Томас Паренти
Джек Домет

Кибер безопасность

Harvard Business Review Press

Что руководителям нужно знать и делать

МИФ Бизнес

Томас Паренти

Кибербезопасность. Что руководителям нужно знать и делать

«Манн, Иванов и Фербер (МИФ)»

2020

УДК 004.056:004.49
ББК 67.408.135.2

Паренти Т.

Кибербезопасность. Что руководителям нужно знать и делать / Т. Паренти — «Манн, Иванов и Фербер (МИФ)», 2020 — (МИФ Бизнес)

ISBN 978-5-00-169461-8

Компании тратят огромные средства, чтобы их активы и данные были под надежной защитой, однако киберриски только возрастают, что лишь усугубляет проблему. И никакие новые технологии или раздувание бюджета не в силах переломить эту ситуацию. Томас Паренти и Джек Домет больше 30 лет занимаются вопросами кибербезопасности. В этом руководстве они систематизируют свой опыт, описывают все известные и популярные инструменты, обстоятельно объясняя, почему одни работают, а другие нет, а также делятся передовыми практиками. Вы убедитесь, что защита от кибератак не сводится к набору задач для IT-отдела, а, наоборот, предполагает развертывание надежной сети, охватывающей все, что происходит в компании, – от стратегии и ключевых видов деятельности до бизнес-модели и рабочих процессов. Если вы руководитель и хотите стать лидером по кибербезопасности – эта книга для вас. На русском языке публикуется впервые.

УДК 004.056:004.49
ББК 67.408.135.2

ISBN 978-5-00-169461-8

© Паренти Т., 2020
© Манн, Иванов и Фербер (МИФ), 2020

Содержание

Предисловие партнера издания 7
Введение. Стратегическое руководство по цифровому управлению 9
Часть I. Проблемы 14
Глава 1. Банальные сентенции 15
Конец ознакомительного фрагмента. 19

Томас Паренти, Джек Домет Кибербезопасность. Что руководителям нужно знать и делать

Научный редактор Екатерина Гришина

Издано с разрешения Projex International LLC acting jointly with Alexander Korzhenevski Agency

Все права защищены.

Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

© 2020 Thomas J. Parenty and Jack J. Domet. Published by arrangement with Harvard Business Review Press (USA) via Alexander Korzhenevski Agency (Russia). Unauthorized duplication or distribution of this work constitutes copyright infringement.

© Перевод на русский язык, издание на русском языке, оформление. ООО «Манн, Иванов и Фербер», 2021

⁂

Посвящается Копернику

Предисловие партнера издания

Мы все время думаем о безопасности. Мы хотим, чтобы наши дети ходили в безопасную школу, жили в безопасном районе. Мы покупаем детские кресла в машины и надеваем на малышей шлем, когда отпускаем их кататься на велосипеде. Мы ищем экологически безопасные продукты, считаем «химию» опасной и остерегаемся ее. Мы не смотрим близко телевизор, надеваем шапку, когда холодно, и переходим улицу по пешеходному переходу – все ради безопасности.

В обычной жизни это происходит на автомате, но мы учимся первым делом определять угрозу. Шлем на ребенке, когда он катается на велосипеде, нужен потому, что существует угроза упасть. На улице угроза – это автомобиль, а в районе – хулиганы.

И, как показывает опыт, без преувеличения, всего человечества, всякий раз изменение уклада жизни, создание чего-то нового, развитие жизни привносят новые, ранее неизвестные угрозы.

Когда-то наши очень далекие предки научились добывать и поддерживать огонь. В каком-то смысле это создало угрозу пожаров. Промышленная революция навсегда изменила наш мир, ведь благодаря ей появилось все то, чем мы сейчас пользуемся. Но в то же время она породила и новые угрозы – аварии и травматизм на производстве, техногенные катастрофы, загрязнение окружающей среды. Автомобили перевернули наш мир и тоже породили новые угрозы – аварии, смерти на дорогах, загрязнение воздуха и ряд других.

