Эллисон Сэрра

Кибер-безопасность: правила игры

Как руководители и сотрудники влияют на культуру безопасности в компании

альпина PRO

Эллисон Сэрра

Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании

«Альпина Диджитал»

2019

Сэрра Э.

Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании / Э. Сэрра — «Альпина Диджитал», 2019

ISBN 978-5-9075-3443-8

В апреле 2021 года данные более полумиллиарда пользователей Facebook оказались в открытом доступе. В том числе на одном из хакерских форумов опубликовали телефонный номер Марка Цукерберга. Защищал ли основатель одной из крупнейших социальных сетей свои данные, соблюдал ли меры кибербезопасности? Конечно. Но когда речь идет о киберпреступности, даже самой лучшей защиты бывает недостаточно. По результатам исследования Verizon об утечке данных 2018 года, сотрудники прямо или косвенно ответственны за четверть всех взломов компаний. Повысив уровень кибергигиены персонала и подготовив их к возможным информационным угрозам, можно значительно снизить риск утечки данных компании и сохранить репутацию, если это все же произойдет. Эллисон Серра, старший вице-президент и директор по маркетингу McAfee, написала книгу «Кибербезопасность: правила игры» для людей, которые хотят подготовить компанию к возможным атакам со стороны киберпреступного мира. Книга полна легко применимых советов о том, как обеспечить максимальную безопасность компании: научить сотрудников правильно обращаться с личными и корпоративными данными, найти недостающих специалистов по информационной безопасности, подключить к обсуждению этих вопросов совет директоров, встраивать инструменты защиты на этапе разработки продукта и своевременно и грамотно реагировать на взломы. Если сделать кибербезопасность частью культуры организации, вероятность того, что компания пострадает от информационной атаки, станет гораздо ниже.

ISBN 978-5-9075-3443-8

Содержание

Эллисон Сэрра
Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании

Переводчик *Людмила Смилевска*
Редактор *Мария Приморская*
Руководитель проекта *И. Позина*
Корректоры *Е. Жукова, Н. Казакова*
Дизайнер *А. Маркович*
Компьютерная верстка *Б. Руссо*

* * *

Фрэнку, любви всей моей жизни, – тому, кто читал каждую написанную мною страницу, включая эту.

Спасибо, что любишь меня и поддерживаешь.

Глава 1
Как я испортила Пасху

Бывали у меня воскресенья и получше.

16 апреля 2017 года, Пасха. Мы с мужем сидели дома, только закончили ужинать. Настало долгожданное время насладиться покоем и нашим новым увлечением – запойным просмотром Netflix. Знала бы я тогда, что вот-вот сыграю главную роль в собственной драме, заслуживающей гораздо большего внимания…

Загорелся экран моего телефона – пришло сообщение от Шатель, руководителя нашего отдела по подбору персонала. Мы с ней тесно общались. Всего 12 дней назад мы помогли McAfee отделиться от Intel в качестве одной из крупнейших независимых компаний в области кибербезопасности. Я не удивилась ее сообщению на Пасху – думала, она просто прислала мне поздравления с праздником. Но речь там шла не об этом.

«Загляни к нам в соцсети. Дело плохо».

Я открыла страницу McAfee в очень известной социальной сети, название которой не буду здесь упоминать, – и пришла в ужас.

Кто-то взломал профиль нашей новорожденной компании, которой едва исполнилось 12 дней, и исписал страницу самыми грязными и непристойными выражениями, какие только могут прийти в голову. Такое не лучшим образом сказалось бы на любой фирме. Но стоит объяснить, насколько плохо, бесконечно плохо это было для нас.

Оскорбительные надписи резко противоречили всему, что представляла наша организация. Мы только что перезапустили бренд с новым слоганом «Вместе – сила», отражавшим нашу веру в то, что для защиты мира от киберугроз нужно использовать все возможные средства. Мы только что представили сотрудникам новые ценности компании, одна из которых – *всеобъемлющая* открытость и прозрачность. И мы были лидерами в области *кибербезопасности*. Что подумают клиенты о нашей способности сохранить их самые ценные цифровые активы, если мы не можем защитить даже собственный профиль в одной из крупнейших соцсетей? И вдобавок ко всему, именно моя команда – маркетинговая организация – отвечала за управление профилями компании во всех социальных медиа, включая этот, «опороченный» прямо у меня под носом.

