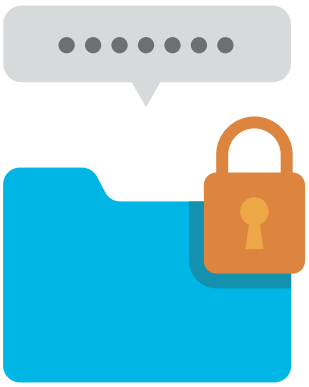
Официальный документ для бизнеса

Безопасность начинается с конечной точки

Определение приоритетов безопасности конечных точек

Предоставлено

Сводное резюме



За последние 12 месяцев 82% организаций столкнулись с киберугрозой или взломом.[1] Частота, серьезность и ущерб от киберпреступлений продолжают расти.

Парадигма «предотвращения и защиты» — обеспечения безопасности сетевого периметра с брандмауэром — уже больше не актуальна. Более эффективен подход «обнаружение и реагирование».

Но ИТ-бюджеты не поспевают за развитием кибербезопасности. 77% расходов по-прежнему уходит на предотвращение и защиту.[2] Всего 36% менеджеров по ИТ-безопасности считают, что их бюджета недостаточно для эффективной защиты конечных точек.[3]

Но вы можете надежно защитить ваши данные. С помощью правильных технологий (от решений типа «обнаружение и реагирование» до отдельных устройств), правильной стратегии и необходимых ресурсов организации могут защититься от киберпреступников.

Без увеличения инвестиций в кибербезопасность и выделения средств на по-настоящему эффективную защиту число нарушений безопасности будет расти, как и ущерб от них.

Введение

Кибербезопасность в эпоху аморфных сетей
60% ИТ-руководителей считают, что их системы защиты не справляются с растущим объемом и усложнением кибератак. 80% ведущих специалистов по безопасности считают, что риски в виде продвинутых постоянных угроз (APT), криминальных групп, поддерживаемых государством хакеров и хактивистов растут и являются главной проблемой для ИТ-безопасности.[4]

И они правы. Правительство Великобритании оценивает ущерб от киберпреступности в 27 миллиардов фунтов, это «серьезная сумма, которая будет расти», при этом потери для бизнеса составляют 21 миллиард фунтов.[5]В отчете о состоянии конечных точек, проведенных Ponemon в 2016 г., 78% компаний сообщили об увеличении степени серьезности кибератак до 47% в 2011 г.

Но не стоит обращать внимание только на внешние угрозы, так как при этом все ресурсы могут оказаться выделенными только для предотвращения атак и защиты периметра.

Хотя внешние атаки (вирусы, вредоносные программы, фишинг) более распространены, инсайдерские атаки обходятся дороже.[6] Многие из внешних атак вызваны внутренними уязвимостями, такими как несоблюдение протоколов безопасности сотрудниками и незащищенные устройства, подключенные к сети. Около 81% респондентов, опрошенных Ponemon, указали их самой главной угрозой ИТ-безопасности.

В будущем ситуация станет еще хуже. Конечная точка — это самое слабое звено любой сети, а с ростом популярности концепций BYOD, удаленной работы и Интернета вещей конечных точек станет еще больше. Это значит, что число точек входа для хакеров также вырастет.

Бизнес-сети далеко ушли от контролируемых сетей из настольных компьютеров, соединенных по Ethernet, и стали аморфными структурами из корпоративных и личных устройств, которые получают доступ к данным через множество узлов WiFi внутри сети и за ее пределами.

Но все не так плохо. Компаниям нужно просто внедрить новый подход к кибербезопасности. Новые стратегии, которые позволяют реагировать на меняющиеся формы киберпреступности. Новые технологии, способные отражать все более сложные угрозы.

В этом официальном документе мы изучим природу и масштаб угрозы, чтобы лучше понять нашего врага, прежде чем перейти к вопросу о том, как добиться кибербезопасности в эпоху миллионов устройств, незащищенных сетей и облачных платформ.

