ТЕХНОЛОГИЧЕСКИЙ ОТЧЕТ IDC

Новый взгляд: сеть как сенсор и средство контроля и обеспечения безопасности

Октябрь 2015 г.

По материалам *Прогноза общемирового развития корпоративной сетевой инфраструктуры* (Worldwide Enterprise Network Infrastructure Forecast), 2015–2019 гг., Авторы: Нолан Грин (Nolan Greene), Рохит Мера (Rohit Mehra), Рич Костелло (Rich Costello) и др. IDC № 258012

По заказу Cisco

Современные корпоративные сети имеют беспрецедентное значение для достижения коммерческих целей. В результате по проводным и беспроводным сетям передается все большее количество конфиденциальных данных. Из-за такого обилия ценной информации организации становятся мишенью для хакерских атак и вредоносных приложений. При этом, те же самые характерные особенности сети (интеллектуальность и распределенная архитектура), которые привлекают киберпреступников, могут также превращать сеть в инструмент упреждающей защиты. Обеспечивая мониторинг и сегментацию трафика, современная корпоративная сеть способна стать сенсором и средством контроля и обеспечения безопасности.

Введение

С развитием явления, которому компания IDC дала название «третья платформа», появилась новая парадигма технологий и приложений на основе облака, мобильности, больших данных и социальной бизнес-модели. Сеть стала играть стратегическую роль в инновационном развитии. Одна из причин этой перемены заключается в том, что третья платформа обеспечила круглосуточный доступ к важнейшим приложениям, оптимизируя совместную работу, устраняя временные и пространственные барьеры и ускоряя инновации. По мере стремительного роста числа новых устройств и приложений по корпоративной сети передается все больше строго конфиденциальных данных. Это повышает требования к безопасности на всех уровнях — от ядра до периметра. На самом деле 80 % компаний рано или поздно станут объектом хотя бы одной успешной атаки. Даже если исключить серьезные случаи взлома, в среднем предприятия ежегодно несут убытки на сумму 1,3 млн долларов США из-за угроз их безопасности и атак.

Выражаясь лаконично, сегодня корпоративные сети являются беспрецедентно сложными. Каждый узел, приложение, сертификат, облако, устройство и пользователь, обращающийся к сети, могут стать мишенью для вируса или хакера. Любая атака с помощью вредоносной программы или других методов, если ее немедленно не обнаружить и не устранить, может быстро распространиться от точки проникновения по всей сети. Однако интеллектуальная взаимосвязь сетевых ресурсов, которая предоставляет злоумышленникам благоприятную возможность для атаки, может также служить одним из самых ценных преимуществ. Это преимущество заключается в том, что сетевую аналитику можно использовать для заблаговременного обнаружения и устранения многих видов атак и нарушений. С развитием аналитики сеть может применяться как средство контроля, оперативно передающее сведения об угрозах. Сеть может использоваться для определения «нормального» состояние среды и быстрого обнаружения отклонений. Это укрепляет роль сети как ресурса обеспечения безопасности по мере того, как сеть все больше превращается в средство регулирования доступа к сети с целью сдерживания атак.

Постоянно меняющаяся цель в отношении обеспечения безопасности

В результате широкого использования сотрудниками многих организаций личных мобильных устройств, а также массового распространения решений для обеспечения мобильности сотрудников, в корпоративной сети становится все больше устройств. Личные устройства сотрудников усложняют задачу защиты сети и могут даже увеличить объем конфиденциальных данных, передающихся по сети. Чем больше устройств подключается к корпоративной сети, тем больше оконечных устройств необходимо защищать. Одновременно с этим, поскольку сотрудники следуют своему желанию использовать мобильные устройства для выполнения критически важных задач, активно растет и развивается экосистема мобильных облачных приложений. Эти приложения еще больше усложняют потоки сетевого трафика, поскольку приложения и связанные с ними данные могут размещаться внутри или за пределами организации, в общедоступном или частном облаке. Приложения затем передаются на различные узлы корпоративной сети (от головного офиса до филиалов) и даже на подключенные к сети мобильные устройства удаленных сотрудников. Приложения не только представляют собой новую поверхность атаки с большим объемом конфиденциальных данных, но и могут открыть вредоносным элементам доступ к сети.

