червя) Агентство перспективных оборонных исследовательских проектов (Defense Advanced Research Projects Agency, DARPA), научно-техническая организация Министерства обороны США, в 1988 году выделило средства Университету Карнеги — Меллона на создание первого координационного центра реагирования на инциденты компьютерной безопасности (CERT Coordination Center, CERT/CC) [209]. К 1990 году Форум групп реагирования на инциденты информационной безопасности (Forum of Incident Response and Security Teams, FIRST) стал некоммерческой организацией, «объединяющей группы реагирования на инциденты ИБ и обеспечения безопасности из всех стран мира во имя создания безопасного Интернета для всех». По состоянию на 2022 год в сообществе FIRST состояли 657 команд из 101 страны мира [2].

По словам Рича Петиа, директора первого центра CERT/CC, одна из его задач заключалась в том, чтобы помогать военным ведомствам создавать собственные CERT-центры [114]. В 1993 году в ВВС была создана группа реагирования на инциденты компьютерной безопасности AFCERT (Air Force Computer Emergency Response Team) [25]. Вскоре после этого их примеру последовали и другие службы. Работа, проделанная военными CERT-центрами, способствовала созданию в 1998 году Объединенной оперативной группы по защите компьютерной сети (Joint Task Force — Computer Network Defense, JTF-CND) [232]. Создание военных CERT-центров привело к тому, что координация защитных и разведывательных действий в рамках организации (главная задача SOC-центра) начала утверждаться в качестве лучшей практики общего назначения для сетевых защитников, работающих в крупных организациях военного, правительственного, коммерческого и академического профиля.

Что касается коммерческого сектора, то первые поставщики управляемых услуг по обеспечению безопасности (managed security service provider, MSSP) появились в конце 1990-х — начале 2000-х годов. По сути, MSSP — это SOC-центры, предоставляющие услуги на контрактной основе. Президент Клинтон создал систему ISAC (Information Sharing and Analysis Center) — структуру центров анализа и обмена информацией [50]. В феврале 2015-го президент Обама создал структуру организаций, занимающихся анализом информации и обменом ею (Information Sharing and Analysis Organization, ISAO), устранив юридические сложности, чтобы сведениями об угрозах могли обмениваться любые организации, а не только группы, занимающиеся защитой критической инфраструктуры [168].

Организации CERT, ISAC, ISAO и MSSP предоставляют услуги SOC-центра тем, кто не может организовать такой центр самостоятельно, или оказывают дополнительную помощь тем, кто в состоянии это сделать. В какой-то момент между 2002 и 2012 годами начала приобретать популярность идея о том, что сетевые защитники, работающие в коммерческом секторе, должны создавать и эксплуатировать собственные SOC-центры.

Современное состояние центров мониторинга информационной безопасности. Сегодня многие средние и крупные коммерческие организации либо имеют собственные внутренние SOC-центры, либо передают эту функцию (или ее часть) стороннему MSSP. Иногда SOC-центр функционирует наравне с NOC-центром, а иногда является его подразделением.

Небольшие организации обычно рискуют больше и не имеют централизованного пункта для координации действий различных групп. Зачастую вопросами ИТ и безопасности занимается одна и та же небольшая команда. Новейшей разработкой в коммерческом секторе являются услуги SOC-центров, предоставляемые в виде SaaS-приложений, также известные как SOC из коробки.

Однако SOC-центры могут сильно различаться по своей функциональности. Исходя из истории и эволюции операционных концепций, можно подумать, что SOC представляет собой единый центр, координирующий все вопросы, связанные с обеспечением безопасности организации, но это не так. Его функции варьируются от простого мониторинга определенных частей сети без возможности внесения изменений в политику безопасности до полного контроля над стеком безопасности при каждом развертывании данных. Кроме того, SOC-центры отвечают за реагирование на инциденты, с которыми сталкивается организация. Об этой функции мы поговорим в главе 5.

Развертывание SOC-центра — важнейшая основанная на первичном принципе тактика для предотвращения реализации убийственной цепочки вторжения. Ранее в этой главе я привел аргументы в пользу того, что предотвращение реализации убийственной цепочки вторжения — важнейшая стратегия, вытекающая из абсолютного основополагающего принципа кибербезопасности. И точно так же, как управление идентификацией и доступом (IAM) — важнейшая базирующаяся на первичном принципе тактика для реализации стратегии нулевого доверия (поскольку без IAM это сделать невозможно), развертывание SOC-центра или другого подразделения, выполняющего те же функции, — важнейшая тактика для недопущения

реализации убийственной цепочки вторжения. Без него предотвратить вторжение невозможно. Кто-то в организации должен:

- отслеживать информацию о сценариях действий противника (см. текущую главу);
- осуществлять оркестрацию и мониторинг средств внутреннего стека безопасности (см. текущую главу);
- управлять работой группы реагирования на инциденты (см. главу 5);
- разрабатывать и проводить учения «фиолетовых» команд, а также распространять их основные результаты (см. текущую главу);
- управлять программой обмена разведданными (см. текущую главу);
- осуществлять мониторинг программы управления уязвимостями (см. главу 3);
- выполнять подключение к процессу DevOps (см. главу 7).

Все эти тактики прямо или косвенно поддерживают стратегию предотвращения реализации убийственной цепочки вторжения. Однако SOC-центры поддерживают и другие стратегии:

- нулевое доверие — мониторинг программы составления спецификации программного обеспечения (см. главу 3);
- нулевое доверие — мониторинг программы управления идентификацией и доступом (см. главу 3);
- обеспечение устойчивости — мониторинг и помощь в разработке мероприятий по резервному копированию и восстановлению (см. главу 5);
- автоматизация — разработка и проведение учений, связанных с хаос-инженерией, а также распространение их важнейших результатов (см. главу 7);
- обеспечение устойчивости — мониторинг программы обеспечения соответствия нормативным требованиям (см. главу 7);
- прогнозирование рисков — расчет киберрисков для организации (см. главу 6).

Разумеется, не все SOC-центры решают каждую из этих задач. Некоторые выполняют функции, не указанные в приведенном списке. Однако помните о том, что SOC-центр, как правило, не отвечает за применение всех этих тактик внутри организации, равно как и те бизнес-подразделения, на которые в наибольшей степени влияют решения, принимаемые SOC-центром. Скорее всего, ни одна команда в организации не несет такой ответствен-

ности. Именно этим руководство обосновывало создание операционных центров на протяжении многих веков, особенно в современную эпоху. Когда задача становится настолько масштабной, что для ее выполнения требуется несколько команд, возникает необходимость в операционном центре для координации их совместных усилий. Иными словами, когда ваша организация становится настолько большой, что Кевин (ИТ-специалист, ремонтирующий ноутбуки, мобильные телефоны и принтеры в офисе) уже не справляется с объемом работы, службы безопасности создают SOC-центр для управления рабочим процессом и осуществления защитной функции, как и говорил Фридрих Клемм.

Для эффективной реализации первичных принципов кибербезопасности сетевые защитники должны иметь централизованный пункт (физический или виртуальный), куда будет стекаться актуальная информация из сферы кибербезопасности. Аналитики анализируют эту информацию и дают рекомендации руководству. Руководство принимает решения, а затем SOC-центр координирует их реализацию отдельными командами или, что еще лучше, использует для этого автоматизацию, чтобы не привлекать людей.

Дальнейшие устремления. Позвольте внести ясность. Возможно, в мире найдется несколько организаций, которые используют свои SOC-центры для реализации всех тактик, основанных на базовых принципах кибербезопасности. Однако о большинстве сказать этого никак нельзя. Они выполняют мониторинг. Они собирают данные. Их SOC-аналитики перебирают миллиарды записей в журналах в поисках признаков компрометации. Большинство из них не пытается противостоять вражеским кампаниям на всех этапах убийственной цепочки. Вместо этого они сосредоточиваются на блокировании доступа к техническим уязвимостям, которые могут быть использованы противником для достижения успеха. Большинство SOC-аналитиков вообще не участвуют в разработке плана обеспечения устойчивости. Многие из них даже не могут произнести «DevSecOps», не говоря уже о том, чтобы сделать вклад в развитие философии инфраструктуры как кода. SOC-центр может иметь некоторый контроль над развертыванием стратегии нулевого доверия и ее политикой, но не над всем планом. Большинство SOC-аналитиков не имеют представления о том, как рассчитывать вероятность наступления существенного киберсобытия в будущем, но не потому, что не способны на это, а потому, что никто из руководителей не обучал их этому и не ставил перед ними такой задачи. Единственная тактика, применение которой многие из них все же контролируют, связана с разведкой. Но даже эти усилия не направлены на победу над противником на всех этапах убийственной цепочки, и руководство, скорее всего, не привлекает команду разведки к расчету киберрисков для организации.

Все это может подвигнуть вас на то, чтобы рассмотреть свою программу обеспечения безопасности сквозь призму первичных принципов. Недостаточно иметь организацию, называемую SOC-центром. Создаваемый вами SOC должен поддерживать реализацию стратегий, базирующихся на первичных принципах, иначе зачем он вообще нужен? Но я понимаю, что это трудно. Переориентация SOC-центра на базовые принципы идет вразрез с общепринятой практикой обеспечения информационной безопасности, применявшейся на протяжении 20 лет. Даже если вы согласитесь со мной, что такие перемены необходимы, вероятность того, что вам удастся убедить высшее руководство централизовать принятие решений по безопасности и преодолеть сопротивление бюрократии, невелика. Но это необходимо сделать, и это возможно.

В начале книги я рассказал об одной из причин успеха Илона Маска. В частности, он был убежден в том, что постепенное совершенствование чего-либо без учета конечной цели — это залог неудачи. Опираясь на базовые принципы, он сумел создать ракету для полета на Марс, роскошный электромобиль и источник доступной солнечной энергии, тогда как многие считали невозможным добиться хотя бы одной из этих целей. Не утверждаю, что такой образ мышления — единственное, что обеспечило Маску успех. Я просто говорю, что без него Илон не добился бы всего того, что имеет.

С начала 1900-х годов концепция SOC-центра постепенно совершенствовалась, и ее эволюция все еще продолжается. Нам предстоит пройти долгий путь, чтобы однажды в будущем создать SOC-центр, способный поддерживать применение всех тактик, направленных на реализацию наших стратегий, основанных на базовых принципах кибербезопасности.

Оркестрация стека безопасности: тактика предотвращения реализации убийственной цепочки вторжения

Я уже упоминал, что в начале 2000-х годов был командиром группы реагирования на инциденты компьютерной безопасности в армии США (Army Computer Emergency Response Team, ACERT). Современный Интернет тогда только начинал развиваться. За пару лет до этого появилась «Википедия». В том же году компания Apple запустила сервис iTunes, но до появления первого iPhone оставалось еще четыре года. Тем временем в армии мы все еще пытались понять, что

такое кибероперации, и каждая организация, способная правильно написать приставку «кибер» в трех случаях из пяти, считала, что ей необходимо их освоить.

Одной из моих обязанностей в рамках ACERT была координация наступательных и оборонительных кибероперациий, проводимых в интересах всех армейских заинтересованных сторон (включая службы разведки, связи, правоохранительные органы, юридическую службу, войска информационных операций и многие другие), а также коллег из ВВС, ВМС и морской пехоты. Это были так называемые силы «Раздела 10», и моей задачей было убедиться в том, что их действия не мешают тому, что делают силы «Раздела 50» в АНБ и Центральном разведывательном управлении (ЦРУ).

Под «Разделом 10» и «Разделом 50» имеются в виду разделы Кодекса США, в которых, помимо прочего, содержатся законы, регулирующие деятельность вооруженных сил и их использование («Раздел 10»), а также вопросы слежки, тайных операций и шпионажа («Раздел 50»). Многие, наверное, не знают, что слежка и шпионаж находятся в ведении американских шпионских организаций. Силы, деятельность которых регулируется «Разделом 10», в основном участвуют в войнах. Существуют некоторые исключения, но в целом разделение труда именно таково. Теоретически это означает, что армия не занимается шпионажем, если не работает непосредственно на АНБ, а разведывательное сообщество не участвует в войне, если только речь не идет о непосредственной поддержке вооруженных сил.

Я упоминаю об этом потому, что в то время (в начале 2003 года) США и некоторые их союзники готовились начать вторжение в Ирак. В ходе подготовки армейские киберслужбы были застигнуты врасплох. Ранее мы разделили оперативный контроль над киберактивами армии между региональными CERT-центрами (RCERTs) Северной Америки, Южной Америки, Европы, Тихоокеанского региона и Южной Кореи. Но не обеспечили свое присутствие в Юго-Западной Азии (SWA). А оно нам было необходимо. Поэтому мы в кратчайшие сроки призвали на службу множество резервистов и отправили их в этот регион как раз к моменту начала вторжения.

Команда RCERT сразу же заметила признаки непрерывного прощупывания электронного периметра RCERT SWA, исходящие из нескольких регионов и стран Ближнего Востока. Ничего хорошего это не предвещало. Мы беспокоились о том, что эти плохие парни,

кем бы они ни были, могут нарушить работу вновь созданной сети, предназначенной для поддержки танков и пехоты после пересечения ими исходного рубежа в момент начала наступления (час «Ч»). Нам нужен был план противодействия такому развитию событий.

И мы перешли в режим невидимости.

Мы разработали план, позволяющий нажатием одной кнопки перевести всю инфраструктуру RCERT SWA на новые домены и IP-адреса. По сути, когда наступил час «Ч», инфраструктура RCERT SWA стала невидимой для любой внешней организации, пытающейся за нами следить. RCERT SWA остался полностью функциональным, но для внешнего мира исчез с радаров, как клингонский звездолет, использующий маскировочное устройство. Это продлилось недолго, может быть, один день, но так и было задумано. Нашей целью было вызвать замешательство и дезориентацию у тех, кто собирался помешать нашей армии в начале войны.

Мне нравится эта история, потому что она подчеркивает то, что всем организациям, занимающимся защитой сети, необходимо осуществлять оркестрацию стека безопасности, то есть развертывание политики и стратегии на оперативном оборудовании в режиме реального времени.

Зачем нам оркестрация? На заре развития Интернета (конец 1990-х годов) оркестрация не представляла особой проблемы. В стеке безопасности было всего три инструмента: межсетевые экраны, системы обнаружения вторжений и антивирусы. Когда нужно было изменить политику, мы вручную авторизовались в каждой из этих систем и вносили изменения. К 2021 году среды превратились в чрезвычайно сложные системы систем, развернутые на нескольких островах данных, таких как гибридные облака, SaaS-приложения, внутренние дата-центры с унаследованными системами и мобильные устройства. По сравнению с давними временами сложность последовательной и быстрой оркестрации стека безопасности с учетом стратегий, базирующихся на первичных принципах (нулевое доверие, предотвращение реализации убийственной цепочки вторжения, обеспечение устойчивости, автоматизация и прогнозирование рисков), возросла в разы. По правде говоря, большинство из нас не очень хорошо справляется с этой задачей.

Но существует несколько подходов, которые ИБ-специалисты могут использовать для облегчения этого бремени. Одним из них является DevOps или DevSecOps.

DevOps и DevSecOps. В 2003 году, когда компания Google занималась только интернет-поиском, она решила передать задачу управления сетью разработчикам [321]. А что делают разработчики, столкнувшись с подобной задачей? Они ее автоматизируют. Вместо того чтобы заставлять технических специалистов вручную авторизоваться в системе сетевых устройств для обновления конфигураций, SRE-инженеры Google автоматизировали эти низкоуровневые задачи, или «тойл», как они это называют. В том же году компания Amazon развернула внутреннюю программу на основе парадигмы «инфраструктура как код» — набор общих инфраструктурных сервисов, к которым мог обращаться любой сотрудник компании, не изобретая каждый раз велосипед. Вскоре руководители Amazon осознали, что на основе этих сервисов можно создать операционную систему для Интернета. Это привело к запуску платформы AWS в 2006 году [125].

То, что делали Google и Amazon в те годы, сегодня называется DevOps или инфраструктура как код, но это название появилось в отрасли только в 2010 году. Сегодня, спустя 20 лет с момента создания, Google и Amazon относятся к тем немногим интернет-гигантам (наряду с Netflix, Microsoft и некоторыми другими), которые доминируют в сфере электронной коммерции.

Инновационные стартапы, те самые, которые в 2010 году придумали название DevOps, поняли: для того чтобы выделиться на рынке, им необходимо предоставлять свои услуги по модели SaaS, используя парадигму инфраструктуры как кода. Эта история подробно описана в двух книгах, вошедших в Зал славы Cybersecurity Canon: *Site Reliability Engineering*, написанной командой Google [321], и «Проект “Феникс”» Джина Кима [323]. При таком подходе в процессе разработки приложений специалисты встраивают в систему способы управления стеком безопасности в большом масштабе и с высокой скоростью. Прочитайте раздел о Netflix Chaos Monkey (см. главу 7), если хотите узнать о разработке стратегии обеспечения устойчивости на основе методологии DevSecOps, которая, по сути, представляет собой парадигму «кибербезопасность как код».

Платформы оркестрации. Второй подход заключается в развертывании коммерческого инструмента, который выполняет основную часть работы за вас. Эксперты в области безопасности, такие как Джон Олцик (главный аналитик Enterprise Strategy Group), начали говорить об этой концепции еще в 2015 году [108, 170]. Они указывали на необходимость в сервисах, способных автоматизировать сбор телеметрической информации от защитных средств, принимать на ее основе решения по поводу политики и развертывать новые и обновленные политики в стеке безопасности. В основе данной концепции лежит понятие контура обратной связи или контура управления из области системной инженерии. И это хорошая идея.

Но одна из главных проблем заключается в том, что большинство средних и крупных организаций использует слишком много инструментов. Согласно результатам опроса 1200 вице-президентов по безопасности, представленным в отчете Panaseer 2022 Security Leaders Peer Report, среднее количество защитных инструментов, которыми мы пользуемся, составляет 76 [79]. Это гораздо больше, чем те три инструмента, которыми мы управляли два десятилетия назад.

Платформы оркестрации «всё в одном» начали выпускать на рынок примерно в 2017 году такие крупные поставщики межсетевых экранов, как Checkpoint, Cisco, Fortinet, Juniper и Palo Alto Networks. Помимо традиционных функций брандмауэра, эти платформы предусматривали дополнительные услуги по подписке для реализации стратегий нулевого доверия, защиты от убийственной цепочки вторжений и обеспечения устойчивости. Благодаря этому вместо интеграции 76 отдельных защитных средств практики могли развернуть одну платформу оркестрации в различных формфакторах на каждом из островов данных. Она выполняла многие из задач, которые реализовывали отдельные инструменты, но контролировалась единой согласованной политикой. Там, где это было возможно, сервис по подписке интегрировался с другими автоматически. Минусом было то, что такой набор услуг, вероятно, представлял собой не самое лучшее сочетание инструментов из той или иной категории. Плюс же заключался в том, что они, скорее всего, были достаточно хороши, имели дополнительное преимущество в виде полной интеграции с другими сервисами, предоставляемыми по подписке, там, где это было возможно, и автоматически обновлялись, пополняясь новейшими средствами предотвращения вторжений, которые предоставлял производитель. Поскольку у этих поставщиков брандмауэров было множество клиентов, разбросанных по всему миру, они собирали много телеметрических показателей деятельности злоумышленников в режиме реального времени. Если им удавалось разработать новые средства предотвращения вторжений благодаря тому, что они наблюдали в сети клиента А, то выгоду от этого получали все их клиенты.

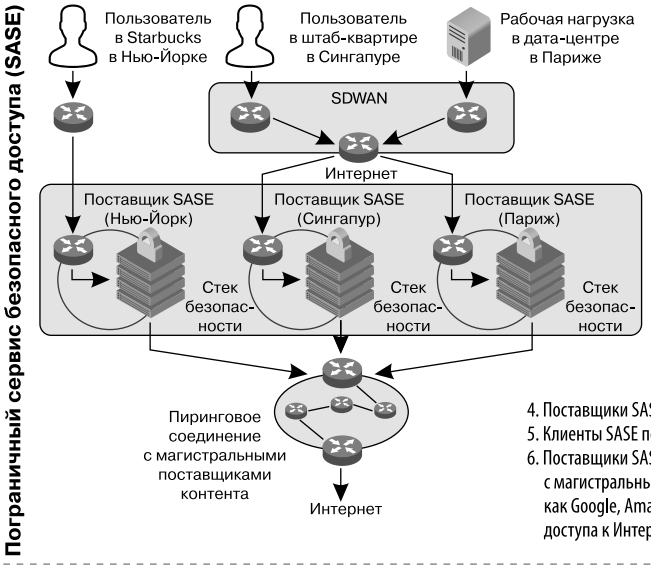
Оркестрация, автоматизация и реагирование на инциденты безопасности (SOAR). То, что основную часть работы по обеспечению безопасности можно доверить одному поставщику, не получило широкого распространения. Большинство ИБ-специалистов хотели подстраховаться, используя нескольких поставщиков. К тому же платформы были довольно дорогими, и организации небольшого и среднего размера не могли их себе позволить. Эти же компании, скорее всего, не применяли методологию DevOps, несмотря на ошеломительный успех стартапов в начале 2010-х годов. Это

подводит нас к третьему, гибридному подходу под названием «оркестрация, автоматизация и реагирование на инциденты безопасности» (security, orchestration, automation and response, SOAR).

В 2017 году компания Gartner ввела этот термин для описания SOC-инструмента нового типа, способного взаимодействовать с другими устройствами в стеке безопасности и позволяющего автоматизировать процесс обработки повторяющихся паттернов данных [74]. Например, если начинающие SOC-аналитики 1000 раз за смену проводят пальцем влево для просмотра одного и того же оповещения системы обнаружения вторжений, инструмент SOAR облегчает автоматизацию этого действия. Автоматизация делает SOAR-инструменты уникальными по сравнению с инструментами управления событиями и информацией о безопасности (security information and event management, SIEM), которые по большей части просто собирают телеметрию. Однако я ожидаю того, что со временем эти два вида функциональности объединятся. SOAR-решения уже предусматривают функции SIEM, а SIEM-инструменты уже имеют функции SOAR. Однажды настанет момент, когда их уже нельзя будет различить.

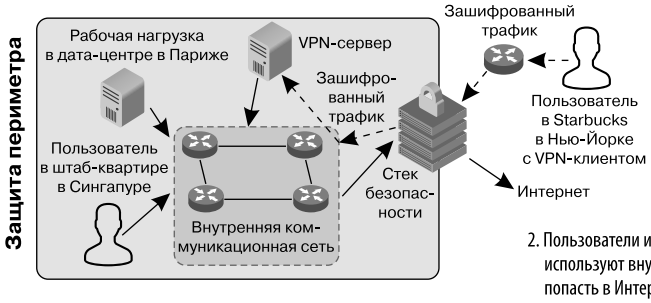
Инструменты SOAR отлично справляются с уменьшением шума, с которым сталкиваются сотрудники SOC. На моем последнем месте работы в качестве CSO нам удалось сократить количество оповещений, поступающих в SOC-центр для обработки каждый квартал, с 1 млрд до 500. Это потрясающе. Если бы SOC-аналитики сделали только это, их жизнь стала бы намного проще. Однако у SOAR/SIEM-платформ есть еще кое-какие неиспользованные возможности. Нам не обязательно работать в одностороннем режиме приема. Эти инструменты уже умеют взаимодействовать со всеми устройствами в стеке безопасности. Что, если использовать их в качестве DevOps-моста? Мы могли бы создавать в рамках SOAR-инструментов структуры нулевого доверия, предотвращения реализации убийственной цепочки вторжений, обеспечения устойчивости и прогнозирования рисков, позволяющие обновлять стек безопасности нажатием одной кнопки. Однако я еще не видел, чтобы кто-то делал это в реальности.

SASE и SSE. Еще один вариант заключается в использовании пограничного сервиса безопасного доступа (secure access service edge, SASE) или родственного ему пограничного сервиса обеспечения безопасности (security service edge, SSE). Концепции SASE и SSE переворачивают старую модель защиты периметра с ног на голову, используя облачного провайдера в качестве первого пункта назначения для любого сетевого трафика, покидающего локальный объект (рис. 4.5).



Характеристики

1. Интернет-трафик от пользователя, находящегося **вне** инфраструктуры организации, сначала направляется к поставщику SASE
2. Интернет-трафик от пользователя, находящегося **внутри** инфраструктуры организации, сначала направляется на логический метауровень программно-определяемой глобальной сети (SDWAN). SDWAN принимает решения о маршрутизации, основываясь на самом коротком пути до поставщика SASE
3. Поставщики SASE имеют несколько интернет-узлов по всему миру
4. Поставщики SASE поддерживают стек безопасности
5. Клиенты SASE поддерживают политику стека безопасности
6. Поставщики SASE устанавливают пиринговые соединения с магистральными поставщиками контента, такими как Google, Amazon и Facebook, для обеспечения быстрого доступа к Интернету



Характеристики

1. Интернет-трафик от пользователя, находящегося **вне** периметра, шифруется с помощью VPN-клиента и направляется на VPN-сервер через стек безопасности. Стек безопасности не может осуществлять мониторинг этого трафика. Пользователи VPN имеют доступ ко всем ресурсам, находящимся внутри периметра
2. Пользователи и рабочие нагрузки **внутри** периметра используют внутреннюю коммуникационную сеть, чтобы попасть в Интернет через стек безопасности

Характеристики

1. Сначала интернет-трафик направляется к поставщику SSE
2. Поставщики SSE имеют несколько интернет-узлов по всему миру
3. Поставщики SSE поддерживают стек безопасности
4. Клиенты SSE поддерживают политику стека безопасности
5. Поставщики SASE устанавливают пиринговые соединения с магистральными поставщиками контента, такими как Google, Amazon и Facebook, для обеспечения быстрого доступа к Интернету

Рис. 4.5. Сравнение технологий SASE, защиты периметра и SSE

Локальными объектами могут быть здания штаб-квартир, офисы продаж, центры обработки данных, облачные рабочие нагрузки, а также удаленные сотрудники, работающие дома или в местном кафе. Компания Gartner ввела термин SASE в 2019 году и определила три элемента, которые отличают поставщика SASE, например, от обычного поставщика управляемых услуг по обеспечению безопасности (MSSP).

- *Стек безопасности*. В модели разделяемой ответственности поставщик услуги SASE поддерживает работу всех инструментов стека безопасности, которые он предоставляет. Заказчик определяет политику. Диапазон вариантов стека безопасности весьма широк. Как потребителю, вам следует проявлять осторожность. Если вы решились на использование такой модели, убедитесь в том, что стек безопасности поставщика SASE способен обеспечить реализацию всех обсуждаемых в этой книге стратегий, базирующихся на первичных принципах кибербезопасности.
- *SDWAN*. Поставщик SASE подключается к вашему метауровню SDWAN, чтобы обеспечить прохождение всего трафика через стек безопасности и максимально эффективную маршрутизацию. Это хорошая новость. Плохая новость заключается в том, что вам необходимо иметь этот метауровень SDWAN. Я не говорю, что он чем-то плох, — лишь указываю на то, что он является еще одним элементом вашего стека безопасности, добавляющим сложности.
- *Пиринг*. Модель SASE работает только в том случае, если она не замедляет обычный интернет-трафик. Если ваш поставщик SASE имеет всего несколько облачных центров по всему миру, через которые должен проходить весь ваш трафик, это может серьезно ограничить пропускную способность. Для решения этой проблемы ваш SASE-провайдер может установить пиринговые соединения в своих дата-центрах с такими крупными сетями поставщиков контента, как Google, Amazon и Netflix. Например, ваши сотрудники в Сингапуре могут воспользоваться обширной оптоволоконной сетью Google, чтобы подключиться к стеку безопасности поставщика SASE. Во время разговора с SASE-провайдерами попросите их описать свою схему пиринговых соединений.

К 2022 году ИТ-практики осознали, что компонент SDWAN не столь уж необходим в архитектурной модели SASE. Этот компонент вполне хорош, и если он у вас есть, то вам, безусловно, стоит его использовать. Но для всех остальных компания Gartner предложила в качестве альтернативы сервис SSE, который, по сути, представляет собой сервис SASE, лишенный метауровня SDWAN [260].

Применение SASE/SSE — это модифицированная версия использования платформы оркестрации одного поставщика. Хорошая новость заключается в том, что применять данную модель гораздо проще, чем самостоятельно развертывать и поддерживать платформу оркестрации на всех своих островах данных. В этом случае все обслуживает поставщик SASE/SSE. Клиенту достаточно управлять политикой. Минусом является то, что нам пока неясно, насколько дорогими будут услуги SASE/SSE в будущем. Сейчас мы находимся на первом этапе этой игры. Однако по мере роста клиентской базы поставщики систем безопасности, вероятно, достигнут определенного эффекта масштаба, что может способствовать снижению цен.

Из описанных ранее четырех вариантов самый простой — использование поставщика SASE/SSE, за которым следует развертывание единой платформы оркестрации. Сегодня оба эти варианта, как правило, требуют больших расходов. Если поставщикам SASE удастся снизить стоимость услуг, то за архитектурой SASE/SSE будущее, особенно для малых и средних организаций. Принятие философии DevSecOps, скорее всего, правильный путь для вашей организации, если она стремится стать интернет-гигантом вроде Google, Netflix и Amazon. Однако если вы только начинаете осваивать этот подход, то вам придется подождать несколько лет, чтобы получить нечто более или менее полезное. Я полагаю, что большинство организаций находятся где-то посередине и используют модель SOAR/SIEM, но, скорее всего, они применяют ее лишь как средство уменьшения шума в данных SOC-центра, а не как платформу для оркестрации.

Важность оркестрации для предотвращения реализации убийственной цепочки вторжений. Суть стратегии предотвращения реализации убийственной цепочки вторжений довольно проста и сводится к развертыванию средств обнаружения и предотвращения всех известных сценариев действий противника на всех островах данных и всех этапах цепочки. Ничего сложного. Однако при разборе данной фразы каждое существительное (средства обнаружения и предотвращения, сценарии действий, острова данных, убийственная цепочка) экспоненциально увеличивает сложность задачи. Сотрудники SOC-центра, пытающиеся делать все это вручную, не справляются с нагрузкой. Чтобы не отставать от меняющегося ландшафта угроз, сетевым защитникам необходимо каким-то образом упростить свои среды и максимально автоматизировать рабочий процесс. Именно для этого и нужна оркестрация систем безопасности, и существует несколько архитектур, которые могут в этом помочь. В данном разделе мы рассмотрели некоторые из них:

- DevOps и DevSecOps;
- платформы оркестрации;
- SOAR;
- SASE и SSE.

Для успешного предотвращения реализации убийственной цепочки вторжения сетевые защитники должны освоить оркестрацию в совершенстве.

Кибербразведка — это тактика, поддерживающая все стратегии, базирующиеся на первичных принципах кибербезопасности, в первую очередь стратегию предотвращения реализации убийственной цепочки вторжения.

Кибербразведка (cyber threat intelligence, CTI) — это не новая концепция. В той или иной форме она практиковалась еще в 2000-х годах различными военными организациями в США и других странах. Представление о том, что это лучшая практика для коммерческого сектора, начало обретать популярность примерно в 2015 году, после публикации знаменитого документа Lockheed Martin об убийственной цепочке (2010), публикации отчета APT1 компании Mandiant (2013) и первого выпуска фреймворка MITRE ATT&CK (2013). Некоторые коммерческие организации уже занимались кибербразведкой, но основная часть сообщества сетевых защитников этого не делала. К 2015 году большинство известных поставщиков систем безопасности имели собственную команду разведки, публикующую отчеты в маркетинговых целях. Зрелые команды ИБ-специалистов, не работающие на подобных поставщиков, поняли, что им тоже нужна команда разведки для извлечения пользы из этих открытых разведданных.

Что такое CTI? Операции CTI — это не что иное, как обычные разведывательные операции, проводимые в киберпространстве. А сами разведывательные операции существуют с незапамятных времен. По словам профессора Университета Теннесси Веяса Габриэля Люлевичуса, «самые ранние свидетельства о работе разведки содержатся на глиняных табличках Месопотамии, а из Библии нам известно, что в Древнем Израиле шпионы использовались не только политическими, но и религиозными соперниками» [142].

Тема разведки, ее осуществления и измерения ее эффективности весьма обширна. До начала 2000-х годов ее изучением занимались в основном государственные служащие и ученые. В последние 20 лет сектор коммерческой безопасности тоже начал рассматривать эту тему, поскольку она

непосредственно влияет на то, как организации могут защитить себя в киберпространстве или улучшить собственные средства обеспечения ИБ. Однако если вы поищете определение этого термина, то, скорее всего, обнаружите множество вариантов.

Например, по словам А. К. Уэйсмиллера, писавшего для Центрального разведывательного управления в 1996 году, разведывательные операции позволяют получить «достоверную информацию обо всех врагах страны, которые нападают на нее исподтишка» [310]. Он также сказал, что разведданные помогают правительству обеспечить «пассивную или статическую защиту от всех враждебных и скрытых действий». Наконец, он заявил, что разведслужбы выявляют операции конкретного противника, чтобы противостоять им путем проникновения и манипулирования «с целью обращения удара против самого агрессора».

> Мне нравится ход мыслей Уэйсмиллера. Обратите внимание на то, что его пассивная защита соответствует стратегии нулевого доверия, а попытка победить противника — стратегии предотвращения реализации убийственной цепочки вторжения. Если я когда-нибудь встречу Уэйсмиллера в баре, то угощу его пивом.

Кристофер Гэйбел, автор статей для блога Scholastic, дает разведывательным операциям более академическое определение: «Разведывательная операция — это процесс, в ходе которого правительства, военные группировки, предприятия и другие организации систематически собирают и оценивают информацию с целью выявления возможностей и намерений своих противников. Обладая такой информацией, или разведданными, организация может как защититься от своих противников, так и воспользоваться их слабостями» [84].

Я занимался киберразведкой на протяжении более чем 20 лет как в армии, так и в коммерческом секторе и предпочитаю определять эту деятельность как «процесс преобразования необработанной информации в разведданные, на основании которых руководители могут принимать решения».

Все приведенные определения в той или иной степени верны. Если бы мне нужно было выбрать наиболее точно соответствующее действительности,

я бы выбрал определение, предложенное академиком. Но, по моему мнению, избыточное количество мнений о сущности CTI замедлило внедрение этой практики в сообщество сетевых защитников. Абсолютно точно можно сказать, что CTI-операции в одной организации, скорее всего, не будут похожи на CTI-операции в другой.

Процесс разведки — жизненный цикл. Любое обсуждение процесса разведки, будь то традиционная или киберразведка, должно начинаться с рассмотрения ее жизненного цикла (рис. 4.6) [15].

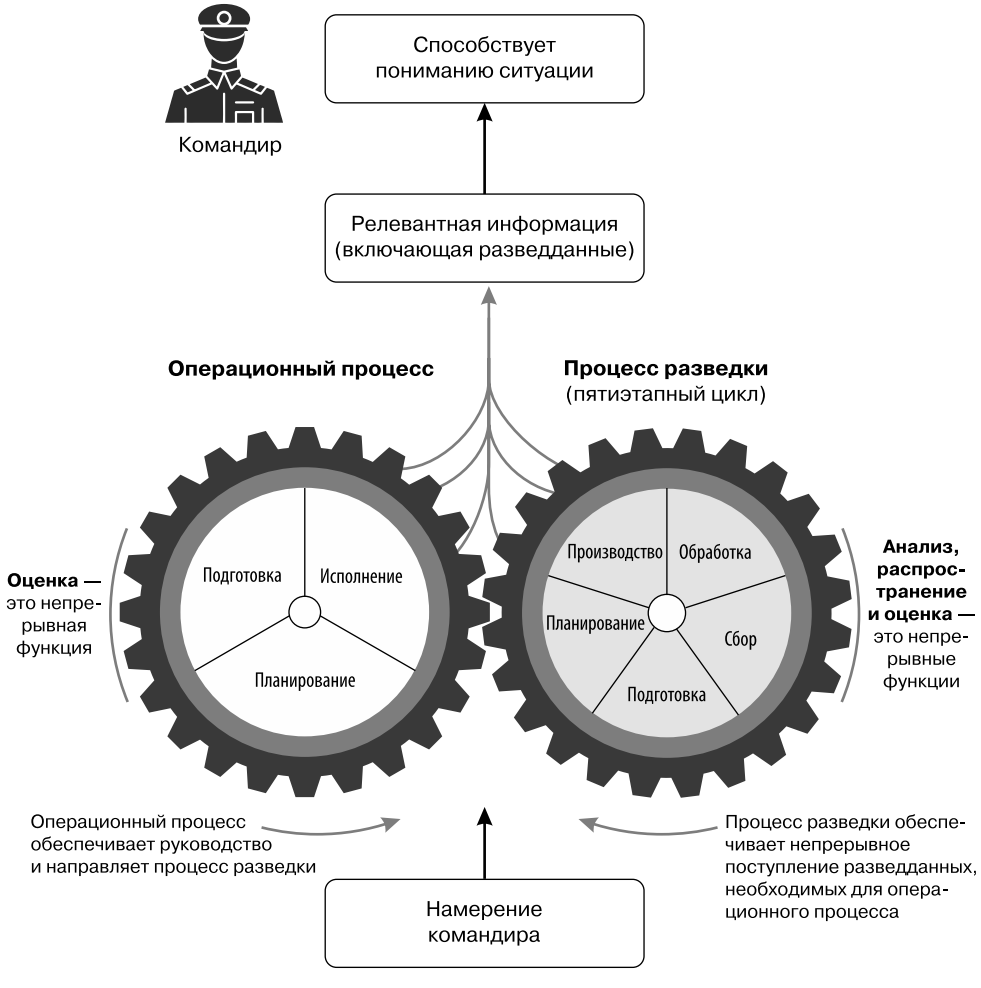


Рис. 4.6. Процесс разведки в армии США (версия 2004 года) [15]

Как пишет Марк Фитиан в своей книге *Understanding the Intelligence Cycle*, происхождение жизненного цикла разведки неясно [176]. Большинство ученых сходятся во мнении, что он возник после Второй мировой войны, когда офицеры разведслужб союзников пытались объяснить, чем они занимались в ходе этого конфликта. По словам Фитиана, «после 1945 года этот опыт начали описывать в американских учебных пособиях, таких как *Intelligence is for Commanders*, написанном подполковником Филипом Дэвидсоном и подполковником Робертом Глассом» [87]. Хотя в своей книге Фитиан критикует данный цикл как слишком сложный для большинства государственных разведывательных организаций по сравнению с повторяющимся пятиэтапным процессом, упрощенный жизненный цикл разведки хорошо демонстрирует ее основные компоненты.

- *Планирование*. Получите у начальника указания в виде требований к критической информации (critical information requirements, CIR). В армии их называют *требованиями командира к критической информации* (commander's critical information requirements, CCIR).
- *Подготовка*. Разбейте эти указания на более мелкие вопросы, называемые *приоритетными требованиями к разведданным* (priority intelligence requirements, PIR) и *требованиями к разведданным* (intelligence requirements, IR).
- *Сбор*. Соберите исходные данные, отвечающие требованиям PIR. Выясните, соответствуют ли имеющиеся у вас данные всем PIR и CIR. Если нет, соберите необходимую информацию.
- *Обработка*. Преобразуйте исходные сведения в разведданные, отвечающие требованиям PIR.
- *Производство*. Создайте один или несколько продуктов разведки, в которых используются PIR-ответы, соответствующие требованиям командира к критической информации. Представьте эти продукты ключевым руководителям в нужное время для принятия более обоснованных решений.
- *Планирование*. Получите обратную связь от ключевых руководителей для дальнейшего улучшения рабочего процесса.
- *Повторение*. Или, как я это называю, повторный запуск цикла разведки.

Жизненный цикл разведки — планирование и требования CIR. Начните с руководства организации. В армии это будет командир. В бизнесе — гене-

ральный директор, совет директоров и другие высшие руководители. Когда боевые подразделения начинают готовиться к очередной оборонительной или наступательной операции, командиры ставят перед своими разведгруппами вопросы, на которые те должны получить ответы для достижения успеха операции. С какого направления будет наступать противник? Насколько велики будут его силы? С каким оружием они придут на поле боя?

> Как вы думаете, откуда у Ли Марвина оказался план здания, когда он готовил своих коммандос к нападению на немецкое шале в фильме «Грязная дюжина» (1967)? А откуда принцесса Лея взяла инженерные планы слабых мест «Звезды смерти», о которых генерал Додонна рассказывал пилотам своих истребителей в фильме «Звездные войны» (1977)? Старшие руководители приказали команде разведки добыть их.

В коммерческом пространстве используется тот же процесс, только с другим набором вопросов. CIR меняются не очень часто. В коммерческом секторе имеет смысл пересматривать их примерно раз в год. Они являются высокоуровневыми, сложными и, скорее всего, ничем не ограниченными. В качестве примера можно привести следующий список, применимый к любой организации.

- *Убийственные цепочки вторжений* (см. текущую главу). Какие наиболее вероятные кампании будут реализованы хакерами для нанесения существенного ущерба нашей организации?
- *Нулевое доверие* (см. главу 3). Что относится к материальным системам и информации в нашей организации и кто должен иметь к ним доступ?
- *Обеспечение устойчивости* (см. главу 5). Какие системы и наборы данных должны быть доступны в случае существенного киберинцидента, чтобы мы могли продолжать предоставлять услуги своим клиентам?
- *Прогнозирование рисков* (см. главу 6). Какова вероятность наступления существенного киберинцидента в ближайшие три года?
- *Автоматизация* (см. главу 7). Какие приоритетные проекты DevSecOps могут сильнее всего повлиять на снижение вероятности существенного ущерба в результате киберинцидента?

Все это актуальные требования CIR для группы разведки. Поскольку мы говорим о базовых принципах кибербезопасности, я хочу сосредоточить функцию разведки на задачах, которые непосредственно уменьшают вероятность существенного ущерба в результате киберинцидента. CTI-операции можно использовать для поддержки всех стратегий, базирующихся на первичных принципах, и более зрелые организации именно так и поступают, однако большинство организаций используют такие операции в первую очередь для предотвращения реализации убийственной цепочки вторжений.

Обратите внимание: здесь предполагается, что у вас есть неограниченные ресурсы для того, чтобы заниматься этой деятельностью. Я знаю, что их нет ни у кого, поэтому чуть позже расскажу о том, как это можно делать в условиях ограниченного бюджета.

Я уже говорил, что требования CIR относятся к тому, о чем хочет знать генеральный директор в сфере кибербезопасности. Но речь не обязательно должна идти о генеральном директоре. Руководителем, для которого разрабатываются CIR, может быть любой сотрудник из руководящего состава, в том числе генеральный менеджер бизнес-подразделения, продакт-менеджер или любой другой руководитель, на которого работает команда разведки.

Жизненный цикл разведки — подготовка и требования PIR. Команда разведки разбивает требования CIR на более мелкие вопросы, на которые можно ответить. Это классический способ решения проблемы, при котором вы продолжаете разбивать исходную проблему на все более мелкие части, пока не получите задачу, которую можете решить, и действуете, отталкиваясь от нее. То же самое происходит и с требованиями PIR. Типичные CIR могут генерировать от одного до более чем 20 PIR в зависимости от сложности. Рассмотрим пример (рис. 4.7).

Требования PIR динамичны. Если CIR могут меняться раз в год, то PIR могут делать это ежедневно, еженедельно, ежемесячно или с любой другой периодичностью. И, даже ответив на один из этих вопросов, вы можете обнаружить, что это не помогает вам ответить на более масштабные вопросы CIR. Например, возьмем следующий вопрос PIR: «Сколько кампаний киберпротивники проводят каждый конкретный день?» Ответ на него не поможет вам ответить на общий вопрос CIR. Само по себе это может быть интересно и полезно в дальнейшем, но напрямую неприменимо. Поэтому вы изменяете вопрос и пробуете снова: «Сколько наиболее вероятных кампаний киберпротивники проводят каждый конкретный день?»

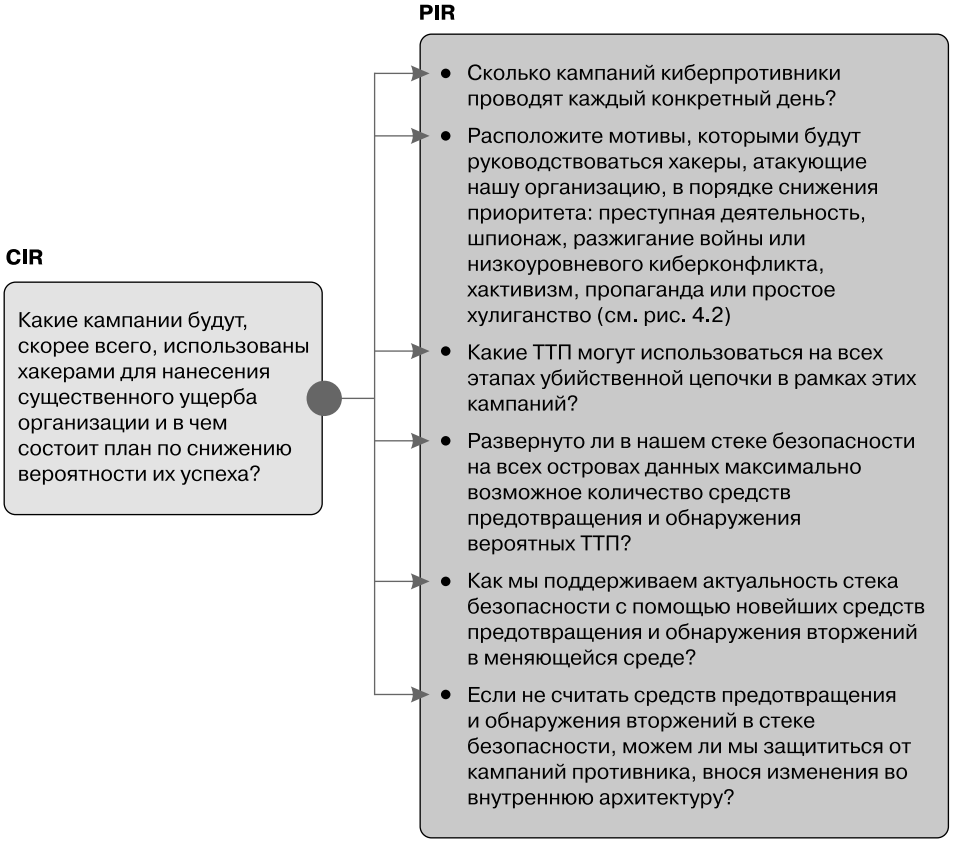


Рис. 4.7. Пример разбиения CIR на множество PIR

Пока вы отвечаете на один PIR-вопрос, ему на смену могут появиться еще пять, поскольку в ходе этого процесса вы узнаете больше подробностей о наборе задач или понимаете, что PIR-вопрос, на который пытаетесь ответить, можно разбить на несколько более мелких и простых вопросов. Например, посмотрите на рис. 4.8.

Иногда возникают интересные вопросы, на которые не нужно отвечать сразу, но которые могут стать актуальными в будущем. В армии такие вопросы называют *требованиями к информации*. Это то, на что следует обращать внимание, и если ответ на подобный вопрос появится, пока команда киберразведки будет выполнять другие приоритетные задачи, то его имеет смысл учесть. Например, если речь идет об атаке, которой может подвергнуться ваша организация, то кто за ней стоит, по мнению сообщества ИБ-специалистов (см. раздел «Некоторые соображения по поводу

атрибуции» ранее), — обычные киберпреступники или гибридная группа, выполняющая заказ государства, но подрабатывающая киберпреступлениями и получающая дополнительный доход для финансирования своей деятельности? Это не слишком важно знать для предотвращения реализации убийственной цепочки вторжений, но может оказаться полезным впоследствии.

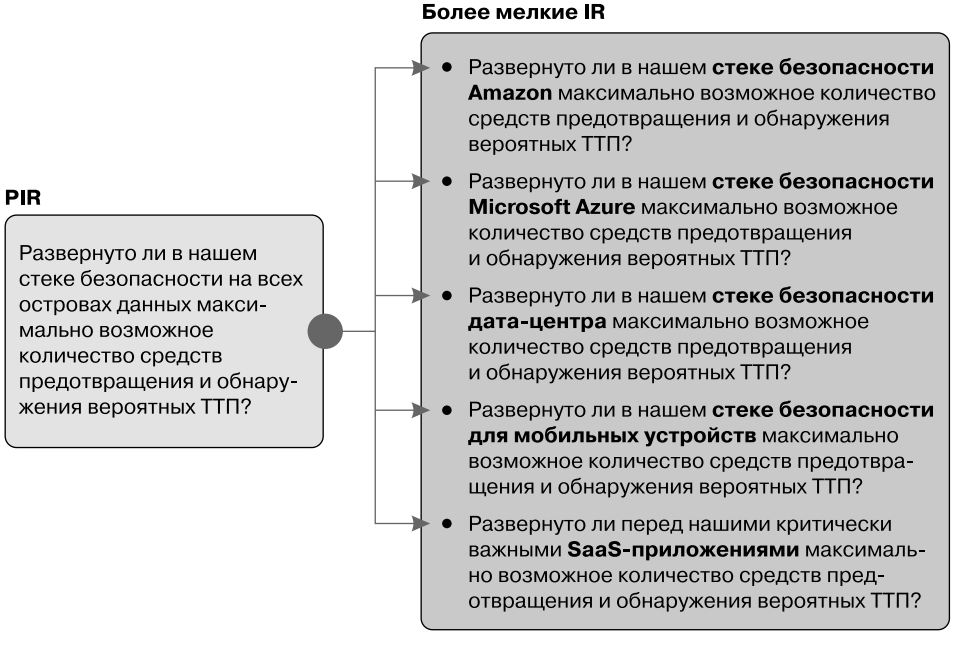


Рис. 4.8. Пример разбиения PIR на более мелкие IR

Жизненный цикл разведки — сбор информации. После постановки PIR-вопросов группа разведки изучает имеющуюся в ее распоряжении исходную информацию и решает, может ли она ответить на них. Если может — хорошо. Если нет, то им придется искать новые источники информации. Это называется *управлением сбором данных* и представляет собой бесконечный процесс сопоставления требований PIR с необработанными разведданными, поступающими в организацию. Источниками таких данных могут быть:

- телеметрия внутренней сети и стека безопасности;
- открытые источники разведданных (OSINT), такие как блоги, посвященные вопросам информационной безопасности, новостные издания,

правительственные оповещения, поступающие от CERT-центров и правоохранительных органов;

- подписные или коммерческие информационные каналы;
- организации, созданные для обмена информацией (например, FS-ISAC и Cyber Threat Alliance);
- соглашения об обмене данными с партнерскими организациями и многие другие.