[1] Исследование безопасности принтеров HPI 2016 (Spiceworks)
[2] Управление реагированием на инциденты, PAC 2015: https://www.pac-online.com/download/19443/155514
[3] Отчет о состоянии конечных точек, Ponemon 2016
[4] Оценка CISO, IBM 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

Масштаб угрозы

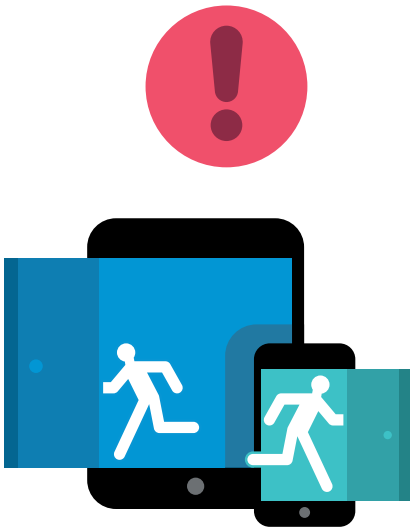
Средняя сумма восстановления от утечки данных для компаний составляет 907 053 долларов США, а потеря прибыли — 13%. В среднем организации требуется девять недель для восстановления.[7]

Около 85% компаний, опрошенных при создании отчета о безопасности принтеров HP в 2015 г., столкнулись с кибератакой/взломом за предыдущие 12 месяцев. 80% опрошенных ИТ-специалистов ожидают, что в следующие три года угроза станет еще серьезнее.[8]

Киберпреступления стоят настоящих денег. Потерянная стоимость украденных или поврежденных ресурсов. Потерянная прибыль из-за репутационного ущерба и потери производительности. Потерянные ресурсы, затраченные на восстановления — время работы службы поддержки, внедрение новых политик безопасности, потери персонала и другие внутренние ресурсы. Штрафы надзорных органов. Падение стоимости акций.

Из-за роста числа устройств, подключенных к сети, риски будут становиться только выше. По прогнозам компании Gartner, из-за Интернета вещей количество подключенных устройств в 2018 г. вырастет до 11,4 миллиарда по сравнению с 6,4 миллиарда в 2016 г. К 2020 г. более 25% выявленных атак на предприятия будут связаны с Интернетом вещей, но при этом всего 10% бюджета безопасности будет уходить на Интернет вещей.[9]

Угроза от кибербезопасности уже является очень серьезной, а в будущем ситуация станет еще хуже.



Формы угрозы

Компании каждый день сталкиваются с бесчисленными кибератаками. Большинство из них — низкоуровневые атаки с использованием вирусов и вредоносных программ. 99% организаций, опрошенных Ponemon в 2016 г., за предыдущие 12 месяцев столкнулись с вредоносными программами. Подобные внешние веб-атаки относительно безвредные и в среднем обходятся организациям в 4 639 долларов США.[10]

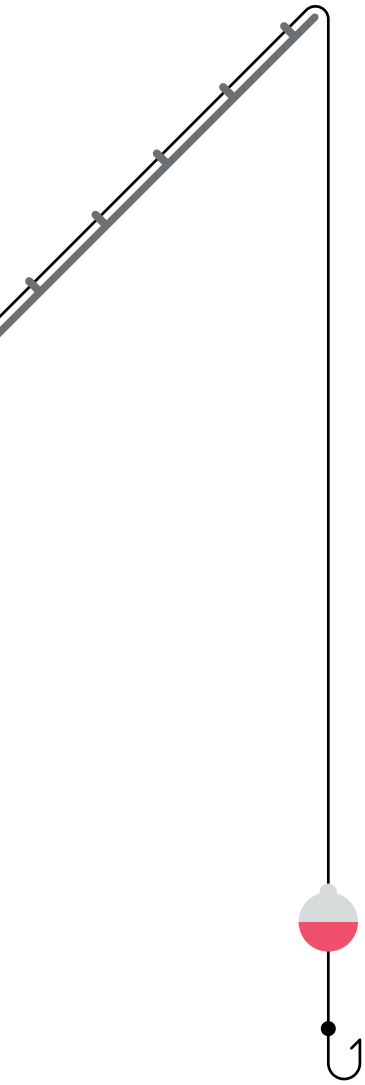
Но число более серьезных атак растет с каждым днем. 51% организаций, опрошенных в 2015 г., подверглись распределенным атакам типа «отказ в обслуживании» (DDoS) с серьезными последствиями, которые в среднем обошлись в 127 000 долларов США. Еще тревожнее то, что 35% организаций стали жертвами атак внутренних злоумышленников, которые в среднем обошлись в 145 000 долларов США.[9]