Все эти угрозы оказались новыми для своего времени. И в этом их отличительная особенность. Первое время мало кто придавал существенное значение возросшей смертности на дорогах в результате автомобильных аварий. И понимание, как быть с этой проблемой, пришло далеко не сразу, ведь ни у кого не было готового решения, как с этой угрозой бороться, – она была новая для всего мира. Наша нынешняя эра – информационная – не исключение. Она тоже привносит свои и, что самое важное, неизвестные ранее угрозы.

Но есть еще один важный фактор угроз. С появлением каждой следующей обнаруживалось, что одни слои общества оказывались менее подготовлены и имели меньшую способность адаптироваться и противостоять угрозе, тогда как другие, наоборот, были более подготовлены и обладали большими возможностями справиться с ней. В наше время это звучит как само собой разумеющееся, но раньше было не так: риск пострадать в дорожно-транспортном происшествии выше у тех, кто едет в автомобиле или находится где-то рядом. Сейчас это всем понятно. В начале же XX века пешеходы и не думали, что они тоже «участники дорожного движения» и что в связи с этим количество угроз для них возросло. Первые эскалаторы воспринимались как аттракцион, и люди, пользовавшиеся ими, были сродни счастливчикам, которым довелось прокатиться на новом инженерном сооружении, а не пользователями технического средства повышенной опасности, как сейчас.

Информационные технологии тоже порождают угрозы. Старое доброе «упал сервер» и «тыкнуть мышкой» живет уже более 25 лет, но тем не менее для многих остается непонятным жаргоном. Чего уж говорить о фишинге, SSL и сертификатах подписи. Отчасти это объясняется стремительностью развития IT, а отчасти их сложностью – ведь информационные технологии трудно визуализировать и представить. Это сплошь абстракции и железная, но порой очень сложная логика.

И основная категория риска в информационных технологиях – это люди, для которых все это не является профессией или хобби. Как следствие, они не владеют специализированными терминами и не способны оценить, какие риски могут нести те действия, которые они совершают. В особую подкатегорию можно выделить людей пожилого возраста: у многих из

них консерватизм и традиции побеждают желание держать руку на пульсе и поспевать за стремительными переменами.

Эта книга поможет новичкам, желающим больше понимать об информационной безопасности, продвинуться в своих познаниях в этой области. Она будет полезна и опытным профессионалам, которые почерпнут в ней много интересных деталей и новых подходов к привычным вещам.

В любом случае, кем бы ни был читатель, занимаясь или просто интересуясь вопросами информационной безопасности, мы делаем этот мир лучше и добрее. Любые знания в этой области помогут обществу развиваться дальше, а незащищенным гражданам жить чуточку спокойнее.

Фёдор Дбар, коммерческий директор компании «Код Безопасности»

Введение. Стратегическое руководство по цифровому управлению

За последнее десятилетие цифровизация окончательно захватила мир. И хотя правительства, компании и общественные организации тратят миллиарды долларов на кибербезопасность, финансовые последствия киберпреступлений растут пропорционально инвестициям в меры защиты.

Открыв газету в любой точке мира, вы наверняка найдете историю о какой-нибудь сокрушительной кибератаке. Например, в 2016 году, в результате киберограбления, Центробанк в Бангладеш лишился $81 млн – значительной части валютных резервов страны. В 2017 году группировка The Shadow Brokers (или кто-то от ее имени) похитила несколько важных разработок Агентства национальной безопасности США. Среди украденного был инструмент EternalBlue, который хакеры затем использовали, чтобы запустить вирус WannaCry. Этот червь заразил более 230 000 компьютерных систем в 150 странах, а убытки, по оценкам, составили около $4 млрд. В 2018 году гостиничная империя Marriott объявила о взломе своей системы бронирования Starwood и об утечке личной и финансовой информации 500 млн гостей. А взлом индийской национальной идентификационной базы Aadhaar позволил хакерам украсть личные, финансовые и биометрические данные практически всего населения страны – 1,1 млрд граждан.

Очевидно, с этим нужно что-то делать.