Это очень важная работа. Топливом для деятельности команды киберразведки является необработанная информация. Если ее источники непоследовательные, плохие или труднодоступные, качество работы этой команды будет страдать. Когда ваша CTI-группа станет более опытной, одному или нескольким сотрудникам придется посвящать этой деятельности полный рабочий день. Она включает в себя не только управление всеми источниками разведданных, но и автоматизацию процессов сбора и создания продуктов разведки, делающих поступающие разведданные полезными для команды.

Жизненный цикл разведки — обработка данных и продукты разведки. На этом этапе в дело вступают разведаналитики, чья работа заключается в потреблении необработанной информации, ее синтезе для получения ответов на PIR-вопросы и создании продуктов разведки, которые руководство может использовать для принятия решений. Преобразование исходной информации в нечто полезное, то есть в оперативные разведданные, — это та характеристика, которая отличает разведаналитика от репортера. И тот и другой оказывают ценные услуги. На деле аналитик выполняет многие из функций репортера, но при этом на него возлагается дополнительная обязанность — консультировать руководство по поводу использования полученной информации. Эти консультации предоставляются в виде продуктов разведки.

Они не обязательно должны быть сложными. Таким продуктом может быть хорошо составленное, но краткое электронное письмо, информирующее генерального директора о том, что в ходе первичной оценки недавно приобретенной компании CTI-команда выявила некоторые пробелы в ее защите от убийственной цепочки вторжений. В связи с этим генеральный директор может решить ускорить процесс перевода компании под защиту внутреннего стека безопасности. Электронное письмо может быть простым, но если CTI-команда использует его, чтобы помочь генеральному директору принять решение, то оно является продуктом разведки.

Продуктом разведки может быть и автоматическая аналитическая панель, с помощью которой руководители компаний будут отслеживать эффективность работы средств предотвращения и обнаружения атак на всех этапах убийственной цепочки в своих компаниях и на основании этого принимать решения о распределении ресурсов. Все зависит от нужд руководства.

Интересно, что и правительственные, и коммерческие разведслужбы используют одну и ту же терминологию для описания услуг, которые они предоставляют своим клиентам. И те и другие называют их продуктами. Я не могу это доказать, но, по-моему, общее употребление этого термина чисто случайно. Тем не менее в том, что касается создаваемых ими продуктов, обе группы должны действовать примерно одинаково. В лучшем случае для каждого коммерческого продукта и продукта разведки должен быть назначен продакт-менеджер, в обязанности которого входят определение его текущего состояния, разработка дорожной карты для будущих изменений и планирование окончания срока службы.

Дело в том, что дизайн продукта разведки не менее важен, чем сам ее процесс. CTI-команда может проделать отличную работу на всех этапах жизненного цикла разведки, но если она не представит конечный продукт начальникам в доступном для понимания и использования виде, то весь процесс пойдет насмарку.

Когда я был вторым лейтенантом, наш командующий каждое утро обходил всех и спрашивал, сварили ли они кофе. По образованию он был учителем, и у него была теория. Представьте, что вы пошли в школу, чтобы освоить десятиэтапный процесс варки кофе, и на первом экзамене безупречно выполнили первые девять этапов, но не смогли включить кофейник в розетку. Какую оценку вы бы получили? Пятерку за то, что достигли 90%-ного результата? Или двойку, потому что так и не смогли сварить кофе? По его мнению, вы должны были получить двойку, потому что кофе так и не был сварен. В контексте армейской подготовки это означало, что все необходимо свести к основным задачам и не беспокоиться о посторонних вещах. При этом основные задачи следует выполнять без ошибок. Если подумать, то это похоже на наш абсолютный базовый принцип кибербезопасности, который сводится к снижению вероятности нанесения организации существенного ущерба в результате киберсобытия, а не к заботе о мелочах, которые на нее не влияют.

Жизненный цикл разведки — производство и распространение. Это может показаться очевидным, но от выбранного вами способа распространения продуктов разведки зависит их полезность для руководства. Распространяете ли вы эти продукты по электронной почте, через Slack или другой механизм? А может быть, ваши клиенты забирают их с веб-сайта, SaaS-платформы или чего-то еще? Или эти разведданные доступны движку DevSecOps в рамках инфраструктуры как кода (см. главу 7), который не требует участия человека в процессе принятия решений? И насколько своевременно вы представляете разведданные? Как и в случае с дизайном продуктов разведки, этот вопрос может показаться почти тривиальным, но это не так. Разумеется, вы должны отправить продукт тому, кто его прочитает и каким-то образом использует. Однако если в еженедельном сводном аналитическом отчете содержится информация, способная сэкономить компании миллионы долларов, а он попадет в папку со спамом в почте генерального директора или не будет прочитан, потому что окажется погребенным под лавиной других документов, на ознакомление с которыми у него нет времени, или дойдет до него уже после наступления события, то жизненный цикл разведки будет нарушен. Способ избежать этого зависит от организационной структуры, имеющихся в вашем распоряжении инструментов распространения, культуры производства и личностных качеств руководителей. Единого решения, подходящего для любых случаев, не существует, поэтому вы должны хорошо продумывать механизм доставки каждого продукта разведки и корректировать его по мере необходимости. Это означает, что жизненный цикл разведки должен предусматривать этап получения обратной связи.

Жизненный цикл разведки — планирование и получение обратной связи. Само собой разумеется, что если создаваемые вами продукты разведки не приносят пользы, то, возможно, их не стоит и создавать. Получение отзывов об их полезности и способах улучшения — неотъемлемая часть процесса разведки. Как и в случае с менеджерами по коммерческим продуктам и руководителями служб безопасности, ключевым компонентом работы менеджера по продуктам разведки является опрос клиентов на предмет того, что им нравится, а что — нет и что они хотели бы видеть в будущем.

За свою карьеру я трижды официально занимал должность CISO, а если учесть работу в качестве командира ACERT (CISO в армии США), то четырежды. Если я и добивался успеха на этих должностях, то отчасти благодаря тому, что регулярно общался с руководителями организаций (клиентами), чтобы узнать их мнение о программах, над которыми работал.

Будьте безжалостны. Если продукт разведки, который создается каждую неделю благодаря усилиям вашей CTI-команды и который, по вашему мнению, — самое лучшее со времен появления нарезанного хлеба, но при этом его никто не потребляет, значит, у вас проблема. Либо никто из ваших бизнес-лидеров не считает его полезным, либо они его не понимают, либо он доставляется таким способом, который затрудняет ознакомление с ним. В этом случае вам нужно либо принять решение об окончании срока службы этого продукта, либо кардинально пересмотреть его дизайн.

Как и я, Стив Винтерфельд (один из редакторов этой книги) в начале 2000-х годов, на заре киберэпохи, был новоиспеченным сетевым защитником в армии США. Тогда мы не знали точно, что стоит отслеживать, а что — нет. Оба регулярно передавали своим командирам списки технических вещей: например, десяти серьезнейших уязвимостей в армейском программном обеспечении, десяти важнейших IP-адресов Китая, десяти опаснейших вирусов, выявленных в армейских сетях, и т. д. Через некоторое время мы заметили, что командиры перестали обращать внимание на то, что мы говорим. Лишь много позже мы осознали, что это объяснялось невозможностью принимать решения на основе этой информации. Мы преподносили им новости, а не разведданные. Требовалось заменить эту информацию чем-то более полезным. Гораздо позже, начав отслеживать активность различных государств в своих сетях, мы стали представлять разведданные, которые командир мог использовать для планирования и принятия решений.

Это касается и коммерческих разведывательных сервисов. В конце 2000-х годов я руководил одной из таких служб под названием iDefense (подразделение VeriSign). Многие из продаваемых нами продуктов напоминали те списки из десяти пунктов, которые я представлял своим командирам в армии, то есть новостные сводки о том, чем занимаются различные хакерские группы по всему миру. Тогда в прессе редко появлялись подобные сообщения, поэтому некоторые организации их ценили. Сегодня в открытых источниках содержится так много информации об этом, что ее трудно даже потребить. Но, оглядываясь назад, могу сказать, что наши продукты не были полноценными разведывательными отчетами. Должен признать, что руководители не могли принимать решения на их основе.

Процесс разведки в условиях ограниченного бюджета. Описанный ранее жизненный цикл стратегии предотвращения реализации убийственной цепочки вторжений предполагает наличие неограниченных ресурсов. У большинства из нас их нет, особенно если речь идет о малом и среднем бизнесе. Что же делать сетевому защитнику в таких условиях?

Независимо от размера организации вам следует искать поставщиков средств безопасности, которые уже делают эту работу за вас. Я бы сосредоточился на основных платформах для обеспечения информационной безопасности и продуктах для конечных точек. Эти поставщики вкладывают значительные средства в развитие своих команд киберразведки как для улучшения их продуктов, так и для демонстрации всему миру того, насколько хорошо они ориентируются в ИБ-ландшафте. Выбирайте тех, кто уже принял стратегию предотвращения реализации kill chain. Они должны отслеживать кампании противников и создавать средства их предотвращения для своих продуктов. Воздействуйте на них с помощью чековой книжки. Не покупайте их продукты, если они напрямую не поддерживают вашу программу инфобезопасности, базирующуюся на первичном принципе, и, в частности, стратегию предотвращения реализации убийственной цепочки вторжений. Направьте их на сайт MITRE ATT&CK Evaluation, на котором поставщики могут доказать, что их набор продуктов позволяет справиться с конкретными кампаниями противника.

Еще лучше выбирать поставщиков, входящих в Cyber Threat Alliance (организация, занимающаяся анализом и обменом информацией, ISAO). На момент написания книги в этой группе состояли около 34 поставщиков, которые договорились делиться друг с другом данными о сценариях действий киберпротивников, чтобы их клиентам не приходилось собирать их самостоятельно. Они также условились, что не будут конкурировать в области качества собираемых, обрабатываемых и распространяемых разведданных. Вместо этого станут соревноваться в том, насколько эффективно их наборы продуктов используют эти разведданные для предотвращения успеха вражеских кампаний. Отличие клуба от других подобных организаций заключается в том, что все члены должны делиться информацией, чтобы состоять в нем, кроме того, для них существует минимальная ежедневная квота. Если вы покупаете и устанавливаете продукт одного из этих поставщиков, то получаете не только услугу по отслеживанию вражеских кампаний от соответствующей команды разведки, но и доступ к результатам работы всех 34 поставщиков. Коллекция разведданных CTA является, пожалуй, самой полной и полезной в отрасли и в этом смысле может конкурировать с результатами работы разведслужб правительства США. Для создания

своей платформы обмена информацией они используют язык STIX [262] и фреймворк MITRE ATT&CK.

По данным некоммерческой организации OASIS, способствующей развитию открытых стандартов в сфере Интернета, аббревиатура STIX расшифровывается как structured threat information expression («структурированное представление информации об угрозах») и обозначает «язык с открытым исходным кодом и формат сериализации, используемый для обмена информацией о киберугрозах» [119]. Данная концепция возникла благодаря электронной рассылке Idea Exchange Working Group (IDXWG), созданной членами US-CERT и CERT.org в 2010 году для обсуждения автоматизированного обмена данными о киберинцидентах [289]. В 2022-м STIX фактически стал стандартным форматом для хранения информации о киберугрозах.

Если ваша организация невелика и не располагает ресурсами для создания группы разведки, способной отслеживать все известные кампании противника, покупайте и устанавливайте продукты обеспечения безопасности у тех поставщиков, которые это делают. Используйте свою чековую книжку, чтобы побудить этих поставщиков участвовать в программах MITRE ATT&CK Evaluation и Cyber Threat Alliance [105]. Это ничего не будет вам стоить, но сделает все сообщество более безопасным. А самое замечательное заключается в том, что при этом вы сможете использовать продукт работы высококлассных команд аналитиков для поддержки своей стратегии предотвращения реализации убийственной цепочки вторжений.

Операции киберразведки как путешествие

На заре развития Интернета создание полноценной команды разведки казалось большинству сетевых защитников настоящей роскошью. Однако в ходе анализа своей ИБ-программы, базирующейся на основополагающем принципе кибербезопасности, мы осознали, что без нее не сможем реализовать ключевые стратегии нулевого доверия, предотвращения реализации убийственной цепочки вторжений, обеспечения устойчивости, автоматизации и оценки рисков. Тем не менее очевидно, что многие не имеют необходимых для ее создания ресурсов. Однако помните, что стратегии — это направление. Вам не обязательно прямо сегодня создавать в своей организации эквивалент АНБ, чтобы получить пользу от этой работы. Это то, к чему всем нам следует стремиться. А пока можете найти поставщиков, которые делают эту работу за вас. Побуждайте их к поддержке ваших программ, базирующихся

на основополагающем принципе кибербезопасности, с помощью чековой книжки. Воспользуйтесь результатами работы программ MITRE ATT&CK Evaluation и Cyber Threat Alliance. Поддерживайте их при любой возможности. Эти усилия делают все сообщество более безопасным и обеспечивают более дешевый способ реализации вашей ИБ-программы.

Операции «красной»/«синей»/ «фиолетовой» команды: тактика предотвращения реализации убийственной цепочки вторжения

«Красная» команда — это своеобразное средство защиты, которое лидеры могут использовать для снижения влияния группового мышления. Этот термин был введен в 1972 году психологом Ирвингом Л. Дженисом, который заметил, что многие люди стремятся не перечить группе, даже если считают общепринятую идею ошибочной [123]. При создании «красной» команды руководство выделяет ресурсы для озвучивания позиции, противоположной общепринятой, в попытке преодолеть тенденцию группового мышления.

Уильям Каплан, автор книги *Why Dissent Matters*, называет «красную» команду десятым человеком [127]: «Десятый человек — это адвокат дьявола. Если в комнате находятся десять человек и девять из них согласны друг с другом, то роль десятого заключается в том, чтобы не соглашаться и указывать на недостатки решения, к которому пришла группа». По его словам, концепция десятого человека родилась из печально известного примера группового мышления — Октябрьской войны Судного дня 1973 года (четвертой арабо-израильской войны, которая велась между Израилем и коалицией арабских государств).

Израильские военные планировщики потерпели классический провал в разведке, когда приняли за основу концепцию «арабских намерений — мировоззрения, не предусматривающего возможности полномасштабного нападения». Они были совершенно не правы. В священный иудейский праздник Йом-кипур египетские и сирийские войска начали полномасштабную атаку на Израиль. По словам Каплана, после этого израильская Комиссия Агранат, собранная правительством для расследования недостатков в работе Армии обороны Израиля (ЦАХАЛ), «создала два новых инструмента: должность десятого человека, также называемую отделом ревизии, и возможность писать служебные записки, содержащие иное мнение».

Римская католическая церковь изобрела аналог «красной» команды в 1587 году, когда папа Сикст V ввел должность адвоката дьявола в процессе беатификации святого Лаврентия Юстиниана (1381–1456) [143]. Согласно Эллен Ллойд из Ancient Pages, этот Advocatus Diaboli должен был играть роль противоборствующей силы, «красной» команды, чтобы гарантировать, что «ни один человек не будет причислен к лику святых необоснованно и слишком быстро. Каждый потенциальный недостаток или возражение должны быть оглашены и оценены, чтобы обеспечить канонизацию лишь поистине достойных».

История знает немало примеров, когда руководство крупных организаций использовало «красную» команду в качестве инструмента. Президент Рейган задействовал эту концепцию еще в 1982 году, сформировав «красную» команду, призванную предугадать все мыслимые способы, которыми Советы могли попытаться обойти договоренности в сфере контроля над вооружениями [183]. После взрыва самолета авиакомпании Pan American, выполнявшего рейс PA-103, в 1988 году президентская комиссия поручила Федеральному управлению гражданской авиации создать «красную» команду для воспроизведения типичных тактик, техник и процедур террористов. В 1998-м Дональд Рамсфелд, будучи председателем Комиссии по оценке угрозы баллистических ракет, состоящей из девяти членов, использовал «красную» команду для проработки различных сценариев на основе данных, имеющихся в распоряжении разведывательного сообщества [190].

В 2003 году, когда я был командиром ACERT, военная разведка обнаружила, что в наших сетях орудуют хакеры, работающие на китайское правительство. Мы объединили всю эту хакерскую активность под кодовым названием TITAN RAIN. Мне нравятся круто звучащие кодовые названия. Это одна из причин того, почему мне нравится заниматься кибербезопасностью. У нас есть крутые названия буквально для всего. Однако на этот раз речь шла не об учениях. Все было по-настоящему. Наша «синяя» команда разработала план защиты, позволяющий противостоять наступательной кампании TITAN RAIN. Но прежде, чем внедрять, мы решили его проверить. Смоделировали сеть NIPRNET на киберполигоне ВВС в Сан-Антонио, развернули оборонительный план «синей» команды и поручили «красной» команде использовать тактики, техники и процедуры TITAN RAIN для прорыва. Когда «красная» команда потерпела поражение, армейское руководство дало нам разрешение на развертывание защитного плана «синей» команды в сети NIPRNET.

В ходе военных учений планировщики для обозначения противоборствующих сторон обычно используют два цвета: синий — для хороших парней, красный — для плохих. Их выбор не случаен. Мы можем поблагодарить за него прусскую армию. Питер Аттиа так писал об этом: «В начале XIX века в прусской армии стали проводиться военные игры для обучения офицеров. Одна группа офицеров разрабатывала план сражения, а другая брала на себя роль оппозиции и пыталась помешать его реализации. В настольной игре "Кригшпиль" (Kriegsspiel в переводе с немецкого буквально "военная игра"), напоминающей популярную настольную игру "Риск", синие фишки обозначали прусскую армию, поскольку большинство прусских солдат носили синие мундиры. Красные фишки представляли вражеские силы — "красную" команду, и с тех пор это название закрепилось» [18].

Когда в 1960-х годах мейнфреймы начали подключать к сети, компьютерные эксперты быстро осознали их уязвимость. Первые разработчики мейнфреймов не имели ни малейшего понятия о модели угроз. Они были озабочены лишь тем, как заставить единицы и нули двигаться в правильном направлении. Но эта ситуация стала быстро меняться. На, пожалуй, первой в истории конференции по кибербезопасности, организованной компанией System Development Corporation в Калифорнии в 1965 году, 15 000 операторов мейнфреймов со всего мира обсуждали способы, с помощью которых недобросовестные люди могут проникнуть в эти новые машины [64].

В конце 1960-х — начале 1970-х годов среди элитных компьютерщиков распространялся документ, написанный доктором Уиллисом Уэром в соавторстве с другими специалистами, под названием *Willis Paper*, в котором, по словам Уильяма Ханта из Колледжа Вильгельма и Марии, «было описано, как шпионы могут взламывать компьютеры, красть или копировать электронные файлы и нарушать работу устройств, используемых для защиты секретной информации. Это исследование положило начало более чем десятилетней работе элитных групп ученых-компьютерщиков, нанятых правительством для проникновения в компьютерные системы, хранящие секретные данные. Все их попытки оказались успешными» [309]. Это были первые пентестеры.

В 1971 году ВВС США заключили контракт с Джеймсом Андерсоном на проведение испытаний с участием «Команды тигров», пытающейся взломать операционную систему Multiplexed Information and Computing Service (MULTICS), предшественницу UNIX. В отчете Андерсона за 1972 год была описана методология проникновения и компрометации этих систем, которая и сегодня является основой всех тестов на проникновение [8].

В настоящее время разница между пентестерами и участниками «красных» команд заключается в том, что пентестеры стремятся выявить любой изъян в системе, подобно адвокату дьявола, и в ходе тестирования им разрешается действовать как угодно. Они пытаются найти способы уменьшения поверхности атаки путем обнаружения ранее неизвестных слабых мест. В этом отношении проведение тестов на проникновение относится к стратегии нулевого доверия (см. главу 3). Сетевые защитники не стремятся остановить конкретного противника с помощью проводимых ими тестов. Они активно ищут бреши в развернутой системе защиты.

Специалисты из «красных» команд, напротив, обычно отслеживают известные кампании противника. Например, согласно базе знаний MITRE ATT&CK кампания, известная как Cobalt Spider, предусматривает использование 31 метода атаки и пяти программных инструментов для компрометации жертв. «Красная» команда, проверяющая сеть организации на предмет ее защиты от атаки Cobalt Spider, может использовать лишь эти 31 метод и пять программных инструментов и больше ничего. Это похоже на мою армейскую историю с TITAN RAIN, о которой я рассказывал ранее. В ходе этого мероприятия сетевые защитники стараются убедиться в том, что атака Cobalt Spider не будет успешно реализована на всех этапах убийственной цепочки.

«Синяя» команда состоит из сотрудников внутренней службы информационной безопасности. В дополнение к повседневной работе по защите организации они берут на себя дополнительную задачу по обнаружению и предотвращению успешной эмуляции атаки Cobalt Spider «красной» командой. В качестве «красной» команды может выступать отдельная наступательная группа, состоящая из сотрудников организации и снабженная знаниями внутренней команды киберразведки об атаке Cobalt Spider, или внешний подрядчик, специализирующийся на предоставлении подобных услуг.

Иногда сетевые защитники называют мероприятие с участием противоборствующих сил операцией *«фиолетовой» команды*, цвет которой является результатом смешения красного и синего. Участие «синей» команды в операциях «красной» дает внутренней службе информационной безопасности несколько дополнительных преимуществ. Во-первых, «синяя» команда получает возможность отработать сценарии реагирования на инциденты, столкнувшись с реальным противником. Кроме того, после окончания этих учений или каждого из их этапов защитники могут спросить у противника,

что он сделал в ответ на действия «синей» команды. Во время реальной атаки Cobalt Spider такого шанса у них не будет. Второе преимущество заключается в возможности индивидуального обучения новичков и аналитиков среднего уровня, входящих в команду, занимающуюся защитой информации. Сидя в SOC-центре и наблюдая за оповещениями, которые не были отловлены инструментами SOAR и SIEM, они мало чему учатся. Но стоит подключить их к участию в учениях «красной» и «синей» команд — их уровень профессионализма начинает быстро повышаться. Подобное обучение бесценно.

Концепция «красной» команды существует по меньшей мере с начала XVI века. В ИТ-пространстве она появилась в виде групп пентестеров в 1960-х и 1970-х годах, когда мейнфреймы стали использоваться в целях государственного управления и коммерческих. С тех пор мы используем тестирование на проникновение для уменьшения поверхности атаки в рамках реализации стратегии нулевого доверия. В начале 2000-х годов стало популярным проведение совместных учений «красной» и «синей» команд, или, если хотите, «фиолетовой» команды, направленных на проверку эффективности существующих средств защиты от атак известных противников по принципу убийственной цепочки. Это обеспечило дополнительные преимущества в виде тренировки групп реагирования на инциденты и ускорения обучения новичков и аналитиков SOC-центра среднего уровня подготовки. Операции «красной» и «синей» команд — важный элемент в наборе инструментов обеспечения информационной безопасности, который помогает снизить вероятность существенного ущерба в результате киберинцидента.

Обмен разведданными: тактика предотвращения реализации убийственной цепочки вторжения

В классическом романе Дж. Р. Р. Толкина «Властелин колец» Гэндальф Серый после долгих лет исследований и размышлений делает открытие [333]. Он понимает, что волшебное кольцо, делающее Бильбо Бэггинса невидимым, — то самое, которое он использовал, чтобы обманом заставить Голлума показать ему выход из пещер под Туманными горами, а также для того, чтобы спрятаться от Смауга в Большом зале Эребора, — на самом

деле является кольцом всевластья. Это единственное оружие, с помощью которого главный злодей Саурон мог бы завоевать все Средиземье, однако в случае уничтожения этого кольца у него не было бы на это никаких шансов. Таким образом, Гэндальф Серый, вероятно, стал первым разведаналитиком, когда-либо изображенным в фэнтезийном романе. Это я просто к слову.

Гэндальф и Элронд (владыка Ривенделла) принимают неординарное решение поделиться этими сведениями со своими соперниками: избранными членами Белого совета, различными кланами эльфов, хоббитами, гномами и людьми. Члены этой группы имеют конкурирующие интересы, но не испытывают ненависти друг к другу. У них нет согласия по многим вопросам, но в отношении уничтожения Саурона их интересы полностью совпадают. Чтобы облегчить решение общей задачи, вполне логично поделиться этой ключевой информацией.

Это идеальная аналогия для современного процесса обмена разведданными в области кибербезопасности. Даже если в мире бизнеса мы конкурируем по всем вопросам, мы можем объединить усилия, чтобы защититься от общей угрозы. Например, несколько банков могут безжалостно конкурировать друг с другом на рынке. Однако злоумышленники, занимающиеся киберпреступностью и кибермошенничеством, действуют не против одного-единственного банка-жертвы. Когда злоумышленники добиваются успеха, они наносят удар по всей отрасли. Это заставляет клиентов терять веру в систему, бояться ее и не доверять ей свои деньги. То же самое можно сказать и о государствах, которые пытаются разорить противника, атакуя его финансовую систему. Такие атаки наносят ущерб не только банку-жертве и финансовому сектору — они отражаются на всей стране, что подрывает доверие ко всей банковской системе. Именно поэтому банковскому сообществу и правительству имеет смысл делиться друг с другом сведениями о киберугрозах, чтобы совместными усилиями победить общего врага.

Все это звучит замечательно, однако в системе существует определенное трение. То, что все мы осознаем наличие общей угрозы, не отменяет недоверия, которое мы испытываем к нашим противникам. Свободные альянсы по обмену разведданными очень трудно удержать от распада и сделать полезными. Даже в книге Толкина братство кольца, состоящее из людей, гномов, эльфов и хоббитов, распалось из-за проблем с доверием.

Таким образом, возникает вопрос: какие подходы работают сегодня в сфере обмена информацией о киберугрозах? Каково текущее состояние этой системы и как можно повысить ее полезность?

Взлом, о котором слышали во всем мире. Второго ноября 1988 года примерно в 20:30 23-летний аспирант Корнельского университета Роберт Таппан Моррис выпустил первого компьютерного червя. По данным ФБР, в течение 24 часов 10 % из 60 000 компьютеров, подключенных на тот момент к Интернету, были выведены из строя [231]. Червь Морриса стал первым глобальным примером применения разрушительного интернет-червя. До этого никто даже не предполагал, что злоумышленники могут использовать в своих целях весь Интернет. Администраторам пострадавших компьютеров пришлось самостоятельно справляться с проблемой, поскольку в то время схемы совместного реагирования на инциденты и обмена информацией еще не были проработаны.

Первые системы ISAC. Как упоминалось в разделе, посвященном SOC-центрам, первые правительственные группы CERT были созданы после появления червя Морриса в 1988 году. Они стали первыми попытками правительств донести информацию об обеспечении кибербезопасности до общественности.

К концу 1990-х годов многие ИБ-специалисты начали осознавать, что им требуется более совершенная система обмена информацией, позволяющая не ограничиваться простым реагированием на такие глобальные инциденты, как появление червя Морриса. Приближался Y2K (2000 год), представлявший собой еще одну глобальную угрозу не только для Интернета, но и для сферы бизнес-вычислений. Согласно Investopedia, под проблемой Y2K понималась «широко распространенная ошибка в компьютерном программировании, которая могла спровоцировать масштабный сбой при смене года с 1999-го на 2000-й» [96]. На заре компьютерной эры программисты, использовавшие язык Cobol, обозначали даты двумя, а не четырьмя цифрами, и ИТ-эксперты ожидали, что с наступлением нового тысячелетия миллионы строк кода реализации бизнес-логики перестанут работать.

Учитывая проблему Y2K и ряд других факторов, президент США Клинтон создал систему ISAC — структуру центров анализа и обмена информацией [50]. Он создал эту систему специально для определенных секторов критической инфраструктуры и намеренно не ввел конкретных требований,

чтобы поощрить разработку инновационных подходов к обмену информацией.

В преддверии наступления нового тысячелетия я отвечал за безопасность сети армейского оперативного центра Пентагона (Army Operations Center, AOC). Круглосуточно работающий AOC представляет собой штаб армии США, откуда поступают все приказы подразделениям на местах. Можете себе представить, как обеспокоено было американское командование возможным нарушением работы в армии, а то и во всем мире. В дополнение к обширной армейской программе обновления кода Cobol, которая продолжалась на протяжении многих лет до фактического наступления 2000 года, AOC-центр вел специальное наблюдение до и во время этого события, чтобы вовремя заметить сбои в компьютерных системах. Мы, так сказать, следовали за солнцем, однако после нескольких лет опасений по поводу грозных предупреждений о возможном конце света при наступлении нового, 2000 года так ничего и не произошло. В связи с этим возникает вопрос: раздули ли сторонники существования проблемы Y2K (к числу которых принадлежал и я) связанную с ней угрозу или программы по улучшению кода Cobol помогли снизить соответствующий риск? Этого мы никогда не узнаем.

FS-ISAC. Из всех ISAC, созданных в те первые годы, ISAC финансового сектора (Financial Sector ISAC, FS-ISAC) стала самой организованной и наиболее обеспеченной ресурсами системой следующего десятилетия. Лидеры банковского сектора привлекли к этому проекту своих самых крупных мыслителей и специалистов [110]. Дениз Андерсон (на момент написания этой книги — президент и генеральный директор Health ISAC) стала сотрудником FS-ISAC № 2 после того, как эта организация наняла первого генерального директора Билла Нельсона. Он нанял Андерсон в качестве своего рода главного операционного директора, которому было поручено пасти котов. По словам Андерсон, Нельсону понравилось то, что она была пожарным-добровольцем и понимала важность и серьезность работы сотрудников служб быстрого реагирования.

Андерсон говорила, что успех FS-ISAC зависел от дальновидных лидеров, которые верили в концепцию обмена информацией. Они завоевали доверие, настояв на том, чтобы их организации внесли свой вклад. Такие люди, как Байрон Колли (работавший в Wells Fargo, а затем в Goldman Sachs),

Джейсон Хили и Фил Венаблс (сотрудники Goldman Sachs), а также Марк Клэнси, Гэри Оуэн и Эррол Вайс (сотрудники Citigroup), подавали пример и настаивали на том, чтобы их организации делились оперативной информацией с членами FS-ISAC.

> Я знаю, насколько важно лидерство, основанное на собственном примере. В 2012 году я способствовал основанию Cyber Threat Alliance — первой организации ISAO для поставщиков систем безопасности. Согласно главному принципу Cyber Threat Alliance каждый участник должен был ежедневно делиться разведывательной информацией, за количеством которой мы пристально следили. Я поставил перед своей командой в Palo Alto Networks задачу делать самый большой вклад. В те дни, когда Palo Alto Networks занимала первое место, я высмеивал других членов альянса за то, что они халтурили. На следующий день, когда они оказывались на вершине таблицы лидеров, высмеивали уже меня.

Протокол Traffic Light. Даже несмотря на пример, подаваемый Citigroup, Goldman Sachs и Wells Fargo, установить доверие между членами FS-ISAC было непросто. По мнению Андерсон и Вайса, одним из ключевых нововведений, которое этому способствовало, была формализация протокола Traffic Light («Светофор»). Координационный центр безопасности национальной инфраструктуры Великобритании (ныне Центр по защите национальных объектов инфраструктуры) разработал протокол Traffic Light (TLP) в качестве метода маркировки и обработки конфиденциальной информации. Билл Нельсон и Байрон Колли узнали о нем на встрече MI5 в Лондоне и внедрили его в FS-ISAC.

По словам Эрика Луийфа и Алларда Кернкама, авторов статьи *Sharing Cyber Security Information Good Practice Stemming from the Dutch Public-Private-Participation Approach*, протокол TLP представляет собой простой метод маркировки и обработки конфиденциальной информации [145]. Один из ключевых принципов TLP заключается в том, что тот, кто предоставляет конфиденциальную информацию, также определяет, может ли эта информация распространяться и насколько широко. Для этого он помечает ее одним из четырех цветов:

- *красный* — информация доступна ограниченной части группы;
- *желтый* — информация доступна членам группы, от которых ожидается некое действие;

- *зеленый* — информация доступна всей группе;
- *белый* — публичная информация.

По словам Андерсон и Вайса, Джим Рут, в то время бывший директором по информационной безопасности в компании Depository Trust & Clearing Corporation, сыграл важную роль в формализации протокола Traffic Light для FS-ISAC. Это означало, что каждое сообщение, передаваемое участниками через портал FS-ISAC, должно было помечаться соответствующим цветом. Благодаря этому члены FS-ISAC стали с меньшей опаской делиться конфиденциальной информацией, поскольку видели, что для ее обработки существуют формализованные процессы.

Андерсон рассказала, что после успешного внедрения протокола TLP в FS-ISAC Форум групп реагирования на инциденты информационной безопасности (FIRST) перенял этот передовой опыт для реализации собственных миссий. Сегодня TLP — стандартная практика для большинства организаций, занимающихся обменом данными.

По словам Вайса, в тот момент все ISAC обменивались информацией о событиях, связанных с реагированием на киберинциденты, передовым опытом борьбы с экзистенциальными угрозами, такими как проблема Y2K, и лучшими практиками. После формализации процедур обмена разведданными, то есть ответа на вопрос «как?», возник вопрос о том, чем именно члены организации собираются обмениваться. Это должны были быть информация и разведданные, ставшие причиной объединения участников.

В начале 2000-х годов Джейсон Хили и Байрон Колли создали комитет FS-ISAC, объединивший разведку угроз с операциями SOC-центра.

Организации ISAC и правительство США. По данным Агентства по кибербезопасности и защите инфраструктуры (CISA) при правительстве США, ISAC представляют собой «некоммерческие организации, созданные владельцами и операторами объектов критической инфраструктуры для обмена данными между правительством и промышленностью» [47].

CISA координирует работу со всеми ISAC в соответствии с директивой президента Клинтона. Но, как сообщается на сайте CISA, некоторым ISAC уделяется особое внимание в силу их характера. К ним относятся:

- *Многоштатный центр обмена информацией и ее анализа* (Multi-State Information Sharing and Analysis Center, MS-ISAC) — организация ISAC для правительств штатов, местных, племенных и территориальных органов власти;

- *коммуникационные ISAC* — организации ISAC для основных операторов связи страны;
- *Центр обмена информацией о финансовых услугах и ее анализа* (Financial Services Information Sharing and Analysis Center, FS-ISAC) — организация ISAC для представителей финансового сектора;
- *Центр обмена авиационной информацией и ее анализа* (Aviation Information Sharing and Analysis Center, A-ISAC) — организация ISAC для представителей авиационной промышленности.

Первые Fusion-центры. Семнадцатого декабря 2004 года Конгресс США принял закон о реформировании разведки и предотвращении терроризма (Intelligence Reform and Terrorism Prevention Act, IRTPA), чтобы обеспечить анализ и ситуационную осведомленность, в том числе в сфере кибербезопасности, на уровне штатов и городов. Орган, отвечающий за эту деятельность, получил название Fusion-центра [55]. По данным департамента правоохранительных органов Флориды за 2022 год, «Fusion-центры были созданы после терактов 11 сентября 2001 года для объединения критически важной информации, хранящейся в различных ведомствах, и обмена разведданными в целях защиты населения» [86]. На момент написания книги в США существовало 79 таких центров.

Первые ISAO. Считается, что ФБР основало первую организацию ISAO в 1996 году, хотя это название появилось лишь два десятилетия спустя. Изначально она называлась InfraGard National Members Alliance или InfraGard National и была призвана упростить обмен информацией между правоохранительными органами и представителями частного сектора [234]. Организация InfraGard — это не CERT-центр, хотя и выполняет схожие функции. Она также не является ISAC, поскольку не обслуживает ни один из секторов критической инфраструктуры правительства США. Это нечто другое. Создав организацию InfraGard, ФБР опередило время, раньше многих осознав то, что сообщества единомышленников могут захотеть обмениваться разведывательной информацией об общих угрозах, в данном случае связанных с киберпреступностью.

И в самом начале, и сейчас одним из камней преткновения в сфере обмена информацией является страх того, что сам акт обмена данными о кибератаках может обернуться судебными исками против его участников. Юристы пострадавших организаций опасаются, что обнародование подобных сведений может побудить клиентов, считающих, что организация не обеспечила должной защиты их персональных данных, подать на нее в суд. Взвесив риск потенциальных исков и выгоду от обмена информацией с сообществом,

юристы сочли его нецелесообразным. Лишь много позже организации, занимающиеся обменом информацией, осознали, что им следует делиться разведданными, касающимися не жертвы, а действий противника на разных этапах убийственной цепочки. Другими словами, нужно обмениваться сведениями о ТТП хакеров, а не подробностями того, что произошло с их жертвой. Обмен такой информацией должен был способствовать усилению защиты всего сообщества.

В 2015 году президент США Обама подписал указ о создании структуры ISAO, который позволил обмениваться информацией о киберинцидентах, не опасаясь судебного преследования [168]. ISAO не зависит от сектора и может представлять собой любую группу организаций-единомышленников наподобие Cyber Threat Alliance. Данный указ также определил порядок финансирования организации по стандартизации ISAO. Кстати, я был сопредседателем Комитета по безопасности и конфиденциальности, способствуя ее созданию. На момент написания данной книги в организации по стандартизации было официально зарегистрировано чуть более 90 ISAO.

Другие правительственные программы обмена данными. По словам сотрудников MITRE Брюса Бакиса и Эдварда Ванга, Министерство внутренней безопасности (Department of Homeland Security, DHS) является центром американской экосистемы обмена информацией о кибербезопасности [21]. В 2018 году президент Трамп подписал закон о создании Агентства по кибербезопасности и охране инфраструктуры, благодаря которому внутри DHS было создано агентство CISA (Агентство по кибербезопасности и защите инфраструктуры США) [154]. Согласно информации, приведенной на официальном сайте министерства, CISA координирует действия по обеспечению кибербезопасности в интересах федерального правительства, выступает в качестве исполнительного органа, принимающего меры по реагированию на инциденты в сфере национальной кибероборонь, и отвечает за обмен разведданными. На CISA работают Национальный центр кибербезопасности и интеграции коммуникаций (National Cybersecurity and Communications Integration Center, NCCIC) и Американская группа реагирования на инциденты компьютерной безопасности (United States Computer Emergency Response Team, US-CERT).

Агентство CISA управляет четырьмя официальными программами обмена информацией — одной на уровне высшего руководства (Joint Cyber Defense Collaborative) и тремя на уровне операторов.

Совместное сотрудничество в области киберзащиты (Joint Cyber Defense Collaborative, JCDC) [281] — группа, созданная в августе 2021 года для расширения сотрудничества с частным сектором [61], состоящая из организаций государственного и частного секторов, а также федеральных, региональных, местных, племенных и территориальных органов власти, призванная объединить усилия высших руководителей из правительства и коммерческого сектора по решению глобальных проблем. Первым примером успешной работы этой группы стало ее реагирование на кризис, связанный с модулем Log4J в 2021 и 2022 годах [184].

Расширенные услуги по обеспечению кибербезопасности (Enhanced Cybersecurity Services, ECS) [274] — изначально нацеленный на поставщиков услуг связи указ № 13636, подписанный президентом Обамой в 2013 году, расширил действие этих услуг на 16 критических секторов инфраструктуры и соответствующие клиентские базы. Министерство внутренней безопасности делится конфиденциальными и секретными данными о киберугрозах с аккредитованными организациями с помощью автоматизированных средств.

Программа сотрудничества и обмена информацией в сфере кибербезопасности (Cyber Information Sharing and Collaboration Program, CISCP) [270] — Министерство внутренней безопасности распространяет несекретную информацию через доверенные государственно-частные партнерства во всех секторах критической инфраструктуры.

Программа Министерства внутренней безопасности по автоматическому обмену индикаторами (DHS Automated Indicator Sharing (AIS) program) [268] — обеспечивает двунаправленный межмашинный обмен несекретными индикаторами киберугроз между центром NCCIC и представителями частного и государственного сектора, организациями ISAC, ISAO, а также международными партнерами и компаниями.

Все это отличные механизмы для совместной работы и обмена разведданными о киберугрозах между правительством США и представителями частного сектора. Критика этих программ связана с тем, что разведданные, которыми делится правительство, оказываются не особенно полезными и в основном распространяются вручную. Программа AIS позволила автоматизировать этот процесс с помощью стандартов STIX и TAXII, однако качество разведданных, получаемых от правительства, было настолько низким, что большинство коммерческих организаций не стали ими пользоваться. Коммерческую

сторону программы JCDC представляет совокупность высококлассных поставщиков услуг обеспечения безопасности и облачных вычислений, таких как AWS, Cisco, Crowdstrike, Microsoft и Palo Alto Networks (на момент написания этой книги их насчитывалось 21), но механизмами обмена информацией являются Zoom-звонки и электронная почта. Спустя 30 лет после создания первых групп реагирования на инциденты компьютерной безопасности обмен информацией между правительством и частным сектором в основном по-прежнему осуществляется вручную и несистемно.

Будущее обмена информацией в сфере кибербезопасности. С точки зрения такой базирующейся на первичном принципе стратегии, как предотвращение реализации убийственной цепочки вторжения, обмен информацией и разведданными является важной тактикой, применяемой на всех уровнях. Правительственные организации, компании из списка Fortune 500 и поставщики систем безопасности имеют ресурсы для создания команд киберразведки, в режиме реального времени собирающих оперативную информацию о поведении противника на всех этапах убийственной цепочки. Как и в примере с советом Элронда, приведенном в начале главы, вполне логично, что эти организации будут делиться подобной информацией со всеми остальными — организациями ISAC, ISAO, Fusion-центрами, поставщиками MSSP, группами CERT, организационными SOC-центрами и обычными потребителями — в попытке обезопасить все сообщество. Тот факт, что у малых и средних организаций нет ресурсов для того, чтобы делать это самостоятельно, подчеркивает суть: имущие могут помочь неимущим. Большинство согласны придерживаться этой стратегии, однако используемая до сих пор ручная и несистемная тактика препятствует прогрессу. Нам необходимо не фундаментально менять стратегию, а внедрять современную тактику.

Представьте себе будущее, в котором некое правительство, обладающее необходимыми разведывательными ресурсами (например, правительство США или другой страны), отслеживает все известные кампании злоумышленников, руководствующихся всевозможными мотивами (преступление, шпионаж, война или низкоуровневый киберконфликт, хактивизм, пропаганда или простое озорство; см. рис. 4.2), в дополнение к активности различных государств, которую отслеживает база знаний MITRE ATT&CK. Теперь представьте, что это правительство отформатировало разведданные с помощью отраслевого стандарта (STIX) и наполнило ими базу знаний, используя модель убийственной цепочки компании Lockheed Martin, модель Diamond Министерства обороны США и фреймворк MITRE ATT&CK. Оно даже могло бы заплатить за все это организации MITRE, поскольку

та является научно-исследовательским центром, финансируемым из федерального бюджета. Затем представьте, что правительство предоставило API-интерфейс, позволяющий всем заинтересованным сторонам легко и автоматически потреблять эти разведданные (см. главу 7). Оно также могло бы разработать схему, в соответствии с которой эти заинтересованные стороны платили бы поставщикам систем безопасности, организациям, занимающимся обменом информацией, таким как ISAC и ISAO и др., за пополнение базы данных телеметрическими показателями, которые те собирают у своих клиентов и членов. Кроме того, правительство может разработать метод ранжирования разведданных по степени их практической полезности. Благодаря этому сетевые защитники, потребляющие разведданные, могут оценить вклад в базу знаний, а правительство — определить, сколько за него нужно заплатить.

Все это может показаться слишком сложным и с технической, и с политической точки зрения, но это не так. Что касается технической архитектуры, то соответствующие модели существуют уже несколько лет. Для реализации этого видения можно использовать как программу Министерства внутренней безопасности по автоматическому обмену индикаторами (AIS), так и систему Cyber Threat Alliance и продукты поставщиков коммерческих систем безопасности. Что касается политики, то правительство США демонстрирует заинтересованность в финансировании программ обмена информацией с 1998 года. Таким образом, это не вопрос воли и ноу-хау. Это вопрос ви́дения.

Единственное замечание в адрес этой концепции заключается в том, что если это новое хранилище разведданных о вражеских кампаниях будет открыто для всех желающих, то и злоумышленники смогут получить к нему доступ. Используя эти данные, они с легкостью узнают о том, что известно потенциальным жертвам об их стратегиях и тактиках. Это поможет им разработать схемы, позволяющие обходить средства предотвращения и обнаружения вторжений, которые жертвы устанавливают для защиты от хакерских кампаний. Все это имеет смысл, но это не реальная угроза.

По сути, эта критика связана со старой проблемой источников и методов, с которой разведывательные организации имеют дело с библейских времен. Мы не хотим, чтобы потенциальные враги знали о том, что нам о них известно и как мы получили эти разведданные, поскольку они могут использовать это против нас. Однако в эпоху DevOps и инфраструктуры как кода это уже не столь важно. Если все сообщество ИБ-специалистов в режиме реального времени обменивается информацией о хакерских кампаниях, которых

в Интернете в любой день насчитывается менее 500, то бремя поиска новых ТТП, о которых не знает ни одна потенциальная жертва, становится неподъемным для отдельной хакерской группы. Даже если она однажды добьется успеха, сообщество быстро поделится этой информацией, что сделает кампанию невоспроизводимой. Даже создание таких новых инструментов, как вредоносное ПО и эксплойты, обходится довольно дорого. Еще дороже с нуля создавать последовательности атак для одноразового использования.

Однако сообщество по обмену разведданными еще очень далеко от реализации этого видения. Для этого у нас уже есть все необходимое, но кто-то должен собрать все воедино. Это мог бы сделать коммерческий сектор, но цена за эту услугу почти наверняка сделает невозможным ее получение малыми и средними организациями, что сведет изначальную задумку на нет. Я не утверждаю, что они не способны найти бизнес-модель, которая будет работать для всех. Я просто говорю, что пока не видел такой модели. Это означает, что какое-то правительство должно будет возглавить этот процесс, однако я пока не вижу ни одной организации, которая бы за это взялась.

Заключение

В этой главе я кратко описал исторические истоки трех наиболее важных моделей угроз последнего десятилетия: убийственной цепочки компании Lockheed Martin, модели Diamond, разработанной Министерством обороны США специально для команд киберразведки, и операционного фреймворка и базы знаний MITRE ATT&CK. Я подчеркнул, что эти модели не конкурируют между собой, а работают в связке друг с другом. Их использование правительственными и коммерческими CTI-командами привело к появлению таких красочных названий вражеских кампаний, как APT1, Fancy Bear, Lazarus Group и Charming Kitten. Однако я сделал оговорку, указав на то, что эти названия не обязательно определяют конкретных людей или правительства, стоящие за соответствующими атаками. Они обозначают последовательности действий хакеров на разных этапах убийственной цепочки, неоднократно наблюдаемые CTI-командами в реальности. Как бы нам ни хотелось связать активность Charming Kitten с иранским правительством, сообщество киберразведки не должно быть абсолютно уверенным в такой атрибуции, за исключением некоторых особых случаев. Но даже в этих случаях атрибуция не особо важна для сетевого защитника с точки зрения реализации стратегий, базирующихся на первичном принципе обеспечения кибербезопасности. Важна лишь атрибуция последовательности атаки, позволяющая всем сете-

вым защитникам развернуть в своем внутреннем стеке безопасности средства предотвращения и обнаружения вторжений для противодействия вражеской кампании на каждом этапе убийственной цепочки. Я также привел аргументы в пользу того, что в каждый конкретный день в Интернете реализуется не так уж много хакерских кампаний и что кому-то следует взять на себя задачу их отслеживания и предоставления собранных разведданных общественности.

Для предотвращения реализации убийственной цепочки вторжения я рекомендовал сетевым защитникам использовать следующие тактики:

- создать SOC-центр или по крайней мере поручить выполнение соответствующих функций одному или нескольким специалистам;
- создать команду киберразведки или хотя бы назначить одного или нескольких человек для выполнения соответствующих функций в рамках SOC-центра;
- оркестровать стек безопасности на всех островах данных с использованием новейших средств обнаружения и предотвращения вторжений на всех этапах убийственной цепочки;
- провести учения «фиолетовой» команды, в ходе которых одна ее половина («красная» команда) воспроизводит известные последовательности атак противника на внутреннюю сеть, а другая («синяя» команда) пытается им противостоять. На каждом этапе учений обе команды должны сравнивать свои результаты для повышения эффективности действий;
- организовать обмен разведданными о последовательностях атак с коллегами, официальными организациями по обмену информацией, такими как ISAC и ISAO, или воспользоваться услугами поставщиков средств безопасности, делающих это за вас.