Я начала действовать. Нужно было связаться с главой нашей диджитал-команды, чтобы понять, что происходит. Я сразу дозвонилась ей, и мне не пришлось объяснять, что звонок никак не связан с Пасхой.

– Я знаю, почему ты звонишь. Мы разбираемся. Наш аккаунт взломали. Мы на связи с [социальной сетью], решаем проблему.

Я начала думать о худшем. Взломанный аккаунт – это одно. Но что если это скоординированная атака на McAfee? Вдруг хакеры нацелились на добычу покрупнее и отвлекли наше внимание этой «пожарной тревогой», чтобы параллельно проникнуть в систему компании?

Руководитель диджитал-команды тут же уверила меня, что наш директор по информационной безопасности уже все проверил и подтвердил: все системы в порядке. На миг я испытала облегчение, но тут же осознала, что нужно сделать еще один звонок. Генеральный директор должен быть в курсе происходящего. И лучше бы мне сообщить ему новости лично. Итак, я набрала его номер, собираясь испортить и ему пасхальное воскресенье. Он взял трубку почти мгновенно.

– Крис, один из наших аккаунтов в социальных сетях взломали.

– Насколько все плохо? – сдержанно спросил он.

– Корпоративные сервера в порядке, Крис. Взломана страница компании на сайте социальной сети.

Я объяснила ему, что случилось. Первым проблему обнаружил Гэвин, наш SMM-специалист. Он был дома и занимался тем же, чем и многие фанаты социальных сетей на выходных, – сидел в сети. Около пяти часов вечера он увидел, что статус на странице компании поменялся на произвольный набор букв. Гэвин предположил, что сообщение случайно написал кто-то из его команды, – и удалил пост.

Затем он связался с сотрудниками, чтобы выяснить, чьих это рук дело. Об обновлении никто ничего не знал.

Вскоре появился новый бессмысленный пост. И теперь он был неслучайным.

Гэвин залогинился в социальной сети и перешел в настройки аккаунта. Имена всех людей, имеющих доступ к управлению страницей, были ему знакомы. Но чтобы перестраховаться, он начал закрывать доступ другим администраторам из списка.

Пока он делал это, страница в браузере обновилась – и его «выкинуло» из аккаунта.

Теперь сомнений в злонамеренности действий не осталось. За секунду Гэвин сообразил, что удаление поста сообщило хакеру: в McAfee знают о взломе. Началась классическая гонка из криминальных фильмов о технологиях: пальцы летали по клавиатуре, появлялись и скрывались значки программ, всплывали сообщения – все в лучших традициях Голливуда. Гэвин и злоумышленник на всех парах в режиме онлайн неслись к одной цели. Даже отсутствие напряженного саундтрека не снижало накала страстей. Гэвин рассказал: «Я старался удалить всех остальных администраторов, и хакер делал то же самое. Он сработал быстрее».

Прежде чем закончить разговор с генеральным директором, мне пришлось поделиться с ним еще одной неутешительной новостью.

– И еще, Крис, зайдя на нашу страницу, вы увидите не только оскорбительные посты, но и картинку, которой заменили лого нашей компании – что-то вроде птицы. Присмотритесь. Это вовсе не птица. Это… кхм… это части тела.

Распространенная вещь в хакерском сообществе – «украшать» взломанные сайты непристойными рисунками, чтобы пометить тех, кто был, как говорят на сленге, «унижен», кого «хакнули». Хакер уже знал, что мы заблокированы и ситуация под его контролем; он повесил пошлую картинку вместо нашего нового логотипа просто так, на всякий случай.

Моя команда максимально вовлекла службу поддержки социальной сети в решение проблемы. Но… в праздники все происходит дольше. Поскольку был уже поздний вечер, нас перевели на сотрудников группы, работающей в Азиатско-Тихоокеанском регионе. Создавалось впечатление, что время физически преодолевало океан, разделяющий нас и службу поддержки. Минуты ползли со скоростью улитки.