Наш опыт консультирования клиентов по всему миру показал: ключевая причина, по которой миллиардные инвестиции в кибербезопасность до сих пор не окупились, – все упорно зацикливаются на технологической стороне проблемы. В центре внимания – главным образом компьютеры и компьютерные системы, а также их уязвимости, а не бизнес-риски для компаний и стратегическое управление в целом.

Конечно, у такого подхода есть причины – как исторические, так и логические. IT-специалисты первыми столкнулись с вопросами кибербезопасности. Они сосредоточились на особенностях атак и механизмах защиты, а также на том, как сделать операционную систему менее уязвимой. Да и в принципе без компьютеров не было бы киберрисков, так что технологические аспекты, несомненно, важны. Излишний фокус на устранении уязвимостей соблазнительно опасен именно потому, что в этом есть резон. Но по ряду причин акцент на технологиях в конечном счете не помогает повысить кибербезопасность, а скорее наоборот – подрывает надежную защиту, как бы парадоксально это ни звучало.

Ни у одной компании нет ресурсов, чтобы решить все технологические проблемы в этой области, да и не все исправления одинаково ценны. Только определив ключевые процессы вашего бизнеса и проанализировав, как киберугрозы могут им навредить, вы расставите приоритеты грамотно и сумеете принять меры. Кроме того, когда специалисты по кибербезопасности вникнут, как именно функционирует ваш бизнес, они тоже смогут действовать правильнее. В частности, им удастся избежать решений и действий, которые, какими бы благими намерениями ни диктовались, не снижают рисков, а порой, наоборот, увеличивают их и ломают отлаженные бизнес-процессы.

Специфика технологий кибербезопасности и язык, которым о них говорят, – зачастую понятный только профессионалам – тоже играют свою роль. Технически не подготовленным стейкхолдерам, например руководству компании, нередко трудно вставить свое веское слово при обсуждении киберугроз. Но если дискуссии будут начинаться с защиты как операционной, так и стратегической деятельности, наиболее ценной для вашего бизнеса, ситуация изменится.

Это позволит вам и вашим коллегам по совету директоров контролировать управление киберрисками.

Только начав с оценки критически важной бизнес-деятельности, а не с технологий, ваша компания поймет, как выстроить адекватную систему кибербезопасности: какие программы купить и какие действия предпринять. Излишний фокус на технологиях также отвлекает внимание от других факторов, влияющих на эффективность продуктов кибербезопасности в значительно большей степени, чем сложность их функционала. Сюда относятся мотивация, стимулы и приоритеты людей, которые пользуются этими продуктами или играют иную роль в защите компании.

Мы не раз сталкивались с ситуациями, когда, например, сотрудники сознательно обходили меры безопасности, мешающие им работать. Иногда мы также наблюдали, как специалисты ослабляли киберзащиту, чтобы избежать дополнительной нагрузки и давления коллег: высокий уровень кибербезопасности вызывал ложные тревоги или нарушал бизнес-процессы. То, насколько эффективно работает команда кибербезопасности, зависит от ее места в структуре компании. Если у руководства другие приоритеты, сотрудники, отвечающие за борьбу с киберугрозами, могут не получить необходимого финансирования и полномочий.

Если компания собирается совершенствовать киберзащиту, необходим правильный катализатор – участие руководства, ваше участие в том числе. Мы считаем, что в основе многих проблем кибербезопасности лежат слабые стороны корпоративного управления, а значит, повысить его эффективность – лучший способ нивелировать риски.

Управление кибербезопасностью начинается «сверху», с совета директоров и топ-менеджмента. Отсюда оно распространяется на всю организацию, что влечет за собой как смещение ответственности (от технических специалистов к высшему руководству), так и смену угла зрения (с технологий на бизнес, его процессы, стратегию и крупные ставки, а также риски, вызванные кибератаками).

Вы представляете ключевые интересы компании в долгосрочной перспективе. Вы отвечаете за ее состояние, развитие и рост. У вас есть полномочия, чтобы инициировать перемены в общей стратегии кибербезопасности. Вы можете вмешаться там, где не справляются рыночные механизмы и не помогают правительственные постановления.