Данная глава была посвящена способам предотвращения и обнаружения вторжений. В следующей главе я расскажу, что произойдет, если вам это не удастся. Помните: развертывание стратегии предотвращения реализации убийственной цепочки вторжения не гарантирует защиты от серьезного киберсобытия. Оно лишь снижает вероятность его наступления. В следующей главе поговорим об обеспечении устойчивости, позволяющей пережить такое событие.

05 Обеспечение устойчивости

> [Устойчивость — это]... способность последовательно добиваться намеченных результатов, несмотря на неблагоприятные киберсобытия.
>
> *Янис Стирна и Елена Здравкович, авторы работы Cyber Resilience — Fundamentals for a Definition*

> То, что нас не убивает, делает нас сильнее.
>
> *Фридрих Ницше, немецкий философ*

Обзор главы

В этой главе я приведу лучшее, по моему мнению, определение понятия устойчивости, а затем опишу четыре тактики ее обеспечения: кризисное планирование, резервное копирование и восстановление, шифрование и реагирование на инциденты. Далее покажу, что для реализации зрелой программы обеспечения устойчивости командам ИБ-специалистов необходимо провести довольно большую работу по планированию, которая обычно выражается в составлении корпоративных планов обеспечения непрерывности бизнеса и аварийного восстановления. В конце я расскажу об отработке этих планов с командой высшего руководства организации.

Что такое устойчивость

Организация ASIS International ввела понятие *киберустойчивости* еще в 2009 году, но оказалось, что данная концепция описывает скорее непрерывность бизнеса [216]. Далее в этой главе я расскажу о разнице между этими двумя понятиями. В 2010 году Министерство внутренней безопасности США определило устойчивость в киберпространстве как «способность адаптироваться к изменяющимся условиям, готовиться к сбоям, противостоять им и быстро восстанавливаться после них» [217]. В 2012-м на Всемирном экономическом форуме понятие *«киберустойчивость»* было определено так: «...способность систем и организаций противостоять киберинцидентам...» [221].

С тех пор оно было доработано другими деятелями. В 2017 году Международная организация по стандартизации (ISO) определила устойчивость как «...способность организации воспринимать изменяющиеся условия и адаптироваться к ним, позволяющая ей достигать поставленных целей, выживать и процветать» [287].

В 2019 году организация NIST стандартизировала определение *киберустойчивости* как «способность предвидеть неблагоприятные условия, стрессы, атаки или компрометацию систем, использующих киберресурсы, противостоять им, восстанавливаться после них и адаптироваться к ним» [271]. NIST также утверждает, что обсуждение киберустойчивости «основано на предположении о том, что противники будут периодически успешно обходить защиту». Это утверждение часто игнорируют и не понимают. Обеспечение киберустойчивости сводится не к защите системы от проникновения противника, а к тому, чтобы предположить ее успешный взлом и разработать план действий, позволяющий продолжить выполнение своей миссии после него.

Однако больше всего мне нравится определение, данное двумя исследователями из Стокгольмского университета в 2015 году. Янис Стирна и Елена Здравкович определяют устойчивость как «...способность последовательно добиваться намеченных результатов, несмотря на неблагоприятные киберсобытия» [32]. Допустите, что злоумышленники успешно пройдут все этапы убийственной цепочки и найдут брешь в вашей броне нулевого доверия, или просто предположите, что в какой-то момент в будущем произойдет масштабный сбой. Затем разработайте стратегию, гарантирующую функционирование основных служб вашей организации при наступлении этих событий.

Примеры устойчивости

Отличный пример устойчивости можно увидеть в фильмах «Терминатор» и «Терминатор-2». В первом фильме Терминатор был создан для выживания. Как и наши современные системы, герой Арнольда Шварценеггера был оснащен различными функциями для идентификации, защиты, обнаружения и реагирования, благодаря которым он мог выживать и защищаться. Однако после атаки Терминатор начал терять функциональность. К концу фильма его функции постепенно перестали работать. Он потерял способность идентифицировать, защищать, обнаруживать и реагировать. Но он выживал.

Терминатор T-1000 во втором фильме франшизы отличался не только живучестью, но и устойчивостью. Он мог предвидеть нападения, противостоять им, восстанавливаться и адаптироваться. Если в него стреляли, его тело поглощало пулю и восстанавливалось. Кроме того, если ему требовалось острое оружие, он мог трансформировать часть своего тела в меч. Точно так же цель обеспечения кибербезопасности не должна сводиться к выживанию. Она должна включать в себя элемент устойчивости, позволяющий организации выполнять свои функции и миссию в агрессивной киберсреде.

Фильм «Терминатор-2» — мой любимый пример устойчивости. Но обычно, когда я привожу этот пример людям моложе 30 лет, они говорят, что никогда не смотрели эти фильмы. Так что он не всегда работает так эффективно, как мне бы хотелось.

Мой любимый пример практической реализации устойчивости — то, что сотрудники Netflix называют *хаос-инженерией*. В главе 7 я подробно опишу конкретный случай, а здесь дам лишь общий обзор. В конце 2008 года инфраструктура Netflix пережила два крупных сбоя, из-за чего компания не смогла доставить DVD по почте своим клиентам [228]. В то время она переходила от традиционных методов разработки программного обеспечения к использованию лучших практик DevOps. В результате в 2011 году компания перевела свою инфраструктуру поддержки из локальной в облачную среду, чтобы обеспечить большую отказоустойчивость бизнес-процессов.

Небольшая команда инженеров Netflix создала свой первый модуль для обеспечения устойчивости под названием Chaos Monkey. Согласно информации с сайта Netflix, «Chaos Monkey — это инструмент, который в слу-

чайном порядке отключает наши производственные экземпляры, позволяя нам убедиться в том, что мы сможем пережить соответствующие сбои без последствий для наших клиентов» [228]. Иными словами, Netflix регулярно запускает приложение, делающее неработоспособными случайным образом выбранные части инфраструктуры, с которыми взаимодействуют клиенты, чтобы их сетевые архитекторы в совершенстве освоили инженерию устойчивости.

В моем мире катастрофы могут произойти когда-нибудь в будущем, но, скорее всего, никогда. По крайней мере я на это надеюсь. Однако в мире Netflix запланированные катастрофы происходят ежедневно. С момента внедрения оригинального модуля Chaos Monkey команда Netflix создала целую серию инструментов для управления хаосом, призванных повысить уверенность компании в том, что она способна пережить катастрофическое событие. Конечная цель Netflix — сделать так, чтобы клиенты не заметили сбоя в работе ее инфраструктуры и я мог продолжать смотреть эпизоды сериала «Ведьмак» так, будто ничего не произошло.

Некоторые сетевые защитники и ИТ-специалисты могли бы назвать действия Netflix впечатляющими и вдохновляющими. Но большинство из нас посчитали бы их безумными. Мы не собираемся выводить из строя свою ориентированную на клиентов инфраструктуру ради того, чтобы ее протестировать. Ее и так довольно сложно поддерживать в рабочем состоянии. Так думает большинство представителей нашего сообщества, и напрасно. Компания Netflix занялась обеспечением устойчивости своей инфраструктуры. Большинство остальных членов сообщества махнули на это рукой.

Еще одним примером обеспечения устойчивости, который я хотел бы привести, является работа команды инженеров по надежности сайтов (SRE-инженеров) компании Google [321]. В 2004 году, когда эта компания занималась только интернет-поиском, ее руководители приняли необычное решение. Вместо того чтобы создать команду сетевых инженеров для управления инфраструктурой, как делает любая другая компания на этой планете, они передали соответствующие обязанности команде разработчиков программного обеспечения. Постановка этой задачи перед группой программистов запустила эффект домино, результатом которого стало появление технологического интернет-гиганта. В самом начале SRE-инженеры писали программы для автоматизации тех работ, которые сетевой инженер выполнял вручную, набирая команды в консоли. Они начали использовать методологию DevOps за шесть лет до того, как в отрасли появилось для нее название. Кстати, так же поступила и компания Amazon, результатом работы которой стал сервис AWS. Со временем монументальное решение,

принятое этими компаниями, привело к возникновению идеи инфраструктуры как кода.

Для описания выполняемых вручную задач SRE-инженеры используют термин «тойл». К этой категории относится нечто повторяющееся, тактическое и лишенное какой-либо долгосрочной ценности. Все мы знаем о преимуществах автоматизации задач, однако SRE-инженеры Google довели ее до высшей степени. Они понимали, что это не панацея, а способ многократного приумножения силы. Если все сделать правильно, это обеспечит согласованность действий всей организации, а созданную платформу впоследствии можно будет легко расширить. Компания Google не просто автоматизировала выполнение критически важных задач — она построила автономную систему, создавшую основу для обеспечения устойчивости. Лично я не могу вспомнить, когда в последний раз продукт Google выходил из строя надолго. Однако мы точно знаем, что внутренние системы компании постоянно отказывают. Их инфраструктура слишком масштабна, чтобы этого не происходило. То, что я никогда этого не замечаю, отражает саму суть понятия устойчивости.

ИТ-устойчивость и ИБ-устойчивость

Описанные ранее действия Netflix и Google имеют большее отношение к ИТ-операциям, чем к обеспечению безопасности, это скорее DevOps, чем DevSecOps, что весьма прискорбно. Однако SRE-инженеры всего мира подали отличный пример сообществу ИБ-специалистов. Проектировать и развертывать цифровую инфраструктуру следует так, чтобы воздействие на организацию было минимальным, даже если хакеры Fancy Bear обойдут вашу систему защиты. Проектируйте ее так, чтобы и в случае захвата сегмента сети хакерами BlackByte бизнес мог продолжать предоставлять услуги. Иными словами, сеть должна быть спроектирована так, чтобы предвидеть атаки, противостоять им, восстанавливаться и адаптироваться. Это и есть устойчивость.

Устойчивость и планы по ее обеспечению

Планы — это не стратегии и не тактики. Это руководства по применению тактических приемов, необходимых для реализации общей стратегии. Помните, что обеспечение устойчивости — это одна из стратегий, базирующихся на первичных принципах кибербезопасности. Нам необходимо последовательно достигать намеченных результатов, несмотря на неблагоприятные события. Мы хотим предвидеть их, противостоять им, восстанавливаться

и адаптироваться. Для этого следует применить одну или несколько тактик, наиболее эффективные из которых рассмотрим в этой главе.

Применение этих тактик требует составления большого количества планов по обеспечению устойчивости. Согласно руководству NIST по планированию действий в чрезвычайных ситуациях для федеральных информационных систем (Contingency Planning Guide for Federal Information Systems SP 800-34 Rev. 1, ноябрь 2010 года) [300] у федерального правительства США должны быть следующие виды планов по обеспечению устойчивости (рис. 5.1):

- *план обеспечения непрерывности бизнеса* (Business continuity plan, BCP) — поддержание и восстановление бизнес-процессов после серьезного сбоя;
- *план обеспечения непрерывности операций* (Continuity of operations plan, COOP) — поддержание работы основных функций на альтернативной площадке;
- *план антикризисных коммуникаций* (Crisis communications plan, CCP) — распространение сообщений о критическом состоянии и борьба со слухами;
- *план защиты критической инфраструктуры* (Critical infrastructure protection, CIP) — защита ключевых компонентов инфраструктуры;
- *план реагирования на киберинциденты* (Cyber incident response plan, CIRP) — смягчение последствий кибератак;
- *план аварийного восстановления* (Disaster recovery plan, DRP) — перемещение информационных систем в другие места;
- *план на случай непредвиденных ситуаций в информационных системах* (Information system contingency plan, ISCP) — восстановление информационной системы;
- *план действий персонала в случае чрезвычайной ситуации* (Occupant emergency plan, OEP) — минимизация вреда жизни и здоровью людей, а также защита имущества в случае возникновения физической угрозы.

В коммерческом мире планировщики обычно сокращают предложенный NIST список планов до двух, направленных на обеспечение непрерывности бизнеса и аварийное восстановление. Однако эти два плана включают в себя ключевые элементы большинства других планов из списка NIST. Если говорить упрощенно, то план обеспечения непрерывности бизнеса предусмотрен на случай форс-мажорных обстоятельств, с которыми могут столкнуться организации, таких как пожар, вооруженное нападение, землетрясение, смерть руководителей и т. д. План аварийного восстановления предназначен для решения проблем с цифровой инфраструктурой, например, в случае сбоя

в работе облачных провайдеров, отключения электричества в центрах обработки данных и кибератак. Таким образом, план аварийного восстановления является частью плана обеспечения непрерывности бизнеса, и именно в его рамках мы будем реализовывать свою стратегию обеспечения устойчивости, базирующуюся на первичных принципах кибербезопасности.

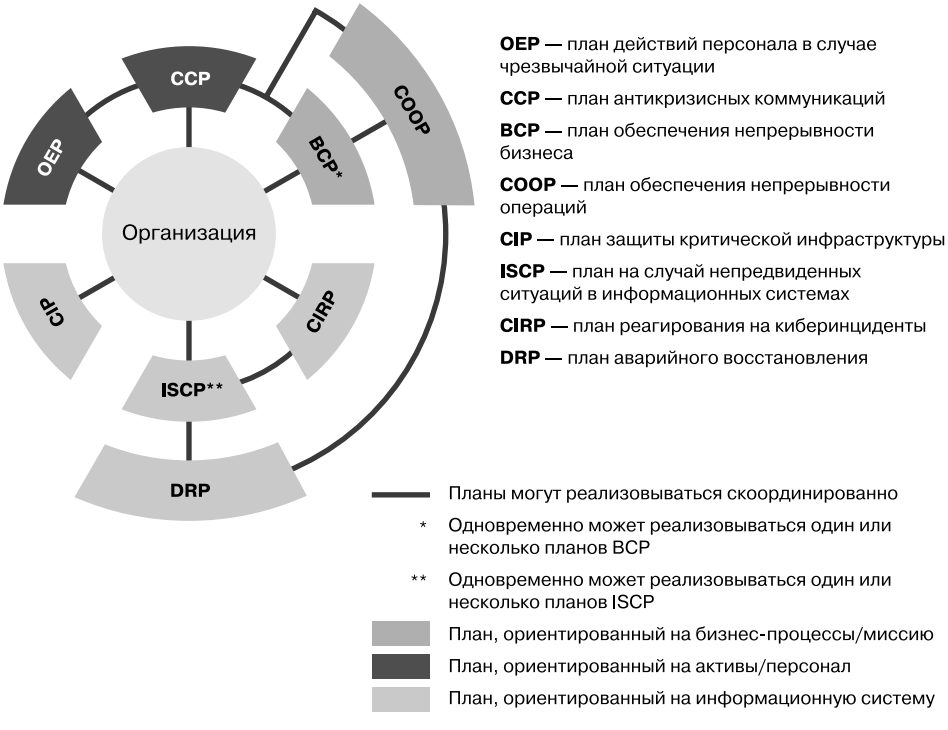


Рис. 5.1. Взаимосвязи между планами, предлагаемыми NIST

В то время, когда я писал эту книгу, федерация Global Resilience Federation опубликовала первую версию фреймворка для обеспечения операционной устойчивости (Operational Resilience Framework, ORF) [155]. Признавая наличие взаимосвязей между организациями, поставщиками и провайдерами, фреймворк ORF распространяет планы обеспечения непрерывности бизнеса и аварийного восстановления на всю экосистему организации. Это предполагает определение минимального количества жизнеспособных внешних продуктов и услуг, необходимых организации для выполнения своих операций во время кризиса. Вспомните сцену из фильма «Эта замечательная жизнь», когда все клиенты банка решили забрать из него свои деньги. Если бы они попытались это сделать, банк очень скоро закрылся

бы, оставив большинство вкладчиков ни с чем. Но этого не произошло благодаря сообразительности Джорджа Бейли, который убедил людей снять ровно столько, сколько им было абсолютно необходимо. Таким образом, все получили то, что им было нужно, и банк смог остаться в бизнесе.

Помимо определения операционных требований, необходимых для удовлетворения минимальных потребностей клиентов во время кризиса, фреймворк ORF предполагает обеспечение устойчивости системы, выражающейся в доступности технических возможностей и соответствующих зависимостей. Например, это может означать восстановление только критически важных для бизнеса данных, а не всей резервной копии.

При разработке плана обеспечения устойчивости необходимо понимать, какие существуют взаимосвязи между людьми, процессами и технологиями. Слишком часто план обеспечения непрерывности бизнеса составляется в отрыве от всего остального, без учета того, что процесс восстановления работы системы может занять недели или даже месяцы или что телефоны, компьютеры и сети, от которых она зависит, имеют собственные зависимости и сроки восстановления.

Фреймворк ORF объединяет бизнес-взгляд на устойчивость с инженерным аспектом системы, о котором говорится в документе *NIST SP 800-160v2 Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, представляющем фреймворк для инженерии киберустойчивости, включающий соответствующие цели, задачи, методы, подходы и принципы проектирования [189]. Одно дело — составить план обеспечения устойчивости и совсем другое — добиться того, чтобы он был одобрен предприятием, регулярно тестировался, изучался персоналом и обновлялся.

У меня есть некоторые претензии к тому, как мы выбираем названия для тех или иных вещей, относящихся к ИБ. Неправильно подобранное название приводит к путанице, которая царит в сообществе годами. Ранее в этой книге я уже привел несколько примеров. Один из них связан с путаницей вокруг смысла термина «нулевое доверие». В данном случае речь идет не о том, что доверять нельзя никому, а об ограничении уровня доверия до необходимого минимума (см. главу 3). Другой пример — путаница между атрибуцией групп противников и атрибуцией кампаний (см. главу 4). Атрибуция должна касаться именно кампаний, а не стоящих за ними хакеров. Третий пример связан с концепцией программно-определяемого периметра

(SDP) (см. главу 3). SDP устраняет периметр, а не создает его. И наконец, есть понятие аварийного восстановления, которое на первый взгляд кажется синонимом непрерывности бизнеса. Если вы новичок в этой области, то, скорее всего, не знаете, что аварийное восстановление — это часть плана обеспечения непрерывности бизнеса. Тщательное продумывание названия в самом начале реализации проекта вне зависимости от того, идет ли речь о будущем международно признанном наборе передовых практик или об очередном внутреннем продукте для модернизации ИТ, позволит избежать путаницы в дальнейшем, когда вам придется объяснять кому-то его суть.

Выпас котов[1]: матрицы распределения ответственности

Когда киберсобытие перерастет в полномасштабный киберинцидент, SOC-центру, скорее всего, не удастся удержать ситуацию под контролем. В этом случае в соответствии с планом обеспечения непрерывности бизнеса, вероятно, придется задействовать другие бизнес-функции. План реагирования на инцидент должен предусматривать способ информирования всех лиц, принимающих решения, и других заинтересованных сторон о том, кто что делает, кто за что отвечает и каковы дальнейшие шаги. Это сложный процесс, который не ограничивается реагированием на киберинциденты. Реализация крупных и сложных проектов в рамках нескольких организационных подразделений была проблемой менеджмента с самых первых дней существования бизнеса.

В конце 1940-х годов голландский консультант Эрнст Хиджамс, работавший в канадской консалтинговой компании Leethan, Simpson, Ltd., предложил линейную диаграмму распределения ответственности (linear responsibility charting, LRC) — графическое представление того, кто отвечает за ту или иную задачу проекта, кто оказывает поддержку, с кем необходимо консультироваться, с кем можно консультироваться, кто дает оценку и от кого зависит окончательное одобрение (табл. 5.1) [223].

---

[1] Фраза описывает управление коллективом ИТ-компании. Специфика работы таких организаций требует особого подхода к людям, которые далеко не всегда признают управление. См. книгу: *Рейнвотер Дж.* Как пасти котов. Наставление для программистов, руководящих другими программистами. — СПб.: Питер, 2019. — *Примеч. ред.*

Таблица 5.1. Пример линейной диаграммы распределения ответственности

Задача	Натан Джордан	Ричард Патрикан	Эндрю Чедено	Доктор Ву	Доктор Ригл
1.0. Понимание требований заказчика	2	1	2	5	5
1.1. Уточнение формулировки задачи	3	1	1	3	3
1.2. Проведение исследования	2	1	1	3	3
1.3. Разработка дерева целей	2	1	1	4	4
1.3.1. Проект дерева целей	2	1	2	4	4
1.3.2. Обсуждение с клиентом	2	1	1	4	4
1.3.3. Пересмотр дерева целей	2	1	1	4	4
2.0. Анализ функциональных требований	3	1	1	4	3
3.0. Разработка прототипов	2	1	1	4	3
3.1. Рисование эскизов на бумаге	2	1	1	4	3
3.2. Создание 3D-чертежей в Autodesk	2	1	1	4	3
4.0. Создание прототипа	2	1	1	4	3
4.1. Создание базового макета	2	2	1	4	3
4.2 Доработка второго прототипа в Autodesk	2	1	1	4	3
4.3. Заказ деталей	2	1	1	4	3
4.4. Печать итогового прототипа на 3D-принтере	2	1	1	4	3
4.5. Сборка устройства с использованием заказанных деталей	2	1	1	4	3
5.0. Оценка альтернатив	1	1	1	3	3
5.1. Взвешивание целей	3	3	1	3	3
5.2. Разработка протокола испытаний	2	1	1	3	3
5.3. Проведение испытаний	1	1	1	2	2
5.4. Составление отчета о результатах испытаний	1	2	2	3	3

Продолжение ⇩

Таблица 5.1 *(продолжение)*

Задача	Натан Джордан	Ричард Патрикан	Эндрю Чедено	Доктор Ву	Доктор Ригл
6.0. Выбор предпочтительного дизайна	2	1	1	3	3
7.0. Документирование результатов проектирования	2	1	1	2	2
7.1. Составление спецификации дизайна	2	1	1	4	6
7.2. Проект итогового отчета	2	1	2	2	2
7.3. Обсуждение дизайна с заказчиком	2	1	1	4	4
8.0. Управление проектом	1				
8.1. Проведение еженедельных совещаний	2	1	1	4	5
8.2. Разработка плана проекта	2	1	1	4	4
8.3. Отслеживание хода выполнения	2	1	1	4	4
8.4. Составление отчетов о ходе работ	2	1	1	4	4

Ключ: 1 — первичная ответственность; 2 — поддержка/работа; 3 — обязательная консультация; 4 — допустимая консультация; 5 — рецензирование; 6 — окончательное утверждение

В начале 1950-х годов по мере развития проектного менеджмента эти диаграммы стали называться RACI-матрицами (от responsible — «ответственный», accountable — «подотчетный», consulted — «консультирующий», informed — «информируемый») или матрицами распределения ответственности (Responsibility Assignment Matrix, RAM) (рис. 5.2) [98].

В 2022 году существовало более десятка версий диаграмм, включающих такие варианты участия, как Sign-off required («Подписывает»), Input required («Делает вклад»), Control («Контролирует»), Suggest («Предлагает»), Facilitates («Способствует»), Qualitative review («Выполняет качественный анализ»), Verifier («Проверяет»), Driver («Продвигает») и т. д. LRC и RAM можно считать общими названиями для такого рода диаграмм, а матрицу RACI и все ее версии, такие как DACI, RAPID, PARIS и т. д., — конкретными типами.

Задача	 Фродо	 Сэм	 Гэндальф	 Арагорн	 Элронд
Решить, что делать с кольцом	C	I	A	C	R
Создать братство	R	C	A	C	R
Донести кольцо до Роковой горы	R	C	A	C	I
Отвлечь и победить врагов	I	R	C	R	I

R — ответственный;
A — подотчетный;
C — консультирующий;
I — информируемый

Рис. 5.2. RACI-матрица для братства, решившего уничтожить кольцо всевластья

Суть в том, что большинство организаций, скорее всего, использует ту или иную версию диаграмм LRC для управления проектом в кризисных условиях в соответствии с планом обеспечения непрерывности бизнеса. И план обеспечения непрерывности бизнеса, и план аварийного восстановления наверняка предусматривают версию такой диаграммы. Когда организации проводят учения с целью тестирования этих планов, матрица RAM обычно является основным документом для проверки того, все ли делают то, что должны. После учений, а также после реального кризиса матрица RAM, как правило, — это первый документ, который следует обновить.

Когда я был командиром армейской группы CERT, между разными подразделениями армии шла отчаянная борьба за право проведения кибероперации. Во многих отношениях она происходит между всеми службами до сих пор. Но в мое время (начало 2000-х годов) она шла между INSCOM (разведывательное подразделение армии США и командование, которому подчинялась группа ACERT) и NETCOM (подразделение связи армии США). Возглавлявшие их генералы решили, что кибероперации будут проводиться совместно этими двумя подразделениями, и поручили мне и майору Ларри Холлу (коллеге из NETCOM) проработать детали. Не зная, как это следует называть, мы с Ларри использовали версию линейной диаграммы распределения

ответственности (LRC). На протяжении нескольких месяцев мы передавали друг другу электронную таблицу со всеми киберзадачами, распределенными между подразделениями, до тех пор, пока руководители не достигали согласия. Процесс был очень сложным, но без диаграммы LRC решить эту задачу было бы просто невозможно.

Как следует задуматься об устойчивости

Обеспечение устойчивости — это еще один способ снижения вероятности существенного ущерба в результате киберсобытия. В случае со стратегиями нулевого доверия и предотвращения реализации убийственной цепочки вторжения мы принимаем активные меры, чтобы предотвратить неблагоприятное событие. При обеспечении устойчивости мы принимаем то, что такое событие произойдет, и планируем действия, позволяющие его пережить.

Это похоже на решение проблемы, связанной с угрозой падения астероида на Землю. В части предотвращения этого события правительство будет пытаться изменить траекторию астероида с помощью какой-нибудь ракеты. А в части обеспечения устойчивости оно будет стремиться к заселению людьми второй планеты, например Марса. Вариант с ракетой позволит сохранить человеческую расу, предотвратив катастрофу. Вариант с переселением на Марс экспоненциально увеличит шансы человечества на выживание в случае столкновения крупного астероида с Землей.

С точки зрения кибербезопасности стратегия обеспечения устойчивости имеет дополнительное преимущество, заключающееся в том, что ее реализация, скорее всего, обойдется дешевле по сравнению с другими стратегиями, предусмотренными в рамках нашей ИБ-программы, базирующейся на первичном принципе кибербезопасности. Внедрение систем нулевого доверия, предотвращение реализации убийственных цепочек вторжения, а также создание полноценной программы автоматизации требует немалых затрат, чего нельзя сказать об обеспечении устойчивости. Это означает, что если вы работаете в небольшом или среднем стартапе, то стратегией, способной дать наибольшую отдачу и снизить вероятность нанесения ему существенного ущерба при наименьших затратах, является обеспечение устойчивости.

Как говорят Стирна и Здравкович, создавайте бизнес-системы, способные последовательно добиваться намеченных результатов, несмотря на неблагоприятные киберсобытия. Далее описаны несколько способов, позволяющих это сделать.

Антикризисное управление: тактика обеспечения устойчивости

В большинстве организаций старший специалист по кибербезопасности, скорее всего, не отвечает за общий план обеспечения непрерывности бизнеса. Коммерческая компания, государственное учреждение или академический институт могут столкнуться с множеством кризисов, помимо атак вымогателей вроде BlackByte или операций кибершпионажа, проводимых различными государствами, наподобие Hurricane Panda. Чтобы подготовить организацию к киберкризису, руководители служб безопасности должны подключиться к существующему аппарату управления кризисными ситуациями в качестве ключевых игроков. От размера организации и обеспеченности команды антикризисного управления ресурсами будет зависеть уровень формальности антикризисного плана. Не вполне очевидным является то, что размер организации и зрелость ее команды по управлению кризисными ситуациями не так важны, как наличие какого бы то ни было плана, позволяющего руководству чувствовать себя комфортно.

Под планом я не имею в виду стостраничный документ, который никто никогда не читает. Напротив, речь идет о плане, с которым сотрудники организации жили, экспериментировали, который корректировали, сгибали, комкали, топтали ногами, разглаживали, рвали, выбрасывали, переделывали и пересматривали столько раз, что он стал для всех второй натурой. В случае срыва плана во время кризиса очень важно, чтобы члены команды хорошо понимали, к чему им следует стремиться, — тогда любые ошибки или импровизации в ходе этого события не помешают достичь желаемого результата.

Во время службы в армии я работал под началом полковника, который очень хорошо это понимал. Он всегда говорил, что план необходим для того, чтобы от него можно было отклониться. Как красноречиво выразился знаменитый боксер-тяжеловес Майк Тайсон: «У каждого есть план, пока ему не дадут по морде» [165]. Этим я хочу сказать, что разница между группой планировщиков и группой переживших кризис заключается в том, что выжившие очень четко представляют себе желаемый результат еще до наступления неблагоприятного события. Неважно, что представляет собой план — стостраничный документ, аккуратно размещенный в цветные папки, с указанием роли каждого руководителя или наспех нарисованную на доске диаграмму. Выжившие настолько хорошо знают друг друга и то, чего хотят добиться, что любая их импровизация, основанная на результатах, способна спасти положение.

Чтобы подчеркнуть суть сказанного, рассмотрим два примера, демонстрирующие то, что следует и чего не следует делать. Первый пример касается взлома RSA Security в 2011 году, а второй — взлома Equifax в 2017-м.

RSA Security: пример антикризисных коммуникаций

Весной 2011 года разведаналитики, работавшие в компании RSA Security, в то время являвшейся подразделением корпорации EMC, заметили, что с правами доступа и поведением учетной записи одного из австралийских сотрудников что-то не так [27, 92]. Последующее расследование выявило масштабную операцию кибершпионажа, проводимую на тот момент еще не получившей названия группой китайских хакеров APT1 («Подразделение 61398» Народно-освободительной армии Китая). Компания Mandiant дала им это название лишь два года спустя [10].

Хакеры из APT1 успешно провели фишинговую атаку на австралийского сотрудника, использовали его аккаунт в качестве плацдарма и продвигались по сети RSA Security, повышая свои привилегии и разыскивая данные, которые собирались украсть. По словам Энди Гринберга из Wired, в данном случае начальные значения для токена RSA SecurID, устройства двухфакторной аутентификации, использовались «десятками миллионов пользователей в правительственных и военных учреждениях, оборонных подрядчиках, банках и бесчисленных корпорациях по всему миру». Получив эти начальные значения, хакеры APT1 могли обойти систему двухфакторной аутентификации во всех этих организациях.

В ходе этой дерзкой кампании кибершпионажа хакеры из APT1 деактивировали устройство безопасности, которое 760 клиентов по всему миру приобрели, распространили, установили и обслуживали для того, чтобы уменьшить поверхность атаки с целью защиты государственных тайн, финансовых данных и другой конфиденциальной информации.

Если бы я был одним из этих клиентов, я бы разозлился и стал активно искать крупнейшего конкурента RSA Security, чтобы заменить продукт SecurID на новую систему, которой мог бы доверять. Когда вы занимаетесь продажей систем безопасности, специально разработанных для защиты секретов, ваши собственные системы, в которых вы храните свои тайны, должны быть неуязвимыми. Полагаю, именно так думали в то время многие клиенты RSA Security. По данным газеты New York Times, некоторые круп-

ные клиенты публично заявили о том, что планируют в кратчайшие сроки сменить поставщика. Среди них были Bank of America, JPMorgan Chase, Wells Fargo и Citigroup [198, 219].

Однако затем руководство RSA Security разработало план антикризисной коммуникации, чтобы спасти компанию. По словам Гринберга, в первую неделю после наступления кризисного события один из сотрудников юридического отдела предложил не сообщать о нем клиентам. Тогдашний генеральный директор Арт Ковиелло был против. Он стукнул кулаком по столу и заявил, что они не только признают факт взлома, но и свяжутся по телефону с каждым клиентом, чтобы обсудить возможные способы защиты. Когда кто-то из сотрудников предложил дать этому антикризисному плану кодовое название «Проект "Феникс"», Ковиелло отверг это предложение, сказав: «Мы не восстаем из пепла. Мы назовем этот проект "Аполлон-13" и посадим корабль без повреждений».

И вот что они сделали. Они немедленно подали в Комиссию по ценным бумагам и биржам отчет о внеплановом существенном событии по форме 8-K. На следующий день, по словам Гринберга, «Ковиелло опубликовал на сайте компании открытое письмо к клиентам RSA» и создал группу из 90 сотрудников для проведения переговоров с каждым из них. Ковиелло и высшие руководители лично участвовали в сотнях таких звонков.

И это сработало. Во II квартале 2011 года компания EMC сообщила, что ее внутренние расходы на ликвидацию последствий инцидента составили около 66 млн долларов [218]. Однако к концу III квартала, по данным CSO Online, EMC сообщила о рекордных доходах. Вот так, а они боялись потерять репутацию из-за этого киберинцидента. Я могу привести веские аргументы в пользу того, что такое быстрое восстановление и такая устойчивость явились заслугой генерального директора компании Арта Ковиелло, разработавшего план антикризисных коммуникаций.

В компании RSA Security (EMC) произошло событие типа «черный лебедь». Это словосочетание стало нарицательным для подобных кризисов благодаря книге Нассима Талеба «Черный лебедь. Под знаком непредсказуемости» [331]. События такого рода настолько маловероятны, что вы никогда их не ожидаете (например, падение метеорита на Землю), но когда они происходят, последствия оказываются катастрофическими. Именно таким было событие, случившееся в компании EMC. По всем законам жанра компания не должна была от него оправиться. Клиенты должны были массово отказаться от ее услуг. Но этого не случилось. Благодаря тому что Ковиелло сосредоточил усилия на поддержке клиентов, большинство из них остались

с компанией до окончания кризиса, несмотря на множество причин уйти. У RSA Security не было антикризисного плана до этого инцидента, но после того, как он произошел, генеральный директор взял на себя ответственность и задал направление, а его команда выполнила поставленные им задачи. Он настолько четко определил желаемый результат, назвав проект «Аполлон-13», а не «Феникс», что вся внутренняя энергия компании сосредоточилась на нем, и успех превзошел все прогнозы.

Теперь рассмотрим находящийся на противоположном конце спектра пример, связанный с утечкой информации из компании Equifax в 2017 году.

Equifax: пример антикризисных коммуникаций

Десятого марта 2017 года китайские хакеры (сотрудники 54-го исследовательского института, подразделения Народно-освободительной армии КНР) создали плацдарм в сетях Equifax [238]. Внутренняя служба безопасности компании обнаружила вторжение более чем через четыре месяца, в конце июля, и сразу же наняла Mandiant в качестве внешней группы реагирования на инциденты. Компания Mandiant обнаружила, что Equifax допустила утечку персональной информации примерно 60 % всех граждан США (то есть 143 млн американских потребителей) [226].

Генеральный директор Equifax Рик Смит не разглашал эту информацию более месяца, но в конце концов 7 сентября обратился к общественности [313]. Он объявил о стандартных мерах поддержки клиентов в связи с утечкой их данных, включающих бесплатный кредитный мониторинг, информационный сайт и кол-центр для решения вопросов — в общем, ничего ценного. Он выдавал информацию по крупицам на протяжении нескольких недель. С самого начала казалось, что Смит придумывает все на ходу. Его сообщение было в лучшем случае запутанным, а в худшем — вводящим в заблуждение.

Через три дня клиенты узнали о том, что могут получить желанную бесплатную услугу кредитного мониторинга только в том случае, если согласятся не подавать на компанию в суд. К 15 сентября Смит уволил ИТ-директора Дэвида Уэбба и руководителя отдела безопасности Сьюзан Маулдин [178]. Двадцать первого сентября сайт с информацией об утечке все еще не был готов, поэтому компания начала направлять клиентов и журналистов на фишинговый сайт, специально предназначенный для проверки принятых мер безопасности. К 26 сентября совет директоров Equifax уволил генерального директора [16]. В марте следующего года Комиссия по ценным бумагам и биржам добилась предъявления обвинения Цзюнь Ингу, бывше-

му ИТ-директору, за использование еще не обнародованной информации об утечке данных для продажи своих опционов на акции Equifax [229]. Казалось, будто вся культура производства компании пронизана непрозрачными схемами и махинациями в духе продавцов подержанных автомобилей. Руководство Equifax не придало первостепенного значения защите собранной персональной информации более чем половины американского населения, поэтому не имело плана аварийного восстановления на случай подобного инцидента. Если у них и был план обеспечения непрерывности бизнеса или план антикризисных коммуникаций, то либо он оказался слишком слабым, либо они предпочли его проигнорировать.

Многие сторонние наблюдатели были согласны с тем, что Смит провалил план коммуникации в период между утечкой данных и своим увольнением [225, 315].

- Он ждал шесть недель, прежде чем объявить об инциденте.
- Вместо того чтобы обратиться к клиентам, он решил создать сайт, который был готов только через несколько недель после объявления об утечке.
- Он предложил клиентам услугу бесплатного кредитного мониторинга, но взамен потребовал отказаться от права на подачу заявления в суд.
- Позже он передумал, однако клиенты должны были отправить Equifax письменное уведомление о своем решении в течение 30 дней. При этом формулировка отказа от услуги, содержащаяся в общих условиях обслуживания, была неверной.
- Поначалу он брал с клиентов деньги за услугу замораживания кредита.
- Компания Equifax присвоила людям, заморозившим свои кредиты, легко угадываемые PIN-коды.

В итоге по меньшей мере четыре руководителя потеряли работу, а подкомитет по вопросам электронной коммерции и защите прав потребителей палаты представителей США вызвал Рика Смита для дачи объяснений. В мае 2019 года компания Equifax сообщила о том, что ее расходы на ликвидацию последствий инцидента составили примерно 1,4 млрд долларов, не считая судебных издержек [198].

Как и в случае с RSA Security, «черный лебедь» Equifax тоже не погубил компанию, но совсем по другой причине. Очевидно, что ее план антикризисных коммуникаций был просто катастрофическим по сравнению с планом RSA Security, однако 143 млн пострадавших американцев не были

клиентами Equifax. По словам Лили Ньюман из Wired, Equifax и два ее конкурента, Experian и TransUnion, являются продавцами потребительских данных [166]. Это означает, что жертвы не выбирали, в какой из этих компаний будут храниться их данные. Иными словами, жертвы не платили Equifax за предоставленные продукты и услуги. По словам Кейт Фаззини с телеканала CNBC, «Equifax — это бюро кредитных историй, собирающее и обобщающее данные о каждом гражданине США с целью их продажи кредиторам и заимодавцам. Они собирают информацию из различных источников (как платных, так и бесплатных), а затем рассчитывают кредитный рейтинг с помощью алгоритмов» [77]. В отличие от RSA Security компании Equifax не пришлось успокаивать разгневанных клиентов.

После объявления об утечке данных цена акций Equifax (EFX) упала на 13 %, но к марту 2020 года восстановилась и продолжила расти. По словам Денниса Кэннона с сайта Rice-Properties, сегодня на компанию Equifax работают более 10 000 человек по всему миру, а ее годовая выручка составляет 3,1 млрд долларов [41]. Итак, компания выжила, а ее руководство — нет.

Ожидаемые результаты

Идея ожидаемых результатов (desired outcomes) возвращает нас к атомарному базовому принципу кибербезопасности, который заключается в снижении вероятности существенного ущерба. Дело в том, что во время киберкризиса, то есть события типа «черный лебедь», обеспечение устойчивости — единственная стратегия, которая имеет значение. Если вы оказались в кризисной ситуации, значит, все остальные стратегии провалились, то есть не помогли ее предотвратить. Что же делать теперь? О недостатках этих стратегий можно будет поговорить после кризиса. А пока нужно решить, на чем руководителям следует сосредоточить усилия.

Возвращаясь к определению Стирны и Здравкович, в кризисной ситуации лидеры должны сконцентрироваться на том, чтобы продолжать предоставлять услуги своим самым ценным клиентам. В случае с RSA Security в 2011 году это означало, что высшее руководство, включая генерального директора, должно было поговорить с каждым из пострадавших клиентов, извиниться за допущенную ошибку и помочь в ликвидации последствий инцидента. Что касается компании Equifax, то я вообще не понимаю, что она пыталась сделать в 2017 году.

В результате изучения литературы, посвященной обеим атакам, складывается впечатление, будто ни одна из компаний не имела формального

антикризисного плана до инцидента. Судя по всему, разница в результатах объясняется тем, что Ковиелло с самого начала определил желаемый результат и наметил план для его достижения, сказав: «Мы посадим корабль без повреждений». По сути, он набросал на доске приблизительную схему действий и обеспечил их выполнение командой. В отличие от него Смит из компании Equifax действовал непоследовательно, и его план существенно менялся в течение всего кризисного периода.

Руководители — занятые люди: используйте их время эффективно

Убедиться в том, что до наступления киберкризиса команда руководителей находится на одной волне относительно желаемых результатов, довольно сложно. Что же для этого нужно делать? «Практиковаться», как сказал скрипач Миша Эльман, когда в Нью-Йорке к нему подошли два туриста и спросили, как попасть в Карнеги-холл [42]. Вне зависимости от того, есть ли у вас стостраничный стратегический план или всего лишь простая схема на доске, очень важно обсудить различные сценарии с командой руководителей, чтобы узнать их реакцию и подтвердить правильность понимания желаемых результатов.

Судя по моему опыту, крупные организации проводят как минимум одно официальное учение в год. Некоторые организуют несколько учений, в ходе которых прорабатывают тот или иной сценарий, например связанный с вымогательством, кибершпионажем или киберактивизмом, и изучают реакцию на него высшего руководства. Цель состоит в том, чтобы ознакомить руководителей с различными тактическими мерами обеспечения устойчивости, которые вы уже применяете для смягчения последствий кризисных событий. В частности, к таким мерам относятся реагирование на инциденты, резервное копирование и шифрование. В ходе учений могут обнаружиться пробелы, о которых вы раньше не задумывались, что вполне допустимо и даже желательно. По сути, это одна из главных причин проведения учений. Еще важнее возможность увидеть, как высшее руководство реагирует на эти пробелы, и подтолкнуть его к их устранению.

В ходе каждого из учений я всегда узнавал что-то новое. Либо план был недостаточно четким, либо он был неверен в некоторых деталях, либо кто-то из высшего руководства возражал против того, чего мы пытались достичь с помощью этого плана. Однако цель учений заключается не в том, чтобы обсудить с руководителями все возможные сценарии, а в том, чтобы побудить их

принимать решения, которые будут способствовать достижению желаемого результата независимо от конкретного сценария, даже если нам придется отбросить подготовленный план. Другими словами, отрабатывать следует не сценарий, а результат.

Эти учения не обязаны быть формальными. Руководители компании очень занятые люди. Чтобы собрать их раз в год для участия в учениях, требуется провести огромную работу по согласованию их расписания, убедить их в том, что это не пустая трата времени, и быть готовыми к тому, что некоторым придется в последнюю секунду отказаться от участия из-за чрезвычайной ситуации, требующей их немедленного внимания. Даже если генеральный директор является сторонником этого мероприятия, что бывает не всегда, случиться может всякое. Однако есть и более простые подходы.

Один из вариантов, который я с успехом использовал в ходе своей карьеры, — это продолжительный (около 90 минут) обед с командой высшего руководства. Цель состоит в том, чтобы во время обеда положить на стол сценарий, напомнить всем о желаемых результатах, основанных на текущем плане и исходах предыдущих подобных обедов, и получить обратную связь. В ходе обсуждения действий руководителей на каждом этапе реализации сценария глава антикризисной команды расскажет о том, что будут делать остальные сотрудники компании в соответствии с текущим планом, используя матрицу распределения ответственности.

Прелесть этого подхода заключается в том, что даже руководители высшего звена любят бесплатные обеды, они не отнимают у них много времени и это неформальные мероприятия. А люди гораздо охотнее обмениваются идеями, когда едят один и тот же салат. Кроме того, такой подход хорошо работает для малых и средних организаций.

Можете смело приглашать к участию в учениях сторонних лиц. Учения дают вашей организации возможность познакомиться с ними и узнать, чем они могут помочь в случае реальной чрезвычайной ситуации. Что касается аудиторов, то учения позволяют в невраждебной обстановке показать им, как ваша организация следует плану, который они проверяли. Проведение реального аудита предусматривает элемент состязательности, однако в ходе учений аудиторы являются частью команды, и их наблюдения и предложения могут способствовать улучшению плана. И наконец, если организация когда-либо столкнется с судебным разбирательством по причине киберинцидента, участие сторонних лиц и аудиторов может помочь ей защититься.

Чтобы иметь хоть какую-то надежду на успешную реализацию стратегии обеспечения устойчивости, необходимо практиковаться. Дайте своим топ-менеджерам как можно больше возможностей для принятия решений, помогающих достичь желаемого результата, еще до прилета «черного лебедя». Вы же не хотите, чтобы они впервые задумались об этом во время настоящего кризиса. Нужно сделать так, чтобы им было комфортно принимать правильные решения в этой ситуации. Именно это и дает вам антикризисное управление кибербезопасностью.

Резервное копирование: тактика обеспечения устойчивости

Около 15 лет назад я разработал схему резервного копирования нашего семейного архива. Цифровые технологии тогда только начинали входить в моду, и у нас было множество электронных артефактов, хранящихся в мобильных телефонах, цифровых фотоаппаратах (помните такие?) и на домашнем компьютере. В семье из пяти человек (я, жена, две дочери и сын) все это быстро начало выходить из-под контроля. Я понял: кое-что, например драгоценные видеозаписи с участием дочерей, прыгающих по сцене во время постановки «Короля Льва» в танцевальной студии, и файлы налоговых деклараций за 20 лет, стоит собрать в одном месте и сделать резервные копии на случай какой-нибудь катастрофы.

За время работы над постановкой «Короля Льва» мы потратили огромное количество ресурсов на покупку костюмов, репетиции и подготовку представления. Причем в этом была задействована вся семья. Две наши дочери участвовали во множестве номеров, их мама была координатором за кулисами, а мы с сыном отвечали за безопасность (в частности, проводили много времени, регулируя движение на парковке местной средней школы). После постановки всей семьей отправились в «Диснейуорлд», чтобы вознаградить себя за хорошо проделанную работу. И когда мы оказались в центре диснеевского «Царства животных», на пересечении исследовательской тропы в лесу Пангани и пути «Экспресса дикой природы», группа уличных артистов начала петь и танцевать под саундтрек из «Короля

Льва», приглашая посетителей присоединиться. Этот момент просто нельзя было не запечатлеть на пленке. Мои дочери последние шесть месяцев оттачивали танцевальные номера из «Короля Льва» и просто обязаны были показать класс. Я взял в руки видеокамеру и начал снимать. Увы, к моему большому разочарованию, я заснял лишь двух смущенных подростков, неловко раскачивающихся взад-вперед так, будто они только что научились ходить и жевать жвачку. Они даже не попадали в такт музыке.

Пожалуй, это стало моим любимым видео с дочерьми за все время их танцевальной карьеры. Мне нужно было гарантировать то, что никакой компьютерный сбой не приведет к потере этого видео и остального цифрового мусора, который мы накопили за предшествующие годы. И я принялся за работу.

Я не просто разработал схему, которая позволяла автоматически загружать копии всех наших файлов на сервер одного из первых облачных провайдеров, но и создал локальный RAID-массив для своей домашней системы. Если бы какой-то из дисков в массиве вышел из строя, я мог бы просто вынуть его и вставить новый. Это было гениально. Эта система резервного копирования была абсолютно надежной.

Примерно через год произошла неизбежная катастрофа. Жесткий диск моего домашнего компьютера вышел из строя, и я не смог восстановить его работу. Жена бросила на меня панический взгляд, в котором читался вопрос: «А как же все мои файлы?» Я самодовольно ответил ей: «Не волнуйся, у меня есть резервные копии». Собрав новый компьютер, я обратился к своему облачному провайдеру, чтобы восстановить данные. И, к своему ужасу, не обнаружил ни одного фрагмента данных. Я не мог в это поверить. В облаке не оказалось ни одного видео, ни одной фотографии, ни одного файла TurboTax. У меня началась паника. Но тут я вспомнил о RAID-массиве, служившем резервной копией для резервных копий. Восстановить данные мне удалось оттуда.

Все, что я могу сказать: у меня был отличный план, но я полностью провалил его реализацию. У меня была облачная система резервного копирования, и я регулярно проверял, сохраняет ли она файлы.

У меня был RAID-массив, на котором я хранил резервные копии этих файлов. Ошибка была связана с настройкой этих двух систем. Очевидно, я настроил их так, что каждый день система резервного копирования копировала пустой каталог, а не тот, в котором хранились все файлы. Примерно раз в неделю я проверял работоспособность системы и убеждался в том, что все в порядке.

Стыдно признаться, но мне пришлось заплатить за услугу Geek Squad, предоставляемую местным магазином Best Buy, чтобы восстановить поврежденные файлы на домашнем компьютере. Это был довольно унизительный опыт, но именно эту историю моя жена предпочитает рассказывать родственникам и друзьям, когда они начинают задавать вопросы о моей карьере в области кибербезопасности. Это звучит примерно так: «Позвольте рассказать о моем муже, крутом кибербезопаснике, который однажды потерял весь семейный архив за 20 лет».

Как сказал Билл Мюррей в одном из моих любимых фильмов «Гольф-клуб», «хоть это у меня получается». Урок заключается в том, что, если план не реализуется должным образом, ему почти гарантирован провал.

Резервное копирование как стратегия защиты от программ-вымогателей

За последнее десятилетие программы-вымогатели заметно эволюционировали. Когда они только появились, их целевой жертвой был пользователь домашнего компьютера. Киберпреступники взламывали компьютер какой-нибудь бабули, шифровали жесткий диск, звонили ей по телефону и говорили, что если она хочет снова увидеть фотографии своих любимых кошек и внуков, то должна заплатить им 500 долларов в биткойнах.

