ПОЧЕМУ ТРАДИЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ КОНЕЧНЫХ ТОЧЕК МОГУТ ПОДВЕРГАТЬ ВАС РИСКУ

АННОТАЦИЯ

Когда речь идет о безопасности всех компонентов современной распределенной сети, конечные точки остаются наиболее уязвимыми. Повсеместная мобильность привела к наплыву различных мобильных устройств, которые ежедневно подключаются к корпоративным сетям и отключаются от них. Использование общего доступа, ненадежная защита конечных точек и высокая степень анонимности пользователей способствует тому, что устройства становятся главными целями для заражения вредоносным ПО и для других изощренных атак, которые стремятся воспользоваться уязвимостями крупных организаций. И злоумышленники достигают огромных успехов в этом направлении.

Для поддержания конкурентоспособности большинство организаций вступают на путь цифровой трансформации (DX), включая высокий уровень мобильности, использование облачных сервисов и интеллектуальных устройств, поддерживающих Интернет вещей (IoT). Подобные адаптации предоставляют организациям более быстрый и простой доступ к важной информации независимо от того, какое устройство для этого используется. Но по мере расширения распределенных сетей и повышения сложности управления, конечная точка становится слабым звеном в цепи безопасности.

КОНЕЧНЫЕ ТОЧКИ ЯВЛЯЮТСЯ ПОПУЛЯРНЫМИ МИШЕНЯМИ ДЛЯ АТАК

Конечные устройства являются самыми популярными целями для взлома корпоративных сетей. В некоторой степени это связано с ростом количества устройств, подключенных к сети. Отдельный пользователь в любое время может получить доступ к сетевым ресурсам сразу с нескольких устройств: ноутбука, смартфона, планшета или даже с умных часов.

6 млн долл. США
ежегодно тратится из-за неэффективных стратегий управления конечными точками.[1]

Конечные устройства остаются одними из
самых популярных мишеней для взлома
корпоративных сетей.

3,4 млн долл. США
ежегодно тратится только на обнаружение небезопасных конечных точек и устранение последствий.[1]

К сожалению, большинство ИТ-подразделений обрабатывают конечные точки отдельно от остальной сети из-за огромного количества устройств и необходимости в поддержке конечных пользователей. Средство безопасности конечных точек обычно применяется к устройствам в качестве изолированного решения, обычно в виде антивирусной защиты или пакета безопасности конечных точек. Безопасность сети обычно начинается в точке, где конечное устройство подключается к сети. А когда конечная точка подключается к сети, это устройство (и все его содержимое) становится частью локальной (LAN) или глобальной (WAN) сети.

Но по причинам, описанным выше, границу между конечной точкой и сетью становится все сложнее обнаружить и защитить. Эта ситуация усугубляется дополнительными факторами, обуславливающими потребность в улучшении защиты конечных точек.

Первая причина имеет эксплуатационный характер и объясняет потребность в изменении тем, что конечные точки больше не являются унифицированным продолжением корпоративной инфраструктуры. Теперь пользователи могут самостоятельно выбирать устройства, устанавливать программное обеспечение и даже откладывать установку исправлений и обновлений системы безопасности.

Такая независимость пользователей создает явление, которое называется теневыми ИТ-ресурсами. Это конечные точки и приложения, управляемые пользователями, которые не авторизованы и не видны ИТ-специалистам организации. Такое решение передать контроль конечным пользователям ради повышения удобства использования и производительности создает проблемы безопасности. Хотя это было сделано без какого-либо злого умысла, теневые ИТ-ресурсы превратились в широко распространенную тенденцию, которая создает серьезные риски для организаций.[2]

Другая причина для изменений — это повышение риска проникновения угроз. Конечные точки (и ресурсы, к которым они обращаются) не всегда находятся за корпоративным межсетевым экраном. Пользователи могут подключаться к коммерческим приложениям SaaS (программное обеспечение как услуга) или облачным сервисам (таким как Dropbox, Box) как на рабочем месте, так и за его пределами. В некоторых организациях для доступа к корпоративным данным даже не требуется подключение к виртуальной частной сети (VPN). Такой незащищенный доступ делает конечные точки уязвимыми для прямых атак, контакта с зараженными объектами и нарушений, возникающих в результате человеческой ошибки или доверчивости (случайный щелчок на подозрительный файл или ссылку).

В среднем, **4 %** людей попадутся на приманку фишинговой кампании.[3]

Киберпреступники используют эти уязвимости. В прошлом году было зафиксировано 2216 случаев утечки данных. 73 % из этих нарушений были совершены посторонними лицами. Фишинг и претекстинг составляют 93 % процента нарушений. Электронная почта по-прежнему является наиболее распространенным вектором атак (96 %).[4] Достаточно будет сказать, что атаки посредством электронной почты обычно нацелены на конечных пользователей и их устройства. В случае успеха такие атаки могут привести к существенным убыткам. В 2017 году средняя стоимость успешной атаки на конечную точку составила более 5 миллионов долларов США на каждую организацию.[5]

Чтобы обеспечить всестороннюю и эффективную защиту организации, корпоративная система безопасности должна учитывать проблемы, актуальные для используемой среды, и системные недостатки, из-за которых конечные устройства остаются уязвимыми.