В целом картина выглядит так: неослабевающие внешние атаки и редкие, но все более серьезные масштабные атаки, которые вызваны халатностью, если не преступными намерениями. 62% организаций столкнулись с фишинговыми атаками и попытками социальной инженерии с использованием слабостей сотрудников, которые в среднем обходились в 86 000 долларов США.[11]

В отдельном исследовании компании Spiceworks, заказанном HP, были проанализированы атаки, совершенные против 90 организаций в Великобритании в 2014–2015 гг.[12]

[7] Отчет о стоимости рисков безопасности NTT, 2016
[8] Отчет о безопасности принтеров HP, 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] Отчет о безопасности принтеров HPI, Spiceworks 2016

Как происходит взлом данных



В заголовках газет можно увидеть, как хакеры взламывают суперзащищенные сети правительств и крупных предприятий, но реальность намного прозаичнее.

Вирусы могут проникнуть в скомпрометированные сети, для распространения вредоносных программ требуются какие-то ошибки пользователей. Фишинговые атаки и попытки социальной инженерии зависят от них. Масштабные DDoS-атаки и кража информации часто является результатом халастности пользователей.

Известный взлом Dropbox стал возможен из-за беспечного сотрудника, который использовал для внутренних систем такой же пароль, что и для учетной записи LinkedIn.[13] Взлом серверов Демократической партии США был осуществлен, когда Джон Подеста — бывший советник Хиллари Клинтон, щелкнул ссылку в фишинговом электронном сообщении, по ошибке отмеченном как подлинное референтом.[14]

Хакерам не нужна активная помощь для успешной атаки. Такая же опасность связана с несоблюдением протоколов безопасности. Сотрудники все чаще приносят свои устройства на работу и используют коммерческие облачные системы, что создает больше незащищенных точек входа в, казалось бы, безопасную сеть. Они не контролируются корпоративными ИТ-специалистами и могут стать скрытыми уязвимостями.

В большинстве случаев хакерам даже не требуется применять сложные алгоритмы или передовые технологии, им всего лишь нужно, чтобы кто-то повел себя беспечно.

Брандмауэр прорван

Ранее краеугольными камнями кибербезопасности были антивирусы и брандмауэры. Предотвращение и защита. Создание безопасного периметра. В текущей рабочей среде эта стратегия не оправдывает себя.

81% респондентов, опрошенных Ponemon, сказали, что мобильные устройства в их сети стали целью вредоносных программ. К другим растущим рискам безопасности относятся использование сотрудниками коммерческих облачных приложений (72% респондентов), BYOD (69%) и работа сотрудников из домашних и удаленных офисов (62%).[15]

Проще говоря, брандмауэр имел смысл, когда сетевой администратор мог контролировать устройства, подключенные к сети. Но в эпоху, когда сотрудники приносят личные устройства на работу (часто даже несколько устройств без уведомления ИТ-отдела), а число удаленных работников растет рекордными темпами, вы просто не сможете защитить периметр. Каждое непроверенное устройство — это уязвимая конечная точка для хакеров.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0
[15] Отчет о состоянии конечных точек, Ponemon 2016

Перспектива HP: выход за рамки защиты сети

Майкл Ховард (Michael Howard) — глобальный специалист по безопасности HP, об обеспечении безопасности конечных точек

Ключевая и текущая проблема состоит в том, что организации не могут защитить каждую конечную точку из-за недостатка знаний об определенных устройствах и связанных рисках. Они чувствуют себя безопасно под защитой брандмауэра, хотя он больше не может справиться со всеми атаками. Специалистам по безопасности нужно узнать о каждой конечной точке в инфраструктуре и убедиться, что ко всем устройствам применяется несколько уровней защиты от самых сложных атак.