Для того чтобы заставить эту модель работать, группы злоумышленников разработали поразительные бизнес-системы. Сотрудники кол-центра обзванивают бабушек всего мира, объясняют, что они сделали с ее компьютером (шифрование данных), говорят, что ей нужно сделать, чтобы исправить ситуацию, и сколько это будет стоить, помогают создать биткойн-кошелек, перевести на него деньги из банка, а затем перевести их на биткойн-кошелек банды вымогателей, и все это часто на неродном для себя языке.

Их предпочтения в выборе жертвы изменились в 2017 году. По словам Николь Перлрот, журналистки газеты New York Times и автора книги *This Is How They Tell Me the World Ends*, претендующей на попадание в Зал славы Cybersecurity Canon, после того как летом 2017 года северокорейцы запустили вирус WannaCry, а месяцем позже русские осуществили атаку NotPetya, банды разработчиков программ-вымогателей поняли, что атаковать корпорации гораздо прибыльнее [175]. Вместо того чтобы усердно работать ради выманивания 500 долларов у какой-нибудь старушки, в корпоративном мире можно запрашивать выкуп в несколько миллионов долларов.

В 2021 году ФБР заявило об отслеживании активности по меньшей мере 100 уникальных группировок, занимающихся распространением программ-вымогателей [54]. Этот показатель чуть превышает результат приблизительных расчетов, которые мы сделали в главе 4, когда говорили о CAMM-кампаниях, проводимых преступниками, активистами и озорниками, но вполне согласуется с ним. Эти преступные группировки немногочисленны, но в случае попадания вашей организации под их прицел цена для вас может оказаться довольно высокой. Согласно результатам исследования, проведенного компанией Sophos в 2021 году, «средняя стоимость восстановления после атаки с использованием программ-вымогателей в 2021 году составила 1,4 млн долларов США» [4]. Однако нам известны случаи, когда это стоило гораздо больше. Как пишет Энди Гринберг в своей книге *Sandworm*, попавшей в Зал славы Cybersecurity Canon, общие затраты на восстановление после атаки NotPetya в 2017 году для всех жертв, вместе взятых, превысили 10 млрд долларов [91].

По мере развития новой корпоративной модели вымогатели нашли как минимум четыре способа выкачивания денег из новых жертв.

1. Плата за расшифровку данных. При этом речь идет не о том, что они собираются дать вам ключ, который все разблокирует, а лишь о том, что они намерены взять с вас за это деньги.
2. Плата за неразглашение украденных данных. Опять же это не значит, что они этого не сделают, просто они заставят вас за это заплатить.
3. Плата за то, чтобы не продавать украденные данные конкурентам, что несколько отличается от их публикации.
4. Продажа украденных данных заинтересованным сторонам даже после получения выплат, перечисленных в п. 1–3.

Шифрование существенных данных (см. следующий раздел) защитит вас от расходов, связанных с п. 2–4. Зашифрованные данные не имеют ценности для посторонних злоумышленников, потому что они не могут их прочитать. Однако это не застрахует вас от расходов, указанных в п. 1, так как они могут зашифровать ваши уже зашифрованные данные. Им не нужно их читать, чтобы сделать их непригодными для использования организацией-жертвой. Единственный способ защиты от этого риска заключается в создании резервных копий существенных данных и умении восстанавливать их в кризисной ситуации. Как и в случае с шифрованием, это гораздо проще сказать, чем сделать.

У большинства из нас информация разбросана по множеству островов данных, к которым относятся мобильные устройства, SaaS-приложения, дата-центры и гибридные облачные среды. Не существует какой-то одной кнопки, которая позволила бы создать резервную копию данных на всех этих островах и волшебным образом восстановить их в случае катастрофы. Вам придется разработать такую систему, совершенствовать ее и применять на практике. Однако вы можете упростить эту задачу, сосредоточившись на самых существенных данных. Сетевым защитникам не обязательно создавать резервные копии и восстанавливать все данные, генерируемые организацией. Достаточно сделать это только с наиболее важными для бизнеса. Такой подход может значительно сократить количество проблем, однако в зависимости от особенностей организации уровень сложности этой задачи, базирующейся на основополагающем принципе, может варьироваться в широких пределах. Тем не менее по возможности старайтесь не тратить ресурсы на то, что вам не нужно.

Кроме того, в наш век инфраструктуры как кода не стоит забывать о том, что программы, которые вы используете для обеспечения работы критически важных бизнес-систем, тоже являются данными. Помимо базы данных ваших клиентов, группировки вымогателей могут повредить и их. Под критически важными данными я подразумеваю все данные, используемые системой и всем программным обеспечением для поддержания работы бизнеса, коммерческие приложения, за которые вы платите, код, разрабатываемый своими силами, а также свободное ПО, которое вы берете с GitHub.

Для резервного копирования всех этих данных обычно используются три варианта: платформа для централизованного резервного копирования, децентрализованные системы для однократного резервного копирования и внутренняя автоматизация в рамках работы критически важных бизнес-приложений (DevOps). Многие организации применяют гибридный подход, объединяющий все три варианта.

Вариант 1. Платформы для централизованного резервного копирования содержимого всех островов данных

Согласно диаграмме Gartner за июнь 2021 года, касающейся корпоративных платформ резервного копирования и восстановления, существует целый ряд компаний, предлагающих услуги резервного копирования [159]. Большинство из них заявляют о возможности резервного копирования и восстановления файлов и программного обеспечения, хранящихся в виртуальных рабочих нагрузках (таких как VMware и Hyper-V), гибридных облачных средах (например, Google, Amazon и Microsoft), конкретных SaaS-приложениях (в частности, SAP и Exchange) и хранилищах данных (вроде NetApp и Nutanix). Вы можете устанавливать их в облаке или запускать из собственных центров обработки данных. В рамках такой модели за обслуживание всей вашей бизнес-системы отвечает одна организация. Другими словами, одно подразделение, скажем ИТ-отдел, следит за тем, чтобы все работало, а остальные подразделения вносят свой вклад в разработку конкретных политик резервного копирования. Однако такие системы стоят недешево и, вероятно, доступны лишь крупным организациям. Малым и средним организациям придется полагаться на осмотрительность сетевых защитников.

Вариант 2. Децентрализованные системы для однократного резервного копирования

Под децентрализацией я подразумеваю возможность использования решений для резервного копирования и восстановления, разработанных для конкретных наборов данных, требующих защиты. Например, если интеллектуальная собственность вашей компании хранится в экземпляре облака Amazon, можете подумать о возможности применения решений для резервного копирования этого экземпляра. То же самое относится и к другим облачным сервисам. Если в своих дата-центрах вы работаете с коммерческим устройством хранения данных, то можете рассмотреть возможность использования предусмотренной в нем услуги аварийного восстановления. Все подобные устройства имеют ту или иную версию такой услуги. Суть

в том, что вместо одной платформы, применяемой для резервного копирования и восстановления всей существенной информации, хранящейся на всех островах данных, вы будете задействовать специальные решения для резервного копирования и восстановления каждого отдельного набора существенных данных. Это чуть сложнее, поскольку при этом вам придется управлять решениями нескольких поставщиков, что чревато большим количеством проблем. Однако для малых и средних организаций такой вариант может оказаться более доступным.

Вариант 3. DevOps (DevSecOps) для каждого приложения

План DevSecOps должен предусматривать возможность резервного копирования и восстановления при развертывании нового приложения в рамках парадигмы «инфраструктура как код». Именно так поступают крупные компании, например Google, Netflix и Salesforce. Как говорится в книге «Site Reliability Engineering», попавшей в Зал славы Cybersecurity Canon, развертывание систем резервного копирования является частью задачи. SRE-инженеры Google применяют знания из области информатики и инженерии для «проектирования и разработки вычислительных систем». Другими словами, они стремятся создавать надежные решения, а резервное копирование и операции восстановления — ключевая часть этого процесса: «По традиции компании защищают данные от потери, инвестируя средства в разработку стратегий резервного копирования. Однако основные усилия должны быть направлены на восстановление данных, которое отличает настоящие резервные копии от архивов. Как было верно отмечено, на самом деле людям нужны не резервные копии, а возможность восстановления данных».

У компаний из списка Fortune 500 есть для этого средства, однако даже стартапы, создающие новые SaaS-приложения, работают по принципу «инфраструктура как код» и имеют ресурсы для решения этой задачи. Высшему руководству просто нужно направить их на то, чтобы сделать это частью сервиса, который продукт предлагает клиентам. Проблемы с этим вариантом могут возникнуть у старых компаний малого и среднего размера, которые еще не приняли ни модель DevOps (см. главу 7), ни даже облачную модель. Скорее всего, они будут вынуждены ограничиться первыми двумя вариантами.

Как попасть в Карнеги-холл? Надо практиковаться!

Как и в случае с тактикой преодоления кризиса, единственный способ наработки навыков резервного копирования и восстановления — это практика. Подобно SRE-инженерам Google, вам следует помнить: работа не может считаться законченной до тех пор, пока вы не отработаете процесс восстановления и не удостоверитесь в том, что сможете добиться желаемых результатов с использованием восстановленных данных. Нужно совершенствовать эти навыки до тех пор, пока они не станут вашей второй натурой. Вы же не хотите придумывать все на ходу во время реального кризиса? Кроме того, если будете уверены в своей способности восстановить данные, то, когда перед руководством встанет вопрос «Платить ли выкуп?», ответом на него будет «Нет», потому что вы уже неоднократно доказали, что можете восстановить системы самостоятельно.

Шифрование: тактика обеспечения устойчивости

Каждый раз, когда я возвращаюсь к теме шифрования, мне приходится заново изучать определения. Мой стареющий мозг просто не может удержать их в памяти. В одном из моих любимейших фильмов о супергероях «Человек-паук: Через вселенные» все люди-пауки по очереди рассказывают историю своего происхождения, начиная ее словами: «Хорошо, давайте сделаем это еще раз». Давайте и мы сделаем это еще раз для криптографии.

- *Криптография* (рифмуется с фотографией) — искусство и наука создания кодов.
- *Шифрование* — преобразование обычного текста в неузнаваемую форму с помощью шифров, создаваемых криптографами. Для целей этой книги я отношу такие техники, как маскировка данных и токенизация баз данных, к способам сокрытия информации от посторонних глаз.
- *Подпись* — использование хеш-функций или математических односторонних криптографических функций для обеспечения невозможности отказаться. Другими словами, авторы подписанных сообщений или файлов не могут отрицать факт их подписания, а подделка подписи посторонним лицом математически маловероятна.
- *Ключи* — последовательности символов, используемые криптографической функцией для преобразования открытого текста в зашифрованный

или наоборот. Подобно физическому ключу, он блокирует данные, чтобы их мог разблокировать только тот, у кого есть подходящий ключ.

- *Криптоанализ* — обратная сторона криптографии. Это все, что связано со взломом кодов (например, Алан Тьюринг использовал правило Байеса, чтобы взломать код немецких шифровальных машин «Энигма» во время Второй мировой войны, см. главу 6).

А чтобы еще больше все запутать, я скажу, что существует наука криптология, которая охватывает обе дисциплины — криптографию и криптоанализ.

Если любителям компьютерных игр из числа читателей захочется попробовать свои силы в криптологии, есть замечательная компьютерная игра от первого лица *CYpHER*, в которой вам предстоит ходить по музею криптологии и решать многочисленные головоломки, связанные с различными видами криптоанализа, такими как:

- стеганография;
- транспозиция;
- моноалфавитная замена;
- многоалфавитная замена;
- механизированная криптография;
- цифровая криптография.

Лично я не решил даже первую головоломку, но вам, возможно, повезет больше.

Идея криптографии возникла в древние времена. По данным компании Thales Group, примерно в 600 году до н. э. спартанцы использовали устройство под названием «сцитала» для преобразования открытого текста в зашифрованные сообщения [265]. Для расшифровки этих сообщений их друзьям требовалось идентичное по ширине и длине устройство. К 60 году до н. э. римляне уже использовали простой подстановочный шифр, суть которого сводилась к шифрованию сообщения путем сдвига каждой его буквы на некоторое количество символов алфавита. Например, если это количество было равно 3, то буква A исходного сообщения превращалась в букву D закодированного, буква B — в букву E и т. д. В 1553 году Джованни Баттиста Беллазо предложил идею секретного ключа или пароля, используемого двумя сторонами для шифрования и расшифровки сообщений. Другими словами, если Фред и Джинджер захотят обменяться секретными

сообщениями, им обоим понадобится секретный ключ. Фред использует его для шифрования сообщения, а Джинджер — для расшифровки.

К 1917 году американец Эдвард Хеберн изобрел электромеханическую машину, шифрующую сообщения с помощью ключа в виде вращающегося диска [240]. В 1918-м немецкий инженер Артур Шербиус придумал машину «Энигма» с несколькими роторами, которую немецкие военные использовали для обмена закодированными сообщениями во время Первой и Второй мировых войн (принцип работы «Энигмы» подробно описан в главе 7) [174].

К началу 1970-х годов компания IBM разработала блочный шифр [269], ключ которого представлял собой целый блок текста, а не набор из нескольких букв, как у «Энигмы». В 1973 году правительство США приняло этот стандарт шифрования данных (Data Encryption Standard, DES) и использовало его до тех пор, пока он не был взломан в 1997-м [204].

В 1976 году Уитфилд Диффи и Мартин Хеллман разработали схему обмена ключами (протокол Диффи — Хеллмана), сделавшую возможной отправку зашифрованных сообщений без предварительного обмена секретными ключами. Это было грандиозно [139]. Метод называется *асимметричным шифрованием*, и именно он лежит в основе всех современных безопасных веб-транзакций. Его суть заключается в том, что существует открытый ключ, который может использовать любой человек в мире, чтобы зашифровать сообщение, адресованное Джинджер. Но только у Джинджер есть секретный ключ, с помощью которого можно расшифровать отправленные ей сообщения. Эти два ключа (открытый и закрытый) математически связаны между собой, но использовать открытый ключ для чтения зашифрованного сообщения невозможно.

В 1977 году Рон Ривест, Ади Шамир и Леонард Адельман создали алгоритм RSA — первый рабочий алгоритм обмена ключами. К 2000 году расширенный стандарт шифрования AES (Advanced Encryption Standard) заменил стандарт DES, так как был более быстрым и позволял использовать гораздо более длинные ключи.

Данные в состоянии покоя и данные в движении

Мы применяем методы шифрования к данным в состоянии покоя и к данным в движении. Данные в состоянии покоя хранятся где-то на жестком диске. Их никто не перемещает и не обрабатывает. Они находятся там для каких-то будущих целей. Данные в движении перемещаются из точки А в точку Б, например, когда веб-сайт предоставляет контент пользователю

или сообщение электронной почты переходит от отправителя к получателю. Кроме того, они каким-то образом обрабатываются, как, например, при поиске в базе данных или в ходе применения алгоритма машинного обучения к их набору.

Исходя из этого вполне логичным является шифрование как данных в состоянии покоя, так и данных в движении. Сложно ли это? Если вы поразмыслите, то поймете, что количество возможных перестановок для данных, которые должны быть подписаны и зашифрованы, растет в геометрической прогрессии. Каждое физическое устройство, которое взаимодействует с этими островами данных, каждая рабочая нагрузка, действующая в облачной среде, каждый человек, использующий эти устройства и рабочие нагрузки, а также каждая транзакция между людьми и технологиями может быть подвергнута тому или иному криптографическому преобразованию.

Под криптографическим преобразованием я подразумеваю то, что на каком-то этапе процесса некий алгоритм генерирует ключ, применяет его, сохраняет, использует, изменяет или выводит из эксплуатации для каждой транзакции, каждого устройства и каждого пользователя на всех островах данных. Значительный объем и высокий темп выполнения этих важнейших цифровых операций может заставить руководителей служб безопасности свернуться калачиком в SOC-центре и бормотать про себя: «Хоть бы все сработало. Хоть бы все сработало». В документе, написанном специалистами компании Gartner Дэвидом Махди и Брайаном Лоуэнсом в 2020 году, говорится о том, что руководители служб безопасности «с трудом понимают возможности и ограничения корпоративных решений для управления ключами шифрования (EKM) и не знают, как их правильно настраивать» [149]. Под этим они подразумевают то, что большинство из нас не имеет ни комплексной политики шифрования, ни глобального плана. Они предположили, что в лучшем случае наши подходы носят фрагментарный характер и применяются по-разному в каждом конкретном случае. Они также отметили, что в большинстве случаев процесс и политика шифрования не являются организационными императивами.

Хорошая новость заключается в том, что мы можем уменьшить масштаб задачи, имея дело только с самыми существенными данными. К сожалению, это не уменьшает уровня сложности. Оркестрация решений для шифрования существенной информации, хранящейся на всех островах данных, учитывая количество перестановок, по-прежнему остается сложным и очень запутанным делом. Самое страшное заключается в том, что большинство из нас пытается сделать это самостоятельно и вручную. А поскольку все острова данных состоят из различных массивов информации,

для их шифрования требуется множество продуктов, в которые необходимо вкладывать средства. Мы разрабатываем собственные программные инструменты на основе открытого и коммерческого ПО. И даже можем попытаться задействовать облачные SaaS-сервисы для управления ключами, например Google, Microsoft и AWS. До сих пор не существовало единой платформы для шифрования, которая работала бы со всеми островами данных. Однако в скором времени ситуация может измениться. По мнению Махди и Лоуэнса, EKM-решения находятся на склоне просветления диаграммы Gartner, но до достижения плато продуктивности пройдет еще 5–10 лет.

Тактика шифрования, основанная на базовом принципе кибербезопасности, является рекурсивной

Тонкий момент заключается в том, что, какие бы системы и процессы вы ни использовали для шифрования данных своей организации, эти системы и процессы рекурсивным образом становятся существенными. Вы используете систему шифрования для защиты конфиденциальных данных, но поскольку она критически важна для данного процесса, то оказывается существенной и для организации. Если злоумышленник каким-то образом скомпрометирует вашу систему шифрования, то под угрозой окажется все, что вы пытаетесь защитить с ее помощью.

В качестве примера можно привести атаку на SolarWinds с использованием бэкдора, начавшуюся в декабре 2020 года [256]. Это, пожалуй, самая известная атака на цепочку поставок за последнее время, однако ущерб жертвам был нанесен не бэкдором, внедренным в платформу SolarWinds. С его помощью хакеры, стоявшие за кампанией UNC2452, просто создали плацдарм, заразив более 18 000 устройств. Ущерб был нанесен позднее примерно 40 жертвам, в сетях которых злоумышленники искали учетные данные администратора. Хакеры UNC2452 скомпрометировали процесс авторизации на основе облачных токенов, что позволило им генерировать ключи, открывающие доступ к облачным ресурсам. Как вы понимаете, это очень плохо.

Снижение вероятности атаки такого рода на вашу систему шифрования достигается следованием тем же стратегиям, основанным на базовом принципе кибербезопасности, которые мы используем для защиты всех остальных материальных активов.

Нулевое доверие (см. главу 3)

- Осуществляйте централизованное управление ключами. Не отдавайте этот процесс на откуп отдельным командам, которые в нем нуждаются. Он никогда не будет для них приоритетной задачей.
- Ограничьте число учетных записей администраторов, способных генерировать ключи, до абсолютного минимума.
- Пристально следите за этими учетными записями.
- Добавьте авторизацию на основе кворума, при которой для генерации ключей требуется не одна, а несколько учетных записей.

Предотвращение реализации убийственной цепочки вторжения (см. главу 4)

- На момент написания этой книги в базе знаний MITRE ATT&CK техника слабого шифрования (ID T1600) описывалась как компрометация «функций шифрования сетевого устройства для обхода защиты, применяемой для обеспечения безопасной передачи данных».
- Эта техника применяется в рамках как минимум двух вражеских кампаний — APT32 (предположительно, спонсируемой правительством Вьетнама) и UNC2452. Блокирование последовательности действий на всех этапах убийственной цепочки в рамках этих двух кампаний и любых других, задействующих эту технику, было бы разумным подходом.

Обеспечение устойчивости (см. данную главу)

- Полностью развернутая система шифрования представляет собой трубопровод для доставки той «магии», в которой нуждаются ваши клиенты. Если он откажет, вы не сможете ее доставить.
- Спроектируйте систему шифрования так, чтобы она была способна пережить катастрофический сбой.

Прогнозирование рисков (см. главу 6)

- Предусмотрите в своей модели вероятность применения стратегий, базирующихся на первичном принципе кибербезопасности, против системы шифрования. (Это станет более понятным после чтения главы 7.)
- Каждый ваш шаг должен способствовать снижению вероятности нанесения вам существенного ущерба. Другими словами, какова его вероятность без принятия каких-либо мер защиты? Какова вероятность при частичном развертывании программы нулевого доверия? А какова

вероятность при полном развертывании этой программы? Примените этот же пошаговый процесс к стратегии предотвращения реализации убийственной цепочки вторжения и стратегии обеспечения устойчивости.

- Оценивайте целесообразность каждого шага, взвешивая его стоимость относительно степени склонности высшего руководства к риску.

В предыдущем разделе, посвященном тактике резервного копирования и восстановления, базирующейся на первичном принципе кибербезопасности, я сказал, что шифрование — лучший способ уменьшения ущерба в случае атаки вымогателей, поскольку помогает избежать трех из четырех связанных с ней видов расходов, а именно:

- платы за неразглашение украденных данных;
- платы за то, чтобы украденные данные не были проданы конкурентам (что несколько отличается от их публикации);
- последствий продажи украденных данных заинтересованным сторонам даже после получения выкупа.

Это лучшая тактика для борьбы с любым видом кибершпионажа (кражи корпоративных или правительственных секретов). Вы не сможете украсть секреты, если не сумеете их прочитать.

Операции резервного копирования и шифрования относятся к пассивным тактикам обеспечения устойчивости, базирующимся на первичном принципе кибербезопасности. Под этим я подразумеваю то, что руководители служб безопасности развертывают их до киберинцидента, чтобы защитить организацию от любых будущих кибератак. Непосредственно в ходе атаки необходимо применять такую тактику, как реагирование на инциденты.

Реагирование на инциденты: тактика обеспечения устойчивости

На заре развития Интернета (в конце 1980-х годов) не было ни сервиса AOL, ни Всемирной паутины, ни постоянного домашнего подключения к Сети. Чтобы подключиться к ней, пользователям приходилось ехать в университет или на военную базу. А дома они использовали модем с коммутируемым доступом, задействующий телефонную линию для установки соединения с одним из 60 000 компьютеров, подключенных к Интернету в тот период.

По оценкам некоторых экспертов, к 2025 году число подключенных к Интернету устройств достигнет 75 млрд. А тогда Интернет еще не был достоянием широких масс, но он был жизненно необходим правительственным и исследовательским учреждениям.

> Третьего ноября 1988 года я допоздна работал над программой для курса по структурам данных, который изучал в Военно-морской аспирантуре в Монтерее (штат Калифорния). До окончания срока сдачи задания оставалось всего три часа, но я никак не мог подключить свой модем, работающий со скоростью 2400 бод, к университетскому банку модемов и уже начинал паниковать. Я даже не представлял, что вскоре после полуночи 23-летний аспирант Корнельского университета Роберт Таппан Моррис поставит на колени весь Интернет. Он запустил первого в истории интернет-червя, из-за которого Сеть не работала несколько дней, пока UNIX-специалисты по всему миру удаляли его из своих систем.

Как я упоминал в главе 4, червь Морриса побудил Агентство перспективных оборонных исследовательских проектов (DARPA), научно-техническую организацию Министерства обороны США, выделить средства Университету Карнеги — Меллона на создание первого координационного центра реагирования на инциденты компьютерной безопасности (CERT/CC) для управления будущими чрезвычайными ситуациями в этой области. Помимо этого, он спровоцировал в формирующемся сообществе сетевых защитников дискуссию о том, как следует реагировать на киберинциденты, возникающие в организации. В Военно-морской аспирантуре, где я тогда учился, реакция сводилась к тому, что преподаватели, способные правильно произнести слово UNIX три раза из пяти, бегали по коридорам со вставшими дыбом волосами и выкрикивали друг другу такие эзотерические компьютерные термины, как *sendmail*, *rsh*, *telnet* и *finger*. К счастью, теперь есть способы получше.

Мой герой в мире информатики — доктор Клиффорд Столл. Если бы для гигантов компьютерных наук существовал аналог бейсбольных карточек, в моей коллекции были бы карточки с Грейс Хоппер, Аланом Тьюрингом и доктором Столлом. Его книга «Яйцо кукушки», включенная в Зал славы Cybersecurity Canon, на протяжении более чем 30 лет остается одной из самых влиятельных книг по кибербезопасности [297]. Одна из причин этого заключается в том, что он практически в одиночку изобрел схему

реагирования на инциденты. За прошедшие годы разработанные им методы практически не изменились.

В 1986 году доктор Столл работал астрономом в Калифорнийском университете в Беркли и был очень далек от вопросов безопасности. Но его попросили помочь в лаборатории UNIX, расположенной на территории университета, и отследить бухгалтерскую ошибку в компьютерных записях. В те времена университеты взимали со своих студентов плату за использование компьютеров, и каждый месяц в бухгалтерских записях сумма, полученная от всех пользователей компьютеров из числа студентов Беркли, отличалась от фактической на 75 центов. Никто не мог понять, в чем дело. Расследование Столла, нацеленное на исправление этой ошибки, привело к выявлению первой публичной кампании кибершпионажа, проводимой русскими с помощью восточногерманских хакеров-наемников для взлома систем американских университетов и дальнейшего проникновения в американские военные системы. В те времена никаких средств безопасности не существовало, а Интернет напоминал множество жестяных банок, соединенных проводами.

Будучи астрономом по образованию, Столл подошел к решению проблемы как к научному эксперименту. Он разрабатывал гипотезы, ставил эксперименты для их проверки и фиксировал результаты. В 1988 году он опубликовал в журнале Communications of the ACM статью [297], которая в итоге превратилась в книгу, изданную в 1989-м. Если вы еще не прочитали ее, бросьте все и сделайте это. Доктор Столл, как бы это сказать, довольно эксцентричен. Его чудаковатость и жизнерадостность пронизывают всю книгу. Она вам понравится, даже если вы не технарь. Обещаю, вы будете в восторге и в процессе чтения станете свидетелем зарождения лучшей практики реагирования на инциденты.

Я прочитал его книгу за те выходные, которые должен был потратить на работу над своей магистерской диссертацией. В те времена авторы указывали в своих книгах адреса электронной почты, и после окончания чтения я отправил доктору Столлу длинное восторженное письмо. Спустя 15 минут я получил от него очень дружелюбный ответ и с тех пор являюсь его ярым поклонником.

Руководства NIST по обеспечению кибербезопасности и реагированию на инциденты

Основные положения руководства по обработке инцидентов компьютерной безопасности *Computer Security Incident Handling Guide: Special Publication 800-61 Revision 2*, опубликованного Национальным институтом стандартов и технологий (NIST) в 2012 году, занимают три страницы [46]. Только в правительственных документах резюме может быть таким длинным. Далее я в общих чертах расскажу, что там написано.

Согласно федеральному законодательству федеральные агентства должны иметь возможности для реагирования на инциденты и должны сообщать о них Американской группе реагирования на инциденты компьютерной безопасности (US-CERT). Авторы документа различают киберсобытия (наблюдения, сделанные на основе телеметрии сетевых устройств) и киберинциденты (нарушения или неминуемые угрозы нарушения политик компьютерной безопасности). Жизненный цикл реагирования на инциденты состоит из следующих этапов (рис. 5.3).

1. *Подготовка.* Разработайте план реагирования на киберинцидент.
2. *Обнаружение и анализ.* Разработайте схему раннего обнаружения и анализа киберинцидентов.
3. *Сдерживание, ликвидация и восстановление.* Обнаружив противника, не позволяйте ему перемещаться по своей сети. Лишите его возможности незаметно подключиться к ней из другого места. Восстановите работу пострадавших систем.
4. *Подведение итогов.* Проанализируйте свои действия. Внесите улучшения в план для более эффективного реагирования на следующий инцидент.

Другая признанная в отрасли система реагирования на инциденты была разработана коммерческой компанией SysAdmin, Audit, Network, and Security (SANS), занимающейся обучением и сертификацией поставщиков систем безопасности. Ее модель отличается в плане организации, но охватывает ту же область, что и система NIST. Выбор той или иной системы не сводится к определению самой лучшей. Скорее, речь идет о том, какая из них больше подходит для вашей организации.

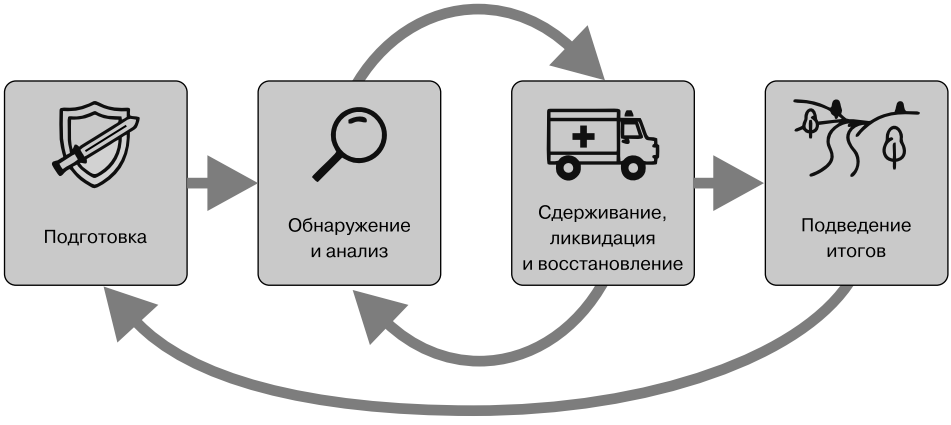


Рис. 5.3. Жизненный цикл реагирования на инциденты [46]

Техническая сторона реагирования на инциденты

Жизненный цикл реагирования на инциденты, предложенный NIST, описывает техническую сторону мониторинга киберсобытий, отраженных в телеметрии развернутого стека безопасности, и их преобразования в киберинциденты, если на это есть основания. Если на шкале размеров ваша организация находится между средними организациями и компаниями из списка Fortune 500, то в ней за реагирование на инциденты, скорее всего, отвечает SOC-центр. Возможно, у вас есть специальная команда для выполнения этой функции, а может быть, вы собираете такую команду при наступлении каждого конкретного события. Если имеется группа кибербразведки (см. главу 4), то она, скорее всего, входит в состав группы реагирования на инциденты. Если же организация располагается ближе к другому концу шкалы, то есть между стартапами и организациями среднего размера, то за реагирование на инциденты, скорее всего, отвечает ИТ-отдел, вынужденный бросать свои обычные дела, чтобы справиться с проблемой.

Говоря в терминах базовых принципов, команда SOC-центра отслеживает телеметрию каждой развернутой тактики нулевого доверия (см. главу 3), предотвращения реализации kill chain (см. главу 4) и обеспечения устойчивости (см. данную главу) в поисках признаков наступления киберсобытия. После накопления свидетельств SOC-центр передает их группе реагирования на инциденты для дальнейшего анализа. В большинстве случаев тревога оказывается ложной. Однако при реальном киберинциденте начинается реализация плана действий, направленного на его устранение. Тем не менее

перевод киберсобытия в разряд киберинцидентов — это скорее искусство, чем наука.

Например, в главе 4 я упоминал о том, что на момент написания этой книги в базе знаний MITRE ATT&CK значилась кампания под названием Cobalt Spider, предусматривающая использование 31 метода атаки и пяти программных инструментов. Если сотрудники SOC-центра выявляют в сети факт применения одного из этих методов, то это считается киберсобытием. Однако это может быть все что угодно: ложное срабатывание, первый признак того, что какая-то хакерская группировка взаимодействует с нашими островами данных, или первые признаки активности именно хакеров из Cobalt Spider. Мы пока этого не знаем. В то же время, если SOC-центр выявит факт применения каждого из 31 метода и всех программных инструментов, это будет свидетельствовать о том, что хакеры, стоящие за кампанией Cobalt Spider, определенно находятся в нашей сети и команда должна реагировать на это как на киберинцидент. Самое сложное заключается в размытости границы, отделяющей киберсобытие от киберинцидента. На каком этапе сбора доказательств команда реагирования на инциденты должна перевести киберсобытие в разряд киберинцидентов? Когда выявит факт использования трех методов и одного программного инструмента? Или десяти методов и трех программных инструментов? Обычно это решение принимается интуитивно, но оно в любом случае важно, поскольку, как только событию присваивается статус инцидента, за его устранение отвечает уже не только SOC-центр, но и другие члены организации в соответствии с антикризисным планом, о котором мы говорили ранее.

В руководстве по улучшению кибербезопасности критической инфраструктуры *Framework for Improving Critical Infrastructure Cybersecurity*, опубликованном NIST в 2018 году и являющемся обновлением первоначальной публикации 2014 года, авторы предложили схему управления рисками кибербезопасности для улучшения защиты критической инфраструктуры правительства США. Это руководство достаточно универсально для того, чтобы его могли применять «организации, работающие в любом секторе или сообществе. Данный фреймворк позволяет организациям вне зависимости от их размера, степени риска и уровня развития средств кибербезопасности применять принципы и лучшие практики управления рисками для усиления защиты и обеспечения устойчивости». По сути, это руководство по реагированию на инциденты.

Руководство мгновенно стало хитом, и теперь ИБ-специалисты используют его в качестве своеобразной модели для оценки зрелости таких пяти

ключевых функций, как идентификация, защита, обнаружение, реагирование и восстановление (рис. 5.4).

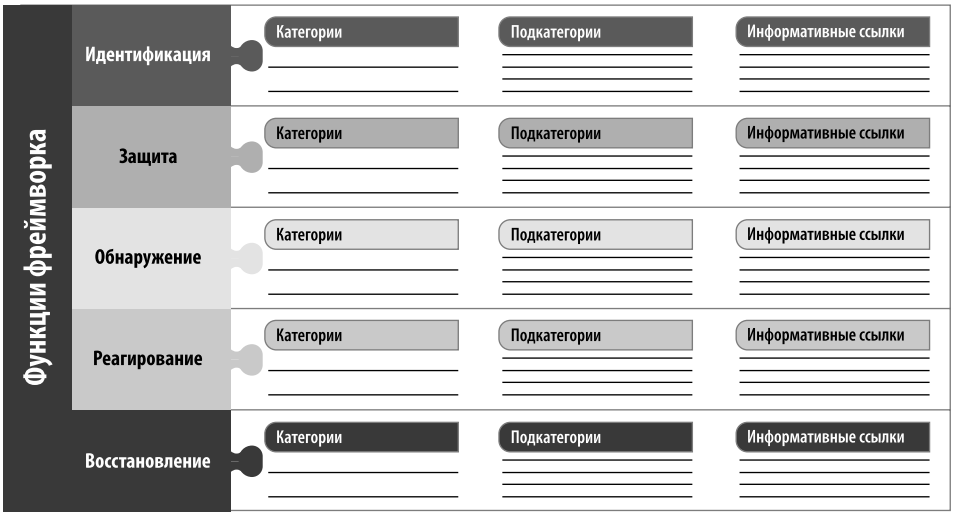


Рис. 5.4. Основная структура фреймворка [23]

Это фундаментальный документ. В его основу были положены очень глубокие анализ и исследования, а итоговый фреймворк представляет собой весьма полезную модель как для определения рамок пространства кибербезопасности в целом, так и для оценки того, насколько зрелой является ваша организация в плане реализации перечисленных пяти функций. Оценка своей оборонительной позиции с учетом этих элементов — вполне целесообразная трата времени и усилий.

Однако это не стратегия и не атомарный базовый принцип. Даже если на этой шкале ваша организация окажется самой зрелой по сравнению со всеми остальными организациями в мире, что вам это даст? Что вы скажете своему руководителю, когда это произойдет? Максимум, что вы сможете сказать, — это то, что выполнили множество пунктов из рекомендованного правительством списка лучших практик. В ответ на это начальник, скорее всего, скажет: «Ну и чем мне это поможет? Что я получу в результате траты денег на достижение этих целей?» Сам по себе фреймворк не поможет вам доказать, что результат этих усилий стоил вложенных в них ресурсов в виде людей, процессов и технологий.

Однако если вы сделаете акцент на первичных принципах и попытке снизить вероятность существенного ущерба в результате киберинцидента,

это изменит ход дискуссии. Скажите своему руководителю, что одной из ключевых стратегий для снижения этой вероятности является обеспечение устойчивости и что каждая тактика, предусмотренная данным фреймворком, способствует именно этому и снижает такую вероятность на определенную величину (я покажу способ ее расчета в главе 6). Имея такую информацию, руководители могут принимать решения относительно распределения ресурсов, сравнивая риски кибербезопасности со всеми остальными рисками, которыми они жонглируют при ведении бизнеса.

Реагирование на инциденты практикуется ИБ-сообществом с момента его формирования (доктор Столл разработал этот метод еще в 1988 году). Руководства NIST *Computer Security Incident Handling Guide* и *Framework for Improving Critical Infrastructure Cybersecurity* определили лучшие практики для решения этой задачи. Таким образом, сетевые защитники могут применять тактики обеспечения устойчивости, связанные с использованием таких функций, как идентификация, защита, обнаружение, реагирование и восстановление, для снижения вероятности нанесения существенного ущерба их организациям. Это очень важно, так как мы не можем запустить реализацию антикризисного плана до тех пор, пока кто-то в организации не скажет, что мы столкнулись с потенциальным киберинцидентом, а за это отвечает группа реагирования на них.

Заключение

В этой главе я привел лучшее, на мой взгляд, определение стратегии обеспечения устойчивости. Используя его в качестве логического продолжения основополагающего принципа кибербезопасности, я описал четыре тактики, сильнее всего влияющие на снижение вероятности причинения существенного ущерба, а именно: кризисное планирование, резервное копирование и восстановление, шифрование и реагирование на инциденты. В следующей главе покажу, как рассчитать степень влияния этих тактик, причем не только для стратегии обеспечения устойчивости, но и для всех остальных стратегий, основанных на базовом принципе кибербезопасности.

06 Прогнозирование рисков

Предсказуемость того или иного события зависит от того, что мы пытаемся предсказать, насколько далеко в будущее заглядываем и при каких условиях.

Филип Тетлок

По сути, все модели ошибочны, но некоторые из них полезны.

Джордж Бокс

Обзор главы

За прошедшие годы многие важные навыки ИБ-специалистов значительно улучшились, но есть один, в освоении которого они практически не продвинулись, — это расчет киберрисков и способность доносить информацию о них до высшего руководства и совета директоров.

В первые годы работы в качестве сетевого защитника, когда кто-нибудь просил меня оценить риски, я ограничивался использованием качественной тепловой карты (электронной таблицы с цветовой кодировкой, где все риски были перечислены вдоль оси *X*, а три уровня потенциального воздействия — высокий, средний и низкий — вдоль оси *Y*) (рис. 6.1) [205]. Как и многие коллеги, я говорил себе, что предсказать киберриск с большей точностью нельзя, что существует слишком много переменных, что кибербезопасность чем-то отличается от всех прочих дисциплин в мире, что эту задачу просто невозможно решить.

Рис. 6.1. Типичная тепловая карта для качественной оценки

Разумеется, все мы ошибались.

Зал славы Cybersecurity Canon полон книг, рассказывающих о том, как можно точно рассчитать киберриск, в частности:

- «Как оценить риски в кибербезопасности», авторы Дуглас У. Хаббард и Ричард Сирсен [334];
- *Measuring and Managing Information Risk: A Fair Approach*, авторы Джек Фройнд и Джек Джонс [81];
- *Security Metrics: A Beginner's Guide*, автор Кэролайн Вонг [318];
- *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, автор Эндрю Джакит [124].

Это отличные учебники, демонстрирующие совершенно иной подход к вероятностному прогнозированию. Я настоятельно рекомендую их изучить. Если эта тема для вас нова, они изменят ваш взгляд на мир. Однако моя претензия ко всем этим книгам заключается в том, что я так и не нашел в них главы под названием «И вот как это делается» или, еще лучше, «Построение диаграммы рисков, которую можно продемонстрировать совету директоров». Ни в одной из книг не содержится ничего похожего. Эта часть всегда оставлялась на откуп читателю в качестве упражнения. И я собираюсь восполнить данный пробел.

В этой главе выполним упражнение, которого так не хватает в перечисленных книгах. Мы рассмотрим два конкретных примера. В первом проанали-

зируем Marvel Studios по схеме «извне внутрь». Я выбрал Marvel Studios по двум причинам. Во-первых, я фанат комиксов. А во-вторых, что более важно, Marvel Studios — это типичная компания среднего размера с точки зрения выручки, поэтому большинство из нас легко может представить на ее месте собственную организацию. Этот анализ проводится по схеме «извне внутрь», потому что мы не принимаем во внимание то, как Marvel Studios защищает себя с точки зрения базовых принципов кибербезопасности (это делается в рамках анализа по схеме «изнутри наружу»). Наша задача — проанализировать вероятность того, что компания, сопоставимая с Marvel Studios по размеру и объему выручки, столкнется с существенным киберсобытием.

Во втором примере мы проанализируем вымышленную компанию Microsoft под названием Contoso как по схеме «извне внутрь», так и по схеме «изнутри наружу». Microsoft использует Contoso в маркетинговых материалах, чтобы продемонстрировать способ использования своих продуктов. Тем не менее подробное описание ее ИТ-архитектуры позволяет сделать некоторые предположения о ее состоянии в плане кибербезопасности, что делает возможным прогнозирование как «извне внутрь», так и «изнутри наружу».

Однако, прежде чем переходить к рассмотрению примеров, я должен познакомить вас с инструментами, необходимыми для подобных расчетов, в частности с методами суперпрогнозирования, оценками Ферми, проблемами «черного лебедя» и правилом Байеса.

Суперпрогнозирование, оценки Ферми и «черные лебеди»

Книга Филипа Тетлока и Дэна Гарднера «Думай медленно — предсказывай точно» [332], являющаяся еще одним кандидатом на попадание в Зал славы Cybersecurity Canon, изменила мое отношение к прогнозированию рисков и заставила поверить в то, что это в принципе возможно.

Доктор Тетлок — весьма своеобразный человек. При просмотре телепередач он часто кричит и грозит кулаком, потому что говорящие головы понятия не имеют, о чем толкуют. В частности, это относится к новостным программам CNN, FOX и MSNBC, ведущие которых приглашают известных экспертов, чтобы те высказали свое мнение по той или иной теме, потому что однажды в жизни им удалось что-то точно предсказать. И неважно, что все их последующие предсказания были ошибочными. Ведущие новостных

программ все равно приглашают их в эфир, представляя их чуть ли не Моисеем, спустившимся с горы Синай с каменными скрижалями.

Доктор Тетлок считал, что эти эксперты должны вести счет, а при их появлении в эфире зритель должен видеть в нижней части экрана фразу наподобие: «За последний год этот эксперт сделал три правильных прогноза из 100 попыток. Возможно, вам не стоит слишком внимательно прислушиваться к его мнению». Доктору Тетлоку так нравилась эта идея, что он провел научное исследование, в ходе которого проверил свою теорию о том, что большинство экспертов — ужасные прогнозисты.

Сотрудничая с Агентством передовых исследований в сфере разведки (Intelligence Advanced Research Projects Agency, IARPA), он разработал тест, в котором участвовали три группы: сотрудники разведслужбы, представители академического сообщества и группа, которую я назвал «Мудрые старцы». Последняя состояла не из стариков — это были обычные люди, имеющие свободное время и любящие решать головоломки. Согласно газете Washington Post, Тетлок попросил участников сделать предсказания, ответив на более чем 500 по-настоящему сложных вопросов, таких как:

- «Будет ли президент Сирии Башар Хафез аль-Асад по-прежнему находиться у власти спустя шесть месяцев?»;
- «Произойдет ли в ближайший год обмен военными ударами в Южно-Китайском море?»;
- «Увеличится ли количество терактов, спонсируемых Ираном, в течение года после снятия санкций?».

По результатам этого теста «Мудрые старцы» превзошли показатели контрольной группы на 60 %. Они обошли представителей академического сообщества из МТИ и Мичиганского университета на 30 и 70 % соответственно, а также сотрудников разведки, имевших доступ к секретной информации. Среди этих мудрецов Тетлок выявил подгруппу, которую назвал суперпрогнозистами. К концу четырехлетнего турнира выяснилось, что эти суперпрогнозисты превзошли остальных «Мудрых старцев» еще на 60 % и могли видеть дальше, чем представители контрольной группы: «Суперпрогнозисты, заглядывающие на 300 дней вперед, давали более точные предсказания, чем обычные прогнозисты, заглядывающие на 100 дней вперед».

Именно это заставило меня изменить свое мнение. Доктор Тетлок продемонстрировал возможность прогнозирования вероятностей в условиях, когда данных мало, проблемная область сложна, а количество переменных,

которые необходимо учитывать, астрономическое. Прогнозирование рисков кибербезопасности соответствует всем этим критериям, а значит, для расчета киберриска требуются суперпрогнозисты.

Сверхспособности суперпрогнозиста

Суперпрогнозисты не обладают какими-то сверхъестественными способностями. Они, конечно, умны, но не чрезмерно. Это не профессора из комиксов про «Людей Икс», не члены общества «Менса» и не профессиональные математики. При составлении прогнозов большинство из них выполняет лишь элементарные математические расчеты. Однако, следуя нескольким ключевым правилам, они дают прогнозы, превосходящие случайные угадывания, сделанные обычными людьми вроде меня. Вот шесть наиболее эффективных правил.

1. **Прогнозируйте в терминах количественных, а не качественных (высокая, средняя, низкая) вероятностей.** Избавьтесь от тепловых карт. Примите то, что вероятность — это всего лишь мера неопределенности. Используйте реальные числа.

2. **Практикуйтесь.** Делайте множество прогнозов и ведите счет, используя систему Брайера (разработана Гленом В. Брайером в 1950 году). В ее рамках прогноз оценивается по двум осям: «Калибровка» и «Разрешение». Калибровка показывает расстояние от вашего прогноза до линии (она отражает то, насколько вы в нем уверены — чрезмерно или недостаточно). Разрешение отражает фактическое наступление предсказанного события.

3. **Используйте оценки Ферми (прогнозируйте сначала извне внутрь, а затем изнутри наружу).** Оценка по схеме «извне внутрь» сводится к рассмотрению общего случая перед изучением конкретной ситуации. Примером является оценка вероятности реализации существенной кибератаки на любую организацию без анализа защитной архитектуры конкретной потенциальной жертвы. Какова вероятность нанесения существенного ущерба случайной компании? Оценка по схеме «изнутри наружу» предполагает рассмотрение конкретного случая с учетом оборонительной позиции компании. Какова вероятность того, что хакеры причинят существенный ущерб компании, в которой развернута зрелая программа нулевого доверия? Оба подхода имеют свои преимущества, но Тетлок советует сначала делать прогноз по схеме «извне внутрь», а затем корректировать его в сторону увеличения или уменьшения по схеме «из-

нутри наружу». Например, если, согласно вашему прогнозу, сделанному по схеме «извне внутрь», вероятность существенного ущерба от кибератаки в текущем году для всех американских компаний составляет 20 %, то этот показатель является базовым уровнем. Отталкиваясь от него, вы можете изменить прогноз в бóльшую или меньшую сторону, оценив эффективность использования организацией стратегий, базирующихся на первичном принципе кибербезопасности, по схеме «изнутри наружу».

4. **Проверяйте предположения.** Пересматривайте свои предположения, отбрасывайте их, ищите новые данные и формулируйте новые гипотезы, а затем корректируйте прогноз.
5. **Смотрите глазами стрекозы.** Используйте доказательства из разных источников. Создайте на их основе единое представление. Сформулируйте свое суждение как можно более четко, кратко, но при этом максимально детально.
6. **Сформулируйте прогноз с доверительной вероятностью 90 %.** Корректируя свой прогноз, помните, что вы хотите быть на 90 % уверены в том, что он отражает реальность. Это означает, что вы должны быть на 90 % уверены в попадании истинного значения в прогнозируемый диапазон. Если это не так, скорректируйте прогноз в бóльшую или меньшую сторону.

Суть в том, что мы можем спрогнозировать вероятность наступления чрезвычайно сложного события с точностью, достаточной для того, чтобы принять решение. Если «Мудрые старцы» могут точно предсказать будущее сирийского президента, то далекие от математики ИБ-директора вроде меня уж точно смогут предсказать вероятность нанесения организации существенного ущерба в результате киберсобытия с погрешностью, находящейся в разумных пределах. В этом и заключается суть прогнозирования рисков кибербезопасности.

Люди не думают в терминах вероятности, но им следует это делать

Тетлок часто рассказывает о провалах разведки США прошлых лет, обусловленных тем, что правительство не рассуждало в этих терминах.

- **ОМП в Ираке.** Двадцатилетняя война, спровоцированная «стопроцентной» уверенностью ЦРУ в существовании оружия массового поражения в Ираке. Спойлер: на самом деле его там не было.

- **Война во Вьетнаме.** Десятилетняя война на почве широко распространенного мнения, что в случае падения Южного Вьетнама во всех странах мира восторжествует коммунизм. Лидеры не просто считали, что это может произойти, — они были уверены в том, что это неминуемо.
- **Операция в заливе Свиней.** Политическая катастрофа президента Кеннеди, вызванная тем, что планировщики не учли вероятность успеха/неудачи при изменении плана в последнюю минуту.

Скрывается ли Усама бен Ладен в бункере?