Казалось, ожидание длилось целую вечность. Взломали не наши сервера, и у меня не было возможности подключить команду специалистов из McAfee к решению сторонней проблемы. Мы могли лишь каждые несколько минут связываться со службой поддержки, чтобы снова получать ответ: «Мы работаем над этим».

Примерно через полчаса они сообщили, что заблокировали *всех* администраторов нашей корпоративной страницы, и доступ к ней остался только у них. Это были хорошие новости: по крайней мере, большего вреда нанесено не будет.

А что насчет плохих новостей? Они не могли просто откатить страницу до версии 30-минутной давности. Согласно протоколу, страницу заблокировали, чтобы никто больше не мог изменять ее, а затем должны были последовать процедуры проверки и анализа. В ходе первой они должны были удостовериться, что мы действительно те, за кого себя выдаем, а не хакер, только притворяющийся McAfee (какая ирония!). Анализ же призван был определить степень взлома – и только затем можно было предпринимать дальнейшие действия.

Но как быть с непристойным аватаром? Он все еще висел на нашей корпоративной странице. Хуже того: платформа работала таким образом, что в личных профилях всех сотрудников McAfee в социальной сети вместо логотипа компании также отображалась эта пошлая картинка.

И в моем тоже.

Когда мы снова связались со службой поддержки, нам сообщили, что «процедуры» еще не закончены. Если следовать их логике, выходило, что единственный шанс откатить страницу – реактивировать, то есть разблокировать аккаунт, но они не сделают этого до тех пор, пока не закончат проверку безопасности.

Серьезно? Как это вообще возможно? С нашей страницей *ничего* нельзя было сделать до окончания проверки. Мы были в полной их власти. Все, что могли предпринять наши сотрудники, – удалить любое упоминание о McAfee из собственных профилей. Те, кто был в курсе происходящего, так и сделали.

Но этого было недостаточно. Я продолжила портить другим пасхальное воскресенье – сообщила о происшествии команде руководителей. Мы позаботились о безопасности серверов компании, но это не означало, что McAfee не будет атакован в других социальных каналах. И, конечно, мы не знали, станут ли следующей мишенью злоумышленников наши руководители – или их профили в соцсетях.

Я разослала руководителям письма и сообщения с просьбой немедленно включить в личных профилях всех социальных сетей многофакторную аутентификацию (подробнее о ней – чуть позже).

Последовав собственному совету, я начала судорожно укреплять безопасность в личных профилях – пока одна очень популярная социальная сеть не завела меня в тупик. Не знаю, что это было: то ли мое тело полностью перешло в режим мобилизации «бей или беги» (когда организм перенаправляет кровоток к основным группам мышц, чтобы скрыться от угрозы или подготовиться к бою – иными словами, уводит подальше от мозга), то ли соцсети стоило сделать настройки безопасности более очевидными. Скорее всего, и то, и другое. Как бы там ни было, я запаниковала и прибегла к отчаянной мере: полностью удалила оттуда личный профиль – и всю его историю.

Час ожидания превратился в два, затем в три, а потом и в четыре. Я регулярно звонила генеральному директору с необходимыми, но раздражающими новостями об «униженном и оскорбленном» профиле нашей компании. Диалоги сводились к следующему:

– Крис, мы все еще работаем с ними. Они не завершили проверку безопасности. Надеемся, все закончится в течение получаса.

Как в том анекдоте про программиста: «намылить, смыть, повторить» – снова и снова, каждые полчаса.

Во время очередного звонка руководитель вытащил козырь из рукава.

– Эллисон, я устал ждать, пока они нами займутся. Я знаю кое-кого из владельцев этой соцсети. Звоню ему.

– Отлично, Крис. Мы пока продолжим подгонять службу поддержки.

Крис связался со своим знакомым и рассказал о нашем случае. Через 30 минут после звонка страницу восстановили в исходном виде. Доподлинно неизвестно, повлиял ли звонок Криса или они просто закончили проверку, но я знала, что теперь ситуация под контролем.