Стратегическое цифровое управление

Многие директора говорили нам, что кибербезопасность – сфера сложная, если не непостижимая. Они признавались, что принимают инвестиционные решения, не опираясь на надежные данные и не до конца понимая суть тех или иных технологий. Многие считают, что кривая обучаемости в этой области слишком крута; другие рассказывают, что не знают, какие вопросы задавать и как оценивать ответы. Часто руководству приходится полагаться на пространные заявления IT-отдела или команды кибербезопасности в духе «здесь все в порядке, но нужно поработать там». Подкованные в технологиях руководители, возможно, и занимаются проблемой грамотнее, но далеко не всегда.

Так не должно быть, но вы можете улучшить ситуацию, просто выполняя свои обязанности по управлению и контролю. Надзор за кибербезопасностью в чем-то схож с «эффектом наблюдателя» в квантовой физике, когда наблюдение за событием влияет на его результат. Ваши запросы мотивируют компанию обращать внимание на соответствующие факторы и процессы и проводить анализ, до которого в противном случае не дошли бы руки.

Взяв на себя ответственность за кибербезопасность, вы не должны нести ее как бремя. Несмотря на расхожее мнение, что это сложная для понимания сфера, наш опыт показывает: она – удел не только технических гениев. Хотя погружение в вопрос, безусловно, важно, для эффективного управления и контроля вам не нужно глубоко разбираться в проблемах кибер-

безопасности. Получение соответствующего образования даст ограниченные преимущества, отнимет много времени – и не факт, что поможет на практике. А вот в ходе привычной деятельности в совете директоров вы точно приобретете необходимые знания.

Чтобы помочь вам, мы разработали руководство по стратегическому управлению в цифровой сфере. Наша система включает четыре базовых принципа, три ключевые задачи и несколько памяток-помощников. Принципы помогут вам сориентироваться при обсуждении вопросов кибербезопасности и принятии решений. Задачи касаются наиболее важных действий, которые компания должна предпринять, и дают основу для контроля. Памятки содержат ряд вопросов-якорей, облегчающих исполнение ваших надзорных функций. Внедрив эту систему цифрового управления, вы станете лидером в области кибербезопасности и научитесь ставить перед коллегами правильные вопросы, а также интерпретировать информацию, которую они вам предоставляют.

Принципы

• *Если вы не понимаете, значит, вам плохо объяснили*. Руководство и сотрудники вашего отдела кибербезопасности обязаны предоставлять вам материалы и отчеты в форме, доступной пониманию неспециалистов.

• *На кону всегда бизнес.* Все вопросы кибербезопасности начинаются и заканчиваются проблемами бизнеса и рисками, связанными с его процессами и стратегией, а не с компьютерами и их уязвимостями.

• *Кибербезопасность должна быть у всех на слуху.* Рабочие процессы компании, ее деятельность и структура – все должно быть неотрывно от заботы о кибербезопасности. Выводите ее из тени, она – не просто часть чьего-то функционала.

• *Не забывайте о мотивации.* Знайте, чего хотят ваши сотрудники. Правильно мотивируйте их. Пусть они тоже будут заинтересованы в заботе о кибербезопасности.

Задачи

Управление киберрисками

Это наиболее важная задача; все остальные опираются на нее и зависят от четкого понимания последствий кибератак. Эффективное управление киберрисками требует грамотной оценки взаимосвязей между наиболее значимыми бизнес-рисками для компании, типами кибератак, которые могут их вызвать, и мерами, способными предотвратить или минимизировать эти риски. Эффективный контроль включает выявление и учет всех нетехнических факторов, которые могут свести на нет даже самые мощные технологии.

Защита компании

Вы существенно укрепите систему кибербезопасности, если задействуете дополнительные инструменты: грамотный подход к организационной структуре компании, выстраиванию ее рабочих процессов и корпоративной культуры. Не менее важно учитывать мотивацию и интересы сотрудников, а процесс оценки угроз должен предполагать ответы на вопросы: «Насколько мы теперь в безопасности?» и «Насколько мы будем в безопасности завтра?» Корректный статус команды кибербезопасности в структуре компании и понимание, нуждаетесь ли вы и ваши коллеги по совету директоров в дополнительной киберэкспертизе, – также важные факторы. Именно от механизмов подотчетности зависит ваша возможность получать ценную информацию, необходимую для принятия обоснованных решений.