Тетлок часто описывает сцену из одного из моих любимейших фильмов «Цель номер один» (2012) с Джессикой Честейн в главной роли. Директор ЦРУ Леон Панетта, которого сыграл великий Джеймс Гандольфини, проводит совещание и просит своих сотрудников ответить на вопрос, находится ли Усама бен Ладен в бункере. Ему нужен ответ «да» или «нет». Один из сотрудников говорит, что после провала, связанного с ОМП в Ираке, они больше ни о чем не могут говорить с уверенностью. Теперь они рассуждают в терминах вероятностей. Это правильный ответ, но не вполне удовлетворительный. В результате дальнейшего обсуждения они получают диапазон вероятностей от 60 до 80 %. Затем к дискуссии подключается героиня Честейн и говорит, что вероятность равна 100 %: «Ладно, хорошо, 95 % — я знаю, что определенность вас пугает. Но на самом деле это 100 %». Кстати, это неправильный ответ. Эта вероятность никогда не была стопроцентной, как бы героиня ни была уверена в своих доказательствах.

Очевидно, что в повседневной жизни мы не рассуждаем в терминах вероятности, даже если умеем это делать. Они нас, как правило, не удовлетворяют. Мы предпочитаем получать ответы типа «да» или «нет». Столкнется ли компания с существенной утечкой данных в этом году? Ответ «да» или «нет» понравится руководителям гораздо больше, чем 15%-ная вероятность. Что им делать с этой 15%-ной вероятностью? Анализ такого ответа потребует от них усилий, размышлений, применения стратегического подхода и проявления гибкости. Кстати, чуть позже в этой главе я расскажу, что именно можно сделать с 15%-ной вероятностью. В то же время ответ «да/нет» — это не более чем условная конструкция наподобие if-then-else, используемой в языках программирования. Если нас могут взломать в этом году, то выделите ресурсы на минимизацию потенциального ущерба, в противном случае потратьте эти деньги на улучшение продукта или увеличение объема продаж. Все просто.

К сожалению, как бы нам ни хотелось жить в фантастическом мире бинарных ответов (да/нет), реальный мир так не работает. В научно-фантастическом романе Нила Стивенсона «Семиевие» персонаж Док Дюбуа объясняет, как он рассчитывает траектории ракет, летящих через район катастрофы: «Это статистическая проблема. В первый же день она перестала быть проблемой ньютоновской механики и превратилась в проблему статистики. И с тех пор она ею и остается» [329]. Именно так. Расчет киберрисков тоже никогда не был вопросом ньютоновской механики. Он всегда имел стохастическую природу, как бы сильно мы ни хотели упростить расчеты, сведя их к использованию легко читаемых тепловых карт. Представители ИБ-сообщества просто не относились к нему как к таковому.

Возможно, пришло время пересмотреть наш способ размышления о вероятностях. Если вы похожи на меня, то ваш опыт изучения статистики, скорее всего, ограничивается учебным курсом «Вероятность и статистика 101», пройденным в колледже. Из него я помню только одну задачу, в которой нужно было рассчитать вероятность того, что следующим из урны, наполненной цветными шариками, будет вынут синий шарик. Это упражнение позволяет познакомиться с концепцией вероятности, но дает крайне ограниченное представление о ней.

Более полезное описание вероятности в контексте кибербезопасности было предложено доктором Роном Ховардом, отцом теории анализа решений (мы с ним не родственники) [109]. Все его исследования основаны на том, что вероятность представляет собой меру неопределенности при принятии решения, а не количество шариков в гипотетической урне.

Вероятность не обязательно относится к данным, а значит, вам не нужно пересчитывать все, чтобы сделать вероятностный прогноз. По его словам, «только человек может присвоить вероятность на основе имеющихся у него данных или других знаний». Подсчет шариков, доставаемых из урны, — это лишь один из способов учета данных, однако великое прозрение Ховарда заключается в том, что «вероятность отражает знание (или незнание) человека о некотором неопределенном различии». Вот что он говорит: «Не думайте о вероятности или неопределенности как об отсутствии знания. Вместо этого думайте о них как об очень подробном описании того, что именно вам известно».

Тетлок взял интервью у настоящего Леона Панетты и расспросил его о том внутреннем совещании ЦРУ и последующей встрече с президентом Обамой, на которой обсуждался вопрос отправки спецназа в Пакистан за Усамой

бен Ладеном. В ходе нее президент тоже получил от сотрудников ряд вероятностей. Однако, изучив их рекомендации, он пришел к выводу, что его сотрудники ничего не знают наверняка. Поэтому вероятность того, что Усама бен Ладен находился в бункере, была оценена как 50/50, что было неправильным выводом. Вероятность была гораздо выше. В конечном итоге он сделал правильный выбор, но с таким же успехом мог бы и не рисковать.

Оценки Ферми являются достаточно хорошими

Итало-американский физик Энрико Ферми был центральной фигурой в изобретении атомной бомбы и прославился своими приблизительными расчетами [35, 275]. Не имея в своем распоряжении практически никакой информации, он часто вычислял некоторое число, которое при последующем измерении оказывалось впечатляюще точным. Известно, что подобные задачи он задавал и своим студентам, например просил их приблизительно определить количество квадратных дюймов пиццы, съедаемой всеми студентами Мэрилендского университета за один семестр, запрещая искать какую-либо информацию и предлагая сначала сделать предположения на глазок. Он понимал, что, разбив большой неразрешимый вопрос (например, о площади съеденной пиццы) на ряд гораздо более простых вопросов, на которые можно ответить (например, о количестве студентов, количестве пиццерий, количестве квадратных дюймов в одном куске пиццы, количестве кусков, съедаемых за день, и т. д.), мы можем гораздо лучше отделить познаваемое от непознаваемого. Удивительно, насколько часто хорошие вероятностные оценки порождаются рядом весьма грубых предположений. Подробнее об этом мы поговорим чуть позже.

Фредерик Мостеллер, выдающийся статистик 1950–1970-х годов, однажды сказал: «По своему опыту статистики знают, что уточнение грубых измерений чаще всего приводит к незначительным изменениям. Статистики могут искренне говорить о том, что измерения нужно проводить более точно, но зачастую они весьма низко оценивают вероятность того, что более точные измерения приведут к существенному изменению политики» [162]. Это означает, что стремление сетевого защитника получить более точные прогнозы рисков неоправданно. Для принятия решений относительно распределения таких ресурсов, как люди, процессы и технологии, вполне достаточно приблизительных оценок.

«Черные лебеди» и устойчивость

Тетлок также говорит о критике своей концепции суперпрогнозирования со стороны его коллеги, Нассима Талеба, автора книги «Черный лебедь. Под знаком непредсказуемости», опубликованной в 2007 году [331]. Талеб утверждает, что прогнозирование невозможно, поскольку историей правит «тирания единичного, случайного, невидимого и непредсказуемого». По словам журналиста газеты New York Times Грега Истербрука, Талеб настаивает на том, что «эксперты — это шарлатаны, верящие в колоколообразные кривые, в которых большинство наблюдений сосредоточено ближе к центру — обычному и познаваемому. Гораздо более мощными являются непредсказуемые результаты фрактальной геометрии, способные в одночасье изменить все». По словам Талеба, «то, что имеет значение, нельзя предсказать, а то, что можно предсказать, не имеет значения. Вера в обратное убаюкивает нас, вселяя ложное чувство безопасности» [71]. Признавая обоснованность этого аргумента, Тетлок говорит: «Черный лебедь — это блестящая метафора для события, которое выходит так далеко за пределы нашего опыта, что мы не способны даже представить его до тех пор, пока оно не произойдет».

Например, если мы выполним приблизительные расчеты (по методу Ферми), то выясним, что в 2021 году Ресурсный центр по борьбе с кражами личных данных (Identity Theft Resource Center) зарегистрировал 1862 утечки, о которых сообщили общественности [80].

Учитывая то, что общественности было доложено не обо всех случаях утечки данных, мы можем округлить эту цифру и предположить, что в 2021 году на американские компании было совершено около 5000 успешных кибератак. Также предположим, что в 2021-м в США насчитывалось около 6 млн коммерческих компаний (чуть позже в этой главе я покажу, как получил это число). Если сделать прогноз по схеме «извне внутрь», то вероятность того, что в 2021 году компания столкнется с утечкой, составляет $5000 / 6\,000\,000 \cong 0{,}0008$ (рис. 6.2). Это очень маленькое число. Позднее я уточню этот прогноз, а пока примите его в качестве исходной оценки вероятности реализации существенной кибератаки на обычную американскую компанию.

По определению, события, с которыми столкнулись эти 5000 компаний, относились к категории «черных лебедей», то есть маловероятно, что они окажут существенное влияние.

5000 успешных киберкампаний в 2021 году

~6 000 000 американских компаний в 2021 году

5000 успешных киберкампаний / 6 000 000 компаний = 0,0008

Вероятность того, что в 2021 году любая из компаний США столкнется с существенным киберинцидентом, составляет 0,0008

Это **практически нулевая** вероятность

Рис. 6.2. Математическая задача № 1: общая оценка Ферми по схеме «извне внутрь»

Ответ Тетлока Талебу заключался в том, что, скорее всего, существует ряд оценочных задач, по которым давать прогнозы слишком сложно, однако это связано в основном со слишком длинным горизонтом прогнозирования. В сфере кибербезопасности сетевому защитнику очень сложно предсказать нанесение организации существенного ущерба в результате киберинцидента в любой момент в будущем, но вы, скорее всего, сможете сделать прогноз, достаточно хороший для принятия решений относительно распределения ресурсов (людей, процессов и технологий), если ограничите горизонт прогнозирования 2–3 годами.

Тем не менее, даже если вы вполне уверены в своем прогнозе, это не значит, что предсказываемое событие обязательно произойдет. Вспомните прогнозы, сделанные некоторыми экспертами относительно президентских выборов в США в 2016 году. Прямо перед началом голосования Нейт Сильвер и команда его веб-проекта FiveThirtyEight спрогнозировали, что вероятность победы Клинтон составляет 71,4 % [203]. Демократы чувствовали себя вполне уверенно. Когда она не победила, многие указали на то, что прогнозы, сделанные на основании опросов, были ошибочными. Однако те, кто их делал, не ошиблись. Основываясь на многих факторах, они полагали, что шанс Клинтон на победу в выборах составлял 70 %. Однако это также означало, что у нее был 30%-ный шанс проиграть, а 30 % — это не пустяк. На самом деле событие, имеющее 30%-ный шанс наступления, является вполне вероятным. Шок, который испытали демократы, еще раз демонстрирует то, что большинство людей, включая некоторых политических обозревателей, не понимают концепцию вероятности.

Решение, предлагаемое Талебом в отношении событий типа «черный лебедь», заключается не в том, чтобы пытаться их предотвратить, а в том,

чтобы постараться их пережить. По его словам, ключом к этому является устойчивость. Например, вместо того, чтобы пытаться предотвратить падение гигантского метеорита на Землю, можно продумать разные способы выживания — возможно, основать колонию на Марсе для спасения человечества. В контексте кибербезопасности это означает, что вместо попытки предотвращения проникновения хакеров Panda Bear в систему организации вам следует позаботиться о том, чтобы она продолжала предоставлять свои услуги во время и после атаки. Это очень похоже на нашу стратегию обеспечения устойчивости, основанную на базовом принципе кибербезопасности (см. главу 5).

К тому же речь не идет о выборе чего-то одного. Вы вполне можете одновременно принимать меры, направленные как на предотвращение негативного события, так и на обеспечение устойчивости.

Изменение мнения

Уже более пяти лет я ищу способ более точной оценки рисков. Я прочитал множество книг, взял интервью у некоторых из их авторов, опубликовал пару статей и даже представил содержащиеся в них тезисы на конференциях по безопасности (на одной из них выступил вместе с Ричардом Сирсеном — автором одной из этих книг).

Когда я только начал заниматься этим вопросом, думал, что главная причина сложности расчета рисков в сфере информационной безопасности заключается в том, что он требует применения изощренной математики, недоступной большинству ИБ-специалистов. Я полагал: для того чтобы убедить высшее руководство в точности моих оценок риска, мне придется продемонстрировать владение такими навыками, как моделирование по методу Монте-Карло и применение байесовских алгоритмов. После этого необходимо будет объяснить, что такое моделирование методом Монте-Карло и алгоритмы Байеса, тем же самым руководителям, которые с трудом понимают, почему мы так много платим за использование брандмауэра. Такой подход казался мне слишком сложным.

За годы изучения этого вопроса я разработал другой способ оценки риска, который заходит достаточно далеко для того, чтобы быть полезным, но не настолько далеко, чтобы казаться слишком эзотерическим и запутанным.

За это время я стал поклонником Ферми и Мостеллера. По словам Нагеша Беллуди, «Ферми считал, что умение угадывать — это навык, необходимый всем физикам» [28]. Я бы сказал, что этот навык может пригодиться любому принимающему решения, особенно тем людям, которые принимают решения в мире технологий и безопасности, масштаб проблем в котором поистине огромен. Процесс получения точной оценки сложный и длительный, однако получить приблизительную оценку, соответствующую верному порядку величины, довольно просто, и этого, скорее всего, достаточно для принятия большинства решений. Даже если окажется, что это не так, вы всегда можете попробовать получить более точную оценку позднее.

К слову, в 2022 году в компании CyberWire, где я работаю в качестве подкастера и руководителя отдела безопасности, была сделана оценка внутренней программы кибербезопасности, основанной на базовом принципе, по схеме «изнутри наружу». Мы оценили свои средства защиты в терминах нулевого доверия, предотвращения реализации убийственной цепочки вторжения, устойчивости и автоматизации. По завершении ознакомили нашего руководителя Питера Килпа со сделанными выводами и сообщили ему свою оценку вероятности существенного ущерба в результате киберсобытия в следующем году. Затем я попросил у него разрешения углубиться в изучение этого вопроса для получения более точного ответа. Его реакция была абсолютно правильной.

Он прикинул, каких затрат и усилий потребует более глубокое погружение, причем не только от команды отдела безопасности, но и от всей компании и особенно от него самого. Откровенно говоря, эти затраты были довольно высоки. Тогда он спросил: «Как вы думаете, какова будет разница между приблизительной и более точной оценкой?» Я сказал, что уточненная оценка, скорее всего, отклонится от приблизительной на пару процентов, но точно не больше чем на десять. Он ответил, что в таком случае ему не требуется более точная оценка для принятия решений относительно будущих инвестиций в обеспечение кибербезопасности CyberWire. Исходная приблизительная оценка была довольно хорошей.

Что и требовалось доказать.

Правило Байеса: еще один способ размышления о рисках кибербезопасности

Доктор Тетлок утверждает (и здесь я с ним согласен), что можно делать прогнозы относительно сложных вопросов, на которые из-за отсутствия исторических данных никто не может ответить с достаточной точностью, и принимать на их основе значимые решения в реальном мире. В частности, я считаю, что мы можем использовать методы суперпрогнозирования для оценки вероятности нанесения нашим организациям существенного ущерба вследствие кибератаки в ближайшие три года.

Методы суперпрогнозирования в целом и приблизительный расчет оценки Ферми по схеме «извне внутрь» в частности — это два столпа прогнозирования рисков кибербезопасности. Третьим столпом является так называемое правило Байеса, которое закладывает математическую основу, позволяющую доказать то, что методы суперпрогнозирования и оценки Ферми работают. Хорошая новость заключается в том, что ИБ-директорам вроде меня не обязательно выполнять сложные математические расчеты для того, чтобы заставить их работать на нас. Достаточно понять концепцию и применять ее при повседневной оценке рисков. Мы можем использовать базовую статистику и экспертные мнения наших сотрудников для получения исходной оценки, а затем изменить этот прогноз в зависимости от того, насколько хорошо организация соблюдает базовые принципы кибербезопасности. Однако прежде, чем показать, как это делается, я должен ознакомить вас с теоремой Байеса.

Теорема Байеса

В 1740-х годах Томас Байес сформулировал собственную интерпретацию концепции вероятности [24]. Однако никто бы не узнал об этой идее, если бы не его лучший друг Ричард Прайс. Хорошо разбиравшийся в науке Прайс нашел неопубликованную рукопись Байеса в ящике стола после его смерти, осознал ее важность, потратил два года на доработку и в 1763 году отправил ее в Лондонское королевское общество для публикации [156].

В своей рукописи Байес (вместе с Прайсом) описывает мысленный эксперимент, иллюстрирующий его гипотезу. Байес просит читателя представить

себе бильярдный стол и двух человек — угадывающего и его помощника. Угадывающий отворачивается от стола, а помощник бьет кием по шару. Задача угадывающего — угадать, в каком месте остановился шар. Взяв лист бумаги и карандаш, он рисует прямоугольник, изображающий поверхность стола. Затем ассистент бьет по второму шару и сообщает угадывающему, с какой стороны от первого шара он остановился — справа или слева. Угадывающий выполняет первоначальную оценку того, с какой стороны стола находится шар. Затем помощник бьет по третьему шару и сообщает угадывающему, с какой стороны от первого шара он остановился. На основании этой информации угадывающий корректирует свою первоначальную оценку. Чем больше шаров использует помощник, тем точнее становится прогноз угадывающего. Он никогда не будет точно знать, где находится шар, но может довольно близко подойти к правильному ответу. Важно то, что качество измерений не меняется. Оно всегда сводится к указанию того, с какой стороны от первого шара остановился очередной шар — справа или слева. Самое главное то, что измерения проводятся многократно. Именно это повышает точность прогноза.

В этом и заключается суть тезиса Байеса. Мы можем сделать первоначальную оценку, какой бы приблизительной она ни была (шар находится где-то на столе), и постепенно собирать новые свидетельства (очередной шар остановился справа или слева от первого), позволяющие корректировать исходную оценку, чтобы приблизиться к верному ответу.

По словам Шэрон Макгрейн, автора книги *The Theory That Would Not Die: How Bayes' Rule Cracked the Enigma Code, Hunted Down Russian Submarines, and Emerged Triumphant from Two Centuries of Controversy*, опубликованной в 2011 году, «обновляя свои первоначальные убеждения с помощью объективной новой информации, мы получаем новое и улучшенное убеждение» [156]. Она утверждает: «Байесовская вероятность представляет собой меру убежденности. А это говорит о том, что мы можем учиться даже на отсутствующих и неадекватных данных, на приблизительных оценках и незнании».

Несмотря на то что Байес был математиком, фактическую формулу вероятности, называемую сегодня теоремой Байеса, разработал не он (рис. 6.3). Это произошло только после того, как Пьер-Симон Лаплас, французский математик, астроном и физик, наиболее известный своими исследованиями устойчивости Солнечной системы и открытием центральной предельной теоремы, в 1774 году самостоятельно пришел к той же идее, что и Байес, и потратил следующие 40 лет на ее математическое обоснование. Сегодня

мы приписываем данную теорему Томасу Байесу, поскольку он был первым, кому в голову пришла эта мысль. Однако нам следовало бы называть ее алгоритмом Байеса — Прайса — Лапласа, так как без участия Прайса и Лапласа о теореме Байеса никто бы никогда не узнал.

Вероятность
Какова вероятность получения свидетельства *(e)* при условии истинности гипотезы *(H)*?

Априорная вероятность
Какова вероятность истинности гипотезы до каких-либо наблюдений?

$$P(H \mid e) = \frac{P(H \mid e)P(H)}{P(e)}$$

Апостериорная вероятность
Какова вероятность истинности гипотезы с учетом полученных свидетельств? (Не поддается прямому вычислению)

Безусловная вероятность
Какова вероятность получения нового свидетельства при всех возможных гипотезах?
$P(e) = \sum P(e \mid H_1)P(H_1)$

Рис. 6.3. Теорема Байеса [3]

Пьер-Симон Лаплас разработал также преобразование, которое легло в основу теории управления [210]. Именно оно обеспечивает работоспособность математики и программного обеспечения, управляющего масштабными физическими процессами. Сегодня оно используется на большинстве промышленных объектов. Таким образом, можно утверждать, что Лаплас тоже является отцом-основателем промышленных систем управления и операционных технологий, составляющих еще одну важнейшую область кибербезопасности.

Априорной вероятностью современные ученые-байесисты называют первоначальную оценку (положение шара на столе). *Вероятность* обозначает вероятность получения нового свидетельства (положение одного шара относительно другого), а *апостериорная* вероятность — новую оценку, полученную в результате объединения первоначальной оценки и вероятности. По словам Макгрейн, «каждый раз при пересчете системы апостериорная вероятность становится априорной вероятностью для новой итерации».

Это весьма элегантная идея, однако научное сообщество решительно отвергло тезис Байеса, после того как Королевское общество опубликовало

его рукопись. Не стоит забывать, что в то время наука отходила от религиозных догм как способа описания мира. Новые ученые-статистики, которых называли частотниками (сторонниками частотного подхода к вероятностям), основывали все свои выводы на наблюдаемых фактах. Им приходилось подсчитывать такие вещи, как количество карт в колоде, прежде чем они могли с уверенностью предсказать вероятность выпадения туза. Мысль о том, что приблизительные оценки Байеса могут быть названы научными в отсутствие наблюдаемых фактов, была предана анафеме, и ведущие статистики атаковали ее при каждом удобном случае на протяжении следующих 150 лет.

По их мнению, современная наука требовала объективности и знания прошлого. Как пишут Хаббард и Сирсен в книге «Как оценить риски в кибербезопасности», в 1749 году Готфрид Ахенвалль ввел в употребление слово «статистика», производное от латинского слова *statisticum*, что означает «относящийся к государству». Понятие «статистика» буквально означало количественное изучение государства. По словам Макгрейн, частотники считали, что безумная байесовская философия требует «...веры и приближений. Это необузданный субъективизм, невежество, называемое наукой».

Однако в реальном мире существуют проблемы, для решения которых невозможно собрать достаточно данных. Руководители беспокоятся о потенциальных событиях, которые никогда не происходили, но могут произойти (например, атака вымогателей). Философия Байеса предоставила возможность давать приблизительные ответы, которые могли бы оказаться полезными в реальном мире. И статистики-аутсайдеры начали экспериментировать с этим методом, пытаясь получить реальные результаты.

Удивительно, но спустя 280 лет теорема Байеса по-прежнему вызывает претензии со стороны научного сообщества. Похоже, в некоторых кругах до сих пор бытует мнение, что человек может быть либо частотником, либо байесистом. Это прискорбно, так как, подобно математическим началам Евклида, теорема Байеса верна, потому что она работает. Я прагматик, твердо убежденный в том, что нам следует использовать те инструменты, которые лучше всего подходят для решения конкретной задачи. Если это инструменты частотников, мы должны применять их. А если лучше подходят байесовские инструменты, то их. Самое замечательное в теореме Байеса заключается в том, что вы можете задействовать и то и другое. К настоящему моменту байесовский набор математических инструментов продемонстрировал так

много примеров решения реальных проблем, что сомнения в нем кажутся абсурдными. Что касается инструментов частотников, то они не очень помогли в прогнозировании рисков кибербезопасности. Я выступаю за то, чтобы ИБ-сообщество опробовало новый набор инструментов. Пришло время освоить байесовский подход.

Использование байесовского подхода для победы над немцами во Второй мировой войне

Я уже упоминал о книге Макгрейн *The Theory That Would Not Die*. В ней изложена захватывающая история эволюции теории Байеса от создания до наших дней, показаны ее успехи и неудачи, а также порожденная ею многолетняя вражда между математиками. Я очень рекомендую прочитать ее, если эта тема вас заинтриговала, а она должна заинтриговать. Если хотите ознакомиться с кратким содержанием этой книги, послушайте выступление Макгрейн, записанное для Google Talk в 2011 году [156]. В своей книге она описывает более 20 примеров успешного применения теоремы Байеса для решения сложных проблем. Из них мне больше всего нравится история применения этой теоремы Аланом Тьюрингом для взлома немецкой шифровальной машины «Энигма» во время Второй мировой войны.

Тьюринг — мой любимый герой из мира компьютерных наук. За свою короткую трагическую жизнь он сделал множество впечатляющих вещей. Он математически доказал возможность создания компьютеров (с помощью машины Тьюринга) в 1930-х годах, то есть за десять лет до их фактического изобретения [305]. Сегодня все компьютеры, которыми мы пользуемся, начиная со смартфона и ноутбука и заканчивая облачными рабочими нагрузками, представляют собой машины Тьюринга. В 1950 году он опубликовал первый тест для определения искусственного интеллекта (тест Тьюринга), по поводу которого лидеры в этой области спорят до сих пор [306]. А его шестилетняя работа в Блетчли-парк по расшифровке немецких сообщений, зашифрованных с помощью машины «Энигма», по мнению некоторых историков, позволила спасти 20 млн жизней и сократила продолжительность Второй мировой войны на четыре года [57]. И для этого он использовал гипотезу Байеса [156].

До войны, во время и после нее существовало множество версий машины «Энигма», но в целом шифровальный механизм состоял из четырех механических частей (рис. 6.4).

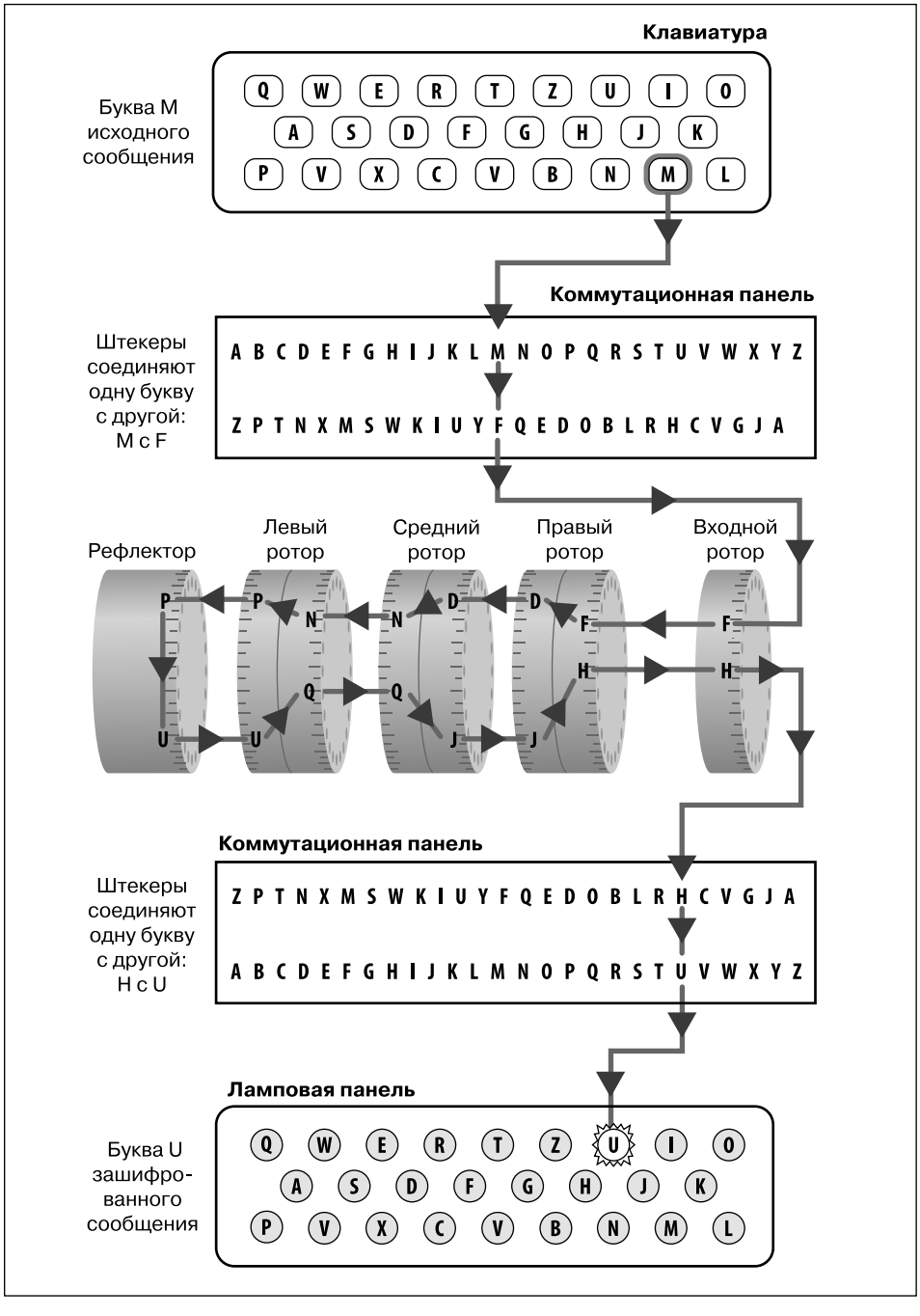


Рис. 6.4. Принцип работы машины «Энигма» [100]

Клавиатура. Шифровальщики набирали исходное сообщение на устройстве, напоминающем печатную машинку. Когда они нажимали клавишу с буквой открытого текста, загоралась лампочка, соответствующая преобразованной букве. Именно эта буква записывалась в зашифрованное сообщение, предназначенное для последующей передачи по радио с помощью азбуки Морзе.

Коммутационная панель. Используя 26 гнезд (по одному на каждую букву алфавита), шифровальщики преобразовывали одну букву в другую (например, F в Z), соединяя соответствующие гнезда с помощью штекеров. Таким образом, значения менялись местами. Если шифровальщик нажимал клавишу F, через систему проходила буква Z.

Роторы. Каждый ротор представлял собой кольцо с уникальным расположением 26 букв и предусматривал начальную позицию, которую шифровальщики регулярно меняли. Машина с трехроторной системой поставлялась с пятью роторами на выбор. Каждый ротор выполняет простую операцию подстановки. Например, контакт, соответствующий букве R, может быть подключен к контакту, соответствующему букве T. Когда шифровальщик нажимал клавишу, правый ротор сдвигался вперед на одну букву. Благодаря этому даже при повторном вводе одной и той же буквы зашифрованные буквы оказывались разными. После 26 смещений правого ротора средний ротор сдвигался на следующую букву. После 26 смещений среднего ротора левый ротор сдвигался на следующую букву. В результате шифровальщики могли использовать более 17 000 уникальных комбинаций, прежде чем они начинали повторяться.

Рефлектор. После прохождения через коммутационную панель и три ротора сигнал попадал в рефлектор (отражатель), который перенаправлял его обратно через роторы, но на этот раз слева направо. Затем сигнал снова проходил через коммутационную панель и наконец попадал на клавиатуру, после чего загоралась лампочка, соответствующая зашифрованной букве.

В общей сложности каждая буква проходила через восемь этапов преобразования: коммутационная панель, три ротора справа налево, три ротора слева направо и снова коммутационная панель. Благодаря такой системе количество способов, с помощью которых немцы могли зашифровать сообщение, составляло почти 159 квинтиллионов (это 159 и десять нулей).

По словам Макгрейн, при содействии математика Гордона Уэлшмана и инженера Гарольда «Дока» Кина Тьюринг разработал высокоскоростную электромеханическую машину для проверки всех возможных вариантов расположения роторов в «Энигме» и назвал ее «Бомба». Это радикальное

байесовское устройство «проверяло догадки, 15-буквенные фрагменты, предположительно, содержавшиеся в исходном сообщении». Поскольку отбросить возможные варианты можно быстрее, чем найти точное соответствие, «Бомба» Тьюринга одновременно проверяла комбинации роторов, которые не соответствовали угаданному фрагменту. Он также изобрел ручную байесовскую технику под названием «Банбурисмус», которая «помогала ему угадывать последовательность букв в сообщении, зашифрованном с помощью "Энигмы", хеджировать свои ставки, измерять степень уверенности в истинности своих предположений, используя методы Байеса для оценки их вероятности, и учитывать новые подсказки по мере их поступления». Эта система позволяла «определить положение двух из трех роторов "Энигмы" и сократить число их настроек, подлежащих проверке с помощью "Бомбы", с 336 до 18».

Взлом кодов «Энигмы» требовал оперативных действий. Немцы регулярно меняли ее настройки (конфигурации коммутационной панели и роторов) — чаще всего раз в день, но иногда каждые восемь часов. Тьюрингу требовался способ измерения своих предположений, полученных в результате применения техники «Банбурисмус». Он придумал единицу измерения бан (сокращение от «Банбурисмус»), которая, по словам Ирвинга Джона (Джека) Гуда (одного из ближайших соратников Тьюринга в Блетчли-парк), «выражала наименьший вес доказательства, воспринимаемый интуицией». Макгрейн описывает это так: «Один бан означал вероятность 10 к 1 в пользу истинности догадки, однако Тьюринг обычно имел дело с гораздо меньшими величинами — децибанами и даже сантибанами». Когда совокупное количество банов давало шансы 50 к 1, криптоаналитики были почти уверены в правильности своих 15-буквенных фрагментов. По словам Макгрейн, «каждый дополнительный бан делал истинность гипотезы в десять раз более вероятной». Как уже говорилось, Тьюринг искал способы, позволяющие быстро отбросить неверные догадки, а не найти точный ответ. Когда шансы достигали 50 к 1, он мог остановить процесс.

Если вы думаете, что баны Тьюринга очень похожи на биты Клода Шеннона, вы правы. Шеннон опубликовал новаторскую работу *A Mathematical Theory of Communication* в 1948 году и, согласно научному сайту HRF, «определил мельчайшие единицы информации, не поддающиеся дальнейшему делению. Эти единицы называются *битами* или двоичными цифрами. С помощью строк битов можно закодировать любое сообщение. Цифровое кодирование основано на использовании битов и предусматривает всего два значения: 0 или 1» [200, 224]. Шеннон также ввел понятие информационной энтро-

пии. Как пишет Джейн Стюарт Адамс в потрясающем эссе *The Ban and the Bit: Alan Turing, Claude Shannon, and the Entropy Measure*, информация содержится не в самих битах, а в степени их неупорядоченности в момент поступления [5].

По словам Джеймса Глика, автора книги «Информация. История. Теория. Поток», бит Шеннона «стал точкой опоры, вокруг которой начал вращаться мир... Бит присоединился к дюйму, фунту, кварте и минуте в качестве определенной величины — фундаментальной единицы измерения. Но единицы измерения чего? “Единицы измерения информации”, — писал Шеннон, как будто существует такая поддающаяся измерению и количественной оценке вещь, как информация» [322].

Согласно Гуду, Тьюринг самостоятельно сформулировал идею банов в 1941 году, за семь лет до публикации статьи Шеннона [88]. Интересно то, что в 1943-м Тьюринг на протяжении нескольких дней общался с Шенноном в США [224]. Обсуждали ли они баны и биты в ходе своей встречи? Возможно ли, что Тьюринг натолкнул Шеннона на эту идею? Шеннон категорически это отрицает, и я ему верю. Тьюринг был связан британским законом о государственной тайне. Лишь немногие союзники знали, что происходило в то время в Блетчли-парк. Тьюринг был одним из них, но он никогда не говорил об «Энигме» за пределами этих кругов, даже когда его арестовали и угрожали тюремным заключением. Однако это странное совпадение заставляет задуматься.

В самый разгар войны шифровальный центр в Блетчли-парк представлял собой настоящую фабрику по взлому кодов, где в каждый момент времени работали до 200 «Бомб», которыми управляли около 9000 аналитиков. Благодаря Тьюрингу и шифровальщикам из Блетчли-парк лидеры стран-союзников в большинстве случаев могли ознакомиться с приказами Гитлера раньше, чем немецкие командиры на местах. Жизненная трагедия Тьюринга была обусловлена двумя фактами. Во-первых, он был геем, что в те времена в Великобритании считалось противозаконным, а во-вторых, британцы требовали соблюдения режима секретности в отношении своих возможностей по взлому кодов. Многие сотрудники центра в Блетчли-парк сошли в могилу, так и не рассказав своим семьям о том, чем занимались во время войны. После ее окончания премьер-министр Великобритании Уинстон Черчилль приказал уничтожить все «Бомбы», оставив лишь несколько, чтобы сохранить эту технологию в секрете. Впоследствии оставшиеся «Бомбы» и их преемники, такие как компьютер «Колосс», использовались для шпионажа за русскими, и Черчилль не хотел, чтобы кто-то об этом узнал.

Деятельность, связанная со взломом кодов, была настолько засекреченной, что после войны никто за пределами небольшого закрытого сообщества шифровальщиков не знал, кто такой Тьюринг, чего он добился, а также того, что теорема Байеса является хорошим методом криптоанализа.

Я узнал о Тьюринге в начале 2000-х годов, прочитав роман Нила Стивенсона «Криптономикон» [328]. И с тех пор по кусочкам восстанавливал историю его жизни. Я перечитывал ее много раз, с трудом принимая весь ее трагизм. Один из величайших умов человечества, один из самых блестящих математиков, человек, практически в одиночку спасший 20 млн жизней, был уничтожен в расцвете сил в возрасте 42 лет. Он умер в полном одиночестве, и никто не знал, кем он был на самом деле, в то время, когда это имело наибольшее значение. От этого я буквально впадаю в ярость. И у меня голова идет кругом от одной мысли о том, что все могло быть иначе. Что бы сделал Тьюринг с искусственным интеллектом, если бы после войны его оставили в покое? Какие компьютеры он помог бы создать? Что бы они с Шенноном могли сделать для развития теории информации? Какого прогресса мы могли бы добиться в использовании теоремы Байеса?

Применение теоремы Байеса для прогнозирования рисков кибербезопасности

Как я уже говорил, теорема Байеса — это один из столпов прогнозирования рисков наряду с некоторыми методами суперпрогнозирования и оценками Ферми. Мысль о том, что мы можем приблизительно оценить риск на основе единственной обоснованной догадки (положения первого бильярдного шара), а затем по мере поступления новой информации (появления новых шаров на столе) постепенно уточнять оценку, поистине гениальна. Чтобы оценить риск, вам не нужно собирать данные за несколько лет и подсчитывать все на свете. А самое главное заключается в том, что эта отличная идея подкреплена 250-летней эволюцией математики, вклад в которую внесли многие люди, начиная с Томаса Байеса и Пьера-Симона Лапласа и заканчивая Аланом Тьюрингом и Биллом Гейтсом.

Я потратил много лет на поиски способа, позволяющего рассчитать киберриск для своей организации с точностью, достаточной для принятия правильных решений. Методы суперпрогнозирования, оценки Ферми и теорема Байеса указали мне путь вперед. В следующем разделе я покажу, как это делается, и на конкретном примере продемонстрирую способ вычисления априорной вероятности с помощью оценок Ферми для прогнозирования киберриска.

Практический пример прогнозирования рисков с помощью теоремы Байеса

Чтобы вычислить исходную оценку вероятности нанесения нашей организации существенного ущерба в этом году, мы должны определить вероятность того, что любая из компаний подвергнется существенной кибератаке. Это будет первой оценкой Ферми. В ходе дальнейшего анализа я буду ограничиваться американскими организациями, поскольку об этих компаниях мы имеем гораздо больше сведений, чем о компаниях из других стран мира. Ответы, полученные на основе этих данных, можно использовать для экстраполяции. Но даже в этом случае придется следить как за неопровержимыми фактами, так и за предположениями. Начнем с отчета ФБР о преступлениях в Интернете за 2021 год [248].

Согласно данному отчету, в 2021 году в центр ФБР по сбору жалоб на преступления в Интернете (Internet Crime Complaint Center, IC3) поступило чуть менее миллиона жалоб (847 376). Предположим, что все они сопряжены с существенным ущербом. Скорее всего, это не так, но это будет исходным предположением. По оценкам центра IC3, лишь 15 % организаций сообщают о подобных инцидентах. Сколько же жалоб должно было быть подано? Согласно расчетам, представленным на рис. 6.5, в 2021-м более 5,5 млн (5 649 173) американских организаций должны были подать жалобу в IC3.

Предположения	**Математическая задача № 2**	**Факты**
Все 847 376 инцидентов сопряжены с существенным ущербом	x = количество жалоб, которое должно было быть подано в 2021 году, по оценке IC3	847 376 жалоб получено центром IC3 в 2021 году
IC3: 15 % организаций сообщают об атаках	$\frac{15}{100} = \frac{847\,376}{x}$	

$$x = 100 \times \frac{847\,376}{15}$$

$$x = 5\,649\,173$$

Рис. 6.5. Математическая задача № 2: количество жалоб, которое должно было быть подано в 2021 году, по оценке IC3

Я предполагаю, что существует множество причин, по которым организации не сообщают о киберинцидентах в ФБР, и главная из них может заключаться в том, что инцидент не причинил существенного ущерба. В качестве консервативной оценки предположим, что только 25 % потенциальных инцидентов, о которых не сообщили, были сопряжены с существенным ущербом. Вероятно, их реальное количество гораздо меньше, но на данный момент эта оценка нас вполне устраивает (рис. 6.6).

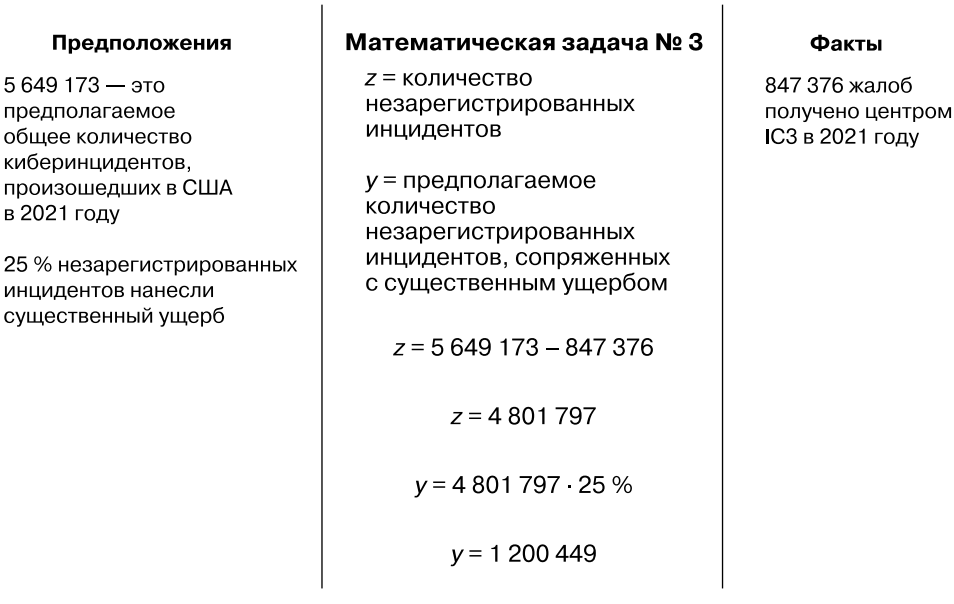


Рис. 6.6. Математическая задача № 3: количество незарегистрированных существенных киберинцидентов, произошедших в 2021 году, по оценке IC3

Количество незарегистрированных инцидентов равно разности между общим числом инцидентов, которые, по оценкам центра IC3, должны были произойти в 2021 году (5 649 173), и числом поданных жалоб (847 376). Таким образом, их количество немного превышает 4,5 млн (z = 4 801 797).

Я предположил, что из 4 801 747 незарегистрированных инцидентов только 25 % были сопряжены с существенным ущербом, что составляет примерно 1,2 млн (y = 1 200 449).

Таким образом, общее количество инцидентов, нанесших существенный ущерб, равно сумме числа жалоб, поступивших в центр IC3 (847 376),

и предполагаемого числа незарегистрированных существенных инцидентов (1 200 449), что составляет чуть более 2 млн (2 047 825) (рис. 6.7).

Предположения	Математическая задача № 4	Факты
Все 847 376 инцидентов сопряжены с существенным ущербом 1 200 449 — это количество незарегистрированных существенных инцидентов	x = предполагаемое общее количество существенных инцидентов $x = 847\,376 + 1\,200\,449$ $x = 2\,047\,825$	847 376 жалоб получено центром IC3 в 2021 году

Рис. 6.7. Математическая задача № 4: предполагаемое общее количество существенных инцидентов, произошедших в 2021 году

Другими словами, по оценкам центра IC3, количество существенных кибер-событий, произошедших в США в 2021 году, составляет чуть более 2 млн (2 047 825). Запомните это число.

Я также предполагаю, что ни одна из организаций не подвергается кибер-атаке дважды за один и тот же год. Скорее всего, это не так, но пока будем придерживаться данного предположения. Допустим также, что все атаки, реализованные различными государствами и нанесшие существенный ущерб, будут включены в статистику центра IC3.

Теперь возникает вопрос: сколько американских организаций могут подать жалобу в центр IC3? Чтобы ответить на него, нужно выяснить количество существующих частных компаний, учебных заведений и государственных учреждений. Согласно данным Бюро переписи населения США, в 2019 году в Соединенных Штатах было зарегистрировано 6,1 млн (6 102 412) компаний [253]. Численность сотрудников в них варьируется от 5 до более чем 500 человек. Пока будем считать, что численность сотрудников не имеет значения для нашего прогноза. Мы знаем, что это, скорее всего, тоже не так, но будем придерживаться данного предположения до тех пор, пока полученные нами сведения его не опровергнут. Также допустим, что в это число входят неправительственные организации (НПО).

По данным Национального центра статистики в области образования, в 2020 году в стране насчитывалась 128 961 школа, включая государственные

и частные дошкольные образовательные учреждения, начальные, средние школы, учреждения послешкольного образования и прочие типы школ [235]. Послешкольное образование представляет собой сочетание четырехлетних и двухлетних программ с разным количеством учащихся. В начальных школах численность учеников тоже варьируется. Мы также допустим, что численность учащихся не имеет значения для нашего прогноза.

Интересно то, что нам неизвестно официальное количество федеральных правительственных организаций. По словам Клайда Уэйна Крюса из журнала Forbes, в 2021 году не существовало никакого официального, авторитетного списка, составляемого какой-либо из этих организаций [58]. Ни одной федеральной правительственной структуре США официально не поручено отслеживать количество остальных федеральных агентств. Я знаю, что это звучит безумно, но, по-видимому, так оно и есть. Крюс перечисляет восемь различных документов, начиная с отчета Административной конференции США и заканчивая списком агентств Федерального реестра, в которых количество правительственных агентств варьируется от 61 до 443 в зависимости от используемого метода подсчета. Давайте возьмем в качестве исходной точки среднее значение — 252.

Наконец, по данным Бюро переписи населения США, в 2017 году в Соединенных Штатах насчитывалось 90 126 местных органов власти [239]. Предположим, что размер местных органов власти также не имеет значения для прогноза.

Итак, в США насчитывается:

- 6 102 412 зарегистрированных компаний;
- 128 961 школа;
- 252 федеральных государственных учреждения;
- 90 126 местных органов власти уровня штата, города, округа и т. д.;
- итого 6 321 751 организация.

Каждая из этих организаций может сообщить о существенном киберинциденте в центр IC3. Учитывая предположение о том, что в 2021 году 2 047 825 организаций должны были подать жалобу в IC3, первая априорная вероятность того, что любая из американских организаций могла подвергнуться существенной кибератаке в том году, составляет примерно 32 % — 2 млн жалоб, деленные на 6,3 млн организаций (рис. 6.8).

Предположения	Математическая задача № 5	Факты
2 047 825 жалоб о существенных инцидентах должно было быть подано в IC3 в 2021 году В США насчитывается 6 321 751 организация	Первая априорная вероятность $= \frac{2\,047\,825}{6\,321\,751}$ Первая априорная вероятность $= 32\,\%$	Недоступны

Рис. 6.8. Математическая задача № 5: первая априорная вероятность того, что любая из американских организаций могла подвергнуться существенной кибератаке в 2021 году

Однако, прежде чем официально назвать это байесовской априорной вероятностью, проверим свои допущения.

- Все 847 376 инцидентов, зарегистрированных центром IC3, были сопряжены с существенным ущербом.
- Только 25 % инцидентов, не зарегистрированных центром IC3, оказались существенными.
- Все атаки, реализованные разными государствами и нанесшие существенный ущерб, включены в статистику центра IC3.
- Ни одна компания не подвергается кибератаке более одного раза за год.
- Количество учащихся или сотрудников организации не имеет значения для прогноза.
- В общее число компаний, перечисленных Бюро переписи населения США, входят НПО.
- Среднее количество федеральных организаций (252), взятое из восьми различных отчетов, довольно близко к фактическому значению.

Это весьма существенные допущения. Однако для получения первой априорной байесовской вероятности они вполне годятся. На данном этапе мы ударяем по бильярдному шару и делаем первое предположение о том, где он остановился. Согласно оценке Ферми, сделанной по схеме «извне внутрь» (метод, применяемый суперпрогнозистами и описанный в книге доктора Тетлока), вероятность того, что в результате киберинцидента будет нанесен существенный ущерб, в 2021 году для любой американской организации составляла 32 %.

Иными словами, если экстраполировать эту оценку, то для любой американской организации вероятность столкнуться с существенным киберсобытием составляет 1:3 в каждом конкретном году.

Минутку, а что насчет меня?

Увидев цифру 32 %, вы, скорее всего, скажете себе: «Все это замечательно, но я работаю в небольшом стартапе, производящем бетон. Не может быть, что для моей компании существует 32%-ная вероятность столкнуться с существенным киберинцидентом в этом году. Эта вероятность должна быть гораздо ниже». Или: «Я работаю в компании из списка Fortune 1000. Не может быть, чтобы эта вероятность составляла всего 32%. Она должна быть гораздо выше. Эта 32%-ная вероятность не имеет для меня никакого значения. Она ничем мне не поможет».

