FORTINET

Чего сегодня ждут ритейлеры от архитектуры систем безопасности

Основные критерии принятия решений

Содержание

FORTINET

Краткий обзор

Кибербезопасность в сфере ритейла в эпоху омниканального клиентского сервиса требует от директоров по ИТ и вице-президентов по ИТ глобального подхода. Поддержка различных технических решений для POS-терминалов, различных облачных приложений, распределенных сетей, мобильных устройств покупателей и других новых технологий определяет потребность в целом ряде решений по обеспечению безопасности. Однако при выборе продуктов, обеспечивающих безопасность, лица, которые принимают решения в области ИТ, должны учитывать и другие системы — необходимый эффект достигается только посредством тесной интеграции между ними. Необходимо решить несколько задач: обеспечить консолидированный, унифицированный подход к выявлению угроз, одновременно компенсируя нехватку квалифицированного персонала в сфере безопасности и решая проблемы снижения производительности сети из-за несовершенства систем безопасности.

01 Безопасность для индустрии в эпоху перемен

Руководители компаний полагаются на своих ИТ-специалистов, ожидая, что те будут внедрять инновации, способствующие росту бизнеса. Это верно для многих отраслей, но особенно актуально для розничной торговли. В частности, обязательным для розничных компаний становится омниканальный подход к обслуживанию покупателей. Как объясняет аналитик: «перед совершением покупки покупатели проверяют цены, сравнивают товары, изучают обзоры и консультируются в социальных сетях. Если вы не представлены везде, ваше ограниченное присутствие плохо скажется как на качестве обслуживания покупателей, так и на вашей прибыли». [1]

Однако, внедряя омниканальный клиентский сервис в стремлении оптимизировать продажи и обслуживание покупателей (и получить преимущество перед своими конкурентами), ритейлеры в то же время увеличивают число потенциальных уязвимостей, и, как следствие, увеличивают поверхность атаки. Чтобы архитектура корпоративных систем безопасности соответствовала уровню новых угроз, которые позволяют пользоваться сложностью сети и отсутствием прозрачности в мерах по обеспечению безопасности, она должна трансформироваться. Планируя ближайшее будущее, ИТ-директора розничных сетей и их команды, которые отвечают за обеспечение безопасности, должны помнить о множестве новых уязвимостей в собственных системах. Ниже приведены некоторые из базовых требований к обеспечению кибербезопасности в розничных компаниях:

Защита сложной среды розничных технологий

Основная проблема, с которой сталкиваются разработчики эффективной архитектуры безопасности современного розничного бизнеса, состоит в сложности корпоративных сетей. Стабильное интернет соединение является обязательным требованием для программного обеспечения торговых POS-терминалов, электронной почты и веб-приложений. Однако, обеспечивая быстрый и удобный доступ к функционалу, необходимому для работы компании, те, кто принимают решения в области ИТ, не должны забывать о безопасности этих соединений.

Многие ритейлеры используют многочисленные приложения для POS-терминалов. Такие решения обслуживаются географически удаленными подразделениями и содержат конфиденциальные финансовые данные покупателей, а, значит, представляют собой заманчивую мишень для взлома. Чтобы их обезопасить, крайне важно использовать средства защиты конечных точек, которые позволят ИТ-персоналу в режиме реального времени обнаруживать, отслеживать и оценивать уровень угроз, с которыми сталкиваются конечные точки. Многие розничные компании снижают риски, сегментируя точки уязвимости своей сети: так, при взломе, они могут изолировать только взломанные системы, сводя к минимуму последствия этих атак для сети в целом.

Внедрение SD-WAN

Еще одним важным аспектом является переход розничных компаний на использование программно-конфигурируемой архитектуры глобальной сети (SD-WAN), которая обеспечивает высокоскоростное подключение к разнообразным системам торговых POS-терминалов и другим приложениям. Многие из сетей внедрили решения SD-WAN, чтобы избавить себя от «узких мест», возникающих при приоритизации приложений, и повысить скорость соединений между географически удаленными подразделениями. Одно из преимуществ технологий SD-WAN состоит в том, что, поскольку больше не надо пропускать весь трафик через корпоративный центр обработки данных, удаленные подразделения получают доступ к скоростным интернет-соединениям. Но это же преимущество плодит новые уязвимости, поскольку часть трафика не защищена системой безопасности центра обработки данных. Мало того, большинство решений SD-WAN не гарантируют надлежащего уровня безопасности.

Инфраструктура с применением технологии SD-WAN требует решений, которые предоставят надежную защиту, не ограничивая производительности сети. Директорам по ИТ, в задачу которых входит обеспечение безопасности архитектуры SD-WAN для розничной сети, следует рассмотреть установку межсетевого экрана следующего поколения (NGFW), способного не только защитить распределенную сеть от угроз, но и минимизировать совокупную стоимость владения (TCO) за счет снижения первоначальных затрат на приобретение, текущих платежей и затрат на установку, обслуживание и обновление.