Им необходимо изучить все закоулки ИТ-инфраструктуры и создать дополнительный уровень защиты в дополнение к стандартным сетевым периметрам. Брандмауэры сами по себе не могут выстоять против сложных атак, поэтому всем компаниям нужна политика безопасности с несколькими уровнями защиты для каждой конечной точки, чтобы они могли соблюдать нормативные требования и не платить увесистые штрафы.

Политика HP заключается в том, что безопасность — это ключевой приоритет для каждого нового решения, службы или продукта. Разработчики знают, что им необходимо ответить на вопросы о безопасности и понять, как защитить устройства в сети.

Безопасности следует уделять первоочередное внимание, как никогда прежде. Именно такую политику компания HP применяет много лет.

Многоуровневая защита

Новый подход к обеспечению кибербезопасности должен быть многоуровневым. Защита сети по-прежнему важна, но она должна быть реализована в самих сетях. Многие атаки полагаются на точку входа, которая предоставляет доступ ко всем ресурсам системы. Вспомните об удачном фишинге против Джона Подесты. Конфиденциальная информация должна быть защищена множеством уровнем доступа, чтобы потеря одного ключа не привела к захвату всей системы.

Следует регистрировать и отслеживать все устройства. Одна из самых сложных задач для ИТ-руководителей состоит в защите всех устройств, подключенных к сети, с помощью регулярно обновляемого программного обеспечения (от вирусов, вредоносных и шпионских программ) и их проверке на наличие аномалий. Лучше использовать сами устройства в качестве датчиков, собирая данные в реальном времени для выявления всех вторжений в сетевой периметр, частью которого они являются.

Необходимо применять комплексные механизмы управления безопасностью, а также проводить обучение всех сотрудников протоколам кибербезопасности. Человеческая ошибка (от перехода по неверной ссылке до подключения с потребительского устройства) — главная угроза сети. Число человеческих ошибок можно уменьшить с помощью обучения.

Безопасность устройств

Возможно, самая главная проблема для современной кибербезопасности — контроль над устройствами, получающими доступ к сети.
Первое, простое решение, которое часто применяют — отдельные сети WiFi для гостей и сотрудников, чтобы незащищенные внешние устройства не могли получить доступ к основной сети. Кроме того, необходимо проводить обучение для сотрудников по использованию сети с личными устройствами.

Второй фактор — получение контроля над устройствами сотрудника. Этот аспект необходимо включить в корпоративную политику BYOD (принести личное устройство) или CYOD (выберите свое устройство), при этом CYOD гораздо предпочтительнее, так как вы получаете больше контроля над тем, какие устройства используются, выбираете функции безопасности, способ их настройки, а также методы контроля и мониторинга.

Например, настольные компьютеры HP Elite оптимальнее бюджетных ноутбуков. Каждый компьютер HP Elite использует технологию HP SureStart, которая проверяет систему BIOS каждые 15 минут и восстанавливает исходное состояние при обнаружении аномалий, блокируя доступ злоумышленникам. Из-за этой и многих других функции компьютеры серии HP Elite 800 недавно назвали «самыми безопасными».[16] Но сотрудники вряд ли сами приобретут компьютеры HP Elite.