Однако помните, что первая априорная вероятность аналогична попытке предсказания места остановки бильярдного шара после того, как наш ассистент ударил по нему кием. Теперь нужно проверить свои предположения и выполнить дополнительные измерения. Поэтому мы будем искать новые свидетельства и корректировать 32 %-ный прогноз в бóльшую или меньшую сторону в зависимости от того, что обнаружим. Например, если выяснится, что количество не зарегистрированных центром IC3 существенных киберсобытий ближе к 10, чем к 25 %, скорректируем эту вероятность в меньшую сторону. А если обнаружим, что реальное число федеральных организаций составляет 80, а не 252 (среднее число, которое мы использовали), то скорректируем вероятность в бóльшую сторону. Подобно суперпрогнозистам Тетлока, мы должны постоянно следить за своими предположениями и быть готовыми скорректировать их при появлении новых данных.

На следующем этапе мы будем собирать новые свидетельства, то есть бить по дополнительным бильярдным шарам. В этом нам помогут два исследовательских отчета, опубликованных Институтом Cyentia:

- *Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents* [241];
- *IRIS Risk Retina — Data for Cyber Risk Quantification* [249].

Они лучше всего соответствуют моим соображениям по поводу суперпрогнозистов, байесовской философии и оценок Ферми. Первый отчет Инсти-

тут Cyentia подготовил в сотрудничестве с компанией Advizen (дочерняя компания Zywave), которая предоставила набор данных о кибератаках на компании из списка Fortune 1000 за последнее десятилетие. Я очень доверяю этому набору данных, поскольку все компании из списка Fortune 1000 хорошо известны и по причинам, связанным с соблюдением нормативных требований, их отчетность об утечках данных вполне надежна.

Первый факт, важный для нашего исследования, заключается в том, что за последние пять лет с существенным киберсобытием ежегодно сталкивалось чуть менее одной из четырех компаний из списка Fortune 1000. Это число немного ниже нашей первой априорной вероятности, которая составляла 1:3. Однако Институт Cyentia проанализировал эту вероятность также для компаний, относящихся к разным квартилям, то есть для первых 250 компаний, затем для следующих 250 и т. д. Оказалось, что если ваша компания входит в первый квартиль, то вероятность существенной утечки данных для нее в пять раз превышает аналогичную вероятность для компаний из четвертого квартиля. Согласно данному отчету, вероятность столкнуться с таким киберинцидентом для этих компаний составляет:

- Fortune 250 — 1:2;
- Fortune 251–500 —1:3;
- Fortune 501–750 — 1:5;
- Fortune 751–1000 — 1:10.

Аналогичный анализ был проведен для расчета вероятности того, что компания из списка Fortune 1000 подвергнется нескольким атакам за один и тот же год. Это соответствует одному из наших байесовских предположений. Итак, вероятность этого составляет:

- Fortune 250 — 1:3;
- Fortune 251–500 — 1:7;
- Fortune 501–750 — 1:12;
- Fortune 751–1000 — 1:24.

Последнее, на что следует обратить внимание в данном отчете, — это расчет вероятностей нанесения разных убытков. В нем приведен график — кривая вероятности превышения убытков (рис. 6.9), которая, по словам Брайана Смита из Fair Institute, «...представляет собой способ визуализации

вероятности того, что убытки превысят определенную сумму... По оси *X* откладывается величина годовых убытков для анализируемого сценария. По оси *Y* откладывается процентная вероятность того, что сумма убытков превысит показатель, соответствующий точке пересечения с осью *X*». Это означает, что для разных значений убытков существуют разные вероятности. Согласно отчету Института Cyentia:

- вероятность каких-либо убытков составляет 25 %;
- вероятность того, что убытки превысят 10 млн долларов, — 14 %;
- вероятность того, что убытки превысят 100 млн долларов, — 6 %.

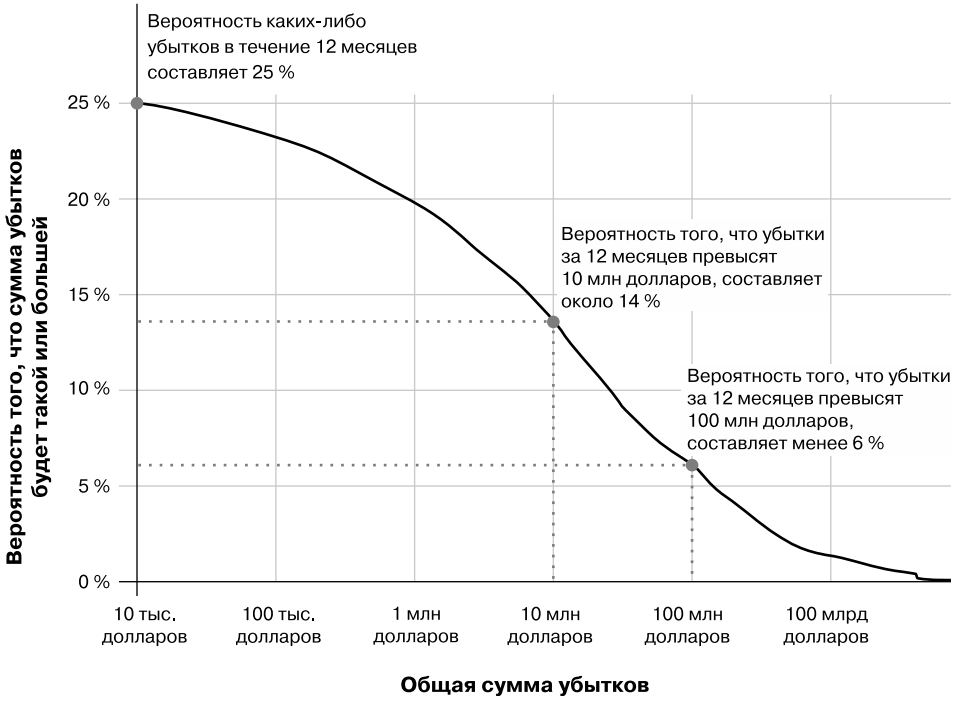


Рис. 6.9. Пример кривой вероятности превышения убытков [249]

Это важно с точки зрения терпимости к риску. Для некоторых компаний из списка Fortune 1000 14%-ная вероятность потери 10 млн долларов — вполне приемлемый риск. Для других же он может оказаться слишком большим по сравнению с остальными рисками, которых руководство пытается избе-

жать. Кривые вероятности превышения убытков позволяют руководителям сделать выбор. Использование тепловых карт с такими качественными значениями, как высокий, средний и низкий риск, не позволяет оценить, находится ли этот риск в пределах допустимого диапазона, тогда как кривые вероятности превышения убытков дают визуальное представление о том, каков допустимый уровень (см. рис. 6.9).

Затем Институт Cyentia объединил три набора данных, полученных от Advizen, Dun & Bradstreet и Бюро переписи населения США, чтобы получить информацию о кибератаках, с которыми столкнулись все американские компании, а не только входящие в список Fortune 1000. В своем отчете Cyentia признает, что по сравнению с набором данных о компаниях из Fortune 1000 этот набор данных не столь надежен, но утверждает, что он лучший из имеющихся. В этом отчете есть раздел, где прогнозируется вероятность существенной утечки данных для каждого коммерческого сектора (строительство, сельское хозяйство, торговля и т. д.). Авторы пришли к выводу, что вероятность столкнуться с существенной утечкой в этом году для любой компании независимо от сектора составляет менее чем 1:100, но с некоторыми оговорками. В ходе переписки по электронной почте Уэйд Бейкер, соучредитель Института Cyentia, сообщил: «Тот факт, что каждый сектор в основном состоит из небольших компаний, значительно снижает типичную вероятность».

Разница между прогнозом Cyentia в 1 % и моим прогнозом в 32 %, основанным на данных центра IC3, довольно велика. Однако, по словам Уэйда, точность прогноза зависит не от сектора, а от размера организации. В их отчете показан довольно большой разрыв в значениях вероятности для компаний, имеющих разный уровень доходов:

- годовая выручка менее 1 млрд долларов (большинство организаций) — менее 2 %;
- от 1 млрд до 10 млрд долларов — 9,6 %;
- от 10 млрд до 100 млрд долларов — 22,6 %;
- более 100 млрд долларов — 75 %.

Авторы отчета также отмечают, что крупные организации сообщат о взломе с вероятностью в 1000 большей, чем небольшие компании с годовой выручкой менее 10 млн долларов, что также смещает данный показатель.

Как учитывать новые данные

Теперь возникает вопрос: как включить эти данные в свой прогноз? Как использовать априорную вероятность в 32 % с этим отчетом? Прежде всего, если вы работаете в компании, входящей в список Fortune 1000, я бы рекомендовал вам не обращать внимания на прогноз, сделанный мною на основе данных ФБР. Отчет Института Cyentia по компаниям из списка Fortune 1000 гораздо точнее отражает ситуацию для этой группы, а надежность этого набора данных позволяет мне с уверенностью говорить о том, что прогнозы для компаний из списка Fortune 1000 более точные по сравнению с моим общим прогнозом для всех компаний. Кроме того, второй упомянутый мною отчет, *IRIS Risk Retina — Data for Cyber Risk Quantification*, посвящен исключительно некоммерческим организациям. Если бы я работал в такой организации, то использовал бы именно этот отчет для определения априорной вероятности.

Но что, если вы работаете не в компании из списка Fortune 1000 и не в некоммерческой организации, а, скажем, в Marvel Studios? Как вам учесть новые данные о размере выручки в своем прогнозе? Если бы мы хотели подставить эти сведения в алгоритм Байеса и выполнить расчеты, то могли бы это сделать. Но мы используем оценки Ферми, которых, скорее всего, будет достаточно.

По данным Zippia — компании, отслеживающей аналитические данные о компаниях, выручка Marvel Studios в 2021 году составила почти 116 млн долларов (115,7 млн) [251]. Таким образом, Marvel Studios, как и большинство организаций, относится к категории компаний с годовой выручкой менее 1 млрд долларов. По данным Института Cyentia, вероятность столкнуться с существенной утечкой данных для компаний такого типа составляет менее чем 2:100. Это сильно отличается от моего прогноза в 32 %, сделанного на основе данных центра IC3.

Учитывая это, должны ли мы уменьшить или увеличить априорную вероятность? Поскольку прогнозное значение Cyentia более низкое по сравнению с моим прогнозом, сделанным на основе данных центра IC3, логично было бы ее уменьшить. Но на сколько? Хотите ли вы понизить прогноз до 2 %? Если считаете, что отчет Института Cyentia по надежности сильно превосходит данные IC3, как было в случае с компаниями из списка Fortune 1000 или с некоммерческими организациями, можете это сделать. Однако в своем отчете авторы этого анализа говорят о том, что их данные не столь же на-

дежны, как данные о компаниях из списка Fortune 1000. А я вполне уверен в своем прогнозе, сделанном на основе информации центра IC3.

Помните о том, что вероятность Байеса — это мера вашей собственной уверенности. Таким образом, для меня лично этот прогноз не является полным и достаточным, поэтому я бы скорректировал априорную вероятность, основанную на данных IC3, скажем, до 15 % и приступил к поискам дополнительных доказательств в поддержку этого изменения.

Один из приемов, используемых суперпрогнозистами Тетлока при внесении подобных корректировок, заключается в оценке степени собственной уверенности в потенциальном изменении. Они хотят быть уверены в правильности корректировки не на 100 %, а примерно на 95. Я знаю, что все это довольно абстрактно. Как можно быть уверенным в чем-то на 95 %? Как можно оценить разницу между 95 и 85 %? Лично я не знаю, как это сделать. Один из приемов, используемых суперпрогнозистами, заключается в том, чтобы сделать ставку, то есть спросить себя: готов ли ты поставить 100 долларов на то, что предполагаемая корректировка верна? Ставка подразумевает определенный риск и обязательства. Заключая пари, вы можете быть уверены в чем-то, но не на 100 %. Так что, если вы настолько уверены в своей корректировке, что готовы поставить на нее 100 долларов, это можно назвать 95%-ной уверенностью. Если не настолько уверены, скорректируйте свой прогноз на пару пунктов. Например, я бы не поставил 100 долларов на то, что моя новая априорная вероятность в 15 % верна. А как насчет 17 %? Вот на это я бы поставил 100 долларов.

Напомню, что я взял два разных набора данных, полученных методом частотного анализа. Я использовал данные центра IC3 и несколько оценок Ферми для получения исходной априорной вероятности. Затем с помощью отчета Института Cyentia скорректировал исходный прогноз. Таким образом, согласно моему прогнозу, вероятность нанесения существенного ущерба Marvel Studios в этом году составляет 17 %, что примерно соответствует вероятности 1:5. Помните, что по мере обнаружения новых доказательств своих предположений или появления новых фактов следует корректировать оценку в сторону увеличения или уменьшения. На данный момент априорная вероятность составляет 17 %.

Однако помните, что это всего лишь наша интуитивная оценка Ферми по схеме «извне внутрь». Данный прогноз не имеет ничего общего с фактической оборонительной позицией Marvel Studios, так как мы не проводили

анализ по схеме «изнутри наружу». Он не учитывает никаких защитных мер, которые компания Marvel Studios могла предпринять для укрепления своей позиции, с точки зрения базовых принципов кибербезопасности. Об этом мы поговорим далее.

Анализ по схеме «изнутри наружу»: первичные принципы

С помощью анализа по схеме «извне внутрь» я продемонстрировал, как сетевые защитники могут корректировать исходную оценку по мере поступления новых данных. Мы взяли априорную вероятность, основанную на данных центра IC3, и скорректировали ее с учетом данных Института Cyentia. Теперь можем повторить этот процесс, выполнив анализ по схеме «изнутри наружу». Другими словами, мы можем использовать свой прогноз, сделанный по схеме «извне внутрь», в качестве новой априорной вероятности, а затем оценить эффективность развертывания стратегий, базирующихся на первичном принципе кибербезопасности, и скорректировать априорную вероятность в сторону увеличения или уменьшения на основе новых данных. Для этого следует сделать некоторые допущения.

Предположим, что полноценная реализация каждой из стратегий снижает вероятность нанесения нашей организации существенного ущерба на некоторую величину:

- нулевое доверие — на 10 %;
- предотвращение реализации kill chain — на 10 %;
- обеспечение устойчивости — на 15 %;
- автоматизация — на 5 %.

Эти предположения — всего лишь мои догадки. Вы можете использовать совершенно другие цифры. В дальнейшем мой внутренний суперпрогнозист будет искать новые доказательства, подтверждающие или опровергающие эти значения. А пока они вполне устраивают моего внутреннего аналитика, использующего метод Ферми. Помните о том, что в рамках этой модели обнуление вероятности нанесения ущерба обеспечивается полноценной реализацией всех стратегий. Однако большинство организаций, даже специализирующихся на вопросах безопасности, не могут этим похвастаться.

Анализ по схеме «изнутри наружу»: корпорация Contoso

Чтобы понять, как это работает, проанализируем через призму первичных принципов Contoso Corporation — воображаемую компанию, на примере которой корпорация Microsoft демонстрирует потенциальным клиентам процесс развертывания набора своих продуктов [258]. Согласно Microsoft, данная компания «представляет собой вымышленный, но репрезентативный глобальный производственный конгломерат со штаб-квартирой в Париже». Представьте себе французский аналог компании Fujitsu. Поскольку аналитики Microsoft проделали большую работу по описанию архитектурной структуры корпорации Contoso, мне не придется самому создавать ее предысторию во всех подробностях. Кроме того, не нужно выбирать для проведения анализа реальную компанию наподобие Marvel Studios.

Далее представлена краткая информация о корпорации Contoso.

Общие сведения о бизнесе корпорации Contoso

- В парижском офисе работают 25 000 сотрудников, в каждом из региональных офисов — 2000 сотрудников.
- Компания занимается продажей и поддержкой более чем 100 000 продуктов.
- Годовая выручка составляет 35 млрд долларов (как у Fujitsu).
- Эта компания не входит в список Fortune 1000 и не является некоммерческой организацией.

Техническая архитектура корпорации Contoso

- Компания использует продукт Microsoft 365 для работы с офисными приложениями (электронная почта, текстовый редактор, электронные таблицы и т. д.).
- Сейчас компания переходит от выполнения операций в центрах обработки данных к облачным операциям, но для завершения перехода ей потребуется еще несколько лет.
- Клиенты используют свои учетные записи Microsoft или Google Mail для авторизации на публичном сайте компании.
- Поставщики и партнеры используют свои учетные записи LinkedIn, Salesforce или Google Mail для входа в партнерскую экстрасеть компании.

- Компания развернула сеть SD-WAN для оптимизации подключения к облачным сервисам Microsoft.
- Компания развернула региональные серверы приложений, которые синхронизируются с центрами обработки данных в Париже.

Для развертывания стратегии нулевого доверия компания Contoso:

- использует локальный лес Active Directory Domain Services (AD DS) для аутентификации в облачных ресурсах Microsoft 365 с синхронизацией хеша паролей (PHS) и применяет инструменты сторонних производителей в облаке в качестве служб федерации;
- разработала специальные правила для руководителей и конкретных пользователей из финансового, юридического и исследовательского отделов, имеющих доступ к защищаемым данным;
- собирает с устройств данные о системе, приложениях и драйверах для анализа и может автоматически блокировать доступ или предлагать исправления;
- требует прохождения многофакторной аутентификации (MFA) для получения доступа к конфиденциальным данным;
- разделяет данные на три категории с разными уровнями доступа;
- развертывает службы предотвращения утечек информации (DLP) для Exchange Online, SharePoint и OneDrive;
- разрешает конкретным людям вносить в систему глобальные изменения и получать только временные пароли с помощью своей системы управления идентификацией привилегированных пользователей (PIM) AD DS.

Для обеспечения устойчивости компания Contoso шифрует данные в состоянии покоя и предоставляет к ним доступ только аутентифицированным пользователям.

Для предотвращения реализации убийственной цепочки вторжения компания Contoso использует антивирус Microsoft Defender, чтобы обеспечить безопасность конечной точки.

Поскольку корпорация Contoso — это глобальный производственный конгломерат, а не компания из индустрии развлечений, как Marvel, нам нужно начать с оценки Ферми по схеме «извне внутрь», используя данные центра ФБР IC3. Априорная вероятность составляет 32 %. Однако, по данным Института Cyentia, вероятность того, что компания Contoso (с годовой вы-

ручкой 35 млрд долларов) столкнется с существенной утечкой в этом году, составляет 22 %, что примерно эквивалентно вероятности 1:5.

На сколько следует понизить априорную вероятность в 32 % с учетом новой информации? Я по-прежнему вполне уверен в результатах собственного анализа, проведенного по схеме «извне внутрь» на основе данных IC3. Я меньше доверяю данным Института Cyentia с учетом оговорок, о которых уже упоминал, однако данный прогноз все равно довольно хорош. И готов поставить 100 долларов на то, что фактическая вероятность существенного киберсобытия примерно на 5 процентных пунктов ниже значения моей априорной вероятности, поэтому давайте понизим ее до 27 %.

Используя 27 % в качестве текущей априорной вероятности, мы должны сделать следующий шаг для учета новых данных (дополнительных шаров на бильярдном столе), а именно оценить то, насколько успешно корпорация Contoso реализует стратегии, основанные на базовом принципе кибербезопасности. От того, насколько хорошо или плохо они реализованы, зависит повышение или понижение прогнозного значения.

Анализ по схеме «изнутри наружу»: стратегии, основанные на базовом принципе кибербезопасности

Нулевое доверие. Сокращает вероятность нанесения корпорации существенного ущерба на 8 % из возможных 10. Согласно описанию Contoso имеет мощную программу управления идентификацией и доступом (IAM), которая включает в себя управление идентификационными данными и их администрирование (IGA), управление идентификацией привилегированных пользователей (PIM) и управление привилегированным доступом (PAM). Она обеспечивает своим клиентам, подрядчикам и сотрудникам возможность единого входа в систему и использует технологию многофакторной аутентификации для предоставления доступа к конфиденциальным данным. Что касается управления уязвимостями, то у нее есть мощная программа для продуктов Microsoft и гораздо более слабая — для приложений сторонних производителей. В описании корпорации Contoso нет упоминаний о программе использования спецификаций программного обеспечения (SBOM), однако она отслеживает устройства, приложения и уровни исправлений операционной системы для продуктов Microsoft. В описании также не обсуждается программно-определяемый периметр. Учитывая сказанное,

можно прийти к выводу, что корпорация Contoso уже довольно много сделала для реализации стратегии нулевого доверия. Ей еще предстоит пройти большой путь, но данную стратегию можно считать вполне зрелой.

Предотвращение реализации убийственной цепочки вторжения. Сокращает вероятность нанесения корпорации существенного ущерба на 1 % из возможных 10. Contoso не учитывает конкретные тактики противника. Ее стек безопасности в основном состоит из продуктов Microsoft, и у нее есть возможность передавать телеметрические данные от этих продуктов в SOC-центр, однако в описании нет никаких упоминаний о том, что у Contoso есть такой центр, группа разведки, «красная»/«синяя»/«фиолетовая» команда или желание делиться с коллегами информацией о сценариях действий противника. Я готов снизить вероятность нанесения ей существенного ущерба только на 1 %, поскольку Contoso использует антивирус Microsoft Defender для автоматической защиты конечных точек от вредоносных программ, однако у нее нет программы предотвращения реализации убийственных цепочек вторжений.

Обеспечение устойчивости. Сокращает вероятность нанесения корпорации существенного ущерба на 1 % из возможных 15. У Contoso есть хорошая программа шифрования, которая работает с ее многоуровневой программой обеспечения нулевого доверия. При этом я не нашел в описании никаких упоминаний о кризисном планировании, программах резервного копирования, реагирования на инциденты и даже о примитивных инструментах хаос-инженерии. Корпорация Contoso вполне может отразить атаку неопытных разработчиков программ-вымогателей, однако любая атака профессиональных хакеров, скорее всего, нанесет ей существенный ущерб.

Автоматизация. Сокращает вероятность нанесения корпорации существенного ущерба на 0 % из возможных 5. В описании Contoso нет упоминаний ни об инженерии надежности сайта (SRE), ни о DevSecOps, ни о программе Agile-разработки, ни о защите собственного кода, ни о попытках отслеживания применяемых компонентов с открытым исходным кодом. Насколько я могу судить, эта компания не пользуется преимуществами автоматизации. В архитектурных документах Contoso ничего не говорится также о системах обеспечения соответствия нормативным требованиям. В главе 7 я расскажу о том, как можно учесть в прогнозе риск несоответствия требованиям.

Учитывая все эти корректировки (8 % за нулевое доверие, 1 % за предотвращение реализации убийственных цепочек вторжения, 1 % за обеспечение устойчивости и 0 % за автоматизацию), я готов поставить 100 долларов на то, что вероятность нанесения корпорации Contoso существенного ущерба

в результате кибератаки в этом году составляет 17 %, что примерно соответствует вероятности 1:5. Такова новая априорная вероятность для корпорации Contoso (рис. 6.10).

Предположения	Математическая задача № 6	Факты
32 % — исходная априорная вероятность для всех американских организаций, полученная на основе данных центра IC3 по схеме «извне внутрь» 27 % — априорная вероятность для Contoso, скорректированная в сторону уменьшения с учетом размера выручки на основании отчета Cyentia Уменьшение на 8 % за нулевое доверие Уменьшение на 1 % за предотвращение реализации убийственных цепочек вторжения Уменьшение на 1 % за обеспечение устойчивости Уменьшение на 0 % за автоматизацию	x = следующая априорная вероятность для корпорации Contoso, полученная в результате анализа по схеме «изнутри наружу» x = скорректированная априорная вероятность для корпорации Contoso, полученная по схеме «извне внутрь», — корректировка за нулевое доверие — корректировка за предотвращение реализации убийственных цепочек вторжения — корректировка за обеспечение устойчивости — корректировка за автоматизацию $x = 27\ \% - 8\ \% - 1\ \% - 1\ \% - 0\ \%$ $x = 17\ \%$	Недоступны

Рис. 6.10. Математическая задача № 6: следующая априорная вероятность для корпорации Contoso, полученная в результате анализа по схеме «изнутри наружу»

Что теперь? Укладывается ли уровень риска в допустимый диапазон?

Если бы я был руководителем отдела безопасности компании Contoso, то мне нужно было бы рассмотреть несколько дальнейших шагов и проверить некоторые предположения. Во-первых, следовало бы выяснить, какая сумма в долларах является для компании существенной. Если годовая выручка составляет 35 млрд долларов, будут ли потери 10 млн долларов считаться существенными? А 100 млн долларов? Следует ли скорректировать эту сумму в бóльшую или меньшую сторону? И как вообще определить ее? Для

этого нужно было бы провести несколько бесед с финансовым директором, генеральным директором и членами совета директоров. Кроме того, эта цифра, скорее всего, будет меняться со временем в зависимости от того, насколько успешно идут дела у компании. Старайтесь обновлять это значение ежегодно, обращаясь к высшему руководству.

Я бы взял за основу кривую вероятности превышения убытков Института Cyentia для компаний из списка Fortune 1000, нашел значение на этой кривой и скорректировал свой прогноз в бóльшую или меньшую сторону. Например, по данным Института Cyentia, для компаний из списка Fortune 1000 существует 14%-ная вероятность потерять 10 млн долларов или больше. Если 10 млн долларов существенная сумма для Contoso, то 14%-ная вероятность приведет к снижению текущей априорной вероятности в 17 % на один или два пункта, скажем до 15 %, что эквивалентно вероятности 3:20.

Следующий шаг заключается в определении того, находится ли текущее прогнозное значение в пределах допустимого диапазона риска. Если руководство считает, что вероятность 3:20 — это приемлемый риск для бизнеса, то значительных инвестиций в людей, процессы и технологии делать не нужно. Команде ИБ-специалистов следует поддерживать и, возможно, повышать эффективность реализации тактик нулевого доверия, предотвращения реализации убийственных цепочек вторжения, обеспечения устойчивости и автоматизации, но в развертывании каких-либо новых инициатив нет необходимости. Если же руководство посчитает вероятность 3:20 неприемлемой и потребует ее снижения до 10 % (что эквивалентно вероятности 1:10), то мне придется спланировать кое-какие действия.

В первую очередь я бы обратил внимание на устойчивость. Корпорация Contoso имеет довольно слабый план обеспечения устойчивости, и некоторые улучшения базовой ИТ-функциональности (например, автоматическое резервное копирование, практика восстановления, кризисное планирование и реагирование на инциденты) могли бы значительно снизить риск, потребовав при этом гораздо меньших затрат по сравнению с другими стратегиями, базирующимися на первичном принципе кибербезопасности. В конце концов, достижение эффективности в предотвращении реализации убийственных цепочек вторжения — удовольствие не из дешевых. При этом не стоит забывать о стоимости мероприятий, направленных на снижение риска. Если затраты на выполнение этой задачи превышают убытки 10 млн долларов, которых мы пытались избежать, возможно, стоит вернуться к началу и разработать менее затратный план. В этом и заключается суть практического прогнозирования рисков безопасности.

Заключение

Я долго искал способ донесения информации о киберрисках до членов совета директоров. Я боролся с недостатком знаний в области статистики и пытался придерживаться частотного подхода, полагая, что мне требуется максимально возможное количество данных и подсчет всего на свете. Но в глубине души понимал, что существует более эффективный способ.

Благодаря книге доктора Тетлока о суперпрогнозировании я осознал, что ИБ-специалистам не требуются точные ответы для принятия решений относительно инвестирования ресурсов в улучшение безопасности. Мы можем делать довольно хорошие приблизительные оценки (оценки Ферми), тратя на это совсем немного времени и получая вполне действенные ответы. А затем я узнал о том, что теорема Байеса представляет собой математическую основу, объясняющую, почему методы суперпрогнозирования работают.

Проанализировав примеры с Marvel Studios и Contoso Corporation, вы можете возмутиться тем, что я прогнозирую киберриски для многомиллионных компаний на основе предположений. Я это понимаю. От частотного подхода нелегко отказаться. Однако стоит помнить о том, что люди гораздо умнее нас с вами, в частности Алан Тьюринг, применяли эти методы для решения более сложных задач, чем расчет киберрисков. Возможно, и вам стоит попробовать. Кроме того, за прошедшие 20 лет старый способ сбора всех данных и использования качественных тепловых карт так и не доказал своей эффективности. Пришло время задуматься о переменах.

07 Автоматизация

Выживает не самый сильный и не самый умный вид, а тот, который лучше всех приспосабливается к изменениям.

Чарльз Дарвин

В настоящее время DevOps напоминает скорее философское движение, нежели набор описательных или предписывающих практик.

Джин Ким

Обзор главы

В этой главе мы поговорим об автоматизации. Традиционно ИБ-сообщество не относило вопросы автоматизации к компетенции специалиста по информационной безопасности, что является огромной ошибкой с точки зрения образа мышления, базирующегося на первичном принципе кибербезопасности. Из-за этой ошибки ИТ-сообщество сильно оторвалось от ИБ-сообщества в плане освоения передовых методов разработки программного обеспечения. Здесь я объясню, почему сейчас самое время наверстать упущенное. Я расскажу о важности автоматизации с точки зрения избавления от рутинных и чреватых ошибками задач, выполняемых вручную. Затем опишу процесс эволюции подходов, используемых сообществом разработчиков ПО, начиная от диаграмм Ганта, появившихся в начале 1900-х годов, и заканчивая современной методологией DevOps, и объясню, почему DevSecOps — это логичный следующий шаг. Затем затрону сложную тему автоматизации систем обеспечения соответствия нормативным

требованиям в рамках развернутой архитектуры, основанной на базовом принципе кибербезопасности. Ее сложность заключается в том, что соответствие нормативным требованиям не оказывает серьезного влияния на снижение вероятности существенного ущерба, однако в зависимости от отрасли, в которой вы работаете, может оказаться необходимо включать телеметрию развернутых тактик, основанных на базовом принципе, в свою систему обеспечения соответствия. В конце главы я расскажу об относительно новой концепции хаос-инженерии, представляющей собой продвинутую автоматизированную тактику обеспечения устойчивости, которая сегодня применяется только в крупных организациях, предоставляющих глобальные услуги, перебои в оказании которых недопустимы.

Важность автоматизации системы безопасности

Сегодня ИТ- и ИБ-специалисты используют термины *DevOps*, *DevSecOps* и *«инженерия надежности сайта»* для описания философии и лучших практик, связанных с быстрой разработкой программного обеспечения и парадигмой под названием «инфраструктура как код». Эти движения возникли лишь в 2000-х годах, хотя их корни лежат в 1960-х. К началу 2010-х годов стало ясно, что стартапы могут использовать эти стратегии, чтобы конкурировать с более консервативными и медлительными компаниями, а гиганты Кремниевой долины, такие как AWS, Google и Netflix, — для достижения господства в отрасли. Однако ИБ-сообщество не спешило принимать эти идеи. В мире Интернета, в котором правят данные, специалисты по безопасности все еще полагаются на инструменты и полуручные процессы при выполнении своей работы. Некоторые из инструментов, в частности SOAR (оркестрация, автоматизация и реагирование на инциденты безопасности) и SIEM (управление событиями и информацией о безопасности), весьма хороши, но это всего лишь полумеры. Они не позволили ИБ-сообществу принять модели инфраструктуры как кода. Одно дело — собирать телеметрию стека безопасности и автоматически анализировать данные, чтобы удалить шум из сигнала, совсем другое — построить основанную на базовом принципе кибербезопасности систему DevSecOps, которая:

- выполняет мониторинг и обновляет программу нулевого доверия, включающую сопровождение спецификаций программного обеспечения (SBOM), управление уязвимостями, идентификацией и доступом;

- ищет известные сценарии действий противника на всех этапах убийственной цепочки и на всех островах данных;
- мгновенно обновляет стек безопасности на тех же островах данных, внедряя меры противодействия, основанные на вновь собранной разведывательной информации об убийственной цепочке;
- автоматически собирает информацию об угрозах и обменивается ею с коллегами;
- осуществляет мониторинг и управляет системами непрерывного резервного копирования и шифрования всех существенных данных;
- регулярно тестирует процесс восстановления этих существенных данных;
- проверяет устойчивость системы и оценивает ее способность к непрерывному предоставлению услуг в случае катастрофы;
- собирает телеметрию из всех систем, основанных на стратегиях, базирующихся на первичном принципе кибербезопасности, для поддержки программы обеспечения соответствия нормативным требованиям;
- собирает статистику системы и оценки Ферми, которые позволяют спрогнозировать риски для организации, то есть получить следующую байесовскую априорную вероятность.

Преимущества, обеспечиваемые ИТ-сообществу этими передовыми методами разработки ПО, могли бы снизить вероятность нанесения существенного ущерба нашим организациям, если бы ИБ-сообщество тоже их приняло. Это довольно масштабная задача. Невозможно автоматизировать всю эту функциональность в одночасье. Но главное — начать. Каждый шаг, сделанный в направлении автоматизации систем, способен значительно улучшить ситуацию. Если я вас еще не убедил, позвольте мне объяснить, как ИТ-сообщество к этому пришло.

Ранняя история развития философий разработки программного обеспечения

В эпоху динозавров (1960-е годы), когда компьютеры были больше домов, крупные проекты по разработке программного обеспечения еще не предусматривали стандартной методологии. Тогда мы только учились обращаться с этими штуками, называемыми *мейнфреймами*. При разработке ПО ученые-компьютерщики опирались на устоявшуюся теорию управления проектами общего назначения, в частности на диаграммы Ганта 1910-х годов и метод критического пути, ставший популярным в 1950-е [137].

В 1956 году Герберт Бенингтон изобрел первую версию каскадной модели разработки программного обеспечения [30]. Интересно то, что изначально заслуга ее изобретения приписывалась не Бенингтону, а доктору Уинстону Ройсу, который в 1970 году опубликовал критику этой модели, даже не упомянув ее названия [161]. Однако в его статье содержались красивые диаграммы, показывающие процесс, состоящий из таких этапов, как определение требований, анализ, проектирование, реализация, тестирование и эксплуатация, которые перетекают один в другой сверху вниз, подобно водопаду. В 1976 году Белл и Тейлор назвали эти диаграммы каскадной моделью, и название в течение некоторого времени прочно ассоциировалось с доктором Ройсом [97].

В 1980-е годы, в начале компьютерной революции, разработка программного обеспечения переживала полномасштабный и всеми признанный кризис. Уже в 1960-е годы инженеры-программисты оказались не способны создавать системы, необходимые заказчикам, а организации не могли нанять достаточное количество программистов для выполнения этой работы. В 1970-е годы сложность этой задачи превысила все возможные пределы. В своей лекции при получении премии Тьюринга в 1972 году отец-основатель информатики Эдсгер Дейкстра сказал об этой проблеме следующее: «Основная причина [кризиса программного обеспечения] заключается в резком росте мощностей вычислительных машин!.. Пока этих машин не было, программирование вообще не представляло проблем... А теперь, когда у нас появились гигантские компьютеры, программирование превратилось в столь же гигантскую проблему» [68].

Это очень напоминает современную ситуацию в сфере кибербезопасности. Наши системы безопасности сильно усложнились, и на протяжении многих лет в отрасли наблюдалась нехватка квалифицированных ИБ-специалистов.

В 1985 году в целях преодоления кризиса программного обеспечения Министерство обороны США потребовало использования каскадной модели от всех подрядчиков, несмотря на критику Ройса, запустив медленный прогресс в области производства программного обеспечения [208]. По словам Алексея Крутикова, «хотя сам Ройс считал, что каскадный процесс производства ПО должен быть итеративным, выступал за выпуск пилотных версий и микромоделей, каскадная модель ошибочно считалась и до сих пор считается последовательной методологией». Последовательной она была потому, что разработчикам не разрешалось переходить на следующий уровень до завершения работы на текущем [246]. Если разработчики вносили изменения на этапе реализации, команде приходилось возвращаться и начинать все с нуля. В результате на реализацию многих проектов уходили годы, а команды тратили на документирование требований столько же

времени, сколько и на написание кода. Сравните это с современными средами DevOps, в которых обычной целью является ежедневное внесение в кодовую базу не менее десяти изменений [7].

Agile бросает вызов

В 1990-е годы некоторые разработчики-бунтари начали экспериментировать с различными способами совершенствования этого процесса, в частности с методологиями Rational Unified Process (1994), Scrum (1995) и Extreme Programming (1996) [137]. В феврале 2001 года 17 программистов отправились в Юту, чтобы провести длинные выходные, катаясь на лыжах и обсуждая процесс создания программного обеспечения. Результатом этой поездки стал Agile-манифест (манифест гибкой разработки программного обеспечения), который предполагал отказ от каскадной модели и принятие концепции создания реального рабочего кода как вехи на пути прогресса [148].

До этого момента разработка ПО сводилась к созданию программ общего назначения, то есть приложений, предназначенных для решения конкретных задач бизнеса, правительственных и научных кругов. В те времена мало кто говорил об использовании программного обеспечения для управления ИТ-инфраструктурой и о создании безопасного ПО. Но в какой-то момент ситуация стала меняться, и сообщество разработчиков начало наблюдать параллельное развитие как в области повышения безопасности всего программного обеспечения, так и в области развертывания кода в качестве инфраструктуры.

Когда мы задумались о безопасности?

В 2000 году самой популярной операционной системой для настольных компьютеров была Windows. Она была установлена примерно на 75 % настольных компьютеров по всему миру [76, 273]. В мае того же года хакеры выпустили червь ILoveYou, за которым последовала целая серия других червей [207], поражающих продукты Microsoft Windows (операционные системы и браузеры) по всему миру на протяжении 2001 года:

- июль — червь Code Red;
- август — червь Code Red II;
- сентябрь — червь Nimda;
- октябрь — червь Klez и др.

В феврале 2002 года Билл Гейтс (председатель совета директоров и главный архитектор программного обеспечения Microsoft) решил реализовать инициативу под названием *Trustworthy Computing* («Вычисления, заслуживающие доверия»). Он приостановил развертывание новых версий ОС Windows с тем, чтобы разработчики сосредоточились на вопросах безопасности. Результатом стал первый жизненный цикл безопасной разработки (SDLC) компании Microsoft [89, 303].

В 2003 году Дэйв Уикерс и Джефф Уильямс из компании Aspect Security, специализирующейся на консультировании по вопросам разработки ПО, опубликовали учебную статью, посвященную текущим проблемам в области создания безопасного программного обеспечения. Впоследствии она превратилась в список OWASP Top 10 — справочный документ, описывающий наиболее важные уязвимости веб-приложений [59].

Чтобы было ясно: дело не в том, что разработчики программного обеспечения не думали о создании безопасных систем, просто у них не было примеров, на которые они могли бы ориентироваться, и сообществом еще не были приняты лучшие практики. Откровенно говоря, бизнес-лидеры и продакт-менеджеры об этом и не просили. В начале 2000-х годов сообщество стало делать первые шаги к изменению этой ситуации.

Разработка инфраструктуры

В 1994 году компания Amazon начала работу над сервисом Merchant.com, призванным помочь таким ретейлерам, как Target и Marks & Spencer, в создании сайтов интернет-магазинов на базе движка Amazon для электронной коммерции [160]. Благодаря этим усилиям десять лет спустя был создан сервис AWS. В 2003 году Amazon начала реализовывать внутренние проекты по модели «инфраструктура как код» (зачатки DevOps), представлявшие собой набор общих инфраструктурных сервисов, к которым любой сотрудник мог получить доступ, чтобы каждый раз заново не изобретать колесо. Вскоре руководители Amazon поняли, что на основе этих сервисов можно создать операционную систему для Интернета. Это открытие ускорило развитие AWS.

В 2004 году, когда компания Google была всего лишь поисковой системой, а не тем интернет-гигантом, каким является сегодня, руководство компании приняло неординарное решение. Вместо того чтобы возложить ответственность за управление сетью на ИТ-команду, как было принято в то время, оно поручило эту задачу команде разработчиков.

Эта группа SRE-инженеров занялась автоматизацией однотипных инфраструктурных задач, в которые могли вкрасться ошибки и которые не представляли особой ценности для будущего компании. Они обозначили эти задачи термином «тойл» и внесли существенный вклад в развитие движения DevOps, которое получило свое название только шесть лет спустя [163].

В марте 2008 года доктор Гэри Макгроу опубликовал первый отчет *Building Security In Maturity Model* (BSIMM), представлявший собой обзор более чем 30 компаний, в котором были описаны инициативы и мероприятия, связанные с обеспечением безопасности ПО [267]. Данный отчет не предписание, а всего лишь сборник лучших практик в области обеспечения безопасности ПО, которых придерживаются организации-участники. Цель его создания состоит в том, чтобы дать специалистам возможность ознакомиться с тем, что делают их коллеги по отрасли в плане разработки безопасного программного обеспечения. В 2009 году Правир Чандра опубликовал первую предписывающую модель лучших практик в сфере обеспечения безопасности под названием *Software Assurance Maturity Model* (SAMM) [286]. Ее руководящий характер проявляется в том, что она четко указывает организациям, что они должны делать для создания безопасных программных систем. Благодаря этим двум моделям ИБ-сообщество получило возможность соизмерять свои действия с практиками коллег по отрасли (BSIMM) и рекомендациями экспертов (SAMM).

В 2006 году компания Amazon представила сервис AWS, положив начало облачной революции [59]. В 2010 году корпорация Microsoft последовала ее примеру, запустив конкурирующий сервис Azure [1]. Компания Google вышла на этот рынок в 2012 году со своей платформой Google Cloud Platform (GCP) [158]. Существуют и другие, более мелкие поставщики облачных услуг. После появления сервиса AWS облако стало стимулом, побуждающим ИТ-сообщество рассматривать инфраструктуру как код. Однако даже после того, как Agile-методология заменила каскадную модель в качестве стандартного метода разработки программного обеспечения, этот процесс по-прежнему осуществлялся мучительно медленно. Стартапы, рожденные в облаке, осознали, что они могут добиться большего, используя программное обеспечение для создания конкурентного преимущества. С помощью программного обеспечения они могли обновлять свои продукты и услуги через Интернет, существенно опережая своих конкурентов, которым все еще приходилось поставлять физическое оборудование. Они понимали, что могут достичь успеха на рынке программных приложений, если сумеют упростить этот процесс.

DevSecOps: важнейшая тактика автоматизации

В 2009 году методология DevOps начала развиваться как лучшая отраслевая практика, чему способствовали три родственные идеи:

- доклад Джона Оллспоу и Пола Хаммонда на конференции Velocity 2009 года под названием *10+ Deploys per Day* («10+ развертываний в день») [246];
- упомянутый ранее метод разработки Agile [7];
- книга Эрика Риса «Бизнес с нуля», которая повлияла на многие компании Кремниевой долины в период с 2007 по 2010 год [325].

Суть идеи DevOps сводится к необходимости более тесной интеграции между операциями разработчиков программного обеспечения и ИТ-операциями (ITOps); иными словами, труд разработчиков, команды по обеспечению качества и аналитиков безопасности не заканчивается после передачи нового кода или обновлений ИТ-операторам для развертывания. До появления методологии DevOps разработчики просто передавали свой рабочий код операторам и никак не участвовали в ночных телефонных переговорах, вызванных тем, что развернутый код не работает должным образом или приводит к поломке какой-то другой части системы. Вместо создания искусственных черных ящиков внутри каждой команды, в которые поступают обновления и после доработки передаются в следующий черный ящик, методология DevOps предлагает признать то, что создание, развертывание и сопровождение обновлений — это одна большая система систем, которой нужно управлять соответствующим образом. Суть этой идеи состоит в том, что организациям следует распространить Agile-методологию, которую применяют их команды разработчиков ПО, на всех участников цикла развертывания: продакт-менеджеров, специалистов по маркетингу, разработчиков, специалистов по контролю качества, системных инженеров, системных администраторов, операционистов, администраторов баз данных, сетевых инженеров и специалистов по безопасности. Методология DevOps предполагает использование Agile-подхода на всех этапах жизненного цикла систем, включая проектирование, разработку, тестирование, развертывание и сопровождение вплоть до вывода из эксплуатации.

В 2013 году Джин Ким, Кевин Бер и Джордж Спаффорд опубликовали книгу «Проект “Феникс”. Как DevOps устраняет хаос и ускоряет развитие

компании», попавшую в Зал славы Cybersecurity Canon [323]. Авторы отразили в ней суть движения DevOps в форме романа, поскольку хотели сделать ее доступной большему числу людей, то есть не только технарям, но и бизнес-лидерам широкого профиля. В этой истории один из членов совета директоров, похожий на Оби-Вана Кеноби, помогает ИТ-директору трансформировать бизнес. Будучи гуру в области производства запчастей, он на протяжении всей истории передает мудрость DevOps, говоря о том, что ИТ-операции должны напоминать рационализацию производства на заводе автомобильной компании Toyota. Руководители Toyota внедрили свою знаменитую производственную систему (TPS) сразу после Второй мировой войны с целью минимизации отходов на всех этапах работы. Исследователи и бизнес-лидеры изучают систему TPS уже более 50 лет, и Ким с соавторами считают, что процесс разработки программного обеспечения должен напоминать процесс производства автомобилей в рамках этой системы. Авторы «Проекта “Феникс”» многое заимствуют из книги Майка Ротера «Тойота Ката» [327], а идея непрерывного совершенствования является ключевой концепцией, которую член совета директоров, похожий на Оби-Вана, прививает ИТ-директору.

Примерно к 2014 году такие интернет-гиганты, как Amazon, Apple, Netflix и Google (FAANG), стали лидерами отрасли, чему в немалой степени способствовало принятие философии DevOps. Их конкуренты, использующие старый каскадный метод разработки программного обеспечения, могли тратить годы на развертывание нового сервиса для своих клиентов. А в это время компании, освоившие методологию DevOps, развертывали революционные сервисы на лету и постепенно улучшали их, выпуская по десять обновлений в день.

Что случилось с ИБ-сообществом

Сейчас вы, возможно, говорите себе: все это хорошо, но куда подевались специалисты по безопасности? В случае с OWASP, BSIMM и SAMM они по крайней мере участвовали в обсуждениях. Однако в период между 2008 и 2017 годами казалось, что ИТ-сообщество с его новомодной моделью DevOps совершенно оторвалось от ИБ-сообщества. Даже в романе «Проект “Феникс”» руководители службы безопасности были не частью движения DevOps, а сторонними наблюдателями, не вполне уверенными в правильности нового направления. В конце концов они приняли его, но это случилось ближе к завершению истории.

В марте 2021 года в ходе интервью Джон Уиллис, один из авторов книги «Руководство по DevOps», сказал, что люди, вовлеченные в развитие DevOps, похлопывали себя по спине за создание этого замечательного движения, но при этом все мы примерно на восемь лет почти полностью забыли о безопасности. Люди говорили о DevOps и безопасности, но без особых подробностей [316, 324]. Примерно в 2017 году Шеннон Лиетц, в то время работавшая в Intuit, заявила свои авторские права на название DevSecOps [288]. Она создала фонд и веб-сайт, призванные сделать обеспечение безопасности частью DevOps. Это вызвало некоторые споры среди участников движения, поскольку многие из них приписывали эту идею себе, однако, по мнению Уиллиса, это не имело значения. Когда Лиетц создала фонд, эта концепция снова оказалась в фокусе внимания ИТ- и ИБ-специалистов, что способствовало развитию методологии DevSecOps.

DevSecOps движется в верном направлении

В 2021 году компания Gartner поместила DevSecOps на склон просвещения (Slope of Enlightenment) своей диаграммы зрелости технологий (Hype Chart) примерно в 2–5 годах от плато продуктивности (Plateau of Productivity) [101]. В том же году Министерство обороны США формализовало собственный процесс, опубликовав первую версию документа *DevSecOps Reference Design* [69].

Если ваша организация в той или иной форме использует модель DevOps, то, скорее всего, у нее есть собственная версия конвейера непрерывной интеграции и непрерывной доставки (continuous integration/continuous delivery, CI/CD). CI/CD-конвейер — это лучшая практика DevOps, которая, согласно принципам компании Synopsys, «предполагает частое и надежное внесение инкрементальных изменений в код. Автоматизированные этапы сборки и тестирования, выполняемые в рамках процесса непрерывной интеграции, обеспечивают надежность изменений кода, сливаемого в репозиторий. Затем этот код быстро и беспрепятственно поставляется пользователям в рамках процесса непрерывной доставки».

Эти конвейеры представляют собой сложные программные проекты на основе модели «инфраструктура как код», которые, по словам Тери Радичела (DevSecOps-эксперта AWS), «помимо технологий, требуют соответствующей архитектуры и правильного проектирования. CI/CD-конвейер

является частью более крупной архитектуры безопасности, которая должна быть хорошо продумана. В противном случае ваша стратегия обеспечения безопасности будет либо вечно говорить об облаке, так и не добираясь до него, либо напоминать выпас котов» [180]. Данное Тери описание выпаса котов относится исключительно к интеграции сообществом разработчиков практик обеспечения безопасности общего назначения в уже существующие DevOps-системы. Согласно принятому в IBM определению, DevSecOps — это «интеграция задач по обеспечению безопасности в каждый этап разработки программного обеспечения» [244]. То, что подобный образ мышления получил такое распространение, — это замечательно, и ИБ-сообществу следует это приветствовать. Однако это не имеет ничего общего с автоматизацией архитектуры, основанной на базовом принципе кибербезопасности, которую я описал в начале главы. В некоторых организациях развернуты отдельные фрагменты этой инфраструктуры, но ни у одной из них нет всеобъемлющей системы или даже намерения ее создать.

Это еще одна причина мыслить в терминах первичных принципов. Если мы хотим снизить вероятность нанесения нам существенного ущерба, то при усложнении наших сред и возникновении нехватки людей для управления ими руководство службы безопасности может воспользоваться автоматизацией выполняемых вручную задач как еще одним из рычагов.

