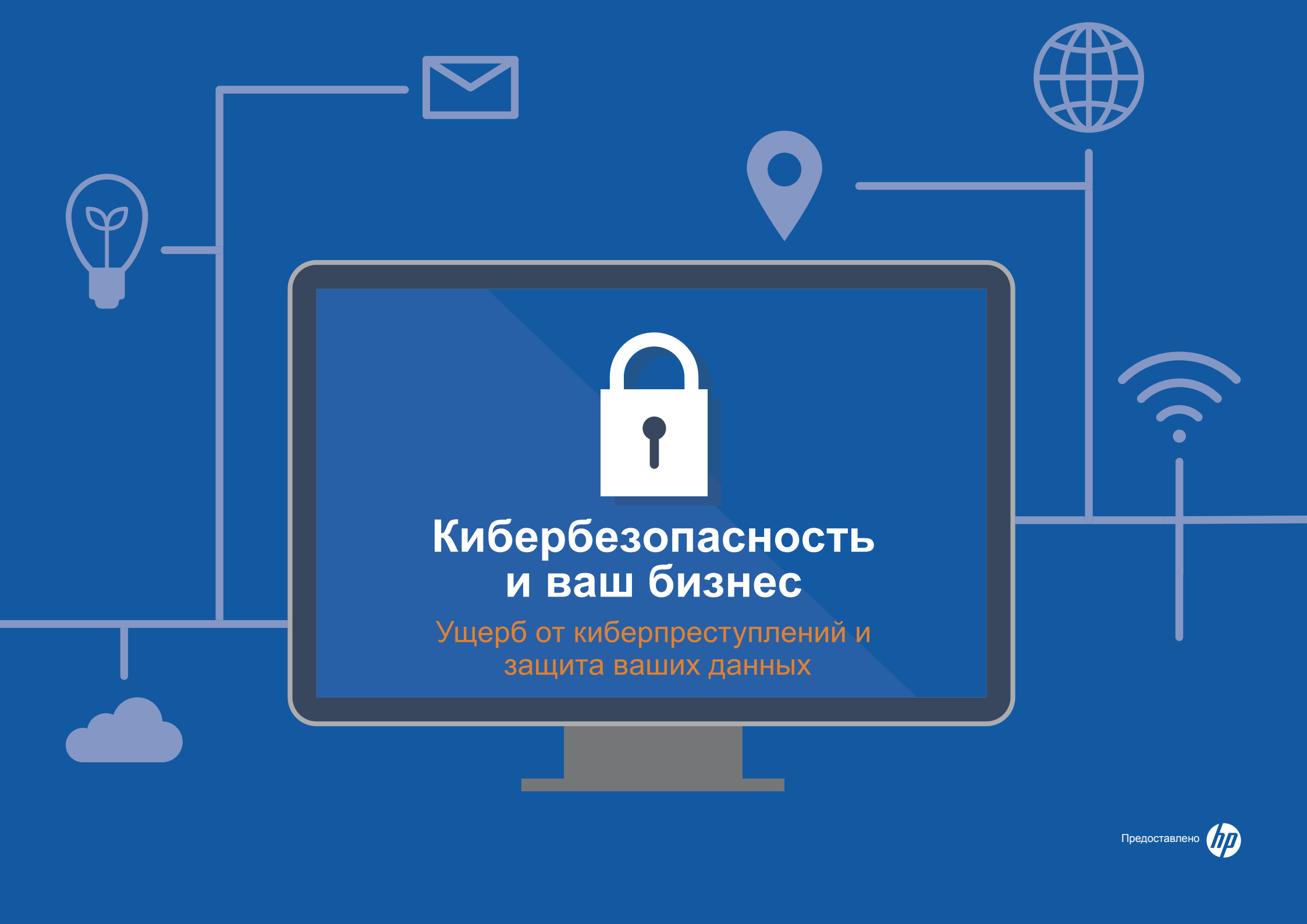


Кибербезопасность и ваш бизнес

Ущерб от киберпреступлений и защита ваших данных

Предоставлено

Содержание

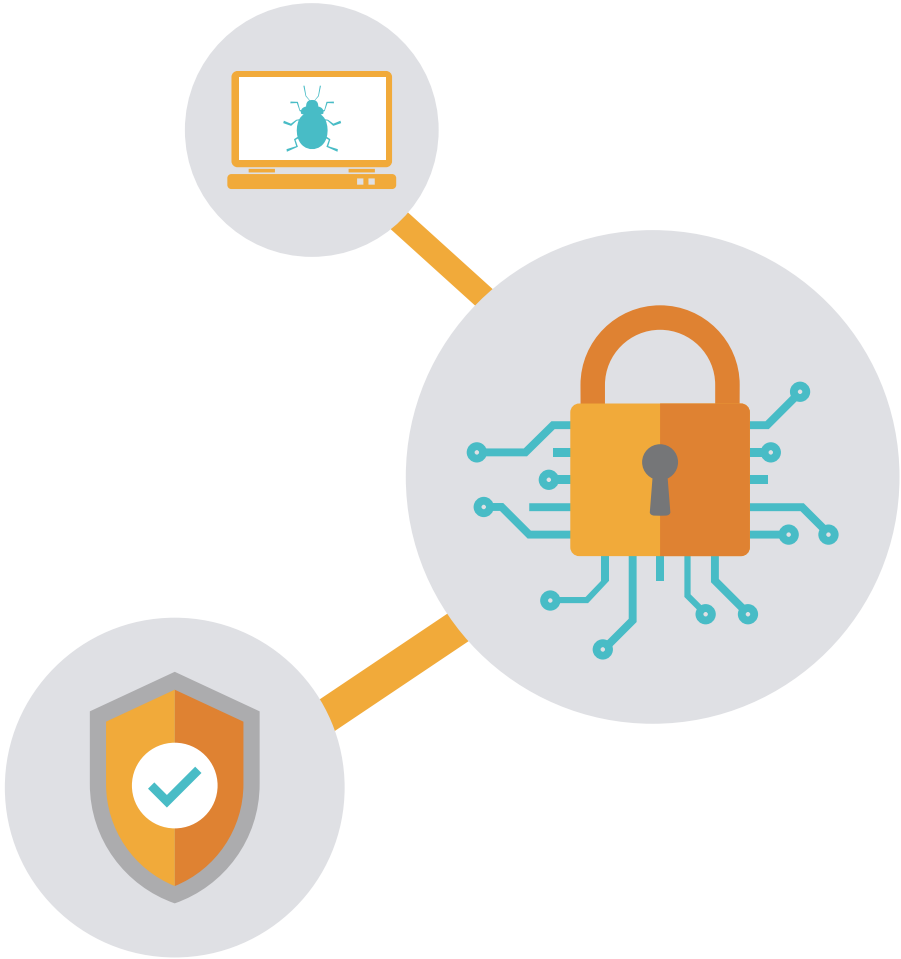
Введение

«Многие руководители считают, что киберпреступность станет главным риском для нашего поколения». Деннис Чесли (Dennis Chesley), ведущий глобальный консультант по рискам, PwC[1]

Киберпреступность — это не новая угроза, но она растет с каждым днем. Хакеры становятся лучше и получают больше точек входа для взлома сети. Из-за Интернета вещей количество подключенных устройств выросло в разы, при этом они часто служат самой простой точкой входа. Цели атак становятся все больше, а простои — масштабнее.

21 октября 2016 г. поставщик DNS из США — компания Dyn подверглась крупнейшей в истории распределенной атаке типа «отказ в обслуживании» (DDoS). Некоторые из крупнейших мировых веб-сайтов, включая Netflix,[2] Amazon и Twitter, стали недоступны на длительное время.