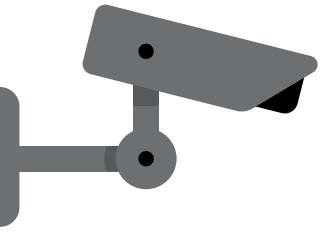
Чаще всего они предпочитают использовать собственные устройства по двум причинам:
1. Потребительские устройства во многих случаях лучше, чем предоставляемые на работе инструменты
2. Сотрудникам нравится использовать знакомые им технологии

Применяя эффективную политику CYOD, организации могут предоставить работникам новейшие устройства с регулярными обновлениями, которые лучше личных, и сохранить контроль над безопасностью этих устройств. Поэтому мы продаем продукты HP по модели «устройство как услуга» (DaaS).

Необходимо включить все устройства в стратегию безопасности, даже те, о которых часто забывают. 80% респондентов, опрошенных IDC, сказали, что ИТ-безопасность важна для их бизнеса, но только 59% считают безопасность принтеров таким же важным аспектом, хотя более половины из них столкнулись с инцидентами, связанными с безопасностью принтеров за последние 12 месяцев. Это очевидная «слепая зона».

Среднее число взломов до внедрения политики безопасности принтеров составляло 9,9 в год со средним ущербом в размере 521 400 долларов США (включая штрафы). После внедрение политики безопасности принтеров среднее число нарушений упало до 1,5, что позволяет экономить 200 часов рабочего времени сотрудников в год и 250 000 долларов США расходов, включая затраты на аудит и соблюдение требований.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] Бизнес-ценность безопасности принтеров, IDC 2015



Проактивное обнаружение и реагирование

77% бюджета на ИТ-безопасность тратится на технологии предотвращения и защиты, такие как антивирусы и брандмауэры, согласно исследованию PAC. Но это неэффективный процесс. Исследование также показало, что 67% опрошенных организаций столкнулись с кибератакой за предыдущие 12 месяцев, а 100% стали жертвами атаки в прошлом в целом.[18]

Антивирусы, в частности, на удивление неэффективны. Компания Damballa провела тестирование, преднамеренно атакуя сеть для оценки реагирования антивирусов. Им потребовалось более шести месяцев, чтобы найти все вредоносные файлы.[19] Это согласуется с другим результатом исследования PAC — компаниям требуется от одного до шести месяцев, чтобы понять, что они стали целью атаки.

Для защиты конечных точек больше нельзя полагаться только на технологии предотвращения. Растущее число заражений вирусами и вредоносными программами, а также врожденная незащищенность BYOD/мобильных работников означают, что нарушения безопасности неизбежны. Никто не предлагает полностью отказаться от технологий предотвращения и защиты, но подход обнаружения и реагирования, определенно, должен получить более высокий приоритет.

Необходим непрерывный мониторинг в реальном времени, для которого в идеале используются сами конечные точки, уведомляющие другие компоненты сети в случае взлома. Это позволит ИТ-специалистам удаленно реагировать на атаки, используя такие процессы, как:

- удаленное отключение устройств;
- удаление зараженных процессов и процессов, распространяющих вредоносные программы;
- помещение файлов в карантин;
- отключение сети для изоляции зараженных устройств.[20]

Только приняв тот факт, что нарушения безопасности неизбежны, и внедрив протоколы реагирования (а также технологии, необходимые для их реализации), можно обеспечить кибербезопасность в наше время, когда предотвращение больше не является надежной защитой.

«Ни одна технология не может обеспечить защиту, если люди будут работать против них».

Джозеф Стейнберг (Joseph Steinberg) [21]

Безопасность сотрудников

Безопасность пользователей важна не менее (или даже более) защиты самих устройств.
Каждый сотрудник должен пройти обучение в сфере кибербезопасности. Они должны знать о всех рисках фишинга. О просмотре подозрительных веб-сайтов. О скачивании подозрительных вложений. Им нужно знать о политике надежных паролей — следует использовать уникальные надежные пароли для каждого входа в систему, а также соответствующей диспетчер паролей для их хранения.