Утром понедельника мы выпустили статью в интранете, чтобы все сотрудники узнали о случившемся в выходные. Помните, я говорила про одну из важных ценностей McAfee – всеобъемлющую открытость и прозрачность? Мы были обязаны объяснить людям, что случилось, особенно учитывая, что публикация отвратительной картинки вместо лого нашей компании затронула их личные страницы. Быть открытым и честным в неловких ситуациях очень сложно, но совершенно необходимо, чтобы жить в соответствии с ценностями.

* * *

Я рассказала эту историю не только потому, что она интересная, и не для того, чтобы вы подумали: «О, лучше уж она, чем я!» В ней заключается краткое содержание всего, о чем пойдет речь в этой книге, потому я и начала с нее.

Чтобы вы почувствовали, как покупка этой книги начала оправдывать себя с первой же главы, я расскажу вам, как произошел взлом и что мы делали после. И самое главное – я опишу действия, которые вы можете предпринять *утром следующего рабочего дня*, чтобы с вами этого не случилось.

Наученные горьким опытом

Снова получив контроль над аккаунтом, мы попросили службу поддержки социальной сети назвать имя администратора, ответственного за изменения.

Оказалось, это была сотрудница одного из наших агентств по размещению в СМИ (назовем ее Джули), которая больше не работала в компании. Ее учетные данные были украдены подростком, связанным с крупным киберпреступным синдикатом. Джули допустила ошибку, которую совершали многие до нее: проигнорировав правила цифровой гигиены, установила слишком простой пароль. Она использовала один и тот же код для доступа к нескольким учетным записям, включая профиль в этой социальной сети. И поскольку она была авторизованным администратором корпоративной страницы, ее личные учетные данные открывали доступ не только к ее профилю, но и к нашему. И когда злоумышленники взломали один из ее аккаунтов и продали данные в даркнет, хакеры просто опробовали этот пароль и в других социальных сетях. После этого они нанесли удар по корпоративной странице McAfee через административный доступ Джули. Остальное было детской забавой.

Задним умом мы все крепки, и этот случай – не исключение. Итак, уязвимость номер один: ***Джули использовала один пароль*** для своего личного и нашего корпоративного аккаунта на платформе соцсети (будучи одним из администраторов нашей страницы) – тот же, что и для других своих учетных записей. Если бы она вводила уникальные пароли, тогда данные, купленные злоумышленниками в даркнете, были бы бесполезны. Что хуже? Узнав о взломе аккаунта, Джули быстро сменила пароль. Но ей не удалось изменить его в других учетных записях, в том числе в важной для этой истории. Это ее вина.

Уязвимость номер два: ***мы должны были требовать двухфакторной аутентификации в социальных сетях от всех администраторов.*** Это означает, что для входа в систему им понадобилось бы ввести не только правильный пароль, но и одноразовый код, отправленный, например, на телефон. Если не ввести код в течение нескольких секунд или минут после попытки входа, вы не попадете в систему. Существует несколько версий этого типа аутентификации, и я, конечно, все упрощаю – но в целом все понятно. Это наша вина.

Уязвимость номер три: ***мы проводили проверку аккаунта недостаточно часто и не поняли вовремя, кому больше не нужен доступ***. Джули работала на нас, но мы должны были исключить ее из списка администраторов после окончания проекта. Нас могли взломать и пока она активно сотрудничала с нами, но отсутствие «гигиены» только усугубило ситуацию. Это точно на нашей совести.

Все эти действия могли значительно снизить вероятность взлома. Но, допустим, каким-то невероятным образом достаточно мотивированный, везучий и даровитый хакер смог проникнуть в нашу учетную запись в соцсети. Давайте разберемся, как превентивные меры помогли бы нам после обнаружения взлома.

Мы могли ***разработать процедуру блокировки действий всех администраторов страницы, не позволяющую хакерам узнать, что мы в курсе атаки.*** Удалением бессмысленных постов мы только привлекли их внимание. А когда они увидели, как мы закрываем доступ администраторам, они стали работать на опережение.

Нам повезло, что Гэвин оказался на взломанной странице в пасхальное воскресенье. В противном случае мы могли бы не узнать об атаке так быстро. Теперь у нас есть инструмент, который использует средства машинного обучения для обнаружения необычных изображений, ненормативной лексики, оскорблений и других аномальных материалов на страницах социальных сетей. Он *немедленно предупреждает* нескольких членов нашей команды о такой необычной активности.