В январе 2017 банк Lloyds столкнулся с серьезными проблемами с онлайн-процессами. Клиенты не могли проверить баланс счета или совершить платеж. Мобильное приложение также было недоступно. Хотя банк Lloyds этого еще не подтвердил, по слухам простой был вызван DDoS-атакой.[3]



Источники: [1] PwC: Исследование глобального состояния информационной безопасности 2016 [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html [3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Введение

Такие атаки не просто вредят репутации. Они стоят реальных денег.

В опросе о безопасности принтеров, проведенном в 2016 г. компанией Spiceworks, 34 процента организаций указали, что нарушение системы безопасности увеличивает число обращений в службу поддержки и/или время, затрачиваемое на поддержку, 29 процентов указали, что нарушение системы безопасности снижает производительность/эффективность, а 26 процентов сообщили об увеличении времени простоя систем в качестве главной проблемы.[4]

Около 60 процентов ведущих специалистов по безопасности, опрошенных компанией IBM в рамках оценки CSO, сказали, что навыки злоумышленников превосходят защитные меры их организаций.[5] Обеспокоенные ИТ-директора указали кибербезопасность как одну из 10 ключевых проблем десятилетия, а согласно исследованию тенденций компании SIM, она занимает вторую позицию.[6]

Многие из этих неприятностей можно предотвратить. Далее мы рассмотрим основные заблуждения, касающиеся кибербезопасности, и более подробно остановимся на том, как киберпреступность влияет на бизнес и что можно сделать, чтобы защититься от атак. Наконец, мы взглянем в будущее и обсудим, что нас ждет, и как к этому подготовиться.

Источники: [4] Исследование безопасности принтеров HP 2016, Spiceworks [5] Оценка CSO IBM 2014 [6] Опрос об ИТ-тенденциях компании SIM 2015

Развенчание мифов о кибербезопасности

Пять основных заблуждений,

из-за которых компании могут подвергнуться кибератакам

В заголовки газет попадают утечки данных в известных мировых компаниях, но на самом деле любая организация находится под угрозой. Вот пять мифов о кибербезопасности, из-за которых компании могут оказаться уязвимыми для хакеров.

Нарушение системы безопасности

Утечки данных

Методы обеспечения безопасности

Антивирусное программное обеспечение

Кибератака

1 Компании могут быстро устранить последствия любого инцидента

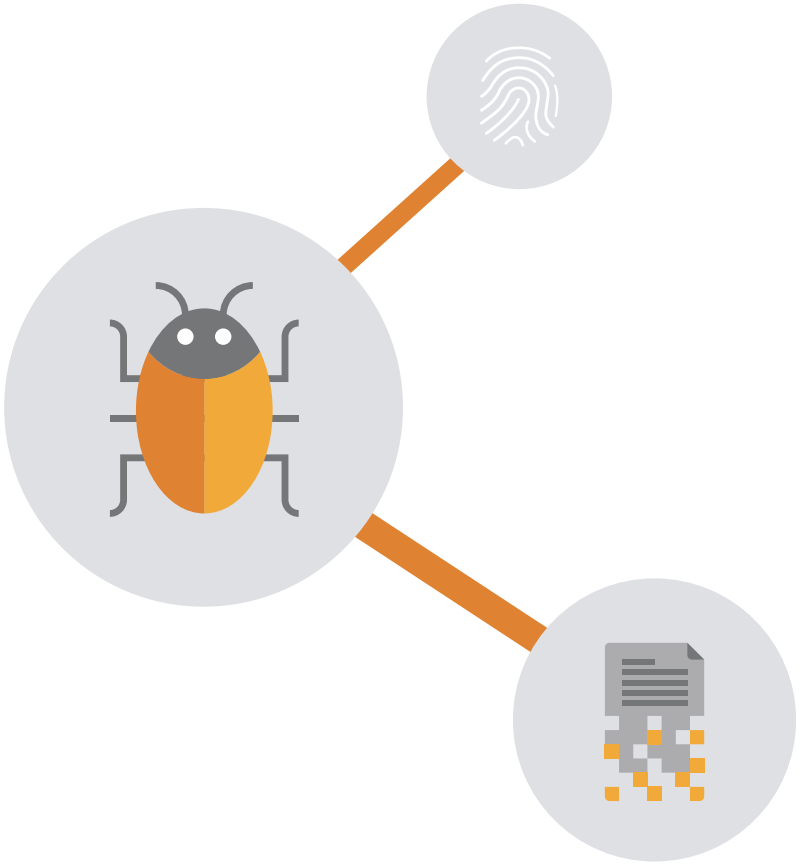
Даже сейчас по-прежнему трудно оценить ущерб кибератак для коммерческих организаций. Считается, что воздействие любой утечки можно понять по снижающейся цене акций.

Но акции — это только первая часть истории. Их стоимость может вырасти через несколько недель, но более долгосрочные потери продолжают накапливаться. Новые программы обеспечения безопасности. Новый персонал. Юридические расходы.

Все эти факторы могут серьезно нарушить работу компании на длительное время после взлома. И расходы продолжают расти. В недавнем исследовании компании Ponemon указано, что среднегодовой ущерб от взлома вырос с **7,7 млн долларов США** в 2015 г. до **9,5 млн долларов США** в 2016 г.[7]

Источник: [7] Исследование Ponemon Institute об ущербе от киберпреступности 2016

2 Утечки данных происходят редко, поэтому серьезная защита не нужна



Компания IDC обнаружила,[8] что доля организаций, которые столкнулись с утечкой данных, в 2016 г. достигла 99 процентов. При этом число компаний, которые сообщили о 6–10 взломах в год, выросло с 9 процентов в 2014 г. до 18,9 процентов в 2016 г.[9]

Эти показатели вполне могут оказаться заниженными. Очень часто об утечках никому не сообщают, так как компании стремятся избежать негативного освещения в прессе
.

Этот миф также не учитывает «истощающий» эффект утечки. Возможно, в вашей компании произошла только одна утечка. Но даже один инцидент может вызвать серьезные трудности.

Источники: [8] IDC [9] Исследование Ponemon Institute об ущербе от киберпреступности 2016

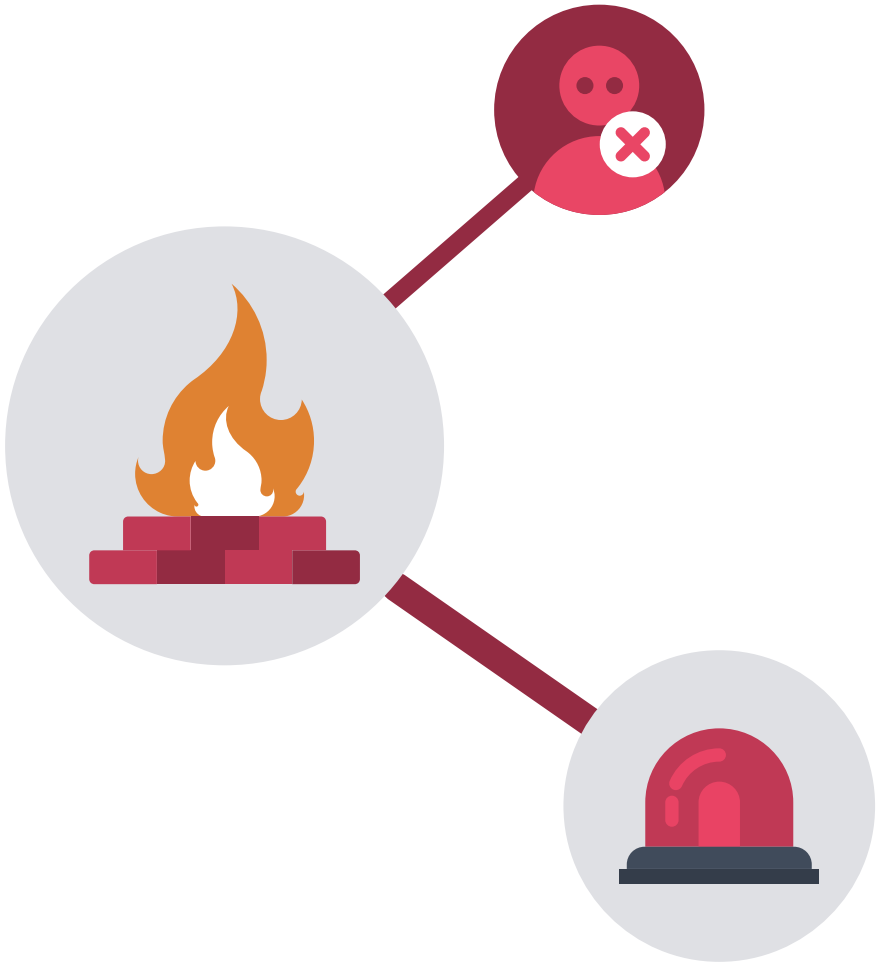
3 Мы наняли ИТ-специалиста для защиты, и нам больше ничего не нужно знать