Им необходимо сообщить о важности регулярного обновления защитных программ на своих устройствах, чтобы упростить задачу ИТ-отдела. Они должны использовать только безопасные устройства для доступа к корпоративным сетям и не применять личные устройства во внешних, незащищенных сетях для доступа к конфиденциальным данным.

Многие опытные эксперты по кибербезопасности рекомендуют выполнять моделированные фишинговые атаки (даже создавая фальшивые фишинговые веб-сайты) и проводить обучение на формальном уровне. Так как большинство злоумышленников полагаются на человеческий фактор, будь то халатность или преступные намерения.

Это вызвано тем, что люди — это самое слабое звено в любой сети.

[18] Управление реагированием на инциденты, PAC 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] Контрольный список для обнаружения конечных точек — HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Заключение

Расходы на ИТ-безопасность следует перераспределить с технологий предотвращения и защиты на методы обнаружения и реагирования для конечных точек

Для защиты данных организации в современной ИТ-среде (на фоне растущих киберугроз и потери контроля над сетевым периметром) требуется концептуальный сдвиг и больше ресурсов.

Необходимо изменить концепцию сети. Идея сети как забора вокруг набора устройств больше не применима. Пришло время осознать реальность. Сеть — это химера. Она возникает при подключении каждого устройства и каждой конечной точки. Защита сети — это защита конечной точки. Каждая конечная точка состоит из двух элементов: устройства и его пользователя. Необходимо учитывать оба элемента.

Но для обеспечения безопасности в этой новой парадигме требуется гораздо больше, чем простая среда из компьютеров, соединенных по Ethernet. Необходимо больше ресурсов, без которых по-настоящему защитить данные невозможно. Это понимают 61% опрошенных Ponemon специалистов.

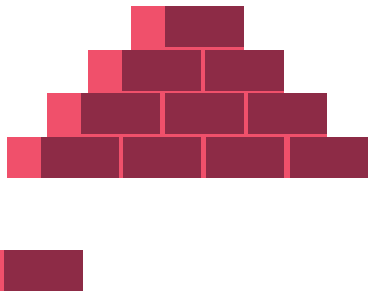
Главное — убедить в этом других сотрудников организации. Всего 36% респондентов считают, что их бюджета и персонала достаточно для защиты конечных точек. 69% считают, что ИТ-отдел не соответствует запросам сотрудников на поддержку. 71% считает, что политики безопасности конечных точек сложно применять.[22]

80% ИТ-руководителей думают, что соблюдение нормативных требований — лучший способ обосновать их программы безопасности, но при этом считают соответствие требованиям наименее важной причиной для расходов. Соблюдение требований означает соответствие минимуму.[23]

Лица, принимающие ИТ-решения, должны убедить высшее руководство в важности обеспечения безопасности. Расскажите им о рисках слабой системы защиты (расходы на восстановление, потери прибыли, падение стоимости акций) и впечатлите их экономией в долгосрочной перспективе. Многие решения безопасности дают преимущества и в других областях. Это может быть повышение производительности после внедрения политики безопасности принтеров и повышение эффективности за счет регулярно обновляемых устройств в рамках гибкой программы CYOD по подписке (например, HP DaaS). Вы можете сформулировать убедительное экономическое обоснование.

Это трудная задача. Но со временем (из-за взрывного роста числа устройств в эпоху Интернета вещей и более сложной природы кибератак) она станет еще сложнее. Но ее вполне можно решить. С правильными технологиями, стратегиями и ресурсами мы сможем защитить наши конечные точки. Мы можем сохранить данные в безопасности.

Чтобы узнать о модели «устройство HP как услуга» и о том, как реализовать гибкую и безопасную программу CYOD, посетите **эту страницу.**



Регистрация для получения обновлений
hp.com/go/getupdated

Поделитесь с коллегами

Оценить документ

4AA7-1089RUE

[22] Отчет о состоянии конечных точек, Ponemon 2016

[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697