Безопасность многооблачной инфраструктуры

В то же время, розничные компании переосмысливают свою локальную технологическую инфраструктуру. К тому же большинство из них переходят к многооблачным средам, используют приложения и хранят важные данные в частных, общедоступных и гибридных облаках и в облачных приложениях «программное обеспечение как услуга» (SaaS). Эти облачные приложения отлично справляются с обеспечением определенных типов функционала для распределенных розничных сетей, однако они же усложняют корпоративную ИТ-структуру и открывают новые окна для потенциальных кибератак.

В силу особенностей их инфраструктуры облачные приложения очень сложно защитить. Они развернуты на оборудовании, которое находится за пределами корпоративного центра обработки данных и его традиционных систем безопасности, и требуют в связи с этим нового подхода к безопасности. Решения по обеспечению безопасности должны «уметь» разделить хранилище данных между различными облаками, в которых работает компания, чтобы ИТ-специалисты получали четкую, консолидированную информацию об угрозах и мерах по снижению рисков, а также их анализ для всех приложений компании, независимо от того, где они размещены.

63%

случаев утечки данных в розничной торговле происходит в результате взлома веб-приложения.[2]

Приложения для электронной почты и выхода в сеть

Как и любая другая компания, розничная сеть обязана предоставлять сотрудникам доступ к электронной почте и веб-приложениям, чтобы они могли эффективно исполнять свои обязанности. Электронная почта остается излюбленной мишенью для кибератак, и, чтобы ее защитить, требуются продвинутые специализированные решения. Исследования в этой сфере показывают, что в прошлом году 94% компаний подвергались фишинг-атакам.[3]

Традиционные средства защиты электронной почты часто никак не связаны с общей системой сетевой безопасности. Однако, если система безопасности электронной почты не передает информацию об атаках (успешных или нет) в общую инфраструктуру безопасности компании, возникают возможности для успешного взлома данных где-то еще. Вместе с тем, можно предотвратить кибератаки в других компонентах сети, а электронная почта окажется от них не защищенной.

Недавнее исследование показало, что 84% всех успешных атак на точки уязвимости было направлено не на одну из них, а сразу на несколько: например, пострадали рабочие станции, ноутбуки, серверы, устройства интернета вещей (IoT) и/или конечные точки в облаке в различных комбинациях.[4] В действительности 20% атак прошло со взломом 100 и более точек уязвимости. Чтобы дать эффективный отпор кибератаке, нацеленной на электронную почту разных конечных точек, требуется координация между различными компонентами систем безопасности компании.

Веб-приложения тоже уязвимы для киберугроз. 63% случаев утечки данных в розничной торговле происходит в результате взлома веб-приложений.[5] Кибератака — проблема для любого директора по ИТ, но в омниканальной розничной компании, которая значительную часть дохода генерирует через продажи в интернет-магазине, безопасность и бесперебойная работа веб-сайта являются первостепенной задачей. Во многих случаях для розничной компании важнее обеспечить безопасность веб-сайта, чем защитить торговые POS-терминалы.

Таким образом, руководители в сфере ИТ нуждаются в комплексном, многоуровневом подходе к обеспечению безопасности веб-приложений, который гарантирует защиту от 10 наиболее распространенных угроз по версии Проекта по обеспечению безопасности открытых веб-приложений (OWASP), от распределенных атак отказа в обслуживании (DDoS-атак) и других известных типов атак. Вместе с этим ритейлерам требуется и межсетевой экран веб-приложений с искусственным интеллектом (ИИ), способный обнаружить новые угрозы, которые ранее системами безопасности не регистрировались. Например, в межсетевом экране веб приложений заложен инструментарий, который позволяет уменьшить количество ложных срабатываний, что повышает эффективность и помогает предотвращать кибератаки в режиме реального времени.

Как и другие используемые розничными компаниями технологии обеспечения безопасности, решения по безопасности электронной почты и веб-приложений должны быть интегрированы в общую корпоративную структуру безопасности, где они обмениваются информацией с корпоративными межсетевыми экранами, системами сетевой безопасности, решениями облачной безопасности и другими элементами общей структуры безопасности.

Точки беспроводного доступа

В эпоху омниканального обслуживания розничным сетям нужно также учитывать, что источником новых уязвимостей может стать и беспроводной доступ в интернет, который они предоставляют своим покупателям. Стандартные технологии коммутации не справляются с уязвимостями, возникающими при открытии сетей в магазинах для сторонних устройств. И это серьезная проблема, ведь безопасность точек беспроводного доступа крайне важна для розничных компаний, которым необходимы как безопасные точки беспроводного доступа, так и специализированные решения для обеспечения безопасной коммутации.