Лидерство в кризисе

Хотя компания не должна пренебрегать превентивными и защитными мерами, лучше быть во всеоружии: вдруг кризис, вызванный кибератакой, все же грянет? Здесь помогут планирование, подготовка и координация в двух взаимосвязанных областях. Во-первых, компании необходимо научиться распознавать атаки и защищаться от них – для этого нужна квалифицированная команда реагирования. Во-вторых, топ-менеджеры должны встать у руля во время киберкризиса, то есть понимать, как относиться к тем или иным ситуациям и какие решения принимать. Используя собранную информацию и материалы, разработанные в процессе снижения рисков, руководители смогут наметить план действий заранее.

Памятки

Каждая памятка состоит из четырех элементов. Первый – запрос, касающийся той или иной задачи в области кибербезопасности. Формулировки приведены так, чтобы вы могли сразу их использовать. Второй элемент – краткое обоснование запроса с точки зрения защиты вашей компании и деятельности по управлению киберрисками. Далее приводятся примеры и описания документов, отвечающих запросу. Последний элемент – действия, рекомендованные для контроля запроса. Чтобы использовать памятки, опыт в технической сфере не нужен. Зато эти материалы помогут вам всесторонне оценить эффективность управления в области кибербезопасности и киберрисков.

Как пользоваться книгой

Мы написали эту книгу, чтобы помочь вам как руководителю компании осуществлять контроль над политикой кибербезопасности. Поскольку эта обязанность требует участия многих ваших коллег, здесь также есть рекомендации исполнительным директорам и руководителям, отвечающим за кибербезопасность, – как по защите компании, так и по выполнению их обязанностей перед вами и советом директоров. Принципы и советы, изложенные в книге, применимы и в других типах организаций, в том числе государственных учреждениях и некоммерческих организациях.

В книге четыре раздела. Каждый вносит вклад в ваше понимание кибербезопасности и того, чему нужно уделить внимание в этой сфере.

• Первая часть, «Проблемы», раскрывает причины, по которым меры в области кибербезопасности порой неэффективны, а разобраться в теме так сложно. Вы сможете критически взглянуть на решения, принимаемые вашей компанией.

• Следующая часть рассказывает о четырех принципах цифрового управления. Ими вы сможете руководствоваться, принимая решения в области кибербезопасности, – особенно если столкнетесь с новыми и неожиданными проблемами.

• Третья часть посвящена основополагающим задачам в области кибербезопасности. Ваша компания должна их решать, а вы – контролировать процесс. Каждая задача затрагивает важнейшие факторы, необходимые для достижения успеха, но часто упускаемые из виду.

• Заключительный раздел, «Памятки», включает подробные таблицы, которые помогут вам проверить, как компания справляется с задачами.

В книге мы также расскажем о нашумевших киберпреступлениях и приведем примеры из собственного опыта работы. Все это призвано показать, как принципы и методы цифрового

управления работают в реальной жизни, а также к каким последствиям может привести невнимательное отношение к ним.

Часть I. Проблемы

Начнем с двух вопросов

• Вы замечали, что общеизвестная информация о кибербезопасности порой выглядит сомнительно, но эти сомнения трудно конкретизировать?

• Приходило ли вам в голову, что о киберугрозах обычно говорят языком, малопонятным для простых смертных, и это неоправданно?

Если ваш ответ «да», то интуиция вас не подвела. Разница между тем, что кажется истинным в области кибербезопасности, и тем, что таковым является, огромна. Прежде чем перейти к принципам разумного управления в цифровой сфере и поговорить о связанной с этим ответственности, давайте сдернем завесу тайны с бытующих здесь банальных сентенций, теневых факторов и распространенных заблуждений. Именно они напускают тумана и превращают обсуждение проблем кибербезопасности в непроходимый темный лес.