> **Примечание.** Я не буду называть конкретный инструмент по двум причинам. Во-первых, программы приходят и уходят, у каждой из них свой уровень эффективности и каждой из них – свое время. Иными словами, в период запуска инструмент может быть очень эффективным – до тех пор пока хакеры не найдут способ его обойти. Я не знаю, когда вы будете читать эту книгу, а потому не стану хвалить то, что, возможно, больше не использую.
>
> Вторая причина, по которой я скрою название этого инструмента, заключается в том, что McAfee является важной мишенью для хакеров по всему миру. Оставляя их теряться в догадках, какие именно средства мы используем, мы помогаем снижать угрозу. Поискав описания инструментов в сети, вы быстро найдете то, что можно опробовать.

Вернемся к урокам, которые мы вынесли.

Мы не были знакомы с протоколом действий службы поддержки соцсети в подобных ситуациях. И очень зря. Только постфактум мы узнали о том, что их политика требует блокировки аккаунта на много часов, вне зависимости от того, насколько велики изменения на странице. ***Теперь мы узнаем о подобных процедурах заранее*** – до размещения корпоративных страниц на других сайтах.

Мы на собственном горьком опыте убедились, как много значат деньги. Поскольку мы тратили приличную сумму на продвижение в социальной сети через агентства, самой платформе мы казались менее значимым аккаунтом, чем были на самом деле. Это могло повлиять на быстроту реакции. Теперь ***мы оплачиваем продвижение напрямую на платформах социальных сетей*** – чтобы наши инвестиции были на виду и приносили нам уровень сервиса, которого мы заслуживаем.

Кроме того, мы узнали, что ***сторонние компании, с которыми мы ведем бизнес, могут не иметь надежных методов обеспечения безопасности***. Это особенно важно, если это ваши филиалы или у них есть доступ к вашим системам. В частности, у небольших сторонних компаний, с которыми вы поддерживаете отношения, может не быть подразделений ИТ и безопасности, не говоря уже о строгой политике киберзащиты.

И наконец, последний удар под дых. Как показало вскрытие, McAfee даже не был изначальной целью атаки. Когда хакер получил доступ к личным данным Джули, он понятия не имел о том, что она администратор корпоративной страницы компании. Он не знал, кто такая Джули: ему было все равно. Он просто охотился за паролями, стремился определить, к чему они откроют доступ, – к личному банковскому счету, сети компании или чему-то еще. Как только он нашел тот, который случайно подошел к странице McAfee в этой социальной сети, он вывалил на всех, кого мог, целый ушат оскорблений, унизив при этом компанию. *Даже для хакеров удача иногда важнее мастерства.*

Еще несколько важных уроков

Составьте список людей, с которыми вы можете связаться в такой ситуации. Держите их контакты под рукой – там, где вы и ваша команда легко сможете их найти. Эти списки должны быть не только у ваших людей, но и у сотрудников, обслуживающих сайт компании, ее социальные сети, облачное хранилище и так далее.

В чьи-то рабочие обязанности должна быть включена регулярная проверка доступа к аккаунту, а помимо этого – удаление из списка администраторов людей, чья работа больше не связана с текущими проектами.

Используйте многофакторную аутентификацию. Некоторые наши системы автоматически определяют, когда пользователи входят в них, а когда выходят – даже если выключение произошло всего на несколько минут, например, для смены компьютера. При работе в системах с меньшим уровнем прямого контроля – таких как облачные сервисы, например, – мы просим сотрудников присылать скриншоты, показывающие, что многофакторная аутентификация включена.

Можете себе представить, как тщательно мы теперь изучаем социальные сети, прежде чем разместить там свою страницу. В дополнение к мерам, описанным выше, мы задаем следующие вопросы:

- Как вы обрабатываете личную информацию?
- Какую технологию вы используете? (На основе ответов мы проводим оценку уязвимости).
- Как работает ваша система управления доступом?
- Какие сторонние инструменты можно подключить к вашей платформе, чтобы автоматизировать откат контента, необходимый после взлома?
- Каков алгоритм возвращения взломанного хакерами аккаунта под контроль?
- Какого соглашения об уровне реагирования на атаку и возвращения клиенту контента в том виде, каким он был до взлома, вы придерживаетесь?