Привлечение эксперта — это хорошая идея, но это не отменяет того факта, что каждый сотрудник компании также должен быть хорошо осведомлен о методах защиты данных.

Представьте коллегу, который, сам того не подозревая, скачивает вредоносное вложение электронной почты или посещает небезопасный веб-сайт и заражает сеть компании вирусом, который замедляет компьютеры или отправляет киберпреступникам конфиденциальную информацию. Согласно отчету о киберугрозах компании CyberEdge за 2016 г., организации назвали «низкий уровень знаний сотрудников о методах обеспечения безопасности» главной проблемой, которая не позволяет им защититься от угроз. Эта причина обошла такие пункты, как «маленький бюджет» и «отсутствие квалифицированного персонала».[10]

Источник: [10] Исследование Ponemon Institute об ущербе от киберпреступности 2016

4 В наших системах используется надежное антивирусное программное обеспечение, поэтому мы хорошо защищены

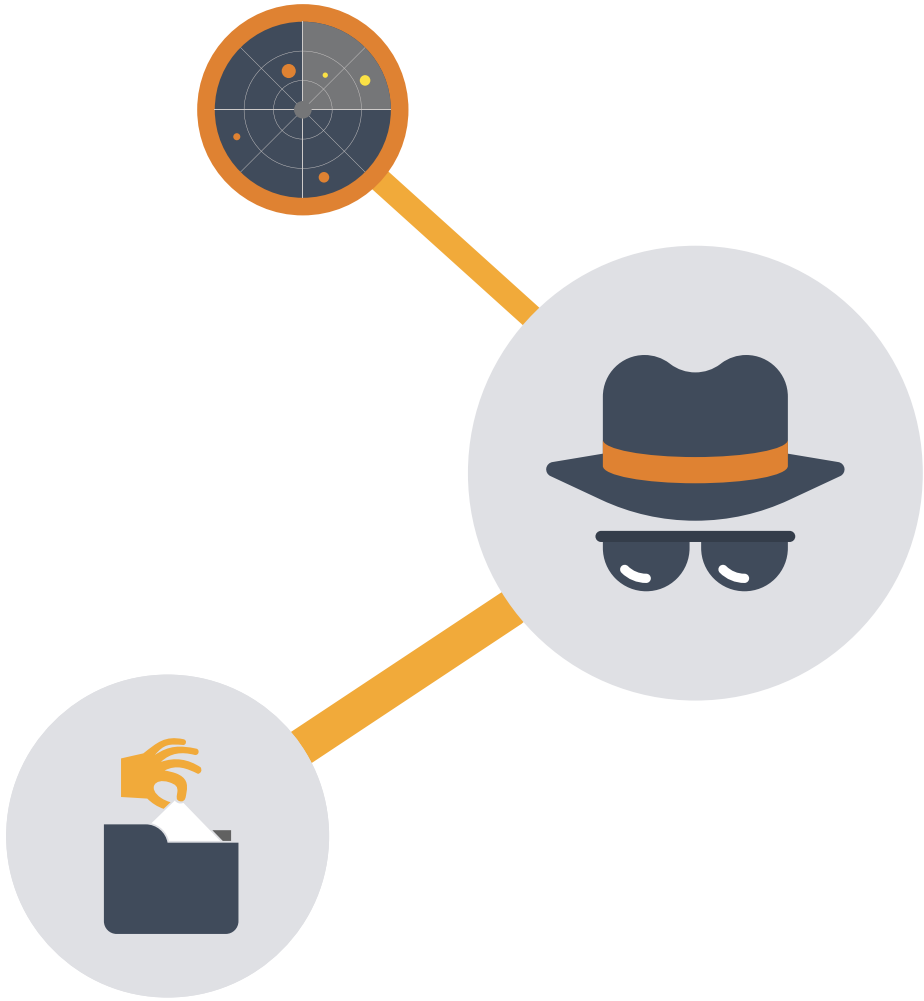


Антивирусное программное обеспечение, по сути, сканирует системы в поиске вредоносных программ, скачанных с веб-сайтов или из электронных сообщений. Но у злоумышленников есть другие способы, чтобы обойти этот уровень защиты.

К кибератакам, которые антивирус не способен предотвратить, относятся распределенные атаки типа «отказ в обслуживании» (DDoS), когда веб-сайт перегружается посторонним трафиком и замедляется или перестает работать; веб-атаки, когда хакеры внедряют вредоносный код в сайт для кражи данных или удаленной слежки; а также доступ через краденые устройства.

5 Если нарушитель попадет в систему, мы сразу это заметим

Обнаружить кибератаку не всегда просто. Вредоносные программы, которые попадают в систему, могут не сразу нарушать ее работу. Они могут начать следить за системой, передавая хакеру информацию для подготовки нацеленных атак — часто для получения доступа к различным сетевым ресурсам.



Такие атаки на конкретные системы называют продвинутыми постоянными угрозами (APT). APT-атаки непрерывно отслеживают и получают данные из определенной ИТ-инфраструктуры с течением времени и обычно остаются необнаруженными.

По оценке консультационной ИТ-фирмы Daisy Group, половину компаний в Великобритании можно взломать меньше чем за час.

СОВЕТ:
Мониторинг исходящих данных для обнаружения необычного роста объема трафика позволяет обнаружить кражу данных — возможно, это APT-атака.

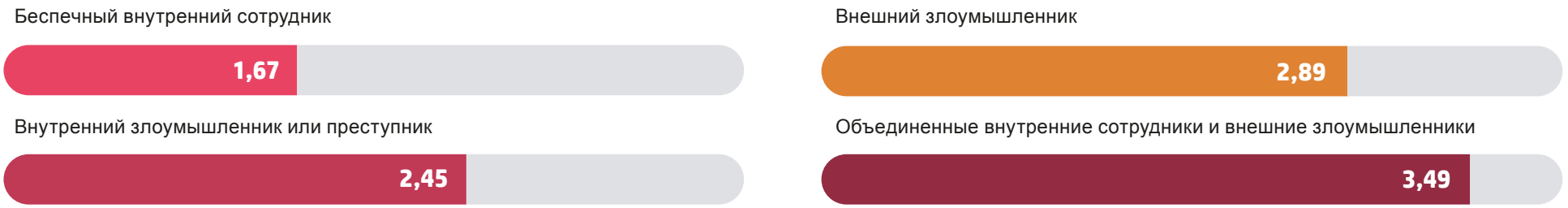
ПРИМИТЕ МЕРЫ:
Выберите программное обеспечение с защитой данных, такое как HP SureStart, которое автоматически восстанавливает систему BIOS компьютера при обнаружении атаки и предотвращает компрометацию данных.

Откуда берутся угрозы?