02 Сложность архитектуры систем безопасности

При разработке ИТ-отделами розничных компаний архитектуры безопасности, выходящей далеко за рамки защиты сетевого периметра, часто возникает желание выбрать независимые решения, которые кажутся лучшими в своем классе для каждой конкретной задачи — от защиты конечных точек до облачной безопасности и от решений для электронной почты до межсетевого экрана или контроля беспроводного доступа. Однако это приводит к разрозненными политикам и практикам, которые в конечном итоге подрывают сетевую безопасность. Если не интегрировать решения по обеспечению безопасности в единую систему, они не будут эффективно обмениваться критически важными данными об угрозах и, следовательно, не смогут обеспечить скоординированный ответ в случае кибератаки.

Розничные компании нуждаются в интегрированных решениях для обеспечения безопасности, каждое из которых отвечает за соответствующие уязвимые компоненты сети: конечные точки, электронную почту, веб-приложения, подключения SD-WAN, точки беспроводного доступа, а также межсетевые экраны на границах сети.

Как только один из компонентов системы безопасности обнаружил угрозу, он должен немедленно оповестить об этом остальные компоненты структуры безопасности. Это позволит обеспечить автоматическую реакцию каждого из них на выявленную угрозу.

Кроме того, интегрированная архитектура безопасности, разработанная для скоординированного и своевременного реагирования на угрозы по всей поверхности атак, очень важна для компаний, потому что им нужно быть во всеоружии, чтобы отражать все новые и новые угрозы, и при этом компенсировать дефицит необходимых знаний у персонала службы безопасности.[6] Любая задержка в реагировании на атаку дает злоумышленнику возможность нанести максимальный ущерб.

Проблемы с прозрачностью мешают соответствовать требованиям

На фоне новых проблем с обеспечением безопасности розничные компании также должны обеспечить соответствие стандартам и нормативам. Требования таких документов, как Общие положения Европейского союза о защите данных (GDPR), отраслевых стандартов (напр., стандарта безопасности данных индустрии платежных карт PCI DSS) и стандартов безопасности (напр., стандарта Национального института стандартов и технологий NIST) означают, что ИТ-персонал должен получать все необходимые данные о безопасности как для создания отчетов для целевой аудитории, так и для быстрого реагирования в случае взлома данных. Соответствие этим требованиям потребует от компаний не только централизованного и последовательного контроля политик, но и прозрачности для всей поверхности цифровых атак.

Только 12% участников недавнего исследования заявили, что между их командами NOC и SOC налажено тесное взаимодействие.[7]

Устранение барьеров между NOC и SOC

Еще одним аспектом, на который стоит обратить внимание ИТ-отделам розничных компаний при разработке архитектуры безопасности, является связь между центром мониторинга информационной безопасности (SOC) и сетевым операционным центром (NOC). Многие разделяют SOC и NOC, считая, что их процессы и задачи персонала не пересекаются, и этот подход подрывает защищенность розничного бизнеса.[8]

NOC компании хранит информацию о том, где запущены приложения и установлены ли обновления для системы безопасности. При кибератаке NOC может предоставить информацию о том, какие конечные точки уязвимы и насколько серьезна эта угроза для компании — и эта информация крайне важна для эффективного реагирования. Однако эти атаки не выявить без информации о возникающих угрозах, которую собирает и хранит SOC.

Если NOC и SOC не обмениваются важными данными об угрозах, ИТ-специалисты не получают необходимой информации об угрозах в реальном времени. К сожалению, во многих компаниях функции этих центров до сих пор полностью разделены: Только 12% участников недавнего исследования заявили, что между их командами NOC и SOC налажено тесное взаимодействие.[9]

Интеграция центров NOC и SOC крайне важна. Но она возможна только при использовании специализированных инструментов управления безопасностью и аналитикой, которые обеспечивают прозрачность всех операций за счет координации и оптимизации панелей мониторинга и рабочих процессов.

03 Дополнительные соображения

Помимо налаживания коммуникации между всеми компонентами системы безопасности, в розничном бизнесе важно еще и предусмотреть варианты сегментации или микросегментации сетей. Возможность оперативно сегментировать сеть сама по себе способна локализовать потенциальные угрозы. Это снижает их доступ к сетевым данным и приложениям, тем самым сводя потенциальный ущерб к минимуму.

Контроль сетевого доступа

Также в архитектуре обеспечения безопасности с микросегментацией конечных точек должны быть предусмотрены сетевые политики и средства управления доступом, которые используют аналитические технологии для создания профилей различных конечных точек сети, а затем определяют соответствующие уровни доступа и сегментации для каждой из них. Этот подход в сочетании с непрерывным мониторингом конечных точек снижает уязвимость компании в борьбе с уже известными и еще не известными угрозами.