Глава 1. Банальные сентенции

Сфера кибербезопасности переполнена суждениями, которые, может, и звучат разумно и убедительно, но на практике бесполезны и даже контрпродуктивны. К сожалению, их так часто повторяют, что они обрели статус непреложных истин и искажают многие представления об этой сфере и способах добиться в ней эффективных результатов.

Итак, вот три главных, наиболее вредных киберпредрассудка:

- Это все человеческий фактор!
- Спасайте бриллианты короны!
- Киберугрозы не стоят на месте!

Это все человеческий фактор!

«Проблема не в технологиях, а в людях». Иногда это утверждение звучит иначе: «В сфере кибербезопасности человек – самое слабое звено». Хотя люди время от времени забывают флешки в USB-портах, открывают письма с вредоносными вложениями и в целом ведут себя беспечно, не стоит сводить все беды к этому. За многие возникающие проблемы ответственны сами специалисты по кибербезопасности: они не способны понять поведение рядового пользователя в цифровом мире, к тому же существующая система поощрения недостаточно мотивирует их на качественную работу.

Для полноты картины сравним, как человеческий фактор влияет на обеспечение безопасности в повседневной жизни и в мире компьютерных сетей. Проверим тезис на прочность.

В офлайне мы давно поняли, что определенным сферам, локациям и ситуациям присущи повышенные риски, которым люди не всегда уделяют должное внимание. Чтобы нивелировать влияние опасных факторов, мы принимаем меры по защите и стремимся минимизировать возможный ущерб: например, устанавливаем отбойники на шоссе и «лежачих полицейских» возле школ. Мы учитываем поведенческие паттерны и не обвиняем людей в том, что они… скажем так, порой безответственны и неосторожны. Мы не ожидаем, что они исправятся только потому, что мы рекомендуем это сделать.

В цифровом мире все с точностью до наоборот: мы редко пытаемся уберечь или подстраховать людей от ошибок и необдуманных действий. Зато беспощадно ругаем их за случившееся, а в качестве решения проблемы предлагаем изучить правила компьютерной безопасности.

Тайна потерянной флешки

В 2007–2008 годах в Гонконге имело место девять случаев непреднамеренной утраты личных и медицинских данных граждан – в общей сложности 16 000 человек. В итоге Больничное управление Гонконга обратилось к нам за помощью. Перед нами стояла задача – разобраться в истинных причинах потери данных, скорректировать политику конфиденциальности и предложить меры по улучшению системы безопасности[1].

В одном случае сотрудница администрации в Больнице принца Уэльского (район Новые Территории) оставила флешку в такси. Сделать вывод, что всему виной отсутствие базовых знаний о кибербезопасности, так же легко, как во время просмотра фильма предположить, что человек с пистолетом, стоящий над трупом, и есть убийца.

Чтобы лучше разобраться в причинах инцидента, мы задали девушке всего два вопроса.

[1] “Report of the Hospital Authority Taskforce on Patient Data Security and Privacy,” http://www.ha.org.hk/haho/ho/hesd/Full_Report.pdf.

1. ***В чем состоят ваши рабочие обязанности?***

Как оказалось, сотрудница выставляла другим госпиталям счета за проведение клинических исследований в лабораториях больницы.

2. ***Зачем вы копируете информацию на флешку?***

В действиях девушки не было ничего ужасного; они диктовались логикой; многие сотрудники крупных компаний сталкиваются с подобным. На ее компьютере отсутствовала нужная для работы программа Excel. Поэтому она копировала на флешку электронные таблицы, полученные от других больниц, а затем переносила на компьютер коллеги, у которого Excel был. При этом она постоянно и безуспешно просила IT-отдел установить Excel на ее компьютер.

Итак, всему виной действительно человеческий фактор, но связанный не с делопроизводителем, а с сотрудниками IT-отдела, не удосужившимися установить коллеге необходимую программу. Когда они это сделали, риск утечки данных из-за потери флешки исчез, поскольку отпала потребность ее использовать.

Пример показывает, что люди стремятся хорошо выполнить свою работу, даже если при этом нарушают требования безопасности. Девушка не осознавала, что ставит под угрозу данные пациентов. Она просто не нашла другого решения проблемы.