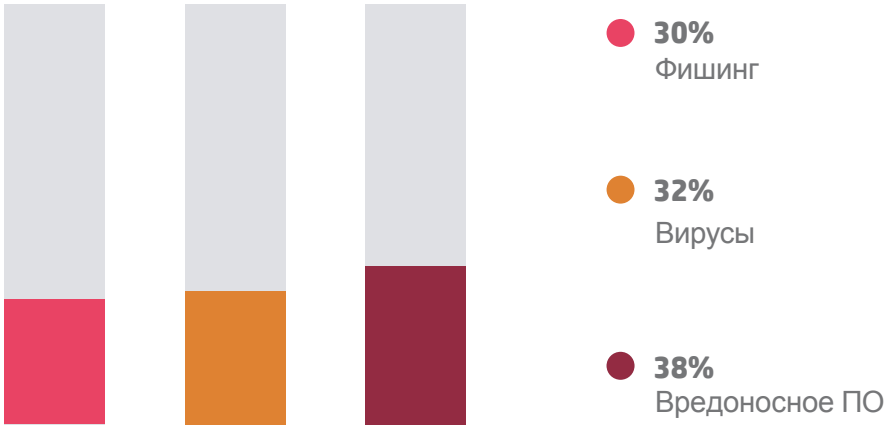
Первый шаг для защиты сети — выявить самые слабые звенья

Самая вероятная причина утечки данных:[11]

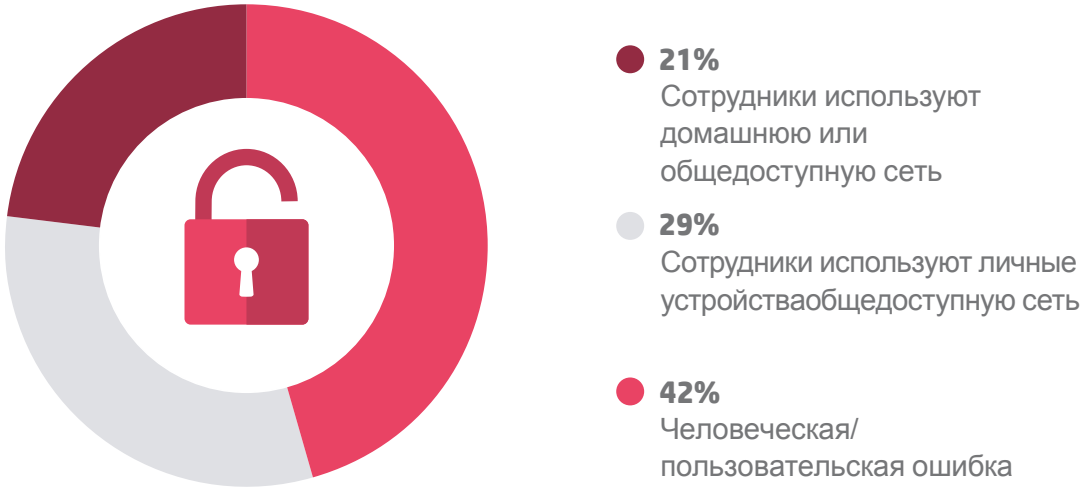
1 = наиболее вероятно 4 = наименее вероятно



Самые распространенные типы внешних угроз:



Как происходят внутренние нарушения безопасности:[12]



Источники: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Исследование Ponemon Institute об ущербе от киберпреступности 2015

Во сколько обходится устранение последствий?

Самые дорогостоящие типы кибератак:

25%

£1,000,000

Вредоносные программы и код

Программы, которые создают лазейки в системе, повреждают файлы или крадут данные (это могут быть скрипты, вирусы и черви)

24%

£960,000

Распределенные атаки типа «отказ в обслуживании»

(DDoS) — это перегрузка сайтов и серверов организации посторонним веб-трафиком

16%

£640,000

Веб-атаки

Атаки, нацеленные на посетителей вашего сайта, такие как внедренный код,перенаправляющий браузеры на вредоносные сайты

13%

£520,000

Краденые устройства

Потерянные сотрудниками устройства с корпоративными учетными данными могут привести к краже данных и мошенничеству с персональными данными

9%

£360,000

Фишинг и социальная инженерия

Мошеннические электронные сообщения или всплывающие окна, маскирующиеся под настоящие для кражи учетных данных

9%

£360,000

Внутренние злоумышленники

Сотрудники, которые передают конфиденциальную информацию

4%

£160,000

Ботнеты

Сети из зараженных компьютеров, которые используются для вредоносных действий, например для рассылки спама

Источник: [13] Исследование Ponemon Institute об ущербе от киберпреступности 2015

Влияние киберпреступлений на бизнес

Настоящий ущерб от киберпреступлений всегда больше стоимости устранения последствий взлома

Нарушения системы безопасности обходятся невероятно дорого. Грубо говоря, взлом системы может повредить финансовому состоянию вашей компании тремя способами.

Ресурсы компании

Очевидно, вам необходимо восстановить работу систем. Для этого требуется много работы и средств. А это значит, что другие проекты, приносящие прибыль, придется приостановить.

Штрафы

К вам могут применить санкции за несоблюдение требований к безопасности (например, HIPAA). После вступления в силу «Общих положений о защите данных» (GDPR) в ЕС в следующем году компании, которые не будут соблюдать новые требования, могут оштрафовать на 4% от глобальной выручки. На вас даже могут подать в суд, если утечка приведет к нарушению конфиденциальности клиента.

Поврежденная репутация

Возможно, это самый дорогостоящий аспект взлома. Клиенты, пресса и общественность в целом надолго запоминают взломы систем компаний.Восстановление прежнего уровня доверия может занять долгое время.

Анатомия непредвиденного взлома

Когда в 2014 г. взломали компанию Sony Pictures, хакеры просто зашли через парадную дверь.[14]

Согласно хакеру с псевдонимом «Lena», участнику группы Guardians of Peace (GOP), которая взяла на себя ответственность за атаку, компания Sony «больше не занимается физической безопасностью». Они получили доступ к сети Sony, зайдя в здание и украв учетные данные компьютера системного администратора.

После этого они разместили вредоносные программы, которые извлекли частные файлы, исходный код и пароли для баз данных Oracle и SQL. С их помощью хакеры украли графики производства кинокартин, электронные сообщения, финансовые документы и многое другое, а затем большую часть материалов опубликовали в сети.

Хакеры угрожали опубликовать другие секретные и совершенно секретные данные, если компания не откажется от проката кинофильма «Интервью».

В итоге Sony капитулировала — компания потеряла неразглашенные кассовые сборы и понесла сокрушительный репутационный ущерб.

Компания Sony сделала две ошибки. Не приняла меры для защиты физического доступа к корпоративным данным от злоумышленников и не вложила средства в организацию многоуровневой системы безопасности, которая помогла бы защитить конфиденциальную информацию после первоначального взлома.

Эксперт по безопасности Брюс Шнейер (Bruce Schneier) написал после атаки: «Перед достаточно квалифицированным, финансируемым и мотивированным злоумышленником не устоит ни одна сеть». Главное — понять, где именно ваша сеть уязвима.
Возможно, это парадная дверь.

ПРИМИТЕ МЕРЫ:
Создайте план реагирования на взлома для каждого отдела — от ИТ до обслуживания клиентов, — чтобы свести время восстановления к минимуму.