ПОВЕРХНОСТЬ АТАКИ УВЕЛИЧИВАЕТСЯ

По результатам одного из исследований, 63 % организаций не могут контролировать конечные устройства после того, как они покидают корпоративную сеть, а 53 % респондентов отметили, что за последние 12 месяцев увеличилось количество конечных точек, зараженных вредоносным ПО.[6] Когда зараженный ноутбук или смартфон сотрудника подключается к внутренней сети, организация может подвергнуться воздействию любых угроз (например, вирусов или вредоносных программ), с которыми устройство контактировало, когда было отключено от сети.

В зависимости от типа угроз, присутствующих на зараженной конечной точке, может быть несколько вариантов последствий разной степени серьезности. Во-первых, угрозам не нужно выходить за пределы самого устройства, чтобы нанести ущерб организации. Ноутбуки, планшеты и торговые терминалы (POS) могут обрабатывать или хранить ценные данные или IP-адреса в локальной памяти. В случае заражения вредоносное ПО может мгновенно извлечь эти данные.

Во-вторых, после повторного подключения зараженного устройства к внутренней сети, некоторые угрозы могут использовать учетные данные этой конечной точки для перемещения внутри организации и поиска ценных данных. Вредоносное ПО может незаметно собрать учетные данные и сохранить для будущих атак.

И наконец, этот шаблон подключения также может инициировать вспышки вредоносного ПО. Когда вредоносное ПО заражает одно устройство, угроза использует это подключение и учетные данные конечной точки, чтобы заразить как можно больше других устройств в сети. К числу недавних эпидемий вредоносных программ относятся WannaCry, Petya/GoldenEye и Bad Rabbit. Эти атаки использовали программы-вымогатели и вирусы-шифровальщики, которые не только блокировали зараженные конечные устройства, но и распространялись по сети по типу «червей», стараясь нанести максимальный ущерб и выманить как можно больше денег.

С каждым днем объем, скорость распространения и изощренность атак только растет. Недавнее исследование Forrester, в котором приняли участие 342 руководителя отдела безопасности, показало, что самая большая проблема кибербезопасности заключается в адаптации к быстро меняющейся природе киберугроз.[7] В то время как на конечных точках используются стандартные антивирусы, современные угрозы становятся слишком быстрыми, слишком большими и слишком сложными для изолированных, локализованных средств защиты, установленных на каждой машине.

ИЗОЛИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ НЕ СМОЖЕТ ЗАЩИТИТЬ СЛОЖНЫЕ СРЕДЫ

Устаревшие средства контроля безопасности, разработанные для сетей предыдущего поколения, просто не успевают за потоком постоянно меняющихся угроз. Поскольку существующие решения безопасности конечных точек находятся на локальных устройствах, они не подключаются к другим компонентам более масштабной архитектуры безопасности и не взаимодействуют с ними.

В таких условиях конечные точки не могут получать данные об угрозах «нулевого дня» и делиться ими. Из-за этого система безопасности не может быстро и эффективно реагировать на крупные атаки и взломы. Сложная и разрозненная сетевая топология многих текущих архитектур безопасности работает в интересах новых угроз, которые выходят за пределы конечной точки прямо в открытую сеть.

По результатам недавнего опроса ИТ-специалистов, посвященного безопасности конечных точек, сложность управления и развертывания оказалась одной из трех самых главных проблем (наряду с отсутствием адекватной защиты и большим количеством ложноположительных предупреждений).[9] Существует несколько причин, по которым управление конечными точками стало таким сложным.

Во-первых, сложность управления конечными точками является частью более масштабной проблемы — сложности системы безопасности. ИТ-специалисты прилагают немало усилий для эффективного управления и защиты всей сети, поскольку архитектуры безопасности основаны на огромном ассортименте изолированных и специализированных средств защиты. Эти продукты, как правило, добавляются частями и по разным причинам: чтобы устранить новые уязвимости в системе безопасности, удовлетворить потребности растущей сети (например, проверка SSL/TLS, SD-WAN) и соответствовать постоянно меняющимся стандартам соответствия и нормативным требованиям.