Еще больше усложняет ситуацию для предприятий появление Интернета вещей (Internet of Things, IoT). Интернет вещей — это «сеть сетей», состоящая из оконечных устройств («вещей»). Эти устройства идентифицируются уникальным образом и взаимодействуют друг с другом через IP без участия человека в локальном и глобальном масштабе. По оценкам IDC, к 2020 году в мире будет развернуто почти 30 млрд IoT-устройств. Эти оконечные устройства (или сенсоры) увеличивают число потенциально уязвимых мест в сети. На раннем этапе развития Интернета вещей интерфейсы безопасности могут быть непростыми в настройке и даже могут затруднять интеграцию с общей инфраструктурой безопасности. Отсутствие четко определенных подходов к обеспечению безопасности Интернета вещей ощущается особенно остро. Значительная ценность Интернета вещей заключается в тех данных, которые могут собирать IoT-устройства (сенсоры). Объем, охват и глубина этих данных являются поистине ошеломляющими. Уже сегодня работая во многих производственных средах, IoT-устройства собирают огромные массивы ценных структурированных и неструктурированных данных. С точки зрения необходимости защиты этих данных, их значительная часть является строго конфиденциальной. Возможность извлечь максимальную выгоду из Интернета вещей существенно зависит от тесной интеграции системы сетевой безопасности.

Учитывая рост мобильности сотрудников, появление эффективных бизнес-приложений, размещаемых в общедоступном облаке, и стремительное развитие Интернета вещей, ИТ-отделам необходимо пересмотреть свой подход к защите сети. Это четко понимают руководители, в чьи функции входит принятие решений в сфере сетевой безопасности. Недавний опрос специалистов по безопасности, проведенный IDC, показал, что 52 % респондентов обеспокоены тем, что сотрудники недооценивают важность соблюдения правил безопасности. Почти столько же опрошенных (45 %) озабочено растущей сложностью атак. В то же время значительная часть респондентов (38 %) считает, что их бюджеты являются недостаточными для эффективного решения новых проблем.

Эти усугубляющиеся трудности, наряду с нехваткой финансирования и ресурсов сетевой безопасности, могут существенно ухудшить возможность ИТ-отделов обнаруживать и устранять угрозы, а также предотвращать подобные взломы в будущем. По наблюдениям специалистов IDC, может пройти больше года, прежде чем изменения в инфраструктуре безопасности на базе третьей платформы (например, усиление защиты оконечного оборудования и управление пользователями) получат широкое распространение в организации. В эпоху третьей платформы необходимо внедрять гибкую, интеллектуальную и масштабируемую архитектуру сетевой безопасности, основанную на платформе и полностью интегрированную в сетевую инфраструктуру. Эта модель обеспечения безопасности сети использует характерные для сети распределенные аналитические функции, в результате чего сеть превращается из уязвимого объекта атак в средство защиты от угроз. Злоумышленники действуют быстро, и система защиты сети должна так же оперативно реагировать, используя для этого любую возможность.

Сеть как ресурс для обеспечения безопасности

По мере того как управление сетями становится все более стандартизированным, предприятия получают беспрецедентные возможности мониторинга своих сетей — от центра обработки данных (ЦОД) до периметра и всех географически распределенных местоположений. Таким образом, организации могут отслеживать устройства, пользователей и приложения. Благодаря возможности сбора всех этих данных, наряду с все возрастающей способностью анализировать данные, современные сети получили беспрецедентную возможность обнаруживать необычные или подозрительные действия. Различные виды злоупотреблений в сети, включая вредоносные программы, аномальные потоки трафика, несанкционированное использование приложений и прочие нарушения политик, а также неконтролируемые устройства и точки беспроводного доступа, можно легко обнаружить, поместить в карантин и устранить благодаря сетевой аналитике.