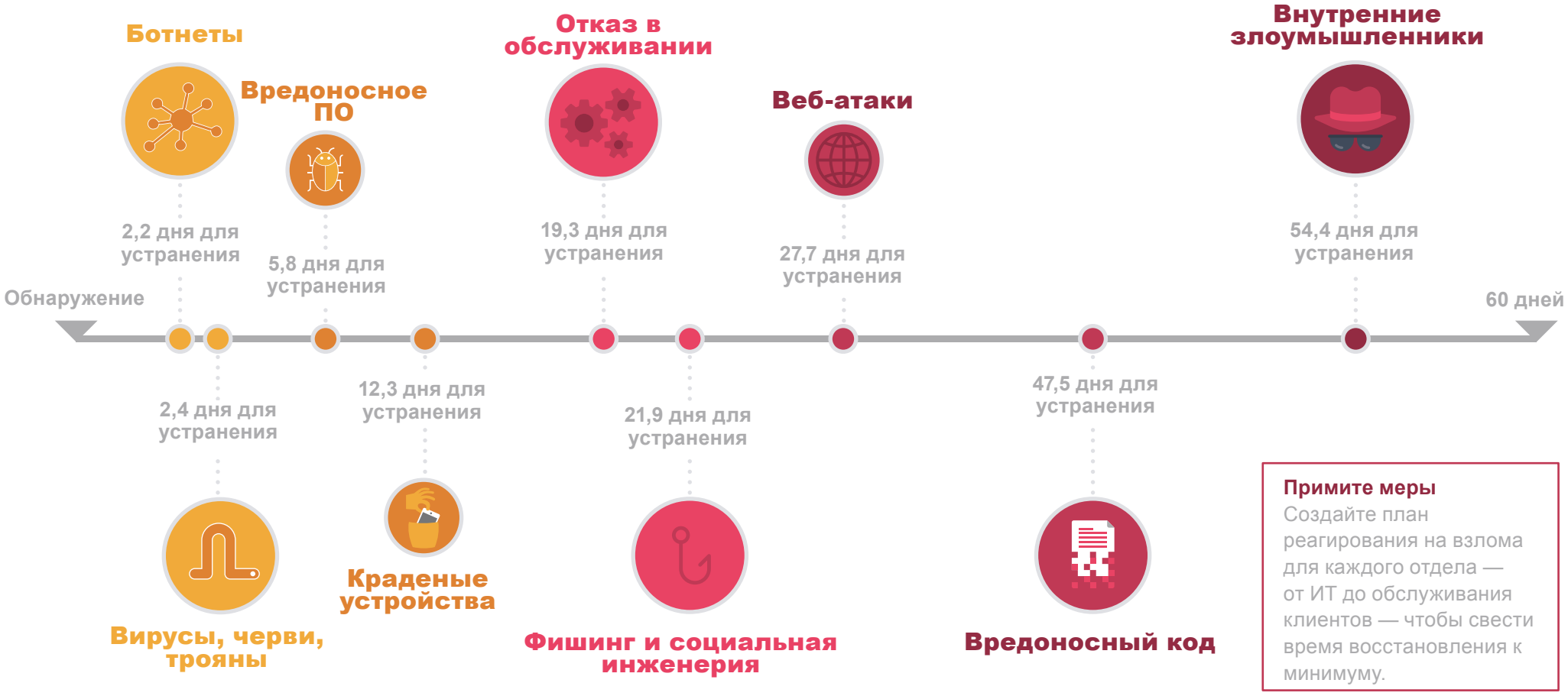
СОВЕТ:
Многие виды вредоносных программ передаются как вложения электронной почты. Обучите персонал распознавать подозрительные файлы, которые могут выглядеть как подлинные документы.

- Приблизительный ущерб от киберпреступности для бизнеса в Великобритании: 21 млрд долларов США[15]
- Средний ущерб от киберпреступности на компанию в Великобритании в 2016 г.: 5,7 млн фунтов[16]
- Компании из Великобритании, которые пострадали от взлома или кибератаки в 2015–2016 гг.: 66 %[17]

Источники: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Сумма 7,21 млн долл. преобразована в фунты
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Киберпреступность: время восстановления

Сколько времени уходит на восстановление последствий взлома?
По оценке Ponemon Institute[18], для этого требуется в среднем 46 дней.
Это пугающая цифра для британского банковского бизнеса, который должен работать без каких-либо перерывов



Примите меры
Создайте план реагирования на взлома для каждого отдела — от ИТ до обслуживания клиентов — чтобы свести время восстановления к минимуму.

Источник: [18] Исследование Ponemon Institute об ущербе от киберпреступности 2015

Как защитить бизнес от киберпреступлений

Ключевые советы и стратегии для киберзащиты предприятий

Вот шесть основных целей для хакеров, взламывающих корпоративные системы, и меры, которые вы можете принять для защиты от них.

Клиентские базы данных

Облачные службы

Смартфоны и планшеты сотрудников

Ошибки сотрудников

Интернет вещей

Сетевые шлюзы

В современном цифровом мире, где данные играют все более важную роль, киберпреступность может принимать различные формы. Киберпреступники часто охотятся на информацию, а с ростом числа подключенных к сети устройств на рабочих местах (от смартфонов и планшетов до WiFi-принтеров) количество точек доступа, доступных хакерам, также увеличивается.

1 Клиентские базы данных

Финансовые данные — далеко не единственная цель злоумышленников. Имена и адреса электронной почты могут использоваться для мошенничества с личными данными, рассылки спама и взлома других учетных записей.

Крупная удача для серьезных хакеров — взломать компании, которые обслуживают еще более масштабные предприятия. Это цифровой эквивалент проникновения в хозяйственный магазин, из подвала которого можно попасть в хранилище национального банка.

Если хакеры проникают в небольшую систему, они получают эффективный доступ к клиентским данным, размещенным более крупными клиентами. Как может быть скомпрометирована клиентская база данных? Вирусы, черви и трояны, скачанные с вредоносных сайтов и электронных сообщений, могут внедрить код, позволяющий хакерам войти в систему и украсть данные.

Как защитить данные клиентов

- Используйте защитное программное обеспечение, созданное для предприятий, которое обеспечивает защиту сети, электронной почты и конечных точек.
- Всегда обновляйте защитное программное обеспечение для блокировки новых вредоносных программ.
- Скачивайте обновления системных программ, так как старые приложения могут содержать уязвимости, которыми хакеры могут воспользоваться.

2 Облачные службы

Как защитить данные клиентов

- Зашифруйте самые важные данные, используя такие инструменты, как технология Smartcrypt от компании PKWARE, которая использует политики доступа для определения сложности шифрования. Таким образом авторизованные пользователи видят данные, которые им необходимо видеть, а неавторизованные пользователи не видят ничего.
- Создайте надежный пароль для облачной учетной записи. Кроме того, точно укажите в параметрах облачной учетной записи, кто может получить доступ к вашим данных и что они смогут с ними делать.
- Используйте двухфакторную проверку подлинности, например код для смартфона вместе с паролем, чтобы изменять облачные данные, например скачивать, удалять или перемещать файлы.

Облачные вычисления стали фундаментом корпоративной инфраструктуры.

По данным опроса об облачных вычислениях, проведенного компанией IDG в 2016 г.[19], 70 процентов предприятий хотя бы частично используют облачную инфраструктуру, а компания Tripwire обнаружила, что 90 процентов используют облако для инфраструктуры и (или) хранения данных, в том числе особо важных.[20]

Безопасность, конечно же, вызывает озабоченность, но на самом деле в облаке данные в большей сохранности, ведь они хранятся на внешних серверах компании, репутация которой напрямую зависит от защиты этих данных.

Поэтому 64 процента предприятий, опрошенных Tripwire, считают облако безопаснее традиционных систем.

К счастью это мнение не далеко от правды — согласно опросу, проведенному компанией BIS в 2015 г.[21], всего 7 процентов компаний (крупных и мелких) пострадали от взлома облачных служб (чаще всего из-за потери прав доступа или слабых паролей). Однако для полной защиты облачным системам требуется надежный механизм управления безопасностью. Вспомните про парадную дверь Sony.

Источники:

[19] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey

[20] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/

[21] Опрос малого бизнеса 2015. Подразделение бизнеса, инноваций и квалификаций

3 Смартфоны и планшеты сотрудников

Многие люди используют личные устройства для выполнения рабочих задач.