Фишинг, бессмысленный и беспощадный

Люди часто открывают вложения в электронных письмах и кликают по ссылкам, что приводит к установке шпионских программ. Хакеры стали куда умнее: они нередко используют в рассылках информацию, почерпнутую из социальных и профессиональных сетей, а потому отличить фишинговые письма от обычных все труднее. Хотя несколько нигерийских принцев все еще жаждут вручить вам миллионы долларов, их сообщения постепенно вытесняются другими, гораздо более убедительными.

Калифорнийский университет в Беркли собирает базу данных о фишинговых атаках и пополняет ее образцами таких посланий. Нашлось даже поддельное письмо от HR-отдела самого университета (рисунок 1)[2].

Рисунок 1. Пример фишинговой атаки

От: <HR@berkeley.edu> <HR@berkeley.edu>
Subject: Message from human resources
Дата: 13 апреля 2017 Время: 21:29:54
Кому: XXXXX@berkeley.edu
Уважаемый XXXXX@berkeley.edu
Информационное письмо направлено HR-отделом.
Пройдите по этой ссылке, чтобы авторизоваться и просмотреть документ. Спасибо!
Калифорнийский университет в Беркли, HR-отдел.
© 2017. Попечительский совет Калифорнийского университета. Все права защищены.

Уведомление о конфиденциальности: это сообщение и все вложенные файлы могут содержать охраняемую законом конфиденциальную информацию, предназначенную исключительно для использования

[2] Berkeley Information Security Office, “Phishing Example: Message from Human Resources,” https://security.berkeley.edu/news/phishing-example-message-human-resources.

> физическими и юридическими лицами, которым оно адресовано. Если вы не относитесь к числу предполагаемых получателей, пожалуйста, удалите сообщение со всеми вложениями. Дальнейшее использование, копирование, раскрытие информации и ее распространение, а также ссылки на содержание письма и вложенных файлов строго запрещены.

Письмо кажется настоящим. Просьба авторизоваться для просмотра документа не вызывает подозрений: это стандартная практика для многих организаций, особенно при работе с конфиденциальной информацией. Отдел IT-безопасности университета Беркли в данном случае порекомендовал проверять достоверность ссылки, прежде чем переходить по ней. Наведите на нее курсор, и внизу экрана появится адрес веб-сайта. Затем нужно убедиться, что ссылка действительно ведет на страницу HR-отдела, а не на ресурс мошенников.

Такой совет одобрило бы большинство экспертов по кибербезопасности, но есть два нюанса. Во-первых, просмотр рабочих писем – рутина, с которой часто хочется покончить побыстрее. Многие решат, что наведение курсора на ссылку, изучение и проверка веб-адреса займут слишком много времени. Во-вторых, далеко не каждый рядовой пользователь сумеет проверить достоверность веб-адреса. Компания не может вменять это сотрудникам в обязанность.

Обучение основам безопасности

Это распространенный способ снизить риски фишинговых атак и внедрения вредоносного ПО в корпоративные компьютерные сети. Однако даже сотрудники компаний, специализирующихся на кибербезопасности, не могут похвастаться блестящими результатами подобных тренингов. Компания Intel Security (в прошлом McAfee) протестировала 19 000 человек в 140 странах, и только 3 % из них выявили все фишинговые имейлы в выборке из десяти сообщений, а 80 % не нашли ни одного[3]. Никакое обучение основам безопасности не решит эту проблему: достаточно одному сотруднику кликнуть на вредоносную ссылку или зараженное вложение, чтобы фишинговая атака достигла своей цели.

Отстрел на подлете

Еще один инструмент борьбы с фишингом – современные технологии, предназначенные для выявления вредоносного ПО заранее, на этапе установки. Но как гарантированно поймать всех воров и шпионов? Первоначально здесь помогало составление списка сигнатур, то есть своего рода отпечатков пальцев известных образцов вредоносных программ, и их сравнение. Новая программа не прошла проверку на «отпечатки пальцев»? Система безопасности блокирует запуск. Продвинутые антивирусы принимают во внимание также дополнительные характеристики, в том числе поведение потенциально вредоносного ПО. Однако проблема остается, и разработчики антивирусов пытаются своевременно обновлять свои продукты, не отставая от ухищрений хакеров.