Чья это вина?

Безусловно, провайдер социальной сети сможет доказать, что мы сами не сделали несколько очевидных шагов – не свели к минимуму количество администраторов, регулярно проверяя их список, не настояли на использовании уникальных надежных паролей и так далее. Но решению проблемы не способствовала и его жесткая политика, в рамках которой очевидно взломанная грубейшим образом страница должна была оставаться неизменной до окончания проверки. И, конечно, сотруднице агентства не стоило использовать одинаковый пароль для нескольких учетных записей.

Но обратите внимание: главу я назвала «Как *я* испортила Пасху». Нет, я не взламывала корпоративную страницу McAfee. Не я предоставила такую возможность злоумышленнику. И в то пасхальное воскресенье я *меньше всего* хотела разбираться с ситуацией, возникшей в результате цепи нелепых ошибок. С учетом всего сказанного я могу лишь взять на себя ответственность за все произошедшее. Ведь, в конце концов, эта корпоративная страница находилась в ведении моей команды. И мы не выполнили свой долг – не приняли разумных мер для ее сохранности.

Личная ответственность – вещь неприятная. Немногим из нас доставляет удовольствие обдумывать, что можно было сделать лучше или иначе для предотвращения несчастного случая. Уклонение – гораздо более нормальная человеческая реакция. Тем не менее именно наша

тяга к отказу от личной ответственности остается ключевым оружием в арсенале хакерского сообщества.

Слишком долго кибербезопасность была «чьей-то там» проблемой. Слишком многие считают кибербезопасность мутной темой, не заслуживающей их личного времени, не говоря уже об ответственности. Эта книга ставит целью изменить данную парадигму, хотя бы помочь сделать скромный шаг к признанию ответственности, которую мы все разделяем как сотрудники – и, в конечном итоге, защитники – наших организаций. Если наша компания не может рассчитывать, что мы примем разумные меры предосторожности, чтобы уберечь ее драгоценные цифровые активы, то кому она вообще может доверять?

Однако позвольте мне отвлечься от своей «мелодрамы» и обозначить настоящую проблему. Дело не в том, что сотрудники в большинстве своем *не хотят* поступать правильно. Гораздо чаще они просто не знают, *как* это делать.

Кибербезопасность – это командный спорт, в котором каждый должен играть на своей позиции в любую минуту. Дополнительные инструменты могут быть чрезвычайно полезными; но только когда люди, программы, процедуры, регулярные проверки и другие факторы работают вместе, они образуют эффективную защиту.

Помните о важном факторе

Еще один важный элемент, позволяющий минимизировать киберугрозу, – честность. Я определенно выхожу из зоны комфорта, начиная книгу со своим именем на обложке с описания досадного сбоя в системе безопасности, произошедшего у меня под носом. Могло ли быть хуже? Конечно. Этого никогда не должно было произойти? Конечно.

Могли ли вы оказаться на моем месте? И снова – конечно.

Рассказывая эту историю, я хочу задать тон честности, который необходим и в вашем бизнесе, нацеленном на сопротивление плохим парням. Вам необходимо развить культуру безопасности, которая позволит людям не только помогать друг другу, но и быть взаимно честными при обнаружении подозрительных действий. И честность эта – без гнева, обвинений или возмездия – позволит культуре работать.

Кроме того, я описываю взлом нашей страницы, чтобы вы сразу учли наши уроки и применили полученные знания, чтобы устранить щели в броне вашей безопасности.

Почему я?

На рынке не наблюдается недостатка в книгах по кибербезопасности от заслуживающих доверия талантливых авторов с самым разным опытом. Вы можете прочитать расследования журналистов, проанализировавших самые знаменитые взломы в истории. Можете ознакомиться с авторитетным мнением корифеев – основателей отрасли. Еще больше информации вы найдете у технических экспертов, которые весьма подробно разбирают сложные элементы кибербезопасности.