Политики BYOD (использования собственных устройств сотрудников) для компаний — это эффективный метод применения смартфонов, которые уже есть у сотрудников. Эта тенденция набирает обороты: 53,2 процента организаций собираются внедрить политики BYOD в течение следующих двух лет.[22] Но эти устройства могут стать крупной добычей для хакеров.

Приблизительно каждое пятое приложение для Android содержит какие-то формы вредоносного кода, который может попасть в файлы и системы компании для слежки или кражи информации.

Эта угроза становится все опаснее: 64,9 процента организаций считают, что объем угроз, нацеленных на их мобильные устройства, вырос.[23]

Сотрудники, телефоны которых украли, также могут неосознанно проложить дорогу хакерам. Телефонный вор может продать устройство на черном рынке, где злоумышленники смогут извлечь ценные сведения для проникновения в компанию жертвы или системы более крупного клиента. Организации оценивают свои возможности защиты от угроз для мобильных устройств как 3,54 из 5. Это самая низкая оценка для всех возможных угроз, которые были затронуты в опросе.[24]

Как защитить личные устройства сотрудников

- Установите средство обнаружения угроз, например X-Ray от компании Duo для устройств с Android, чтобы упростить отслеживание вредоносных приложений и подозрительного кода.
- Попросите сотрудников включить удаленную очистку данных (доступно бесплатно для Android, iPhone и Windows Phone, а также по подписке для BlackBerry), чтобы в случае потери конфиденциальные корпоративные и личные данные можно было удалить.
- Попросите сотрудников включить шифрование на смартфонах, чтобы защитить данные (оно включено по умолчанию на новых телефонах с iOS и Android).

Источник: [22] Отчет о защите от киберугроз 2016, CyberEdge [23] ibid [24] ibid

4 Ошибки сотрудников

Как помочь сотрудникам

- Расскажите сотрудникам о рекомендациях для обеспечения кибербезопасности и регулярно проводите тренинги, посвященные новым угрозам.
- Разработайте протокол безопасности, адаптированный для вашего бизнеса и обрабатываемых данных.
- Создайте команду для распространения политики кибербезопасности среди сотрудников, клиентов и деловых партнеров.

Основная догма кибербезопасности — надежная парольная политика, и все равно 31 процент крупнейших взломов в 2015 г. были связаны с сотрудниками.

Злоумышленники часто используют человеческие ошибки, подбирая слабые пароли, перехватывая документы, которые передаются по незащищенному подключению, или проводя фишинговые атаки против определенных сотрудников.

5 Подготовьтесь к Интернету вещей

Исследовательская фирма IDC прогнозирует, что число устройств, подключенных к Интернету, в 2020 г. вырастет с 13 до 30 миллиардов.[25]

Компьютеры в офисе по крайней мере защищены паролями и, в идеале, специальным программным обеспечением, но подобные меры часто не применяются для очередей и заданий печати.

Такие незащищенные принтеры (и другие сетевые устройства) могут стать жертвой «прослушивающих программ», которые перехватывают задания печати и сетевой трафик, имена пользователей и пароли, которые передаются на сервер киберпреступников.

Стоит отметить, что вызвавший широкий резонанс взлом Dyn был связан с сетью веб-камер наблюдения, произведенных компанией XiongMai Technologies (по данным фирмы Flashpoint).

Это подчеркивает тот факт, что любое устройство в сети может стать точкой входа, и уровень защиты сети равен уровню защиты наименее безопасного устройства в ней. 97 процентов организаций применяют механизмы защиты для настольных компьютеров и ноутбуков, 77 процентов — для мобильных устройств и 57 процентов — для принтеров.[26] Единственный способ сохранить данные в безопасности — использовать механизмы защиты для каждого конечного устройства.

Как подготовиться к Интернету вещей

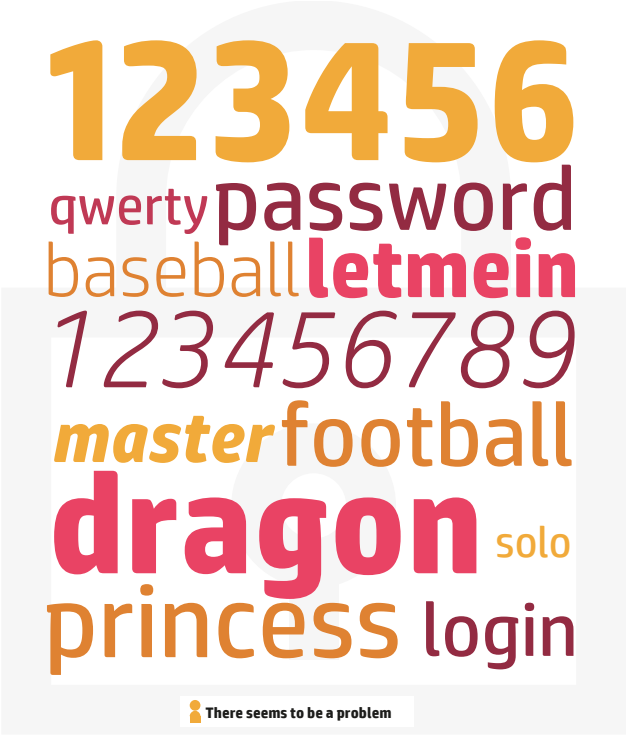
- Удалите или отключите ненужные функции на оборудовании, так как чем больше функций, тем больше потенциальных точек входа для хакеров.

Источники: [25] PwC: Исследование глобального состояния информационной безопасности 2016 [26] Исследование безопасности принтеров HP, Spiceworks 2016

Пароли и программы-вымогатели

Самые распространенные пароли

В начале 2013 г. репортер Ars Technica, который никогда не занимался киберпреступлениями и не взламывал системы, защищенные паролем, получил 8 000 из более чем 16 000 зашифрованных паролей за один день*. Каковы шансы, что такие распространенные пароли устоят против опытного хакера?



Что такое программа-вымогатель

Киберпреступники все чаще используют программы-вымогатели — вид вредоносных программ, которые взламывают систему, шифруют данные и требуют выкуп в биткойнах. В 2013 г. троян Cryptolocker заразил тысячи систем, что привлекло внимание Национального агентства по борьбе с преступностью Великобритании и его подразделения по борьбе с киберпреступностью. Рассмотрим подробнее, как работают такие виды атак.

1. Установка	Вредоносный код попадает на ваш компьютер после непреднамеренной загрузки через электронную почту или вредоносный веб-сайт.
2. Оповещение головного узла	Вирус-вымогатель подключается к домашнему серверу для получения ключа шифрования.
3. Шифрование ваших файлов	Вирус-вымогатель сканирует файлы в вашей сети и шифрует их, делая их недоступными.
4. Вымогательство	Обычно на экране компьютера появляется сообщение с временным ограничением и суммой, которую нужно оплатить для расшифровки до удаления файлов.
5. Оплата	Владелец компании может приобрести цифровую валюту, например биткойн, для перевода злоумышленнику в надежде расшифровки файлов.

* Splashdata

6 Сетевые шлюзы

Когда хакеры хотят проникнуть в сеть, они могут использовать DDoS-атаку — тысячи зараженных вирусами компьютеров вместе создают столько трафика, что сеть не выдерживает такой нагрузки.

Часто злоумышленники, проводящие DDoS-атаки, хотят отвлечь администраторов сайта, пока они крадут данные или устанавливают вредоносные программы для будущих атак. DDoS-атаки часто проводятся взломщиками-дилетантами, которые хотят вывести веб-сайт из строя, просто потому, что они могут это сделать. Даже несколько часов простоя веб-сайта может плохо сказаться на прибыли и репутации компании.