DevSecOps как стратегия, основанная на базовом принципе кибербезопасности

В этой книге я описал пять стратегий: нулевое доверие, предотвращение реализации убийственной цепочки вторжения, обеспечение устойчивости, прогнозирование рисков и автоматизацию. Для реализации первых четырех предусмотрен ряд тактик. Например, в случае с нулевым доверием одной из необходимых тактик является создание надежной программы идентификации и авторизации. Для защиты от убийственных цепочек вторжения следует изучать сценарии действий противника. Для обеспечения устойчивости компании требуется хорошая программа резервного копирования и восстановления существенных данных. Для прогнозирования рисков ИБ-специалисты должны овладеть навыком оценки рисков по схемам «извне внутрь» и «изнутри наружу». И это лишь малая толика того, что требуется сделать для снижения вероятности существенного ущерба.

Однако служба безопасности не может и не должна делать все это в отрыве от того, что уже делает ИТ-служба. Зачем изобретать колесо? В конце концов, суть концепции DevOps заключается в том, чтобы поручить разработку и операционную деятельность одной команде вместо разнесения этих задач по разным черным ящикам, которые не сообщаются друг с другом. ИБ-сообщество должно включиться в существующие CI/CD-процессы. Другими словами, мы должны стать частью внутренней DevOps-программы, вместо того чтобы сопротивляться ей или создавать собственную. В частности, нам нужно найти способы помещения кода в конвейер, который поддерживает реализацию каждой из стратегий.

Напоследок об автоматизации как стратегии

Все описанное ранее представляет собой весьма масштабные и революционные идеи с точки зрения специалиста по информационной безопасности. Однако время для радикальных изменений пришло. Для руководителя службы безопасности эти изменения будут выражаться в том, что часть его команды, возможно самая большая, присоединится к внутреннему движению DevOps в качестве разработчиков или, скорее, продакт-менеджеров для каждого из элементов стратегии, основанной на базовом принципе кибербезопасности. Следует учитывать это при составлении бюджета и обдумывании набора навыков своей команды.

Истина заключается в том, что для полноценного развертывания таких стратегий ИБ-сообществу необходимо автоматизировать решение повторяющихся задач, связанных с обеспечением безопасности и предусмотренных тактиками, способствующими реализации стратегий. Рассматривайте эти усилия по автоматизации как клей, который связывает все воедино, создавая систему систем с петлями обратной связи.

Уже на протяжении двух десятилетий мы развиваем методологии разработки программного обеспечения (каскадный подход, Agile-методологию), проекты на основе модели «инфраструктура как код» (облачные развертывания, DevOps, DevSecOps) и лучшие практики написания кода (OWASP, BSIMMS, SAMM). Эти системы не являются независимыми. Они пересекаются и взаимодействуют друг с другом. До сих пор, по крайней мере в области безопасности, они предполагали ручное выполнение задач, чреватое ошибками. Все мы знаем, что автоматизация может уменьшить

ущерб или по крайней мере обеспечить последовательность в отношении совершаемых ошибок, для избавления от которых можно впоследствии предложить единое исправление для использования в масштабах предприятия. Автоматизация должна стать пятой стратегией, основанной на базовом принципе кибербезопасности, а DevSecOps — тактикой, способствующей ее реализации.

Обеспечение соответствия нормативным требованиям: тактика, базирующаяся на первичном принципе кибербезопасности и пронизывающая все стратегии

Идея соответствия нормативным требованиям, или комплаенса, используется во многих организациях и отраслях. Государственные структуры принимают законы вроде Генерального регламента защиты персональных данных (GDPR), принятого Европейским парламентом для обеспечения того киберповедения, которого ожидают граждане стран Евросоюза [164]. Группы поставщиков, такие как Совет по стандартам безопасности данных индустрии платежных карт (PCI), разрабатывают стандарты соответствия, чтобы избежать государственного регулирования [83]. Комплаенс может применяться также нейтральными сторонними разработчиками стандартов, такими как Международная организация по стандартизации (ISO), в качестве генерирующей прибыль бизнес-модели (ISO взимает плату за использование своих стандартов) [131]. Кроме того, он может использоваться такими государственными органами, как Национальный институт стандартов и технологий США (NIST), в качестве базовой линии для оценки собственной внутренней ИТ-инфраструктуры [215]. Стандарты NIST уже вышли за пределы правительственного сектора США и распространились в коммерческой сфере благодаря тому, что они бесплатны, не зависят от поставщиков и обычно отличаются высочайшим качеством.

Согласно определению комплаенс — это действие, направленное на соблюдение ряда правил. Если они исходят от правительственных законодателей, то имеют вид законов. Если их устанавливают группы поставщиков, то они становятся ценой ведения бизнеса, позволяющей процветать всему сектору. В случае с органами по стандартизации, как правительственными, так

и неправительственными, они представляют собой сторонние нейтральные соглашения, на которые могут ссылаться другие заинтересованные стороны. Организации, соблюдающие эти стандарты, могут сказать, что они следуют общепринятой международной передовой практике.

Индустрия комплаенса

Существует целая индустрия консалтинга, предоставляющая услуги организациям, стремящимся разобраться в хитросплетениях законодательства, связанного с соблюдением нормативных требований. Как правило, эти услуги имеют отношение к комплаенс-оповещениям, календарям и индивидуальным комплаенс-отчетам.

Существуют также специальные GRC-платформы (от governance — «управление», risk — «риски», compliance — «соответствие нормативным требованиям»), которые используются компаниями для контроля над доступностью данных и управления теми ИТ-операциями, которые подпадают под регулирование. По данным ресурса TrustRadius, «в соответствии с федеральным законодательством некоторые финансовые и публично торгуемые компании обязаны выполнять элементы управления корпоративными рисками (ERM). Кроме того, ERM-оценка компании влияет на ее кредитный рейтинг S&P». GRC-платформы помогают им в этом, предлагая услуги по обеспечению соответствия нормативным требованиям, такие как автоматизированное управление и управление аудитами и проверками.

Эти платформы фокусируются на достижении двух бизнес-целей: предотвращении потери данных и рабочих нагрузок и обеспечении соответствия нормативным требованиям. Согласно TrustRadius, «большинство GRC-инструментов способны служить обеим целям, но могут фокусироваться на одной из них в большей степени, чем на другой» [292]. По словам Ника Инмана из Kroll Consulting, около трети его клиентов прогнозируют, что их траты на обеспечение соответствия нормативным требованиям будут составлять более 5 % от выручки [118]. Чтобы было понятно: обеспечение соответствия нормативным требованиям предполагает инвестиции в создание ресурсов (люди, процессы и технологии), способных доказать аудиторам, что компания соответствует предъявляемым требованиям. Речь не идет о вложениях в создание комплексной программы обеспечения кибербезопасности, основанной на первичном принципе. Комплаенс-программы могут помочь выявить пробелы в архитектуре безопасности с помощью системы контрольных списков, однако обратите внимание на то, что в обсуждении

первичных принципов (см. главу 1) комплаенс не фигурирует. Обеспечение соответствия нормативным требованиям — не обязательное условие снижения вероятности существенного ущерба. Есть множество примеров, когда организациям был нанесен существенный ущерб, несмотря на соблюдение ими требований. В отчете ISACA за 2017 год под названием *Compliant, Yet Breached* автор Тони Чандола упоминает более десятка таких случаев [45]. Существуют и другие причины для создания комплаенс-программ, но укрепление оборонительной позиции организации в их число не входит.

Две комплаенс-категории: разрешения и штрафы

В повседневной работе ИБ-специалист обычно сталкивается с двумя комплаенс-категориями. Первая из них — это разрешения. Например, чтобы продавать облачные услуги правительству США, поставщики должны продемонстрировать соответствие своей конфигурации безопасности минимальным требованиям, установленным Федеральной программой управления рисками и авторизацией (FEDRAMP). Создание и поддержка программы безопасности, соответствующей стандартам FEDRAMP, и демонстрация того, что вы достигли этой минимальной планки, — важное условие для ведения бизнеса с правительством США. Другой пример: руководители компаний могут настаивать на том, чтобы их подрядчики и участники цепочки поставок продемонстрировали соответствие стандартам ISO 27000 до утверждения контрактов. В обоих случаях соблюдение стандартов становится своего рода разрешением на ведение бизнеса. Если у вас его нет, вы не сможете выйти на соответствующий рынок.

Ко второй категории относятся всевозможные штрафы и другие наказания, которые ваша организация может понести за несоблюдение требований кибербезопасности. Например, в 2019 году компания Google заплатила штраф 170 млн долларов за несоблюдение закона о защите конфиденциальности детей в Интернете (COPPA) [129]. В 2021-м Европейский парламент оштрафовал компанию Amazon на 877 млн долларов за несоблюдение Генерального регламента защиты персональных данных [138]. Управление по гражданским правам (OCR) США оштрафовало компанию Anthem на 16 млн долларов за несоблюдение закона США о преемственности и подотчетности медицинского страхования (HIPAA) [227].

При этом я не имею в виду штрафы, налагаемые на компании за несоблюдение требований в областях, не связанных с кибербезопасностью. Они оказываются просто астрономическими и чаще всего налагаются на

финансовые учреждения. Например, в отчете Finbold Bank Fines Report за 2020 год самым большим штрафом того года названо мировое соглашение между Goldman Sachs и правительством Малайзии, в рамках которого компания должна была заплатить 3,9 млрд долларов за отмывание денег и мошенничество [242]. Но это был не единичный случай. На одни только американские организации было наложено 12 подобных штрафов на общую сумму 10,9 млрд долларов.

Я не говорю о подобных видах мошенничества. Меня интересует соблюдение требований кибербезопасности. С точки зрения первичных принципов какова вероятность получения существенного штрафа за несоблюдение таких требований в ближайшие три года? И если, по мнению высшего руководства, эта вероятность слишком высока, каковы затраты на ее снижение?

Вероятность существенного ущерба в результате несоблюдения нормативных требований

Чтобы спрогнозировать эту вероятность, я выполню основные шаги, которые описал в главе 6. Однако ввиду большого количества комбинаций законов о соответствии нормативным требованиям, способных повлиять на организацию, не существует единого способа прогнозирования комплаенс-риска. Все зависит от того, насколько велика организация, в какой части света она работает и к какой отрасли относится.

Согласно отчетам CSO Online [259] и DLA Piper [255] в 2021 году в мире насчитывалось более 50 законов о соответствии нормативным требованиям в сфере кибербезопасности. В ближайшие годы количество этих законов значительно увеличится для всех, и сетевым защитникам придется самостоятельно анализировать риск, исходя из своих обстоятельств.

В качестве примера рассмотрим закон США о преемственности и подотчетности медицинского страхования (HIPAA), принятый в 1996 году [11], и прогноз рисков для компании ACM Podiatry, которую управление по гражданским правам (OCR) Министерства здравоохранения и социальных служб оштрафовало в 2022 году [254].

По данным Сташи Смилянич, штатного автора сайта PolicyAdvice, в 2022 году в США насчитывалось 784 626 медицинских компаний [295]. Предположим, что все они подпадают под действие HIPAA. Также допустим, что все они могут с одинаковой вероятностью получить штраф за его нарушение. Скорее всего, это не так. Подобно тому как хакеры стремятся выбирать

в качестве жертв крупные богатые организации (см. главу 6), агентства, осуществляющие надзор за соблюдением нормативных требований, чаще накладывают штрафы на более крупные организации. Однако пока давайте считать, что эта вероятность одинакова для всех.

По данным сайта HIPAA Journal, в 2022 году OCR выписало 17 штрафов за нарушение HIPAA. Таким образом, для отдельно взятой американской медицинской организации вероятность получения штрафа за нарушение этого закона практически нулевая. Для тех 17 компаний, которые все же были оштрафованы, это событие стало «черным лебедем». Будучи одной из этих компаний, ACM Podiatry заплатила штраф 100 000 долларов.

По оценкам компании ZoomInfo, предоставляющей B2B-аналитику клиентам, занимающимся продажами и маркетингом, годовая выручка ACM Podiatry в среднем составляет 15 млн долларов [294]. Если мы воспользуемся оценкой Kroll Consulting, согласно которой многие организации расходуют на комплаенс-программы примерно 5 % от выручки, то ACM Podiatry могла потратить 750 000 долларов, чтобы избежать штрафа 100 000 долларов, или не тратиться на создание этой программы, рассчитывая на то, что ее вообще не оштрафуют. Судя по всему, эта компания пошла по второму пути. Она просто попала в ситуацию типа «черный лебедь».

Штраф 100 000 долларов относит ACM Podiatry к одной из двух возможных категорий [257]. К категории 2 (Tier 2) относятся компании, которые должны были знать о нарушении HIPAA и сделать что-то для его устранения. К категории 3 (Tier 3) относятся компании, которые знали о проблемах и решили не исправлять их. Если ACM Podiatry попадает в категорию 3, то согласно HIPAA ей дается 30 дней на устранение выявленных проблем. Если компания этого не делает, она переходит в категорию 4 (Tier 4) и ее могут штрафовать на 1,5 млн долларов в год вплоть до ликвидации проблемы.

Учитывая размер выручки (менее 1 млрд долларов), компания ACM Podiatry относится к тому же классу риска, по оценке Института Cyentia, что и Marvel Studios из главы 6. Согласно оценке Ферми, выполненной по схеме «извне внутрь», то есть без учета того, насколько хорошо ACM Podiatry придерживается первичных принципов кибербезопасности, вероятность нанесения этой компании существенного ущерба в результате киберсобытия тоже составляет 17 %. В данном случае я должен учесть новые данные о риске, связанном с несоблюдением нормативных требований, и скорректировать 17%-ное значение априорной вероятности в бóльшую или меньшую сторону. Однако, поскольку вероятность получения штрафа

за нарушение закона HIPAA практически нулевая, в корректировке нет необходимости. Таким образом, новая априорная вероятность составляет те же 17 %.

Если говорить конкретно об обеспечении соответствия нормативным требованиям, то руководитель отдела безопасности ACM Podiatry может порекомендовать руководству компании не тратить 750 000 долларов на создание комплаенс-системы, учитывая низкую вероятность получения штрафа. Даже если это произойдет, размер штрафа окажется значительно меньше (100 000 долларов), чем затраты на разработку комплаенс-системы. Это не может считаться умышленным пренебрежением. Отказ от создания инфраструктуры аудита не равнозначен отказу от усиления оборонительной позиции. Глава отдела безопасности должен рекомендовать руководству инвестировать в реализацию стратегий, основанных на базовом принципе кибербезопасности, и если соответствующие программы будут действовать, то аудитор, скорее всего, не найдет нарушений HIPAA. Но если высшее руководство относится к рискам довольно консервативно и настаивает на уменьшении штрафов, руководитель отдела безопасности может рассмотреть возможность страхования с целью покрытия потенциальных расходов.

Это непросто, потому что те 50 с лишним законов, о которых я упомянул ранее, предусматривают разные положения. Ваша ситуация может иметь свои нюансы, так что стоит проконсультироваться с юристами компании, чтобы узнать их мнение. В большинстве законов о соблюдении нормативных требований нет прямого запрета на использование страховки для покрытия расходов, связанных с уплатой штрафов. Тем не менее, по мнению специалистов известной юридической фирмы Jones Day, страховые требования о возмещении расходов на выплату штрафов за умышленное несоблюдение нормативных требований, скорее всего, будут оспорены страховщиком [73]. Что касается компании ACM Podiatry, то ей лучше оставаться во второй категории, к которой относятся компании, не соблюдающие закон HIPAA по ошибке, а не умышленно его нарушающие.

Еще одна причина создания комплаенс-программы связана с угрозой предъявления коллективных исков. Согласно данным Hagens Berman, международной юридической фирмы, специализирующейся на подобных случаях, юристы возбуждают такие дела «от имени группы людей или хозяйствующих субъектов, которые понесли ущерб в результате действий ответчиков» [293]. В качестве примера, связанного с кибербезопасностью, можно привести случай с компанией ZenDesk, инвесторы которой инициировали коллективный иск в 2019 году, утверждая, что в 2016-м в этой компании произошла утечка данных [233].

В целом для снижения угрозы подачи такого рода исков юристы компании могут использовать зрелую комплаенс-программу, чтобы продемонстрировать суду, что руководство приняло разумные меры для предотвращения утечек данных. Однако, как и в случае со штрафами за нарушение нормативных требований, количество коллективных исков в сфере кибербезопасности довольно невелико. Точное число назвать сложно, но, скорее всего, оно находится в диапазоне от 30 до 2000 в зависимости от способа их подсчета. Для отдельно взятой американской компании, число которых превышает 6 млн (см. главу 6), вероятность столкнуться с таким иском весьма мала. Компании ACM Podiatry было бы трудно оправдать затраты в 3/4 млн долларов на создание программы по соблюдению нормативных требований в целях избежания столь незначительного риска.

Последняя причина разработки комплаенс-программы заключается в защите репутации бренда. Если вы пытаетесь убедить потенциальных клиентов приобрести ваши услуги, то можете обнародовать результаты проверки на соответствие нормативным требованиям за последние пять лет, чтобы показать, что вашей компании можно доверять. Однако это маркетинговое решение напоминает трансляцию платного рекламного ролика во время популярного телешоу. В некоторых отраслях это может являться неофициальным разрешением на ведение бизнеса. Если все ваши конкуренты имеют зрелую комплаенс-программу, то создание такой программы может быть необходимым условием работы в этой конкретной сфере.

Является ли соблюдение нормативных требований тактикой, основанной на базовом принципе кибербезопасности?

Обеспечение соответствия нормативным требованиям — это особенная тактика. Если вы посмотрите на дорожную карту первичных принципов кибербезопасности, приведенную во введении, то заметите, что эта тактика пронизывает все базирующиеся на них стратегии, как и тактика DevSecOps. На это есть две причины. Во-первых, при создании комплаенс-программы вам нужно будет задействовать все развернутые тактики, основанные на базовом принципе, чтобы собрать телеметрию, способную удовлетворить аудиторов. Во-вторых, имеет смысл подключиться к существующим в организации процессам непрерывной интеграции и непрерывной доставки (CI/CD), чтобы сократить объем выполняемой вручную работы, связанной с созданием соответствующих отчетов.

Однако с точки зрения стратегий, основанных на базовом принципе кибербезопасности, обеспечение соответствия нормативным требованиям представляет собой просто еще одну тактику, которую мы можем использовать наряду с созданием спецификаций программного обеспечения, организацией деятельности «фиолетовых» команд и шифрованием данных. Однако она не оказывает существенного влияния на размер потенциального ущерба. Причина, по которой я включил ее в список тактик, заключается в том, что в некоторых отраслях, таких как финансы и здравоохранение, специалисты по безопасности, скорее всего, будут привлечены к созданию комплаенс-программы компании, если ее руководство сочтет это необходимым условием ведения бизнеса. Возможно, все именно так, однако соблюдение нормативных требований и трата ресурсов на доказательство этого факта, скорее всего, не сильно снизит вероятность нанесения вам существенного ущерба.

Хаос-инженерия для автоматизации и обеспечения устойчивости

Хаос-инженерия — это дисциплина проведения контролируемых стресс-тестов в CI/CD-средах для выявления недостатков системы, направленная на повышение ее устойчивости. Хаос-инженеры формулируют гипотезы относительно ожидаемого поведения программного обеспечения, разрабатывают эксперименты, направленные на изучение поведения системы при варьировании таких параметров, как пропускная способность и степень загрузки процессора, и проводят эти эксперименты в производственных системах для выявления их слабых мест. Разумеется, это довольно продвинутая тактика, основанная на базовом принципе кибербезопасности, которая не подходит для малых, средних и даже некоторых крупных компаний. Однако если ваша организация оказывает глобальные цифровые услуги и считает сбои в их поставке недопустимыми, то у вас, скорее всего, уже есть команда хаос-инженеров, проводящих подобные эксперименты.

Чтобы понять, почему поставщики глобальных услуг нуждаются в хаос-инженерии, необходимо принять тот факт, что мы больше не живем в линейном цифровом мире. В 1990-е годы, когда Интернет представлял собой полезный бизнес-инструмент, все было довольно просто. Тогда нам так не казалось, но по сравнению с сегодняшним днем тот мир был детским садом. В те времена, меняя что-то, вы примерно представляли, к чему это приведет. Однако современные ИТ-среды представляют собой системы

систем. Они сложны, и большинство из нас понятия не имеет, как они на самом деле работают и каковы реальные зависимости между всеми программными модулями, развернутыми на наших островах данных.

Как пишут Розенталь, Джонс и Эшбахер в книге «Хаос-инжиниринг» [326], «изменение входного сигнала линейной системы приводит к соответствующему изменению ее выходного сигнала. Выходной сигнал нелинейных систем сильно варьируется в зависимости от изменения составляющих их частей». Это сродни старому анекдоту о том, что взмах крыла бабочки в Китае может вызвать ураган в Мексиканском заливе. В данном случае речь идет о том, что сбой в работе жесткого диска, поддерживающего работу какого-нибудь несущественного приложения для мониторинга, запущенного на серверах AWS в Северной Америке, может привести к сбою в работе всей системы.

Ни один человек не в состоянии осмыслить все хитросплетения этих сложных систем. Инженеры-программисты думают, что они на это способны, а команды DevOps-специалистов и SRE-инженеров пишут линейные регрессионные тесты для проверки тех вещей, которые считают истинными. Но эти команды не узнают ничего нового. Они тестируют уже известные свойства системы, например ранее исправленные дефекты и граничные условия основных функций продукта.

По словам Розенталя, Джонс и Эшбахера, подобные линейные регрессионные тесты «требуют того, чтобы разрабатывающий их инженер имел представление об искомых свойствах системы». Хаос-инженерия, напротив, предполагает поиск неизвестного. Хаос-инженеры не заменяют линейные регрессионные тесты, они пытаются решить другую задачу, связанную с обнаружением еще неизвестных недостатков системы.

В основе хаос-инженерии лежит научный метод. Команды DevOps-специалистов формулируют гипотезу об устойчивом поведении системы и проверяют ее, экспериментируя в производственной среде. Обнаруживая разницу между контрольной и экспериментальной группами, они узнают что-то новое. Отсутствие этой разницы дает им больше уверенности в истинности своей гипотезы. Они используют методы минимизации радиуса поражения производственной системы и тщательно контролируют весь эксперимент, чтобы не допустить катастрофических последствий.

В главе 5 я уже упоминал об этой новой тактике и привел в качестве примера компанию Netflix, которая регулярно запускает приложение Chaos Monkey, специально нарушающее работу выбираемых случайным образом

частей инфраструктуры, ориентированных на клиентов, для того чтобы дать сетевым архитекторам возможность отточить навыки обеспечения устойчивости.

Узнав об этой технике, я был ошеломлен ее смелостью и кажущимся безрассудством. За всю свою карьеру я никогда специально не выводил из строя части производственной системы ради эксперимента. Мог сделать это по ошибке, но никогда не делал специально. Теперь я понимаю, что хаос-инженерия работает не совсем так, как мне представлялось тогда. Это, конечно, весьма дерзкий подход, но система, используемая компанией Netflix, уже довольно зрелая, поскольку ее DevOps-команды развивают данную практику с 2008 года. Эти эксперты многому научились за прошедшее время и не станут рекомендовать новичкам начинать с намеренного нарушения работы целых частей производственной системы. К этому следует подходить постепенно.

История развития хаос-инженерии

Хаос-инженерия зародилась в 2008 году в результате нескольких сбоев в работе сервисов Netflix [228]. В то время компания переходила от рассылки DVD по почте к потоковому вещанию. Руководство Netflix публично объявило о своем намерении отказаться от использования собственных центров обработки данных в пользу облачных сервисов AWS. Это была смелая идея, учитывая то, что компания Amazon развернула свой сервис всего двумя годами ранее и его еще нельзя было назвать вполне зрелым.

Первым событием, способствовавшим развитию хаос-инженерии, стал сбой в работе базы данных Netflix, из-за которого компания не могла доставить DVD своим клиентам на протяжении трех дней. Это событие со всей очевидностью свидетельствовало о недостаточной устойчивости (см. главу 5). Затем ближе к Рождеству 2008 года в работе AWS произошел масштабный сбой, из-за которого клиенты Netflix не смогли воспользоваться новым потоковым сервисом. В ответ на это в 2010-м инженеры Netflix разработали свой первый инструмент хаос-инженерии под названием Chaos Monkey, который помог им справиться с проблемой исчезающих экземпляров программной службы, вызванной сбоем в работе сервиса AWS. После этого успеха компания Netflix начала создавать собственную команду хаос-инженеров и задумалась над возможностью масштабирования этой практики. Если команде удалось решить проблему исчезающих экземпляров в малых масштабах, сможет ли она сделать то же самое в масштабах целого региона?

Справедливости ради стоит отметить, что Netflix была не единственной компанией, думающей в этом направлении. В 2006 году SRE-инженеры Google разработали собственную программу тестирования плана аварийного восстановления (disaster recovery testing, DiRT), предназначенную для того, чтобы намеренно вызывать сбои в работе внутренних систем и выявлять неизвестные риски. Однако название их программы (DiRT) было не таким запоминающимся, как у Netflix (Chaos Monkey), поэтому данное направление не получило развития, хотя идея была похожей [33].

К началу 2011 года компания Netflix начала добавлять новые модули, содержащие более полный набор функций обеспечения устойчивости. В конечном итоге эти модули стали известны как Netflix Simian Army. Помимо таких модулей, как Latency Monkey, Conformity Monkey и Doctor Monkey, в этот набор входит и ряд других.

В 2012 году компания Netflix опубликовала исходный код Chaos Monkey на GitHub, и в 2013-м другие организации начали экспериментировать с этой идеей. В 2014 году Netflix учредила должность хаос-инженера и начала работать над уменьшением радиуса поражения, наносимого запланированными сбоями. В 2016-м в Netflix уже существовала целая команда хаос-инженеров, работавших над проектом Simian Army. К тому времени с данной идеей экспериментировал целый ряд компаний, включая Capital One, Google, Slack, Microsoft и LinkedIn.

Какое отношение хаос-инженерия имеет к автоматизации и обеспечению устойчивости

Традиционно проведение линейных регрессионных тестов, деятельность команды SRE-инженеров и DevOps-специалистов, а также обеспечение устойчивости ИТ-систем относились к компетенции ИТ-директора. Однако в сфере обеспечения устойчивости существует определенное разделение труда. ИТ-директор отвечает за DevOps, а руководитель отдела безопасности (CSO) является частью команды. Однако я настаиваю на том, что хаос-инженерия должна находиться в ведении CSO. Кто может быстрее его обнаружить потенциальные и еще неизвестные системные сбои, которые могут повлиять на производство или способность быстро восстанавливаться после инцидента? ИТ-директор решает известные проблемы. С точки зрения первичных принципов кибербезопасности должностной обязанностью CSO должно быть обнаружение в системе неизвестных неисправностей, способных нанести существенный ущерб.

Как утверждают Райнхарт и Шортридж в книге *Security Chaos Engineering*, традиционные программы обеспечения безопасности ориентированы на то, чтобы избежать сбоев [202]. Команды ИБ-специалистов разрабатывают и внедряют в отношении людей, процессов и технологий политики, направленные на предотвращение катастрофы. Однако, по мнению авторов этой книги, именно на неудачах команда информационной безопасности учится лучше всего. Я с этим согласен. Проведение небольших экспериментов, направленных на выявление потенциальных системных сбоев, может быть самым ценным аспектом деятельности ИБ-специалистов.

По словам Райнхарта и Шортриджа, такой образ мышления смещает фокус команды информационной безопасности с чисто оборонительной позиции на создание адаптивной системы. Вместо того чтобы стремиться обеспечить совершенную защиту, следует осваивать навыки, позволяющие изящно устранять сбои. Этот подход очень близок к определению устойчивости, приведенному в главе 5. Он также подразумевает, что по крайней мере в указанных масштабах изящное устранение сбоев будет происходить на уровне инфраструктуры как кода.

Авторы рекомендуют ИБ-сообществу отказаться от театра безопасности (концепция которого была популяризована Брюсом Шнайером, одним из видных мыслителей в этой области) [85]. Согласно этой идее команды ИБ-специалистов выполняют работу, которая создает видимость повышения уровня безопасности, но на самом деле мало что дает. Примером может служить приобретение антифишингового продукта, который доставляет сотрудникам одобренные фишинговые электронные письма, чтобы научить их не переходить по опасным URL-ссылкам. Другой пример — создание программы для борьбы с внутренними угрозами, призванной не позволить сотрудникам взять с собой старые слайды PowerPoint при переходе на новое место работы. Являются ли подобные программы столь же значимыми, как обнаружение в системе организации неизвестных дефектов, способных привести к катастрофическому сбою? Над этим стоит задуматься.

Однако если говорить о традиционной безопасности, то Райнхарт и Шортридж предлагают применить концепцию хаос-инженерии, например, к деятельности «красных» команд (см. главу 4). Вместо того чтобы поручать этой команде поиск бреши в системе безопасности, мы можем сформулировать гипотезу о том, как организация должна реагировать на определенную последовательность атаки, допустим, Wicked Panda. Если мы будем относиться к учениям «красной» команды как к научному эксперименту с выдвижением гипотезы о том, как, по нашему мнению, организация будет реагировать на

атаку Wicked Panda, то можем узнать нечто новое. Если это произойдет, то можно распространить подобный образ мышления на такие традиционные задачи, как обеспечение безопасности контейнеров и CI/CD-конвейеров, мониторинг безопасности, реагирование на инциденты и т. д. Вы можете сказать, что уже занимаетесь всем этим. Однако я предлагаю перейти от примитивного тестирования системы с учетом того, о чем мы уже знаем, к использованию более продвинутого научного метода, направленного на выявление еще неизвестного.

Тем не менее хаос-инженерия — это не для всех. Она является еще одной тактикой, которую мы можем использовать для снижения вероятности нанесения нам существенного ущерба вследствие киберсобытия. Это еще одна стрела в нашем колчане для создания программы обеспечения устойчивости, дополняющая другие стрелы, такие как кризисное планирование, реагирование на инциденты, резервное копирование и шифрование. Эта концепция, вероятно, окажется недоступной для большинства малых и средних организаций, которые с трудом находят ресурсы на поддержание своей деятельности. Однако крупным компаниям Кремниевой долины, предоставляющим услуги по всему миру (таким как Netflix, Google, LinkedIn и т. п.), а также большинству компаний из списка Fortune 500 стоит присмотреться к хаос-инженерии. Вполне вероятно, что многие из этих компаний уже так и сделали.

Заключение

С самого начала компьютерной эры специалисты по безопасности отдавали реализацию стратегии автоматизации на откуп ИТ-сообществу. Разработчики ПО развивали свои философии, начиная с каскадного метода в 1950-х годах и заканчивая Agile-методологией в 2000-х и тактикой DevOps в 2010-х. Появление таких концепций, как нулевое доверие, убийственная цепочка, обеспечение устойчивости и прогнозирование рисков, способствовало эволюции сферы информационной безопасности, но она происходила параллельно, то есть в отрыве от эволюции ИТ-сообщества. Интересно то, что ИБ-специалисты обращаются к поставщикам и платформам для автоматизации отдельных компонентов инфраструктуры безопасности, не понимая того, что их системы столь же важны, как и ИТ-системы организации, и ими тоже следует управлять с помощью методологии DevOps. Существуют лучшие практики разработки безопасного кода в CI/CD-конвейере (OWASP, BSIMM и SAMM), но они не охватывают автоматизацию описанных в этой

книге стратегий и тактик, основанных на базовом принципе кибербезопасности. В данной главе я привел аргументы в пользу того, что ИБ-сообществу следует придерживаться этой стратегии.

Я также рассказал об особенностях концепции соответствия нормативным требованиям, которые заключаются в том, что данная практика не влияет на вероятность существенного ущерба вследствие киберсобытия, но может являться необходимым условием для ведения бизнеса с другой организацией. Далее я отметил, что вероятность получения штрафа за несоблюдение нормативных требований или подачи коллективного иска может оправдать вложение ресурсов в создание комплаенс-программы. Количество законов о соблюдении нормативных требований огромно и постоянно меняется, а универсального правила для прогнозирования соответствующего риска не существует. Используя метод анализа Ферми по схеме «извне внутрь», я показал, как специалист по безопасности в сфере здравоохранения может рассчитать потенциальный риск, однако эти расчеты во многом зависят от размера организации, страны и отрасли, в которой она работает.

В заключение я рассказал об относительно новой продвинутой технике обеспечения устойчивости с помощью автоматизации — хаос-инженерии, которую, скорее всего, будут использовать только зрелые организации с достаточным количеством ресурсов. Тем не менее идеи, связанные с разработкой гипотез и тестированием систем для их проверки, можно использовать и при реализации других тактик, основанных на базовом принципе кибербезопасности, в частности, в рамках учений «красной» команды.

Автоматизация — это важнейшая стратегия, базирующаяся на первичном принципе, которая пронизывает все остальные (см. дорожную карту во введении), и на это есть причина. Как профессионалы в области безопасности, мы можем реализовать не все тактики, предусмотренные каждой из таких стратегий, но те, которые мы реализуем, следует в максимальной степени автоматизировать, чтобы избавиться от выполняемых вручную задач, грозящих ошибками.

08 Подведение итогов

Если вы не любите горох, то это, скорее всего, потому, что вы не пробовали его в свежем виде. Это сродни разнице между чтением отличной книги и ознакомлением с аннотацией на задней обложке.

Лемони Сникет

Подведем итоги: люди — это проблема.

Дуглас Адамс

Написание длинных книг — это трудоемкий и обедняющий акт безрассудства: зачем разворачивать на 500 страницах идею, которую можно объяснить за несколько минут. Гораздо лучше представить, что такие книги уже существуют, и предложить их краткое изложение или комментарий к ним.

Хорхе Луис Борхес

Обзор главы

Эта книга подытоживает мой 30-летний опыт работы в сфере кибербезопасности. Я появился на этой сцене как раз в тот момент, когда Интернет начали использовать деловые, государственные и научные круги. Можно сказать, что я был там с самого начала. Нынешний подход к обеспечению кибербезопасности во многом обусловлен тем, что я и мои коллеги по отрасли узнавали в процессе своей работы. Мы добились значительных успехов, а также совершили несколько крупных ошибок, без которых, впрочем, не обходится ни одно

великое приключение. Большинство ошибок со временем исправляется благодаря триаде «люди, процессы и технологии», когда мы находим новые и более эффективные способы решения определенных задач или понимаем, что метод, который использовался ранее, на самом деле не работает. Ошибка, которую мы еще не исправили, заключается в отсутствии консенсуса относительно сути прикладываемых нами усилий. В сообществе бытует мнение, что если спросить 100 специалистов по безопасности о назначении создаваемых ими ИБ-программ, то можно получить 100 разных ответов. Как правило, они представляют собой некую версию или комбинацию таких идей, как:

- реализация триады КЦД;
- исправление ошибок во всех программах;
- предотвращение установки вредоносного ПО;
- реагирование на инциденты;
- соблюдение правил, предусмотренных фреймворками безопасности;
- соблюдение нормативных требований.

Это вполне достойные тактики, которых вы можете придерживаться, но они не отвечают на самый важный вопрос. Если руководство или совет директоров компании спросит, в чем заключается суть вашей стратегии кибербезопасности и почему, то, назвав в качестве ответа любую из этих тактик, вы, скорее всего, не получите приглашения на следующее заседание. Они не имеют непосредственного отношения к бизнесу, а для их описания используется непривычный для руководителей лексикон. Еще более важно то, что они не доходят до сути вопроса.

По поводу каждого из перечисленных пунктов опытный ИБ-специалист может спросить: «А как насчет?..» Например, реализация триады КЦД — это замечательно, но как насчет онлайн-меню кафетерия? Неужели оно настолько важно для того, чтобы защищать его с помощью этой триады? Устранение ошибок полезно, но как насчет вредоносного ПО? Предотвращение установки вредоносного ПО очень желательно, но как быть с перемещением злоумышленников по сети организации? Реагирование на инциденты важно, но как насчет предотвращения взломов? Фреймворки представляют собой хорошие контрольные списки, но как насчет обеспечения соответствия нормативным требованиям? Соблюдение требований необходимо, но как быть с триадой КЦД, внесением исправлений, защитой от вредоносного ПО и реагированием на инциденты? Очевидно, нам необходима более фундаментальная стратегия, отражающая суть причин, по которым мы занимаемся безопасностью. А значит, следует вернуться к базовым принципам.

Концепция научных базовых принципов возникла еще во времена Аристотеля. Такие великие мыслители, как Евклид, Декарт, Уайтхед, Рассел и Илон Маск, понимали, что для решения сложной проблемы ее необходимо свести к изначальной сути. Евклид свел геометрию к простым постулатам. Декарт свел «Начала философии» к фразе «Я мыслю, следовательно, я существую». Уайтхед и Рассел написали 80 страниц для того, чтобы математически доказать справедливость равенства 1 + 1 = 2. Маск переосмыслил саму природу орбитальных космических полетов. Если эти лидеры мысли смогли сделать это для своих областей знаний, не разумно ли предположить, что ИБ-сообществу тоже стоит попробовать?

Итак, абсолютный базовый принцип кибербезопасности сводится к тому, чтобы **снизить вероятность существенного ущерба в результате киберинцидента в течение следующих трех лет**. Это нередуцируемый принцип. Ни один из ИБ-специалистов не может спросить: «А как насчет?..» — потому что реализация триады КЦД, внесение исправлений, защита от вредоносного ПО, реагирование на инциденты, использование фреймворков безопасности и обеспечение соответствия нормативным требованиям прекрасно вписываются в эту универсальную стратегию, никак не зависящую от размера и целей конкретной организации.

Как и в других областях, атомарный первичный принцип кибербезопасности представляет собой всеобъемлющую стратегию. Четко поняв, что нужно делать, мы можем логически вывести из него множество более мелких стратегий, определяющих, как мы должны при этом действовать.

- **Нулевое доверие.** Уменьшите поверхность атаки, предоставив доступ и разрешения только тем людям, устройствам и программам, которым они абсолютно необходимы для обеспечения функционирования бизнеса в соответствии с пожеланиями руководства.
- **Предотвращение реализации убийственной цепочки вторжения (kill chain).** Разработайте и разверните средства обнаружения всех известных вражеских кампаний и защиты от них.
- **Обеспечение устойчивости.** Во время и после катастрофического события продолжайте выполнять заявленные организацией обязательства так, как будто ничего не произошло.
- **Прогнозирование рисков.** Определяйте вероятность существенного ущерба вследствие киберинцидента с точностью, достаточной для того, чтобы руководители могли принимать взвешенные решения о выделении ресурсов на обеспечение кибербезопасности.

- **Автоматизация.** Сократите количество однотипных и выполняемых вручную задач, являющихся неотъемлемой частью процесса реализации стратегий, базирующихся на первичном принципе.

Эти стратегии вполне понятны. Когда все мы соглашаемся с тем, что главный принцип заключается в снижении вероятности существенного ущерба, из него логически вытекают конкретные шаги, позволяющие достичь поставленной цели благодаря разбиению большой задачи на более мелкие и легко решаемые. При этом выбор тактик для реализации каждой из стратегий весьма велик.

Нулевое доверие

- **Базовая реализация стратегии нулевого доверия.** Нулевое доверие — это путь, который можно начать с использования уже имеющихся систем.
- **Логическая и микросегментация.** Создавайте правила доступа, привязанные к конкретным людям, устройствам и программным приложениям.
- **Управление уязвимостями.** Непрерывный мониторинг всех программных активов — контроль версий, проверка вложенных библиотек пакетов с открытым исходным кодом, текущей конфигурации, истории доступа и подверженности вновь обнаруженным уязвимостям и эксплойтам.
- **Использование спецификаций программного обеспечения (SBOM).** Ведите формальную запись, содержащую сведения о различных компонентах, используемых при создании ПО, и о взаимосвязях между ними в цепочке поставок.
- **Управление идентификацией и доступом (IAM).** Реализуйте управление идентификационными данными (IGA), идентификацией привилегированных пользователей (PIM) и привилегированным доступом (PAM), а также их администрирование.
- **Технология единого входа.** Позвольте пользователям и приложениям авторизоваться один раз, предоставив свои данные доверенному источнику, чтобы больше не приходилось запоминать и вводить пароли.
- **Многофакторная аутентификация.** Используйте два или три фактора для проверки личности пользователя: то, что у него есть, например смартфон, то, что является его биометрическим параметром, например отпечаток пальца, или то, что он знает, например пароль.
- **Программно-определяемый периметр.** Перенесите функцию IAM подальше от существенных систем, которые вы пытаетесь защитить.

Предотвращение реализации убийственной цепочки вторжения

- **Разведка киберугроз.** Задействуйте жизненный цикл разведки для выяснения требований к существенной информации и преобразуйте эти сведения в продукты разведки, применяемые для принятия решений и обнаружения известных кампаний противника.
- **Обмен разведданными.** Налаживайте связи с коллегами-единомышленниками для обмена информацией (в рамках ISAC и ISAO).
- **Оркестрация стека безопасности.** Автоматизируйте процесс сбора информации о действиях противника на всех этапах убийственной цепочки, а также процесс развертывания средств обнаружения и предотвращения вторжений в уже существующем стеке безопасности.
- **Создание SOC-центров.** По мере расширения возможностей организации создайте собственный или привлеките сторонний SOC-центр для управления рабочим процессом и статусом различных групп и функций с целью координации их совместных действий.
- **Операции «красной»/«синей»/«фиолетовой» команды.** Поручите своей «красной» команде эмулировать атаки противника на ваши острова данных, а SOC-центру («синей» команде) — оттачивать навыки реагирования на соответствующие инциденты.

Обеспечение устойчивости

- **Преодоление кризисов.** Разрабатывайте планы с учетом желаемых результатов. Регулярно обсуждайте различные сценарии с людьми, принимающими решения. Если во время реального события реализация плана пойдет наперекосяк, сосредоточьтесь на желаемых результатах.
- **Резервное копирование и восстановление данных.** Создавайте копии всех существенных данных и, что более важно, регулярно практикуйте их восстановление.
- **Шифрование данных.** Шифруйте все существенные данные, находящиеся как в состоянии покоя, так и в движении.
- **Системы обеспечения устойчивости значимы сами по себе.** Системы резервного копирования, восстановления и шифрования данных должны быть защищены с помощью тех же базирующихся на первичных принципах стратегий и тактик, что и другие важные системы.

- **Реагирование на инциденты.** Отслеживайте и расследуйте кибersобытия в рамках SOC-центра, пока вам не станет очевидно, что это настоящие киберинциденты. На этом этапе следует приступить к реализации антикризисного плана, чтобы начать использовать дополнительные ресурсы организации.

Прогнозирование рисков

- **Теорема Байеса.** Выполните первоначальную оценку вероятности нанесения вам существенного ущерба в результате киберинцидента на основе имеющейся информации. По мере сбора дополнительных данных корректируйте эту оценку в бóльшую или меньшую сторону.
- **Суперпрогнозирование.** Вероятность представляет собой меру вашей уверенности. Проведите анализ по схеме «извне внутрь» с целью составления прогноза для общего случая. Скорректируйте первоначальный прогноз, проведя анализ по схеме «изнутри наружу», то есть с учетом того, насколько хорошо ваша организация придерживается стратегий, базирующихся на первичном принципе кибербезопасности.
- **Оценки Ферми.** Для принятия решений о выделении ресурсов на обеспечение кибербезопасности достаточно выполнить приблизительные расчеты, используя методы суперпрогнозирования.

Автоматизация

- **Методология DevSecOps.** Перенимайте методы из арсенала DevOps-специалистов для автоматизации процесса применения тактик, базирующихся на первичном принципе кибербезопасности.
- **Обеспечение соответствия нормативным требованиям.** Если ваша организация нуждается в разрешении на ведение бизнеса или может подвергнуться крупным штрафам и взысканиям за несоблюдение нормативных требований, то, скорее всего, у нее уже есть специальная система для отслеживания прогресса в этом направлении и создания соответствующей отчетности. Такие системы не повышают уровень безопасности организации, однако все, что они собой представляют, должно быть увязано с развернутыми тактиками, основанными на базовом принципе кибербезопасности.
- **Хаос-инженерия.** Хаос-инженерия практикуется в основном крупными компаниями и предполагает использование научного метода для обнаружения неизвестных системных недостатков, которые могут не позволить организации пережить катастрофический сбой.

Заключение

Хочу еще раз подчеркнуть, что я не призываю всех сетевых защитников в равной степени реализовывать описанные стратегии и тактики, базирующиеся на первичном принципе кибербезопасности. Все организации разные. То, что может дать наибольший эффект с учетом таких имеющихся в вашем распоряжении ресурсов, как люди, процессы и технологии, сильно зависит от размера организации. Дело в том, что реализация многих из описанных в этой книге стратегий обходится недешево. Вы должны сопоставить потенциальное снижение вероятности нанесения вам существенного ущерба с допустимым уровнем риска и потенциальными затратами на развертывание и поддержание этих стратегий. Например, крупная компания из списка Fortune 500 вполне может позволить себе внедрить такие стратегии, как нулевое доверие, предотвращение реализации убийственной цепочки вторжения и автоматизация. В то же время для стартапа, находящегося на ранней стадии развития, обеспечение устойчивости, вероятно, обойдется дешевле всего и окажет наибольшее влияние на снижение вероятности существенного ущерба в результате киберинцидента.

Суть в том, что реализовывать эти стратегии стоит, если на то есть причины. Каждая из них способна снизить вероятность существенного ущерба вследствие киберсобытия. Умение измерять степень этого воздействия (прогнозирование рисков) — важнейший навык для всех ИБ-специалистов, особенно для руководителей высшего звена, отвечающих за кибербезопасность. Освоение данного навыка позволит им выбрать наиболее эффективные стратегии и тактики, подходящие для их организации.

Итак, мы рассмотрели все инструменты, необходимые для разработки, создания и совершенствования программы обеспечения кибербезопасности, основанной на образе мышления, базирующемся на первичном принципе кибербезопасности. Теперь можете приступить к снижению вероятности нанесения вам существенного ущерба вследствие киберинцидента. В ходе этого процесса можете время от времени связываться со мной и сообщать о своих успехах (rick.howard@theCyberWire.com).

Рекомендованная литература

1. *Abandy R.* 2022. The History of Microsoft Azure [WWW Document]. Techcommunity. Microsoft.com. techcommunity.microsoft.com/t5/educator-developer-blog/the-history-of-microsoft-azure/ba-p/3574204 (доступ получен 18.12.2022).
2. About FIRST [WWW Document], n. d. FIRST — Forum of Incident Response and Security Teams. www.first.org/about (доступ получен 01.11.2022).
3. *Action I.* 2012. Psychology In Action [online]. Psychology In Action. www.psychologyinaction.org/psychology-in-action-1/2012/10/22/bayes-rule-and-bomb-threats (доступ получен 30.10.2022).
4. *Adam S. S. A.* 2022. The State of Ransomware 2022 [WWW Document]. Sophos News. news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022 (доступ получен 18.12.2022).
5. *Adams J. S.* 2014. The Ban and the Bit: Alan Turing, Claude Shannon, and the Entropy Measure [WWW Document]. thejunglejane. thejunglejane.com/writing/the-ban-and-the-bit-alan-turing-claude-shannon-and-the-entropy-measure (доступ получен 09.11.2022).
6. *Allen D.* 1997. EUCLID, The Elements [WWW Document]. Texas A&M University. www.math.tamu.edu/~dallen/history/euclid/euclid.html (доступ получен 29.10.2022).
7. *Allspaw J., Hammond P.* 2009. Velocity 09: 10+ Deploys Pe. YouTube.
8. *Anderson J. P.* 1972. Computer Security Technology Planning Study (Volume I). Electronics System Division 1.
9. *Andress J., Winterfeld S.* 2011. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier.
10. APT1: Exposing One of China's Cyber Espionage Units | Mandiant. Mandiant.com, 2013.
11. *Archer B.* 1996. Health Insurance Portability and Accountability Act.
12. *Aristotle.* 1996. Physics. Oxford University Press, USA.
13. *Aristotle.* 1999. Encyclopedia Britannica.
14. *Aristotle.* 2009. Physics. Neeland Media.
15. Army, T.U.S., 2007. Army Field Manual FM 2-0 (Intelligence). Digireads.Com.
16. *Arnold C.* 2017. Equifax CEO Richard Smith Resigns After Backlash Over Massive Data Breach. NPR.
17. ASIS International, 2009. Organizational Resilience: Security, Preparedness, and Continuity Management Systems. — Requirements with Guidance for Use, ASIS SPC.1-2009.
18. *Attia P.* 2020b. The importance of red teams. Peter Attia. peterattiamd.com/the-importance-of-red-teams (доступ получен 17.12.2022).
19. *Baker P.* 2021. The SolarWinds hack timeline: Who knew what, and when? [WWW Document]. CSO Online. www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html (доступ получен 17.12.2022).