Однако же в то время, когда я это печатаю, найдется крайне мало книг по кибербезопасности, написанных маркетологами. А уж маркетологами, проработавшими в сфере всего несколько лет, – и того меньше. Так зачем доверять такому автору в столь серьезном вопросе?

Считайте мою книгу чем-то вроде гибрида маркетинга и технологий. Всю свою карьеру я переводила технические концепции на обычный язык. Я изучала взаимодействие работы и технологий, чтобы понять, как меняется корпоративная культура.

Так что если вы в целом не разбираетесь в технологиях, будьте уверены: моя цель – дать вам достаточно знаний для понимания нюансов этой сложной темы, не загружая техническими деталями. Но если вы технологически подкованнее меня, уверяю: я не собираюсь все упрощать.

Просто предложу рецепты, которые каждый сотрудник – как технический, так и любой другой – может применить для защиты своей организации. И, наконец, если вы один из моих собратьев по кибербезопасности, надеюсь, вы с удовольствием прочитаете эту книгу, восприняв ее как возможность дать другим заглянуть в наш мир. А после – передадите коллегам, не связанным с киберзащитой, чтобы они тоже вступили в наши ряды борцов за безопасность.

Почему вы?

Вы можете считать себя человеком, которому нечего привнести в сферу киберзащиты. В конце концов, как могут сотрудники, менеджеры, руководители и члены совета директоров, работа которых не связана с данной сферой, сыграть значимую роль в игре, правил которой, возможно, даже не понимают?

И здесь я обращусь за вдохновением к миру профессионального спорта – он дает нам много примеров успеха командной работы. Я не фанат спорта, но питаю слабость к американскому футболу. У меня остались очень теплые воспоминания из раннего детства: мы с отцом сидим на диване в гостиной и смотрим игру его любимой команды Dallas Cowboys.

Как и миллионы других болельщиков, в мире профессионального спорта я всего лишь зритель. Просмотр игры – это самое короткое расстояние, на которое большинство из нас может к ней приблизиться. Зрители практически не влияют на исход игры. Эта роль возложена на гораздо более важные персоны – спортсменов и тренеров, – чьи талант, упорство и командная работа в конечном счете определяют, одержат ли они победу.

Раньше я верила в это. Но потом узнала о 12-м игроке Seattle Seahawks – американской профессиональной футбольной команды. Во время любого матча на поле выходят по 11 футболистов от каждой команды. Но Seahawks признают 12-го игрока – не менее важную толпу зрителей.

Со временем я поняла, что мы с папой не желали встречи наших «ковбоев» с Seattle Seahawks на их поле. На их стадионе соперников не ожидает теплый прием. Уровень шума, создаваемый «двенадцатым игроком» команды, всего на пару децибел ниже, чем на летной палубе авианосца. И, как оказалось, поддержка зрителей существенно повлияла на исход нескольких игр. За три сезона Seahawks на своем поле одержали 26 побед против двух поражений. «Двенадцатый игрок» дважды установил мировой рекорд по шуму, создаваемому толпой, и даже спровоцировал как минимум одно небольшое землетрясение.

Эта заслуженная футбольная команда знает, насколько важны зрители. 15 декабря 1984 года из уважения к своим болельщикам они изъяли из обращения 12-й номер. Гигантский флагшток с цифрой 12 гордо реет над их стадионом. А когда команда вышла на поле перед игрой в Супербоуле, шествие возглавлял человек с флагом – также с изображением заветного числа.

Неужели «12» (как называют фанатов Seahawks) действительно такие громкие? В целом – да. Но оказалось, что их стадион был специально спроектирован так, чтобы усиливать шум. В отличие от других полей под открытым небом, где шум рассеивается естественным образом, на стадионе Seahawks есть своего рода вторая палуба и навес, которые направляют шум вниз, создавая какофонию, когда болельщики кричат[1]. Руководство команды приложило немало усилий, чтобы сделать «двенадцатого игрока» полноправным участником матчей и прибавить его коллективную мощь к своей.

История о двенадцатом игроке учит нас тому, что зрители могут влиять на исход. Но для этого их нужно вовлекать. Они должны быть полноправными участниками происходящего. И

[1] Louise Bien, "What Makes Seattle's 12th Man So Special?" SB Nation, January 22, 2015, https://www.sbnation.com/nfl2015/1/22/7871519/seattle-seahawks-12th-man-super-bowl-patriots./seattle-seahawks-12th-man-super-bowl-patriots.