Для эффективного использования сети в целях защиты, необходимо рассматривать и использовать сеть в качестве средства контроля и обеспечения безопасности на всех уровнях, включая ЦОД, филиалы и комплексы зданий, а также каждое оконечное устройство и каждое загружаемое на него приложение. Использование сетевой инфраструктуры как инструмента безопасности не заменяет такие традиционные средства, как межсетевые экраны и средства защиты против сложных вредоносных программ, а усиливает эффект этих средств. В следующем разделе рассматривается, как комплексный набор решений Cisco помогает реализовать эту концепцию.

Выбор решений Cisco

В основе портфеля решений Cisco для защиты сети лежит принцип всеобъемлющей безопасности сети. Используя средство NetFlow, позволяющее сети выполнять функцию средства контроля, интегрируя платформу Identity Services Engine (ISE) для детального управления политиками и технологию TrustSec для обеспечения сегментации сети, можно беспрепятственно расширить сетевую защиту от инфраструктуры до конечного пользователя. Средства, рассматриваемые в этом разделе, поддерживают всестороннее использование сети для обеспечения безопасности.

NetFlow и Lancope

В основе подхода «сеть как сенсор системы защиты», предлагаемого Cisco, лежит средство NetFlow, которое способно непрерывно регистрировать все потоки данных, проходящие через маршрутизаторы, коммутаторы и некоторые беспроводные устройства Cisco. Каждый сеанс связи на устройстве с функцией NetFlow дает подробную информацию, в том числе в шести особо важных областях: сканирование сети, обнаружение ботнетов, атаки типа «отказ в обслуживании», атаки посредством фрагментации пакетов, изменение репутации узлов и распространение вирусов-червей.

Данные могут сохраняться для будущего использования, что предоставляет NetFlow возможность выполнять критически важную роль в обнаружении нарушений безопасности. Подробная экспертиза и журналы, в которых фиксируются все процессы обмена данными, создают полную картину подозрительной активности в сети, обеспечивая своевременное обнаружение угроз и их целенаправленное устранение. NetFlow и Lancope StealthWatch совместно повышают прозрачность сети и оповещают об угрозах безопасности в режиме реального времени. Интеграция Lancope StealthWatch с платформой Cisco ISE обеспечивает дополнительную корреляцию между контекстной информацией об устройстве (кто, что, где, когда и как) и сетевым трафиком. Это позволяет быстро изолировать зараженные устройства от сети.

Платформа Identity Services Engine

Identity Services Engine (ISE) — платформа Cisco для управления политиками безопасности, которая предоставляет согласованные средства управления защищенным доступом к проводным и беспроводным сетям и VPN-подключениям. Процесс защищенного доступа с помощью ISE начинается с аутентификации пользователя и классификации устройства. При этом дополнительная контекстная информация ISE помогает принимать более обоснованные решения о предоставлении доступа соответствующего уровня. Используя такие подробные контекстные сведения, как роль, место и время, ISE может ограничивать доступ к сети. Так обеспечивается комплексное управление доступом с точки зрения глубины и охвата. В зависимости от условий политики платформа ISE может избирательно предоставлять доступ отдельным пользователям и устройствам. Единая политика для всей сети повышает эксплуатационную эффективность за счет исключения необходимости применения и управления отдельными или специфическими политиками и благодаря интегрированному контролю за соблюдением политики.

Программно-определяемая сегментация сети с помощью TrustSec

Технология Cisco TrustSec встроена в коммутаторы, маршрутизаторы, беспроводные и защитные устройства Cisco и помогает организациям реализовать программно-определяемую сегментацию сети. TrustSec обеспечивает контроль доступа к важным сетевым ресурсам на основе ролей, созданных в Cisco ISE, в зависимости от параметров идентификации и роли. Цель TrustSec — упростить настройку и администрирование политик, регулирующих обмен информацией в сети, доступ к ресурсам и взаимодействие систем друг с другом. Технология TrustSec начинает работать в ЦОД и распространяется дальше на периметр сети, а также удаленные VPN-подключения.