СОВЕТ.
Используйте оборудование со встроенной защитой, например расширенной проверкой подлинности и инструментами шифрования.

Как защитить сеть

- Используйте системы, которые проверяют трафик, поступающий в сеть и из нее. Неожиданный пик может указывать на атаку, а постоянная, но необъяснимая активность может свидетельствовать о трояне, который передает данные своему серверу.
- Фильтруйте весь трафик, чтобы в сеть попадали только данные, необходимые для ее поддержки.
- Убедитесь, что каждый маршрутизатор, коммутатор и любое другое устройство использует одинаковые версии программного обеспечения и функции, а также всегда устанавливайте последние обновления.

Будущее кибербезопасности бизнеса

Компании становятся все более зависимыми от Интернета, поэтому им просто необходимо реализовать надежные средства киберзащиты.

Сегодня сотрудники приходят на работу с личными устройствами. Компании могут использовать облачные платформы и внешние технические службы. И все больше людей работают удаленно. Обеспечение кибербезопасности становится сложнее, если вы не контролируете ни устройства, ни инфраструктуру, ни рабочее место.

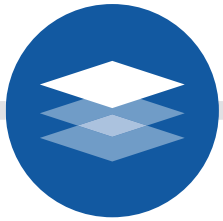
В то же время смартфоны научили нас, что работать можно в любом месте и в любое время. Кафе — такое же хорошее место для работы, как и офис. Мы используем общедоступные сети WiFi для обработки огромных объемов корпоративных и личных данных, при этом смартфоны часто не отличаются надежной защитой. Преступники определенно заметили эту тенденцию. Безопасность находится под угрозой, если мы не уделяем достаточно внимания обстоятельствам, при которых мы работаем.

В ближайшем будущем для надежной защиты потребуется гораздо больше, чем установить антивирус на устройства или обновлять пароли раз в полгода. Компаниям необходимо внедрить расширенные механизмы обеспечения безопасности, которые удаленно работают так же эффективно, как и в офисе с ИТ-администратором. Для распределенных организаций будущего кибербезопасность будет основана на интеллектуальном анализе для выявления необычного поведения и многоуровневой защите всех точек доступа.

Будущее кибербезопасности бизнеса

Аналитика: кибердетектив

Даже если объемы трафика на вашем сайте не велики, из него можно выделить определенные закономерности. Используя аналитические инструменты, которые оценивают и фиксируют любую активность, вы сможете легко проводить диагностику, когда что-то идет не так. Эти средства отслеживают и документируют нормальное поведение, чтобы обнаружить аномалии в дальнейшем. После обнаружения администраторы могут перейти к активным мерам и устранить угрозы, прежде чем они нанесут какой-либо ущерб.



Многоуровневая защита: будьте на шаг впереди злоумышленников

Многоуровневая (или глубокая) защита позволяет несколькими способами обеспечить безопасности каждой точки доступа. Среди популярных подходов — расширенные сертификаты подлинности SSL, которые усложняют подделку учетных данных, необходимых для попадания в защищенную сеть. Если дополнить этот подход многофакторной проверкой подлинности, когда хакерам необходимо подобрать не только пароль, защита станет еще надежнее.

Независимо от конкретной используемой технологии многоуровневый принцип заключается в защите каждой важной области сети определенным образом. Вашим пользователям и партнерам может понадобится больше времени для доступа к важным данным, но за такое неудобство вас вознаградит уверенность в защите вашего бизнеса.

Примите меры сейчас

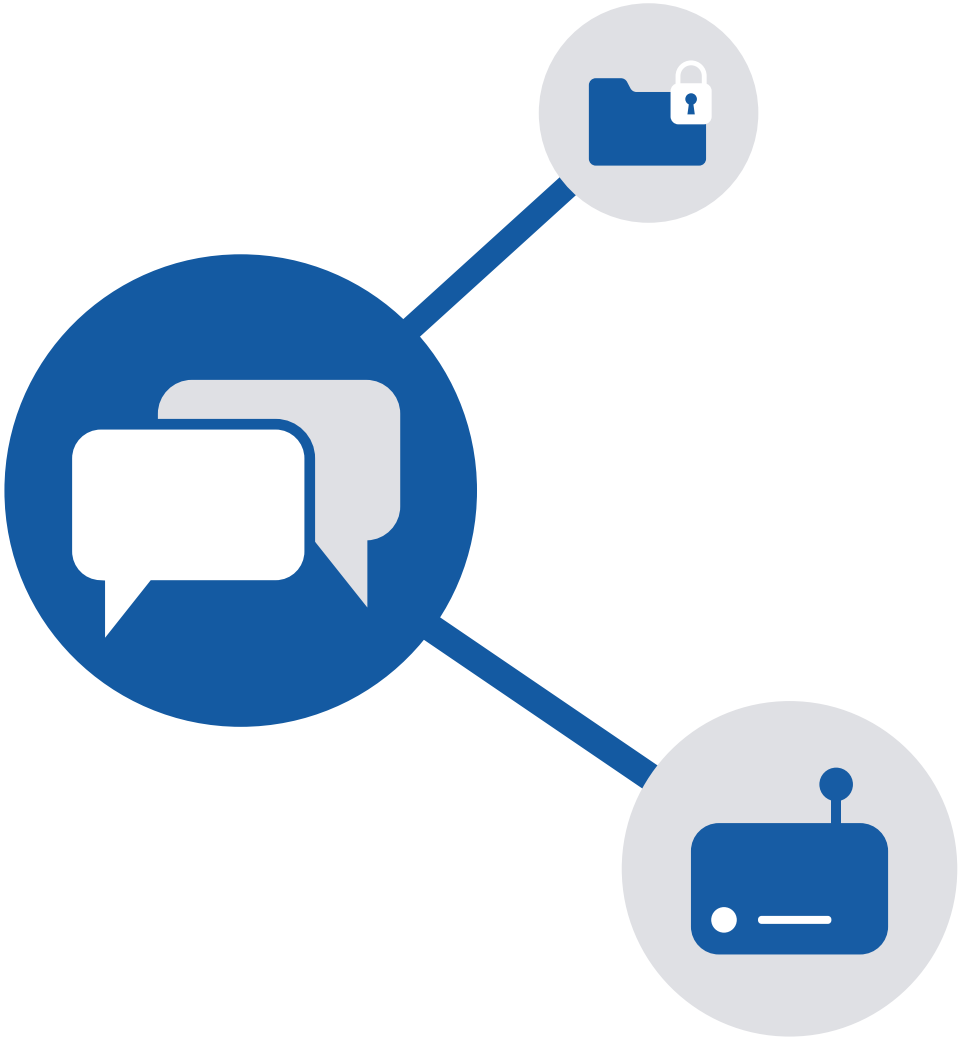
Лучшая защита — инвестиции в программное обеспечение для кибербезопасности и обучение. Начните с аудита ваших систем и инфраструктуры. Делаете ли вы достаточно? Что вы можете улучшить?

Наконец, вы можете позвонить экспертам Hewlett Packard Inc. Наша коллективная база знаний позволяет идти на шаг впереди злоумышленников, а не просто реагировать на совершенные атаки. Чтобы узнать больше, посетите веб-сайт HP.com.

СОВЕТ.
Отслеживайте и документируйте нормальное поведение, чтобы обнаружить аномалии в дальнейшем.

Рекомендации для защиты сетевых устройств

Защита каждого устройства в сети



Исследование в сфере безопасности, проведенное компанией Spiceworks[27], выявило следующие основные источники угроз безопасности бизнеса.

- Ноутбуки и настольные компьютеры: 81% внешние и 80% внутренние
- Мобильные устройства: 36% внешние и 38% внутренние
- Принтеры 16% внешние и 16% внутренние

Какие из этих угроз необходимо предотвратить в первую очередь? Ответ очень прост — все. Хотя это может быть очевидно, но пугающее число организаций по-прежнему выбирают, какие устройства следует защитить.