вот теперь – ваш выход. Я написала эту книгу, чтобы каждый осознал важность собственного участия в непрекращающемся соревновании за кибербезопасность. Никто не обвинит вас в том, что вы не надели форму раньше. Но после прочтения этой книги никто не сможет оправдать вашего отказа от ответственности.

В этой книге я хочу продолжить диалог с того места, на котором заканчивалось так много других текстов: дать новичкам в сфере бизнеса план действий, который они могут немедленно воплотить в жизнь, чтобы стать частью борьбы за кибербезопасность. Если вы все еще сомневаетесь, стоит ли вступать в битву, знайте: вы уже в ней. Киберпреступники надеются на равнодушие и отстраненность сотрудников – так им будет проще наносить удары. Если вы не активный игрок, выступающий за свою компанию, вероятно, вы пешка в руках врага. Если вы цените онлайн-свободу, если вам важно, чтобы данные, которые вы используете для принятия решений, не были скомпрометированы, если хотите, чтобы ваши девайсы использовались во благо, а не во вред, то вы уже разделяете миссию профессионалов сферы кибербезопасности. У вас больше общего с нами, чем вы могли себе представить.

W.I.S.D.O.M.

Руководство McAfee серьезно относится к развитию. Каждый квартал мы собираемся вместе, чтобы снова и снова превращать просто «работу» в «командную работу». Мы учимся у коллег, делимся личными историями о наших профессиональных буднях и даем обещание быть более искренними друг с другом и с нашими сотрудниками. В конце этих встреч мы практикуем инструмент W.I.S.D.O.M. (аббревиатура, складывающаяся в англ. слово «мудрость» – Прим. пер.), о котором узнали от группы компаний AIP, нашего партнера по развитию лидерства. Расшифровывается аббревиатура так: **W**hat **I**'ll **S**ay (and do) **D**ifferently **O**n **M**onday – «Что я скажу (и сделаю) иначе в понедельник». Каждый из нас берет на себя обязательство проработать одну из ключевых областей развития, которые мы обсудили.

Позвольте мне и вас вооружить такой же «мудростью». В конце каждой главы вы найдете советы о том, что можете сделать в понедельник для повышения уровня кибербезопасности вашей организации. Некоторые из них на первый взгляд очевидны, но могут существенно повлиять на ваш успех. Другие потребуют больше работы, но, скажем так: вид стоит того, чтобы забраться на гору. Советов каждый раз будет не более пяти, так как я верю: 20 % усилий дают 80 % результатов.

Рекомендации, которые вы найдете на этих страницах, можно применить на очень широком спектре предприятий. McAfee обслуживает сотни миллионов потребителей по всему миру. Мы работаем с крупнейшими правительственными и корпоративными организациями. Наши решения защищают и задние дворы, и залы заседаний. Мы действительно вас понимаем.

Использовать советы смогут люди, занимающие различные позиции, – от членов совета директоров крупных компаний до рядовых сотрудников. Кибербезопасность слишком важна, чтобы оставлять ее в ведении специалистов узкого технического профиля. Каждый сотрудник, каждое заинтересованное лицо играет свою роль. Эта книга содержит основы, которые помогут вам применить те или иные техники в организации.

Готовясь к выпуску этой книги, в 2017 году McAfee проинтервьюировала 50 руководителей с различным функционалом (включая генеральных директоров, финансовых директоров, ИТ-директоров, директоров по маркетингу и т. д.), – чтобы проверить уровень кибербезопасности их подразделений. Для этой же цели мы провели этнографическое онлайн-исследование, в котором приняли участие 69 сотрудников компаний (можете считать это своеобразной онлайн-фокус-группой). Мы задавали им вопросы, а также давали упражнения, которые подразумевали сотрудничество на протяжении нескольких дней. В начале каждой главы приве-

дены цитаты этих респондентов, которые помогут более четко сформулировать тему обсуждения и рекомендации.

Конец ознакомительного фрагмента.