Во-вторых, несколько консолей для управления разными изолированными продуктами значительно усложняет работу сотрудников. При этом повышается вероятность ошибок, связанных с человеческим фактором. Это усложняет процессы кибербезопасности и увеличивает нагрузку на ИТ-отдел, который и так уже перегружен из-за ограниченного бюджета и нехватки персонала.[10]

Самые популярные векторы атак[8]

- **74 %** угроз проникают в виде ссылки и вложения в сообщениях электронной почты
- **48 %** проникают через браузер посредством обычной или скрытой загрузки
- **30 %** проникают через уязвимости приложений, установленных на конечных устройствах пользователей
- **26 %** проникают через уязвимости веб-серверов или веб-приложений

И наконец доказательство того, что конечные точки оказались недоступными для ИТ. 56 % ИТ-специалистов говорят, что не могут определить, соответствуют ли конечные устройства нормативным требованиям (например, проверить наличие неисправленных уязвимостей), а при проведении испытаний более трети устройств (36 %) не проходят проверку на соответствие требованиям.[11] Эти цифры свидетельствуют о наличии огромного «слепого пятна» внутри организации — не только с точки зрения уязвимости перед угрозами, но и с точки зрения последствий в виде штрафов и потенциальных расходов на юридические услуги в случае взлома.

НЕВОЗМОЖНО ЗАЩИТИТЬ ТО, ЧТО НЕ ВИДНО

В продолжение темы сложности: огромное количество устройств, подключенных к сети, остаются невидимы для ИТ-специалистов и, как следствие, недоступны для управления рисками. Поэтому многим сетевым администраторам не хватает функций комплексного отслеживания и централизованного управления политиками безопасности в сети.

Традиционные средства защиты конечных точек ограничены возможностью отслеживания только самого устройства. Для эффективной защиты конечных точек специалистам по кибербезопасности необходимо видеть все. Это достаточно обширный список: все пользователи, у кого есть доступ к сети, типы подключенных устройств, установленные версии ОС, не исправленные уязвимости, связанный трафик и все используемое программное обеспечение.

ВОЗВРАЩЕНИЕ ВСЕХ ИЗОЛИРОВАННЫХ КОНЕЧНЫХ ТОЧЕК В СИСТЕМУ БЕЗОПАСНОСТИ

Конечные точки больше не могут оставаться в изоляции. Учитывая постоянное появление все более агрессивных угроз, недостаточный ИТ-контроль и повышение сложности бизнеса, корпоративная система безопасности должна обеспечивать максимальную эффективность защиты этих устройств, расположенных на границе сети.

Защита конечных точек — это гораздо больше, чем ответственность ИТ-отдела за настольные компьютеры. Помимо защиты отдельных устройств, эта система должна блокировать пути распространения атаки для обеспечения безопасности корпоративных данных, сетевых ресурсов и информационных систем. При этом она должна стать частью более масштабной интегрированной архитектуры безопасности.

50 % компаний требуется **более 35 штатных сотрудников** для управления конечными точками.[12]

Действие пользователей — это самая распространенная причина проникновения угроз, а также самое популярное средство **обнаружения взлома или заражения** устройств, с которыми они работают.[13]

1 Там же.
2 Кристи Петти (Christy Pettey), Don't Let Shadow IT Put Your Business at Risk, Gartner, 3 мая 2016 г.
3 2018 Breach Data Investigations Report, Verizon, 10 апреля 2018 г.
4 Там же.
5 Чарли Осборн (Charlie Osborne), Fileless attacks surge in 2017, security solutions are not stopping them, ZDNet, 15 ноября 2017 г.
6 The Cost of Insecure Endpoints, Ponemon Institute, июнь 2017 г.
7 Center Security On Advanced Technology, Forrester Consulting, июль 2017 г.
8 Ли Нили (Lee Neely), 2017 Threat Landscape Survey, SANS Institute, август 2017 г.
9 Чарли Осборн (Charlie Osborne), Fileless attacks surge in 2017, security solutions are not stopping them, ZDNet, 15 ноября 2017 г.
10 Джон Олтсик (Jon Oltsik), Research suggests cybersecurity skills shortage is getting worse, CSO, 11 января 2018 г.
11 The Cost of Insecure Endpoints, Ponemon Institute, июнь 2017 г.
12 Там же.
13 Ли Нили (Lee Neely), 2017 Threat Landscape Survey, SANS Institute, август 2017 г.

Fortinet
Смоленская площадь 3,
Регус, офис 610,
121099 Москва
Тел.: +7 (499) 955-24-99

ГЛАВНЫЙ ОФИС
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
США
Тел.: +1 408 235 7700
www.fortinet.com/sales

ОТДЕЛ ПРОДАЖ В ЕБВА
905 rue Albert Einstein
06560 Valbonne
Франция
Тел.: +33 4 8987 0500

ОТДЕЛ ПРОДАЖ В АТР
300 Beach Road 20-01
The Concourse
Сингапур 199555
Тел.: +65 6513 3730

ЛАТИНСКАЯ АМЕРИКА
ГЛАВНЫЙ ОФИС
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Тел.: +1 954 368 9990

227263-0-1-RU