В конце 2017 года компания Malwarebytes, специализирующаяся на антивирусном ПО, проанализировала уровень кибербезопасности почти на 10 млн компьютеров. Выяснилось, что даже самые совершенные антивирусы не смогли выявить почти 60 % участвовавших в эксперименте вредоносных программ[4].

---

[3] Tom Reeve, “Even Security Experts Fail to Spot Phishing Emails, Finds Report,” SC Media, May 19, 2015, https://www.scmagazineuk.com/even-securityexperts-fail-to-spot-phishing-emails-finds-report/article/537183/.

[4] Steve Ragan, “Malwarebytes Is Tracking Missed Detections in Traditional Antivirus,” CSO, November 7, 2017, https://www.csoonline.com/article/3236254/security/malwarebytes-tracking-missed-detections-in-traditional-anti-virus.html.

Ранее, в 2013 году, корпоративная сеть New York Times была взломана с целью раскрыть источники информации[5]. Ее атаковали сорока пятью вредоносными программами. Антивирусы выявили лишь одну из них.

Вернемся далеко в прошлое – к заре сферы кибербезопасности. Следует отметить, что основатель индустрии антивирусных программ уже тогда понимал: их возможности не безграничны. За два года после того, как в 1986 году был создан первый вирус, на бурно развивавшемся рынке антивирусного ПО появилось без малого сорок игроков[6]. Видя, как они множатся, разработчик первого коммерчески успешного антивируса Джон Макафи подсчитал, что «около 75 % продуктов, предлагающихся на рынке, не эффективны, поскольку не способны ни защитить компьютер от значительной части вирусов, ни даже выявить их»[7]. Он публично выражал обеспокоенность из-за того, что «недостаток понимания со стороны пользователей привел к распространению недостоверной информации, излишне эмоциональной реакции и мошенничеству»[8]. В 2018 году в мире было продано антивирусного ПО больше чем на $15 млрд. Ожидается дальнейший рост на уровне 10 % в год[9].

В борьбе с фишингом и прочими киберугрозами хорошо зарекомендовало себя одно технологическое решение. Оно эффективно тем, что освобождает рядовых сотрудников от лишней ответственности (например, переходить ли по ссылке, открывать файл или нет). «Белый список приложений» формируется по принципу: если программа не будет запущена на компьютере, то не сможет причинить никакого вреда. Это немного напоминает список гостей – практику, применяющуюся для ограничения доступа в клубы, на вечеринки и закрытые мероприятия. Вместо того чтобы оценивать каждую программу с точки зрения вредоносности, «белый список» разрешает установку только проверенного ПО, запуск которого точно не нанесет ущерба. В таких условиях не имеет значения, по каким ссылкам переходят пользователи и какие вложения они открывают. Если вредоносной программы нет в «списке гостей», она останется «за порогом».

---

[5] Gerry Smith, “Why Antivirus Software Didn’t Save the New York Times from Hackers,” *Huffington Post*, January 31, 2013, https://www.huffingtonpost.com/2013/01/31/antivirus-software-hackers_n_2589538.html.

[6] “Happy Birthday Brain, the World’s First PC Virus,” *Computer Active* 388 (2013): 9.

[7] *Inventors and Inventions*, vol. 4 (Tarrytown, NY: Marshall Cavendish, 2007), 1033; Laura DiDio, “Antivirus Vendors Form Industry Regulation Group,” *Network World* 5, no. 28 (1988): 17.

[8] DiDio, “Antivirus Vendors.”

[9] MarketsandMarkets, “Endpoint Security Market Worth 17.38 Billion USD by 2020,” press release, accessed May 19, 2018, https://www.marketsandmarkets.com/PressReleases/endpoint-security.asp; Technavio, “Global Antivirus Software Package Market 2016–2020,” accessed May 19, 2018, https://www.technavio.com/report/global-enterprise-application-global-antivirussoftware-package-market-2016–2020.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.