Преимущества использования сети как средства обеспечения безопасности

Сегодня, когда все капитальные и эксплуатационные расходы подвергаются тщательному анализу, ИТ-отделу очень важно убедительно обосновать свои инвестиционные решения и найти способы повысить ценность сети. Сетевая инфраструктура, работающая в качестве сенсора и средства обеспечения безопасности, дает возможность эффективно задействовать ресурсы организации для защиты от угроз, способных нарушить бизнес-процессы и привести к потере прибыли. Комплексная интегрированная инфраструктура сетевой безопасности, подобная инфраструктуре, предлагаемой Cisco, использует ценные метаданные, чтобы быстро получать картину сетевого трафика. Сочетание технологий TrustSec и ISE обеспечивает детальное управление доступом к сети на основе политик, а программно-определяемая сегментация помогает локализовать угрозы и предотвратить их скрытое распространение по сети. Такая парадигма безопасности отличается высокой масштабируемостью, поскольку средства NetFlow, ISE и TrustSec можно развернуть для защиты ресурсов по всей сети.

Проблемы и возможности

Новый взгляд на корпоративную сеть как на средство обеспечения информационной безопасности отражает кардинальное изменение парадигмы. Традиционно считалось, что для защиты необходимо использовать внешние ресурсы, а не средства самой сети. Как и в случае любого радикального изменения концепции ИТ-инфраструктуры, чтобы помочь ответственным лицам понять и принять новую парадигму, необходимо проводить обучение. Кроме того, в компаниях, где уже создана сложная инфраструктура сетевой безопасности, руководство может не поддержать идею модернизации систем (особенно если эти системы работают нормально). ИТ-отдел нередко ищет баланс, стараясь получить максимальную отдачу от вложенных средств и одновременно подготовить инфраструктуру к требованиям будущего. Настоящая ситуация не является исключением.

Однако, как и в большинстве случаев, проблемы заключают в себе и огромные возможности. Как было сказано выше, внедрение сетевой архитектуры с тесной интеграцией защитных компонентов может стать более выгодным вложением средств, устраняя избыточность разрозненных систем защиты сети. Повышение эксплуатационной эффективности и возврата инвестиций при использовании сети как сенсора и средства обеспечения безопасности — лучшее доказательство пользы этой концепции.

Заключение

В эпоху третьей платформы корпоративная сеть играет беспрецедентную роль в повседневных операциях и взаимодействии с заказчиками и сотрудниками, обеспечивая конкурентные преимущества и внедрение инноваций. В то же время хакеры и киберпреступники стремятся использовать сети для получения доступа к огромному объему конфиденциальных данных, передающихся по корпоративным сетям. Это может нанести значительный ущерб и неудобство заказчикам и сотрудникам, а также негативно повлиять на репутацию организации. К счастью, средства защиты можно глубоко интегрировать во все сегменты современной сети, обеспечив беспрецедентные возможности отражения будущих атак. Внедрение сетевой инфраструктуры с тесно интегрированными компонентами безопасности настоятельно рекомендуется на данном этапе развития ИТ. Набор продуктов, подобный предложению Cisco, может стать эффективным решением для организаций.

О НАСТОЯЩЕЙ ПУБЛИКАЦИИ

Настоящая публикация подготовлена IDC Custom Solutions. Мнения, анализ и результаты исследований, представленные здесь, взяты из углубленного исследования и анализа, проведенного и опубликованного компанией IDC независимо (если не указана поддержка конкретного поставщика). IDC Custom Solutions предоставляет материалы IDC в различных форматах для распространения различными компаниями. Лицензия на распространение материалов IDC не подразумевает поддержку или мнение IDC о лицензиате.

Дополнительную информацию об IDC можно получить на сайте www.idc.com. Дополнительную информацию об IDC Custom Solutions можно получить на сайте http://www.idc.com/prodserv/custom_solutions/index.jsp.

Международная штаб-квартира расположена по адресу: 5 Speen Street Framingham, MA 01701 USA. Тел.: 508.872.8200 Факс: 508.935.4015 www.idc.com