Компания HP считает, что любое устройство, которое подключается к вашей сети, должно быть защищено. Проще говоря, уровень безопасности вашей сети равен уровню безопасности наименее защищенного устройства.

Интуиция может подсказывать вам, что безопасность подключенного принтера не так важна, как защита всех рабочих ноутбуков. Но на самом деле риск одинаков. Хакеры давно используют принтеры и любые интеллектуальные устройства, подключенные к сети. Они знают, что такие устройства плохо защищены, но дают такой же доступ к сети.

Источник: [27] Исследование безопасности принтеров HP 2016, Spiceworks

HP: показывая путь в новое время

Мир кибербезопасности меняется. У нас есть инструменты, которые помогут вам защититься.

В мире кибербезопасности нет быстрых исправлений. Для надежной защиты требуется многогранный подход, охватывающий сети, устройства и пользователей. Правильный первый шаг — выбор нужной технологии.

Компания HP ставит безопасность на первое место. Семейство устройств HP Premium Elite отличается уникальными функциями обеспечения безопасности, недоступными у конкурентов, такими как HP SureStart — первая в мире система BIOS с автоматическим восстановлением.

В устройствах HP используются следующие технологии.

- **Bluetooth-блокировка:** устройство автоматически блокируется с помощью Bluetooth, когда вы отходите от него, и разблокируется, когда вы возвращаетесь.
- **Биометрическая защита:** распознавание лица и отпечатков пальцев позволяет предоставить доступ только авторизованным пользователям.
- **Экраны HP SureView*:** если монитор затемнен, посторонние не смогут прочитать данные на нем, что позволяет защитить конфиденциальные материалы при работе в пути.
- **BIOS HP SureStart с автоматическим восстановлением:** все устройства HP Elite проверяют свою систему BIOS каждые 15 минут. При обнаружении аномалии компьютер восстанавливает исходное состояние, лишая злоумышленников доступа.

Компьютеры HP Elite не защитят ваш бизнес самостоятельно. Но они станут надежной первой линией обороны. Посетите веб-сайт www8.hp.com, чтобы узнать о всей линейке продуктов HP Elite.

*Только в отдельных моделях

HP: лидер инновационной печати

Защитите свою сеть с самой безопасной печатью HP*

«Свидетельством долгосрочных инвестиций HP в безопасную печать является его самый широкий и разнообразный набор услуг и решений безопасности представленных на рынке».

– Quocirca, январь 2017 г.**

В устройствах HP используются следующие технологии.

- **Обнаружение вторжений в режиме реального времени:** Обнаружение вторжений в режиме реального времени от HP защищает устройства во время выполнения операций и при подключении к сети: именно в таких случаях происходит большинство атак.
- **Jet Advantage Security Manager:** Данное решение предоставляет ИТ-менеджерам простой способ оценки, и при необходимости, исправления настроек безопасности всех устройств компании для обеспечения соответствия установленным политикам безопасности.
- **BIOS HP SureStart с автоматическим восстановлением:** При перезагрузке HP SureStart обнаруживает вредоносный код и предотвращает его выполнение, а затем инициирует восстановление BIOS. При перезагрузке используется встроенная «золотая» копия.
- **Список разрешенных программ:** Благодаря данной функции в память загружается только аутентичный проверенный код HP. При обнаружении аномалии устройство отключается от сети и перезагружается в безопасном режиме, а также отправляет уведомление в ИТ-отдел.

Источники: *5 Утверждение о «самой безопасной печати HP» сделано на основе опубликованных результатов обзора функций безопасности конкурентных принтеров одного класса, проведенного компанией HP в 2016 г. Только HP предлагает сочетание функций безопасности для отслеживания и автоматической остановки атак и последующей самостоятельной проверки целостности программного обеспечения при перезагрузке.
**Quocirca, «Безопасность печати: непреложное требование в эпоху Интернета вещей» quocirca.com/content/print-security-imperative-iot-era, январь 2017 г.

Глоссарий и дополнительные материалы

Средства управления доступом

Ботнет
Обычно это тип автоматической программы для управления компьютерами, подключенными к Интернету, без ведома владельца. Часто эти компьютеры заражены вредоносными программами. Хакеры используют ботнеты для проведения атак типа «отказ в обслуживании» и вывода веб-сайта из строя.

Средства защиты от потери данных
Широкая категория программного обеспечения, цель которого заключается в мониторинге конфиденциальных данных и предотвращении попыток доступа к ним или их копирования со стороны неавторизованных пользователей. Для защиты точки доступа (конечного устройства) используются различные подходы за счет обхода сети или файловой системы. По оценкам компании Gartner, этот рынок вырос на 25 процентов в 2013 г.

Технологии шифрования
Инструменты, которые делают данные нечитаемыми без определенного декодера. Комиссар по информации Великобритании в прошлые годы активно выступал в поддержку различных видов шифрования. Недавно правительству пришлось поменять свою позицию касательно технологий шифрования из-за жестокой критики.

Брандмауэры
Еще один широкий термин, описывающий устройства, которые используют алгоритмы и другие методы для предотвращения попадания неавторизованного трафика и несанкционированных пользователей в сеть. В следующем поколении таких устройств могут быть объединены функции, которые ранее предоставляли только отдельные устройства, такие как обнаружение вторжений. Они также ориентированы на приложения, т.е. могут отличить веб-трафик от данных salesforce.com и страницы Facebook.

Инструменты управления рисками и соответствием (GRC)
Изначально этот термин описывал широкие и координированные процессы в компании, направленные на управление операциями в соответствии с нормативными требованиями для снижения рисков.

Вредоносное ПО
Широкая категория программ, которая может нанести вред другим системам и даже вывести их из строя. В качестве примера можно привести вирусы, черви и трояны. Кроме того, в исследовании Ponemon, которое цитируется в этой электронной книге, считается, что вредоносные программы отличаются от вирусов, так как они «находятся на конечной точке, но еще не попали в сеть».

Средства контроля периметра
Общая категория, описывающая киберзащиту в точке, где Интернет или другая общедоступная сеть встречается с частной локальной сетью. Обычно для защиты периметра используются различные уровни и типы устройств.

Фишинг
Обычно происходит по электронной почте, когда злоумышленник пытается получить учетные данные с помощью диалогового окна, замаскированного под настоящее.

Инструменты управления политиками
В широком смысле инструменты управления политиками задают стандарт, определяющий, что те или иные пользователи могут видеть, а затем применяют такую политику во всей сети. Согласованность (по крайней мере в теории) улучшает безопасность.

Глоссарий и дополнительные материалы

Аналитические системы безопасности
Широкий спектр аналитических инструментов позволяет собирать и создавать данные, связанные с угрозами. Это могут быть такие системы, как диспетчеры журналов и средства обнаружения сетевых аномалий.

Социальная инженерия
С помощью этой методики злоумышленники принуждают авторизованного пользователя передать им конфиденциальную информацию для получения доступа.

Троянский конь (троян)
Троянские кони, как вирусы и черви, должны быть установлены пользователем, поэтому они очень хорошо маскируются. Трояны могут менять настройки компьютера, удалять файл и создавать «лазейку», которую хакер сможет использовать в дальнейшем.

Вирусы
Вредоносный код, способный копировать себя и распространяться по сети.

Веб-атаки
Чаще всего веб-атака заключается в перенаправлении браузера на вредоносный сайт.

Черви
В отличие от вирусов, которые распространяются с файлом-носителем, черви могут размножаться независимо от файла-носителя, например документа Word или Excel, поэтому они могут нанести серьезный ущерб без человеческого участия. Системы мгновенных сообщений часто становятся источниками червей, например приложение Skype пострадало от такой атаки в 2012 г.