20. *Baker W., Pendergrast A.* 2020. Diamond Presentation v2 0: Diamond Model for Intrusion Analysis — Applied to Star Wars' Battles. YouTube.
21. *Bakis B., Wang E.* 2017. Building a National Cyber Information-Sharing Ecosystem. Mitre.
22. *Bals F.* 2022. 2022 OSSRA discovers 88 percent of organizations still behind in keeping open source updated [WWW Document]. Synopsys. www.synopsys.com/blogs/software-security/open-source-trends-ossra-report (доступ получен 16.12.2022).
23. *Barrett M. P.* 2018. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 [WWW Document]. NIST. www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (доступ получен 18.12.2022).
24. *Bayes T.* 1763. LII. An essay towards solving a problem in the doctrine of chances. By the late Rev. Mr. Bayes, F. R. S. communicated by Mr. Price, in a letter to John Canton, A. M. F. R. S [WWW Document]. royalsocietypublishing.org/doi/epdf/10.1098/rstl.1763.0053.
25. *Bejtlich R.* 2014. A Brief History of Network Security Monitoring. Blogger. taosecurity.blogspot.com/2014/09/a-brief-history-of-network-security.html (доступ получен 17.12.2022).
26. *Bell D., LaPadula L.* 1973. Secure Computer Systems: Mathematical Foundations. Mitre.
27. *Bell S.* 2011. Lessons From the RSA Breach [WWW Document]. CSO Online. www.csoonline.com/article/2129794/lessons-from-the-rsa-breach.html (доступ получен 04.12.2022).
28. *Belludi N.* 2017. The Fermi Rule: Better be Approximately Right than Precisely Wrong [WWW Document]. Right Attitudes. www.rightattitudes.com/2017/08/28/the-fermi-rule-guesstimation (доступ получен 09.11.2022).
29. Ben, 2010. CIA Triad [WWW Document]. ElectricFork. blog.electricfork.com/2010/03/cia-triad.html (доступ получен 29.10.2022).
30. *Benington H. D.* 1983. Production of Large Computer Programs. Annals of the History of Computing 5. P. 350–361. https://doi.org/10.1109/MAHC.1983.10102.
31. *Bissell M.* 2017. What is SSO. YouTube.
32. *Björck F., Henkel M., Stirna J., Zdravkovic J.* 2015. Cyber Resilience — Fundamentals for a Definition, New Contributions in Information Systems and Technologies. Springer International Publishing, Cham.
33. *Bort J.* 2016. Meet Kripa Krishnan, Google's queen of chaos. Insider.
34. *Branstad D. K.* 1987. Considerations for security in the OSI architecture. IEEE Network 1. P. 34–39. doi.org/10.1109/mnet.1987.6434189.
35. *Braun B.* 2011. Fermi Estimations [WWW Document]. BryanBraun. www.bryanbraun.com/2011/12/04/fermi-estimations (доступ получен 09.11.2022).
36. *Broeckelmann R.* 2017. SAML2 vs JWT: Understanding OpenID Connect Part 1 — Robert Broeckelmann. Medium.
37. *Broeckelmann R.* 2018. Kerberos and Windows Security: History. Medium.
38. *Broeckelmann R.* 2019. SAML2 vs JWT: Understanding OAuth2 — Robert Broeckelmann. Medium.
39. *Caltagirone S., Pendergast A., Betz C.* 2011. The Diamond Model of Intrusion Analysis. Center for Cyber Threat Intelligence and Threat Research.
40. *Cameron K.* 2005. The Laws of Identity, Kim Cameron's Identity Weblog.
41. *Cannon D.* 2022. What happened to Equifax after the data breach? [WWW Document]. Rice-Properties. rice-properties.com/qa/what-happened-to-equifax-after-the-data-breach.html (доступ получен 18.12.2022).

42. *Carlson M.* 2020. The Joke [WWW Document]. Carnegie Hall. www.carnegiehall.org/Explore/Articles/2020/04/10/The-Joke (доступ получен 18.12.2022).
43. *Cawthra J., Ekstrom M., Lusty L., Sexton J., Sweetnam J.* 2020. NIST Special Publication 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. National Institute of Standards and Technology (NIST).
44. *Cerf V.* 2000. Vint Cerf on Cyber Hygiene at the Joint Economic Committee.
45. *Chandola T.* 2017. Compliant, Yet Breached. ISACA Journal 5.
46. *Cichonski P., Millar T., Grance T., Scarfone K.* (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology [Online]. doi:10.6028/nist.sp.800-61r2.
47. CISA, n. d. Information Sharing and Awareness [WWW Document]. www.cisa.gov/information-sharing-and-awareness (доступ получен 01.11.2022).
48. Cisco, 2002. Evolution of the Firewall Industry [Online]. docstore.mik.ua/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm (доступ получен в 2022 г.).
49. *Clarke R. A., Knake R.* 2012. Cyber War: The Next Threat to National Security and What to Do About It. Ecco.
50. *Clinton B.* 1998. Presidential Decision Directive/NSC-63 [WWW Document]. White House. irp.fas.org/offdocs/pdd/pdd-63.htm (доступ получен 17.12.2022).
51. *Cohen F.* 1989. Models of practical defenses against computer viruses. Computers & Security 8. P. 149–160. doi.org/10.1016/0167-4048(89)90070-9.
52. *Cohen F.* 1992. [PDF] Defense-in-depth against computer viruses. Computers and Security 11. P. 563–579.
53. *Cohen F.* 2016. Defense in Depth.
54. *Collier K.* 2021. FBI tracking more than 100 active ransomware groups. NBC News.
55. *Collins S.* 2004. Intelligence Reform and Terrorism Prevention Act.
56. *Contributor Q.* 2015. Does Elon Musk's «First Principles» Learning Style Work? Slate.
57. *Copeland P. J.* 2012b. Alan Turing: The codebreaker who saved «millions of lives» [WWW Document]. BBC News. www.bbc.com/news/technology-18419691 (доступ получен 18.12.2022).
58. *Crews C. W. Jr.* 2017b. How Many Federal Agencies Exist? We Can't Drain The Swamp Until We Know. Forbes.
59. *Curphey M.* 2014. The Start of OWASP — A True Story [WWW Document]. Veracode. www.veracode.com/blog/intro-appsec/start-owasp-true-story (доступ получен 18.12.2022).
60. Custom Breach Search [WWW Document], n. d. Identity Theft resource Center. notified.idtheftcenter.org/s/resource#annualReportSection (доступ получен 29.10.2022).
61. Cyberspace Solarium Commission [WWW Document], n. d. www.solarium.gov (доступ получен 18.12.2022).
62. *Daragiu A.* 2019. A review of the evolution of multifactor authentication (MFA) [WWW Document]. Typing. blog.typingdna.com/evolution-of-multi-factor-authentication/.
63. *Denning D. E.* (1986). «An Intrusion Detection Model». Proceedings of the Seventh IEEE Symposium on Security and Privacy. P. 119–131. users.ece.cmu.edu/~adrian/731-sp04/readings/denning-ids.pdf.
64. *Dennis R.* 1966. Security In The Computing Environment. System Development Corporation for the Defense Documentation Center Defence Supply Agency.
65. Department of Defense, 1985. Trusted Computer System Evaluation Criteria [Orange Book].

66. *Descartes R.* 1644a. Principles of Philosophy (Principia Philosophiae): With A Special Introduction. Amazon Kindle.
67. *Descartes R.* 1644b. Principia philosophiae. Google Books.
68. *Dijkstra E. W.* Archive, 1972. The Humble Programmer [WWW Document]. University of Texas at Austin, Computer Science, College of Natural Resources. www.cs.utexas.edu/~EWD/transcriptions/EWD03xx/EWD340.html (доступ получен 06.02.2023).
69. Dod, 2021. DOD Enterprise DevSecOps — Pathway to a Reference Design, DOD Cyber Exchange. Department of Defense.
70. *Douglas J.* 2022. Best practices for a secure software supply chain [WWW Document]. Microsoft Learn. learn.microsoft.com/en-us/nuget/concepts/security-best-practices (доступ получен 16.12.2022).
71. *Easterbrook G.* 2007. The Black Swan: The Impact of the Highly Improbable — Nassim Nicholas Taleb — Books — Review [WWW Document]. The New York Times. www.nytimes.com/2007/04/22/books/review/Easterbrook.t.html (доступ получен 18.12.2022).
72. Editor, 2019. Security Administrator Tool for Analyzing Networks (SATAN). Network Encyclopedia. networkencyclopedia.com/security-administrator-tool-for-analyzing-networks-satan (доступ получен 16.12.2022).
73. *Emmerig J.* 2019. Data Breach Class Actions in Australia. Jones Day.
74. *Engelbrecht S.* 2018. The Evolution of SOAR Platforms [WWW Document]. SecurityWeek.Com. www.securityweek.com/evolution-soar-platforms (доступ получен 17.12.2022).
75. *Euclides*, 2008. Euclid's elements of geometry.
76. *Eylenburg A.* n. d. Operating Systems: Market Shares since the 1970s [WWW Document]. eylenburg. eylenburg.github.io/os_marketshare.htm (доступ получен 18.12.2022).
77. *Fazzini K.* 2019. The great Equifax mystery: 17 months later, the stolen data has never been found, and experts are starting to suspect a spy scheme. CNBC.
78. *Fenn J., Raskino M.* 2008. Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time. Harvard Business Press.
79. *Finnane T.* 2021. Panaseer 2022 Security Leaders Peer Report [WWW Document]. Panaseer. panaseer.com/reports-papers/report/2022-security-leaders-peer-report (доступ получен 04.11.2022).
80. *Fowler B.* 2022. Data breaches break record in 2021. CNET.
81. *Freund J., Jones J.* 2014. Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann.
82. *Fruhlinger J.* 2020. The CIA triad: Definition, components and examples [WWW Document]. CSO Online. www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html (доступ получен 29.10.2022).
83. *Fruhlinger J.* 2022. PCI DSS explained: Requirements, fines, and steps to compliance [WWW Document]. CSO Online. www.csoonline.com/article/3566072/pci-dss-explained-requirements-fines-and-steps-to-compliance.html (доступ получен 04.12.2022).
84. *Gabel C.* 2020. Intelligence Operations. Scholastic.
85. *Glaskowsky P.* 2008. Bruce Schneier's new view on Security Theater. CNET.
86. *Glass M. n. d.* Fusion Center History [WWW Document]. Florida Department of Law Enforcement. www.fdle.state.fl.us/FFC/FFC/ FusionCenterHistory (доступ получен 01.11.2022).
87. *Glass R. R., Davidson P. B.* 1948. Intelligence is for Commanders. Military Service Publishing.

88. *Good I. J.* 2011. A List of Properties of Bayes-Turing Factors. NSA FOIA Case #58820.
89. *Goodwin L.* 2022. Celebrating 20 Years of Trustworthy Computing [WWW Document]. Microsoft Security Blog. www.microsoft.com/en-us/security/blog/2022/01/21/celebrating-20-years-of-trustworthy-computing (доступ получен 18.12.2022).
90. *Grassi P. A., Garcia M. E., Fenton J. L.* 2017. Digital identity guidelines: revision 3. National Institute of Standards and Technology, Gaithersburg, MD.
91. *Greenberg A.* 2020b. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Anchor.
92. *Greenberg A.* 2021b. The Full Story of the Stunning RSA Hack Can Finally Be Told [WWW Document]. WIRED. www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told (доступ получен 18.12.2022).
93. *Greig J.* 2021. With 18,378 vulnerabilities reported in 2021, NIST records fifth straight year of record numbers. ZDNET.
94. *Greig J.* 2021b. Chinese regulators suspend Alibaba Cloud over failure to report Log4j vulnerability. ZDNET.
95. *Hale M.* 2017. Introduction to Cybersecurity First Principles. nebraska-gencyber-modules [WWW Document]. Nebraska-Gencyber-Modules. mlhale.github.io/nebraska-gencyber-modules/intro_to_first_principles/README (доступ получен 29.10.2022).
96. *Halton C.* 2022. The Truth About Y2K: What Did and Didn't Happen in the Year 2000. Investopedia.
97. *Hartson R., Pyla P. S.* 2018. The UX Book: Designing a Quality User Experience. Morgan Kaufmann.
98. *Haworth S.* 2021. RACI Chart Template For Project Managers + Example; How-To [WWW Document]. The Digital Project Manager. thedigitalprojectmanager.com/projects/leadership-team-management/raci-chart-made-simple (доступ получен 13.11.2022).
99. *Hebert A.* 2008. Compressing the Kill Chain [WWW Document]. Air & Space Forces Magazine. www.airandspaceforces.com/article/0303killchain (доступ получен 17.12.2022).
100. *Hern A.* 2014. How did the Enigma machine work? The Guardian. Source: to, C. (2004). Wikimedia project page [Online]. Wikimedia.org.
101. *Herschmann J.* 2021. Hype Cycle for Agile and DevOps, 2021. Linked In.
102. *Higgins K. J.* 2008. Who Invented the Firewall? [Online]. www.darkreading.com/analytics/who-invented-the-firewall- (доступ получен в 2022 г.).
103. *Hill M.* 2022. The Apache Log4j vulnerabilities: A timeline [WWW Document]. CSO Online. www.csoonline.com/article/3645431/the-apache-log4j-vulnerabilities-a-timeline.html (доступ получен 16.12.2022).
104. *Hoffman C.* 2017. The Different Forms of Two-Factor Authentication: SMS, Authenticator Apps, and More [WWW Document]. How-To Geek. www.howtogeek.com/232598/5-different-two-step-authentication-methods-to-secure-your-online-accounts/.
105. *Holseberg K.* 2022. Our Sharing Model [WWW Document]. Cyber Threat Alliance. cyberthreatalliance.org/about/our-sharing-model (доступ получен 01.11.2022).
106. *Howard R.* 2020b. Identity management around the Hash Table, with Rick Howard, Helen Patton, Suzie Smibert, and Rick Doten. The CyberWire.
107. *Howard R.* 2021. Why it's time for cybersecurity to go mainstream. The CyberWire.
108. *Howard R.* 2021i. XDR Explainer Interview with Jon Oltsik. The CyberWire.
109. *Howard R. A., Abbas A. E.* 2015. Foundations of Decision Analysis. Pearson College Division.

110. *Howard R., Anderson D., Weiss E., Collie B.* 2022. Intelligence sharing: A Rick the Toolman episode. The CyberWire.
111. *Howard R., Berlin C.* 2020b. National SIGINT Operations Center (NSOC).
112. *Howard R., Lipner S.* 2022. Обсуждение истории создания концепции триады КЦД.
113. *Howard R., Olson R.* 2020. Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks. The Cyber Defense Review 4.
114. *Howard R., Pethia R.* 2020b. CERT/CC helping the military build their own CERTS.
115. *Hutchins E. M., Cloppert M. J., Amin R. M.* 2010. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation.
116. Illumio, 2015. The Firewall, a Brief History of Network Security [Online]. www.illumio.com/blog/firewall-network-security (доступ получен в 2022 г.).
117. *Ingalls S.* 2021. SBOMs: Securing the Software Supply Chain [WWW Document]. eSecurityPlanet. www.esecurityplanet.com/compliance/sbom (доступ получен 17.12.2022).
118. *Inman N. n. d.* Global Regulatory Outlook 2021: The Future of Global Financial Regulation [WWW Document]. Kroll. www.kroll.com/en/insights/publications/financial-compliance-regulation/global-regulatory-outlook-2021 (доступ получен 04.12.2022).
119. Introduction to STIX [WWW Document], n. d. Oasis. oasis-open.github.io/cti-documentation/stix/intro (доступ получен 02.11.2022).
120. *Irvine A. D.* 1995. Russell's Paradox [WWW Document]. Stanford Encyclopedia of Philosophy. plato.stanford.edu/entries/russell-paradox (доступ получен 29.10.2022).
121. *Irwin L.* 2022. List of data breaches and cyber attacks in February 2022 [WWW Document]. IT Governance UK Blog. www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2022-5-1-million-records-breached (доступ получен 29.10.2022).
122. *Irwin T., Irwin T. H.* 1990. Aristotle's First Principles. Oxford University Press.
123. *Janis I. L.* 1972. Victims of Groupthink: A Psychological Study of Foreign-policy Decisions and Fiascoes. Houghton Mifflin.
124. *Jaquith A.* 2007. Security Metrics. Pearson Education.
125. Javatpoint. History of AWS [WWW Document]. www.javatpoint.com/history-of-aws (доступ получен 01.11.2022).
126. *Juma A.* 2017. Aristotle and the Importance of First Principles — The Startup — Medium. The Startup.
127. *Kaplan W.* 2017b. Why Dissent Matters: Because Some People See Things the Rest of Us Miss. McGill-Queen's Press — MQUP.
128. *Kautz F.* 2021. What is VEX? It's the Vulnerability Exploitability eXchange! [WWW Document]. zt.dev.zt.dev/posts/what-is-vex (доступ получен 17.12.2022).
129. *Kelly M.* 2019. Google will pay $170 million for YouTube's child privacy violations. The Verge.
130. *Kemp J.* 2010. LDAP and Kerberos, So Happy Together. ServerWatch.
131. *Kenton W.* 2022. What Is the International Organization for Standardization (ISO)? Investopedia.
132. *Kerr O.* 2015. Edward Snowden's impact. The Washington Post.
133. *Kindervag J.* 2010. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. Forrester.
134. *Klemm F.* 1964. A History of Western Technology. MIT Press.

135. *Kruszewski D.* 2021. Understanding Vulnerability Exploitability eXchange (VEX). aDolus Technology.
136. *Kruszewski D.* 2021. What is VEX and What Does it Have to Do with SBOMs? [WWW Document]. Adolus. blog.adolus.com/what-is-vex-and-what-does-it-have-to-do-with-sboms (доступ получен 17.12.2022).
137. *Krutikov A.* 2021. Back to School: History of Software Development Methodologies [WWW Document]. Qulix. www.qulix.com/about/blog/history-of-software-development-methodologies (доступ получен 18.12.2022).
138. *Lawler R.* 2021. Amazon fined record $887 million over EU privacy violations. The Verge.
139. *Levy S.* 2001. Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age. National Geographic Books.
140. *Lewis D.* 2006b. Identity 2.0 Keynote. YouTube.
141. *Lipner S.* 1982. Non-Discretionary Controls for Commercial Applications. Proceedings of the 1982 IEEE Symposium Security and Privacy.
142. *Liulevicius V. G.* 2011. Espionage and Covert Operations: A Global History. The Great Courses.
143. *Lloyd E.* 2018. Devil's Advocate — Ancient Phrase Traced To The Roman Catholic Church [WWW Document]. Ancient Pages. www.ancientpages.com/2018/11/19/devils-advocate-ancient-phrase-traced-to-the-roman-catholic-church (доступ получен 01.11.2022).
144. *Luhmann N.* 2018. Trust and Power. John Wiley & Sons.
145. *Luiijf E., Kernkam A.* 2015. Sharing Cyber Security Information — Good Practice Stemming from the Dutch Public-Private Approach, Global Conference on Cyberspace 2015.
146. *Luke C. B. K.* 2012. Recognizing and Adapting To Unrestricted Warfare Practices by China. Air War College.
147. *Lutkevich B.* 2021. identity provider. TechTarget.
148. *Lynn R.* 2018. The History of Agile [WWW Document]. Planview. www.planview.com/resources/guide/agile-methodologies-a-beginners-guide/history-of-agile (доступ получен 18.12.2022).
149. *Mahdi D., Lowans B.* 2020. Gartner Report: Develop an Enterprisewide Encryption Key Management Strategy or Lose the Data, Fortanix.
150. Mandiant, 2021. APT1: Exposing One of China's CyberEspionage Units. YouTube.
151. *Mann D. E., Christey S. M.* 1999. CVE — Towards a Common Enumeration of Vulnerabilities [WWW Document]. CVE. cve.mitre.org/docs/docs-2000/cerias.html (доступ получен 06.11.2022).
152. *Marchuk V.* 2022. Free zero-day vulnerability tracking service — zero-day.cz [WWW Document]. Zer0-Day. www.zero-day.cz (доступ получен 29.10.2022).
153. Materiality definition: the ultimate guide [WWW Document], n. d. Datamaran. www.datamaran.com/materiality-definition (доступ получен 29.10.2022).
154. *McCaul M.* 2018. Cybersecurity and Infrastructure Security Agency Act.
155. *McGlone P.* 2022. Operational Resilience Framework (ORF) Released for Public Comment — GRF. GRF.
156. *McGrayne S. B.* 2011. The Theory That Would Not Die [WWW Document]. Google. www.youtube.com/watch?v=8oD6eBkjF9o (доступ получен 09.11.2022).
157. *McMillan R.* 2012. The World's First Computer Password? It Was Useless Too. WIRED.

158. *Meier R.* 2017. An Annotated History of Google's Cloud Platform - Reto Meier [WWW Document]. Medium. medium.com/@retomeier/anannotated-history-of-googles-cloud-platform-90b90f948920 (доступ получен 18.12.2022).
159. *Mellor C.* 2021. Gartner dumps IBM from 2021 enterprise backup'n'recovery MQ leader corner. The Register.
160. *Miller R.* 2016. How AWS came to be — TechCrunch [WWW Document]. TechCrunch. techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/?guccounter=1 (доступ получен 18.12.2022).
161. *Mkrtchyan R.* 2017. All You Need to Know About the Waterfall Model. LinkedIn.
162. *Mosteller F., Moynihan D. P.* 1972. On Equality of Educational Opportunity: Papers Deriving from the Harvard University Faculty Seminar on the Coleman Report. Wiley.
163. *Murphy N. R., Beyer B., Jones C., Petoff J.* 2016. Site Reliability Engineering: How Google Runs Production Systems. O'Reilly Media, Inc.
164. *Nadeau M.* 2020. What is the GDPR, its requirements and facts? [WWW Document]. CSO Online. www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html?nsdr=true&page=2 (доступ получен 04.12.2022).
165. *Nag A.* 2021. Everybody has a plan until they get punched in the mouth. How did the famous Mike Tyson quote originate? Sportskeeda.
166. *Newman L. H.* 2018. Equifax's Security Overhaul, a Year After Its Epic Breach. WIRED.
167. *Nix E.* 2016. When was the first U.S. driver's license issued? History.
168. *Obama B.* 2013. Executive Order — Improving Critical Infrastructure Cybersecurity [WWW Document]. whitehouse.gov. obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (доступ получен 17.12.2022).
169. *Obama B.* 2013. Presidential Policy Directive — Critical Infrastructure Security and Resilience [WWW Document]. The White House: President Obama. obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (доступ получен 04.12.2022).
170. *Oltsik J.* 2018. The evolution of security operations, automation and orchestration [WWW Document]. CSO Online. www.csoonline.com/article/3270957/the-evolution-of-security-operations-automation-and-orchestration.html (доступ получен 17.12.2022).
171. *Pal V.* 2020. Gartner Hype Cycle: Everything You Need To Know. [WWW Document]. Challenging Coder. challengingcoder.com/gartner-hype-cycle (доступ получен 06.11.2022).
172. *Parker D. B.* 1998. Fighting Computer Crime: A New Framework for Protecting Information. Wiley.
173. *Paula J.* 2019. The Evolution Of IAM (Identity Access Management). Solutions Review.
174. *Perera T.* 2016. ENIGMA Technology and the History of Computers [WWW Document]. Enigma Museum. enigmamuseum.com/enigma-computer (доступ получен 18.12.2022).
175. *Perlroth N.* 2021. This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Publishing.
176. *Phythian M.* 2013. Understanding the Intelligence Cycle. Routledge.
177. *Pines G.* 2017. The Contentious History of the Passport. National Geographic.
178. *Popken B.* 2017. Equifax Execs Resign; Security Head, Mauldin, Was Music Major. NBC News.

179. *Qiao L.* Xiangsui, W., Wang, X., 2002. Unrestricted Warfare: China's Master Plan to Destroy America. NewsMax Media, Inc.
180. *Radichel T.* 2022. My History of DevSecOps — Cloud Security — Medium. Cloud Security.
181. *Raidman D.* 2020. Why We Need a Software Bill of Materials Industry Standard [WWW Document]. DevOps.com. devops.com/why-we-need-a-software-bill-of-materials-industry-standard (доступ получен 16.12.2022).
182. *Ray M.* 2013. Edward Snowden. Encyclopedia Britannica.
183. *Reagan R.* 1982. Establishment Of National Security Council Arms Control Verification Committee, National Security Declsion Directive Number 65. The White House.
184. *Riley T.* 2022. CISA's new JCDC worked as intended, witnesses say at Senate hearing on Log4Shell bug. CyberScoop.
185. *Roberts P.* 2022. A (Partial) History of Software Supply Chain Attacks. Reversing Labs. blog.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks (доступ получен 17.12.2022).
186. *Rose K.* 2012. Foundation 20 // Elon Musk. YouTube.
187. *Rose S. W., Borchert O., Mitchell S., Connelly S.* 2020. Zero Trust Architecture [WWW Document]. NIST. www.nist.gov/publications/zero-trust-architecture (доступ получен 29.10.2022).
188. *Rosenberg J.* 2021. How the DoD Orange Book Paved the Way for Modern Cybersecurity [WWW Document]. Dover Microsystems. info.dovermicrosystems.com/blog/department-defense-orange-book (доступ получен 29.10.2022).
189. *Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R.* 2021b. SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: SSE Approach [WWW Document]. NIST. csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final (доступ получен 18.12.2022).
190. *Rumsfeld D.* 1998. Commission to Assess the Ballistic Missile Threat [WWW Document]. Federation of American Scientists (FAS). irp.fas.org/threat/bm-threat.htm (доступ получен 17.12.2022).
191. Sally, 2015. Apache Logging Services Project Announces Log4j 1 End-Of-Life; Recommends Upgrade to Log4j 2 [WWW Document]. The Apache Software Foundation Blog. news.apache.org/foundation/entry/apache_logging_services_project_announces (доступ получен 16.12.2022).
192. *Saltzer J., Schroeder M.* 1975. The Protection of Information in Computer Systems. Proceedings of the IEEE 63. P. 1278–1308.
193. *Sands J., Sands S., Mahoney J. n. d.* Cybersecurity Principles [WWW Document]. NCyTE, WA. www.ncyte.net/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/cybersecurity-principles.
194. *Sanger D. E.* 2019b. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown.
195. *Sarbani B., Arbutina C. n. d.* Cybersecurity First Principles.
196. *Schwartz M. J.* 2013. Google Aurora Hack Was Chinese Counterespionage Operation. Dark Reading.
197. *Schwartz M.* 2013. Equifax's Data Breach Costs Hit $1.4 Billion [WWW Document]. BankInfoSecurity. www.bankinfosecurity.com/equifaxs-data-breach-costs-hit-14-billion-a-12473 (доступ получен 18.12.2022).
198. *Schwartz N. D., Drew C.* 2011. RSA Security Faces Angry Users Over Breach. The New York Times.

199. *Seeley N.* 2021. Finding the Beginning to Discover the End: Power System Protection as a Means to Find the First Principles of Cybersecurity (Degree of Master of Science). University of Idaho.
200. *Shannon C. E.* 1948. A Mathematical Theory of Communication. System Technical Journal 27, 379–423.
201. *Shea G.* 2021. A Software Bill of Materials Is Critical for Comprehensive Risk Management [WWW Document]. The Foundation for Defense of Democracies. www.fdd.org/analysis/2021/09/29/a-software-bill-of-materials-is-critical-for-comprehensive-risk-management (доступ получен 17.12.2022).
202. *Shortridge K.* Rhinehart, A., 2023. Security Chaos Engineering.
203. *Silver N.* 2016. 2016 Election Forecast [WWW Document]. FiveThirtyEight. projects.fivethirtyeight.com/2016-election-forecast (доступ получен 18.12.2022).
204. *Simmons G. J.* 2009. Data Encryption Standard. Encyclopedia Britannica.
205. Sketchbubble, 2022. Risk Heatmap. [online] Sketchbubble.com. www.sketchbubble.com/en/presentation-risk-heatmap.html (доступ получен 30.10.2022).
206. *Soare B.* 2021. PIM vs PAM vs IAM: What's The Difference? Heimdal Security.
207. *Spencer S.* 2012. Timeline of Computer Viruses [WWW Document]. Mapcon Technologies, Inc. www.mapcon.com/us-en/timeline-of-computer-viruses (доступ получен 18.12.2022).
208. Staff. 1985. Defense System Software Development: DOD-STD-2167A. Department Of Defense.
209. Staff. 1996. Testimony of Richard Pethia, Manager, Trustworthy Systems Program and CERT Coordination Center Software Engineering Institute, Carnegie Mellon University, Before the Permanent Subcommittee on Investigations U.S. Senate Committee on Governmental Affairs [WWW Document]. Federation of American Scientists (FAS). irp.fas.org/congress/1996_hr/s960605m.htm (доступ получен 17.12.2022).
210. Staff. 1998. Laplace transform. Encyclopedia Britannica.
211. Staff. 2004. A Bunch of Hacks [WWW Document]. CSO Online. www.csoonline.com/article/2117332/a-bunch-of-hacks.html (доступ получен 29.10.2022).
212. Staff. 2007. History of SAML [WWW Document]. SAML XML.org. saml.xml.org/history (доступ получен 17.12.2022).
213. Staff. 2007. Jericho Forum Commandments. The Open Group.
214. Staff. 2007. The National Sigint Operations Center [WWW Document]. Wayback Machine. web.archive.org/web/20100527224956/www.nsa.gov/public_info/_files/cryptologic_spectrum/nsoc.pdf.
215. Staff. 2008. NIST General Information [WWW Document]. NIST. www.nist.gov/director/pao/nist-general-information (доступ получен 18.12.2022).
216. Staff. 2009. Organizational Resilience: Security, Preparedness, and Continuity Management Systems. ASIS International.
217. Staff. 2010. DHS Risk Lexicon 2010 Edition. U.S. Department of Homeland Security.
218. Staff. 2011. SecurID data breach cost RSA $66 million-so how much did it cost you? [WWW Document]. SecurEnvoy. securenvoy.com/blog/securid-data-breach-cost-rsa-66-million-so-how-much-did-it-cost-you-asks-securenvoy (доступ получен 04.12.2022).
219. Staff. 2011. What did the RSA breach end up costing EMC? [WWW Document]. Help Net Security. www.helpnetsecurity.com/2011/07/28/what-did-the-rsa-breach-end-up-costing-emc (доступ получен 04.12.2022).

220. Staff. 2012. A tour of AT&T's Network Operations Center (1979) — AT&T Archives. AT&T Tech Channel.
221. Staff. 2012. Partnering for Cyber Resilience. World Economic Forum.
222. Staff. 2013. CSA Announces Software Defined Perimeter (SDP) Initiative [WWW Document]. Cloud Security Alliance. cloudsecurityalliance.org/press-releases/2013/11/13/csa-announces-software-defined-perimeter-sdp-initiative (доступ получен 17.12.2022).
223. Staff. 2014. Linear Responsibility Chart [WWW Document]. SprAid. spraid.onmason.com/project-management/linear-responsibility-chart (доступ получен 12.11.2022).
224. Staff. 2017. Claude Shannon's Information Theory Explained [WWW Document]. HRF. https://healthresearchfunding.org/claude-shannons-information-theory-explained/ (доступ получен 09.11.2022).
225. Staff. 2017. Equifax: An Epic Fail In Crisis Communications [WWW Document]. Strategic Vision PR Group. www.strategicvisionpr.com/equifax-epic-fail-crisis-communications (доступ получен 04.12.2022).
226. Staff. 2017. The Equifax Credit Breach Timeline: What Happened? The Eichholz Law Firm. www.thejusticelawyer.com/blog/the-equifax-credit-breach-timeline-what-happened (доступ получен 04.12.2022).
227. Staff. 2018. Anthem pays OCR $16 Million in record HIPAA settlement following largest health data breach in history — October 15, 2018 [WWW Document]. HHS.gov. www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html (доступ получен 18.12.2022).
228. Staff. 2018. Chaos Monkey at Netflix: the Origin of Chaos Engineering [WWW Document]. Gremlin. www.gremlin.com/chaos-monkey/the-origin-of-chaos-monkey (доступ получен 18.12.2022).
229. Staff. 2018. Former Equifax employee indicted for insider trading [WWW Document]. Department of Justice. www.justice.gov/usao-ndga/pr/former-equifax-employee-indicted-insider-trading (доступ получен 18.12.2022).
230. Staff. 2018. The Evolution of Software Composition Analysis(SCA). E-SPIN. www.e-spincorp.com/the-evolution-of-software-composition-analysissca (доступ получен 17.12.2022).
231. Staff. 2018. The Morris Worm [WWW Document]. Federal Bureau of Investigation. www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218 (доступ получен 17.12.2022).
232. Staff. 2019. Joint Task Force — Computer Network Defense: 20 Years Later [WWW Document]. National Security Archive. nsarchive.gwu.edu/briefing-book/cyber-vault/2019-06-29/joint-task-force-computer-network-defense-20-years-later (доступ получен 17.12.2022).
233. Staff. 2019. Levi & Korsinsky Announces Zendesk Class Action Investigation; ZEN Lawsuit — Levi & Korsinsky, LLP [WWW Document]. Levi & Korsinsky LLP. www.zlk.com/press/levi-korsinsky-announces-zendesk-class-action-investigation-zen-lawsuit (доступ получен 25.11.2022).
234. Staff. 2019. Overview [WWW Document]. InfraGard National Members Alliance. www.infragardnational.org/about-us/overview (доступ получен 02.11.2022).
235. Staff. 2019. The NCES Fast Facts Tool provides quick answers to many education questions (National Center for Education Statistics) [WWW Document]. nces.ed.gov/FastFacts/display.asp?id=84 (доступ получен 09.11.2022).

236. Staff. 2019c. The State of SDP Survey: A Summary [WWW Document]. CSA. cloudsecurityalliance.org/blog/2019/07/02/the-state-of-sdp-survey-a-summary (доступ получен 17.12.2022).
237. Staff. 2020. A Developer's History of Authentication. WorkOS [WWW Document]. WorkOS. workos.com/blog/a-developers-history-of-authentication (доступ получен 17.12.2022).
238. Staff. 2020. Chinese Hackers Charged in Equifax Breach [WWW Document]. Federal Bureau of Investigation. www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020 (доступ получен 04.12.2022).
239. Staff. 2020. From Municipalities to Special Districts, Official Count of Every Type of Local Government in 2017 Census of Governments [WWW Document]. Census.gov. www.census.gov/library/publications/2019/econ/from_municipalities_to_special_districts.html (доступ получен 09.11.2022).
240. Staff. 2020. Hebern Cryptographic Rotor Machine [WWW Document]. Crypto-IT. www.crypto-it.net/eng/simple/hebern-machine.html?tab=0 (доступ получен 18.12.2022).
241. Staff. 2020. Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents. The Cyentia Institute.
242. Staff. 2020. The Bank Fines 2020 report [WWW Document]. Finbold. finbold.com/bank-fines-2020 (доступ получен 04.12.2022).
243. Staff. 2020. The History of Common Vulnerabilities and Exposures (CVE) [WWW Document]. Tripwire. www.tripwire.com/state-of-security/history-common-vulnerabilities-exposures-cve (доступ получен 06.11.2022).
244. Staff. 2020. What is DevSecOps? [WWW Document]. IBM. www.ibm.com/cloud/learn/devsecops (доступ получен 22.11.2022).
245. Staff. 2020. What was the very first antivirus package? Top Ten Reviews.
246. Staff. 2021. A Brief History of Software Development Methodologies [WWW Document]. growin. www.growin.com/blog/history-of-software-development-methodologies (доступ получен 18.12.2022).
247. Staff. 2021. Executive Order on Improving the Nation's Cybersecurity [WWW Document]. The White House. www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity (доступ получен 17.12.2022).
248. Staff. 2021. Internet Crime Report, Internet Crime Complaint Center. FBI.
249. Staff. 2021. IRIS Risk Retina — Data for Cyber Risk Quantification. Cyentia Institute.
250. Staff. 2021. ISO/IEC 5962:2021 [WWW Document]. ISO. www.iso.org/standard/81870.html (доступ получен 17.12.2022).
251. Staff. 2021. Marvel Entertainment Revenue: Annual, Historic, And Financials [WWW Document]. Zippia. www.zippia.com/marvel-entertainment-careers-63407/revenue (доступ получен 09.11.2022).
252. Staff. 2021. SPDX Becomes Internationally Recognized Standard for Software Bill of Materials. Associated Press.
253. Staff. 2022. 2019 SUSB Annual Data Tables by Establishment Industry [WWW Document]. Census.gov. www.census.gov/data/tables/2019/econ/susb/2019-susb-annual.html (доступ получен 09.11.2022).
254. Staff. 2022. ACPM Podiatry HIPAA Enforcement Action [WWW Document]. HHS.gov. www.hhs.gov/hipaa/for-professionals/complianceenforcement/agreements/acpm/index.html (доступ получен 18.12.2022).

255. Staff. 2022. Data Protection Laws of the World. DLA Piper.
256. Staff. 2022. Here Are 24 Reported Victims Of The SolarWinds Hack (So Far) [WWW Document]. PanaTimes. panatimes.com/here-are-24-reported-victims-of-the-solarwinds-hack-so-far (доступ получен 04.12.2022).
257. Staff. 2022. HIPAA Violation Fines — Updated for 2022 [WWW Document]. HIPAA Journal. www.hipaajournal.com/hipaa-violation-fines (доступ получен 18.12.2022).
258. Staff. 2022. Microsoft 365 for enterprise for the Contoso Corporation — Microsoft 365 Enterprise [WWW Document]. Microsoft Learn. learn.microsoft.com/en-us/microsoft-365/enterprise/contoso-case-study?view=o365-worldwide (доступ получен 09.11.2022).
259. Staff. 2022. Security and privacy laws, regulations and compliance: The complete guide [WWW Document]. CSO Online. www.csoonline.com/article/3604334/csos-ultimate-guide-to-security-and-privacy-laws-regulations-and-compliance.html?upd=1633550065086#FISMA (доступ получен 04.12.2022).
260. Staff. 2022. Security Service Edge [WWW Document]. Gartner. www.gartner.com/reviews/market/security-service-edge (доступ получен 05.11.2022).
261. Staff. 2022. SPDX vs CycloneDX — A Detailed Comparison [WWW Document]. ERP Information. www.erp-information.com/spdx-vs-cyclonedx (доступ получен 17.12.2022).
262. Staff. 2022. What is STIX (Structured Threat Information eXpression)? [WWW Document]. Information Security Asia. informationsecurityasia.com/what-is-stix (доступ получен 02.11.2022).
263. Staff. Cloud Security Alliance Issues Expanded Specification for the [WWW Document]. CSA. cloudsecurityalliance.org/press-releases/2022/03/10/cloud-security-alliance-issues-expanded-specification-for-the-software-defined-perimeter-sdp (доступ получен 17.12.2022).
264. Staff. n. d. A brief history of encryption (and cryptography) [WWW Document]. Thales Group. www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption (доступ получен 04.12.2022).
265. Staff. n. d. A Brief History of NVD [WWW Document]. NIST. nvd.nist.gov/general/brief-history (доступ получен 16.12.2022).
266. Staff. n. d. A Timeline of SSC Attacks, Curated by Sonatype [WWW Document]. Sonatype. www.sonatype.com/resources/vulnerability-timeline (доступ получен 17.12.2022).
267. Staff. n. d. About the Building Security In Maturity Model [WWW Document]. BSIMM. www.bsimm.com/about.html (доступ получен 18.12.2022).
268. Staff. n. d. Automated Indicator Sharing [WWW Document]. CISA. www.cisa.gov/ais (доступ получен 18.12.2022).
269. Staff. n. d. Block Ciphers Modes of Operation [WWW Document]. Crypto-IT. www.crypto-it.net/eng/theory/modes-of-block-ciphers.html (доступ получен 18.12.2022).
270. Staff. n. d. Cyber Information Sharing and Collaboration Program (CISCP) [WWW Document]. CISA. www.cisa.gov/ciscp (доступ получен 18.12.2022).
271. Staff. n. d. Cyber Resiliency [WWW Document]. NIST Glossary. csrc.nist.gov/glossary/term/cyber_resiliency (доступ получен 18.12.2022).
272. Staff. n. d. Definition of Identity and Access Management (IAM) — Gartner Information Technology Glossary [WWW Document]. Gartner. www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam (доступ получен 17.12.2022).

273. Staff. n. d. Desktop Operating System Market Share Worldwide [WWW Document]. StatCounter Global Stats. gs.statcounter.com/os-market-share/desktop/worldwide#monthly-201901-202012 (доступ получен 26.11.2022).
274. Staff. n. d. Enhanced Cybersecurity Services (ECS) [WWW Document]. CISA. www.cisa.gov/enhanced-cybersecurity-services-ecs (доступ получен 18.12.2022).
275. Staff. n. d. Fermi Problems: Estimation [WWW Document]. TheProblemSite.com. www.theproblemsite.com/reference/mathematics/estimation/fermi-problems (доступ получен 09.11.2022).
276. Staff. n. d. History of AWS [WWW Document]. Javatpoint. www.javatpoint.com/history-of-aws (доступ получен 16.12.2022).
277. Staff. n. d. History of LDAP [WWW Document]. Ldapwiki. ldapwiki.com/wiki/HistoryofLDAP (доступ получен 17.12.2022).
278. Staff. n. d. Home [WWW Document]. IETF. www.ietf.org (доступ получен 16.12.2022).
279. Staff. n. d. IAM vs PAM vs PIM: The Difference Explained [WWW Document]. MSP360. www.msp360.com/resources/blog/iam-vs-pam-vs-pim (доступ получен 17.12.2022).
280. Staff. n. d. ISO/IEC 19770-2:2015 [WWW Document]. ISO. www.iso.org/standard/65666.html (доступ получен 17.12.2022).
281. Staff. n. d. Joint Cyber Defense Collaborative [WWW Document], n. d. CISA. www.cisa.gov/jcdc (доступ получен 18.12.2022).
282. Staff. n. d. Known Exploited Vulnerabilities Catalog [WWW Document]. CISA. www.cisa.gov/known-exploited-vulnerabilities-catalog (доступ получен 16.12.2022).
283. Staff. n. d. MITRE ATT&CK [WWW Document]. attack.mitre.org (доступ получен 16.12.2022).
284. Staff. n. d. NVD — Categorization of Attacks Toolkit or ICAT [WWW Document]. General. nvd.nist.gov/General (доступ получен 16.12.2022).
285. Staff. n. d. OWASP Top 10:2021 [WWW Document]. owasp.org/Top10 (доступ получен 16.12.2022).
286. Staff. n. d. SAMM model overview [WWW Document]. OWASPSAMM. owaspsamm.org/model (доступ получен 18.12.2022).
287. Staff. n. d. Security and resilience — Organizational resilience — Principles and attributes [WWW Document]. ISO. www.iso.org/obp/ui#iso:std:iso:22316:ed1:v1:en (доступ получен 04.12.2022).
288. Staff. n. d. Shannon Lietz [WWW Document]. DevSecOps. www.devsecops.org/shannon-lietz (доступ получен 18.12.2022).
289. Staff. n. d. The CERT Division [WWW Document]. Software Engineering Institute. www.sei.cmu.edu/about/divisions/cert/index.cfm#history (доступ получен 02.11.2022).
290. Staff. n. d. The Social Security Act of 1935 [WWW Document]. US House of Representatives: History, Art & Archives. history.house.gov/Historical-Highlights/1901-1950/The-Social-Security-Act-of-1935/ (доступ получен 17.12.2022).
291. Staff. n. d. The Unusual Suspects [WWW Document]. BAE Systems | Cyber Security & Intelligence. www.baesystems.com/en/cybersecurity/feature/the-unusual-suspects (доступ получен 17.12.2022).
292. Staff. n. d. Top Governance, Risk & Compliance Platforms 2022 [WWW Document]. TrustRadius. www.trustradius.com/governance-risk-compliance-grc (доступ получен 04.12.2022).
293. Staff. n. d. What is a Class Action Lawsuit? [WWW Document]. Hagens Berman. www.hbsslaw.com/about/what-is-a-class-action-lawsuit (доступ получен 25.11.2022).

294. Staff. n. d. Who is ACPM Podiatry Group [WWW Document]. ZoomInfo. www.zoominfo.com/c/acpm-podiatry-group-ltd/1101297340.
295. *Stasha S.* 2022. Healthcare statistics for 2021 [WWW Document]. Policy Advice. policyadvice.net/insurance/insights/healthcare-statistics (доступ получен 23.11.2022).
296. *Stewart A. J.* 2021. A Vulnerable System: The History of Information Security in the Computer Age. Cornell University Press.
297. *Stoll C.* 1988. Stalking the wily hacker. Communication of the ACM 31.
298. *Stone M.* 2022. The More You Know, The More You Know You Don't Know [WWW Document]. Project Zero. googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html (доступ получен 06.11.2022).
299. *Strom B., Applebaum A., Miller D., Nickel K., Pennington A., Thomas C.* 2020. MITRE ATT&CK: Design and Philosophy. Mitre.
300. *Swanson M., Bowen P., Phillips A., Gallup D., Lynes D.* 2010. SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems [WWW Document]. CSRC. csrc.nist.gov/publications/detail/sp/800-34/rev-1/final.
301. *Taisbak C. M.* 1998. Euclid. Encyclopedia Britannica.
302. The World Economic Forum, 2012. Partnering for Cyber Resilience. N. d, MITRE ATT&CK. attack.mitre.org (доступ получен 29.10.2022).
303. *Trent R.* 2014. The Story Behind the Microsoft Security Development Lifecycle [WWW Document]. ITPro Today: IT News, How-Tos, Trends, Case Studies, Career Tips, More. www.itprotoday.com/strategy/story-behind-microsoft-security-development-lifecycle (доступ получен 18.12.2022).
304. *Tunguz T.* 2015. A SaaS History Lesson — The First SaaS Company's Exceptional Journey by @ttunguz [WWW Document]. Tomasz Tunguz. tomtunguz.com/the-first-saas-company (доступ получен 16.12.2022).
305. *Turing A.* 1936. On Computable Numbers with an Application to the ENTSCHEIDUNGSPROBLEM. Proceedings of the London Mathematical Society.
306. *Turing A.* 1950. Computing Machinery and Intelligence: The Imitation Game. Mind 49, 433–460.
307. *Van der Ham J.* 2021. Toward a Better Understanding of «Cybersecurity» [WWW Document]. ACM Digital Library. dl.acm.org/doi/fullHtml/10.1145/ 3442445#Bib0002 (доступ получен 29.10.2022).
308. *Vance A.* 2015. Elon Musk: Tesla, SpaceX, and the Quest for a Fantastic Future. Ecco.
309. *Ware W. H.* 1970. Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security. The Rand Corporation.
310. *Wasemiller A. C.* 1996. The Anatomy of Counterintelligence. Center for the Study of Intelligence 13.
311. *Washington E.* 2014. On Euclid, Archimedes and first principles [WWW Document]. RenewAmerica. www.renewamerica.com/columns/ washington/140531 (доступ получен 29.10.2022).
312. *Watson R. A.* 1998. Rene Descartes. Encyclopedia Britannica.
313. *Weidlich T.* 2017. Equifax Engages in Almost Wholly Reactive Crisis Communications [WWW Document]. prcg. prcg.com/blog/equifax-engages-almost-wholly-reactive-crisis-communications (доступ получен 04.12.2022).
314. *Whitehead A. N., Russell B.* 1910. Principia Mathematica: to *56. Merchant Books.
315. *Wiener-Bronner D.* 2017. Equifax turned its hack into a public relations catastrophe [WWW Document]. CNNMoney. money.cnn.com/2017/09/12/news/companies/equifax-pr-response/index.html (доступ получен 04.12.2022).

316. *Willis J.* 2012. The Convergence of DevOps [WWW Document]. IT Revolution. itrevolution.com/articles/the-convergence-of-devops (доступ получен 06.12.2022).
317. *Wilson D. D. C. and D. R.* 1987. A Comparison of Commercial and Military Computer Security Policies. IEEE Symposium on Security and Privacy 184. doi.org/10.1109/SP.1987.10001.
318. *Wong C.* 2011. Security Metrics, A Beginner's Guide. McGraw Hill Professional.
319. *Xu S.* 2020. The Cybersecurity Dynamics Way of Thinking and Landscape, in: Proceedings of the 7th ACM Workshop on Moving Target Defense. ACM, New York, NY, USA.
320. *Zetter K.* 2015. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown.
321. *Бейер Б., Джоунс К., Петофф Дж., Мерфи Н. Р.* Site Reliability Engineering. Надежность и безотказность как в Google. — СПб.: Питер, 2021.
322. *Глик Д.* Информация. История. Теория. Поток. — М.: Corpus, 2016.
323. *Ким Дж., Бер К., Спаффорд Дж.* Проект «Феникс». Как DevOps устраняет хаос и ускоряет развитие компании. — М.: Бомбора, 2020.
324. *Ким Дж., Дебуа П., Хамбл Дж., Уиллис Дж.* Руководство по DevOps: Как добиться гибкости, надежности и безопасности мирового уровня в технологических компаниях. — М.: Манн, Иванов и Фербер, 2018.
325. *Рис Э.* Бизнес с нуля: Метод Lean Startup для быстрого тестирования идей и выбора бизнес-модели. — М.: Альпина Паблишер, 2022.
326. *Розенталь К., Джонс Н.* Хаос-инжиниринг. — М.: ДМК-Пресс, 2020.
327. *Ротер М.* Тойота Ката. Лидерство, менеджмент и развитие сотрудников для достижения выдающихся результатов. — СПб.: Питер, 2014.
328. *Стивенсон Н.* Криптономикон. — М.: Fanzon, 2021.
329. *Стивенсон Н.* Семиевие. — М.: Fanzon, 2017.
330. *Столл К.* Яйцо кукушки. История разоблачения легендарного хакера. — М.: Родина, 2022.
331. *Талеб Н. Н.* Черный лебедь. Под знаком непредсказуемости. — М.: КоЛибри, 2022.
332. *Тетлок Ф., Гарднер Д.* Думай медленно — предсказывай точно. — М.: АСТ, 2018.
333. *Толкин Дж. Р. Р.* Властелин колец. Т. 1. Братство кольца. — М.: АСТ, 2014.
334. *Хаббард Д. У., Сирсен Р.* Как оценить риски в кибербезопасности. Лучшие инструменты и практики. — М.: Бомбора, 2023.