Розничные компании часто работают с минимальной наценкой, поэтому эффективность сетевой безопасности — как и других аспектов их бизнеса — это ключ не просто к успеху, но и к выживанию.

Совокупная стоимость владения (TCO) в сфере безопасности

Розничные компании часто работают с минимальной наценкой, поэтому эффективность сетевой безопасности — как и других аспектов их бизнеса — ключ не просто к успеху, но и к выживанию на рынке. Решения по обеспечению безопасности с автоматизированным реагированием на угрозы, равно как и обмен данными между SOC и NOC, сократят объем операций в ручном режиме, таких как мониторинг, регистрация событий, отправка заявок и другие задачи. Также существенно экономит время автонастройка подключаемых устройств для их автоматического развертывания. Такие функции уменьшают количество ошибок и облегчают применение сетевых политик. Все эти функции в совокупности упрощают процессы обеспечения кибербезопасности и снижают совокупную стоимость владения.

Защита без ущерба для производительности сети

Технологии, которые обеспечивают омниканальный подход к обслуживанию покупателей, способны повлиять и на пропускную способность широкополосной связи в разных точках розничной сети. Применение технологий аналитики присутствия, при помощи которых розничные компании отслеживают физическое присутствие покупателей через их мобильные устройства, определяют, сколько времени покупатель провел в магазине, на какие продукты смотрел и т.д., накладывает на производительность сети дополнительную нагрузку. Наблюдения этих систем очень полезны при принятии решений о таргетированных предложениях конкретным покупателям, но они потребляют много ресурсов, что может замедлить все остальное происходящее в сети.

Поэтому в процессе разработки архитектуры безопасности розничным компаниям нужно быть предельно внимательными и следить, чтобы их решения по обеспечению безопасности не снижали производительность сети. При выборе решений для интеграции в единую систему директорам по ИТ необходимо учитывать и средства связи между устройствами. В идеале архитектура безопасности компании должна объединить и интегрировать все решения по обеспечению безопасности, соединив устройства через высокопроизводительную виртуальную частную сеть (VPN), которая обеспечит безопасность связи без ущерба производительности сети для других приложений компании.

04 Заключение

Современный розничный бизнес нуждается в такой сетевой инфраструктуре, в которой системы безопасности были бы интегрированы по всей поверхности атак. Так было всегда, но сегодня, когда любая розничная сеть внедряет много новых разнокалиберных устройств, поддерживает мобильные решения, интернет вещей и прочие новинки цифровой трансформации, достичь интегрированной безопасности становится еще важнее — и еще сложнее.

Решения, которые обеспечивают защиту всех сетевых устройств розничной компании — от сетевой периферии и точек уязвимости до облачных сред — должны обмениваться информацией об угрозах. Они также должны обеспечивать прозрачность процессов безопасности, постоянно предоставлять оценку рисков и встроенную аналитику, чтобы ускорить реагирование на угрозы. Обеспечить безопасность в современном розничном бизнесе – задача не из легких. Однако тщательный выбор решений поможет сделать инфраструктуру безопасности более эффективной и повысит ее способность решать поставленные перед компанией задачи.

[1] «Omni-Channel Retail Strategy: The What, Why, and How of 'In-Store' Shopping (Омниканальная розничная стратегия: Что, почему и как это применять в магазинах),» Shopify Plus, January 9, 2018.

[2] «2019 Data Breach Investigations Report (Отчет о расследованиях утечек данных за 2019 год),» Verizon, March 2019.

[3] «The State of Email Security: 2019 Report (Безопасность электронной почты: отчет за 2019 год),» Mimecast, accessed May 28, 2019.

[4] Lee Neely, «Endpoint Protection and Response: A SANS Survey (Защита конечных точек и реагирование на угрозы: опрос SANS),» SANS Institute, June 12, 2018.

[5] «2019 Data Breach Investigations Report (Отчет о расследованиях утечек данных за 2019 год),» Verizon, March 2019.

[6] «The CISO Ascends from Technologist to Strategic Business Enabler: Understanding the Cybersecurity Skills Shortage (Директора по кибербезопасности уже не техники, а бизнес-стратеги: понимание дефицита навыков кибербезопасности),» Fortinet, August 15, 2018.

[7] Nelson Hernandez, «NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security (Интеграция NOC/SOC: возможности для повышения эффективности реагирования на инциденты в системах кибербезопасности),» SANS Institute, January 26, 2018.

[8] «The NOC and SOC Divide Increases Risk While Breeding Inefficiencies (Разрыв между NOC и SOC повышает уровень риска и снижает эффективность),» Fortinet, September 11, 2018.

[9] Nelson Hernandez, «NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security (Интеграция NOC/SOC: возможности для повышения эффективности реагирования на инциденты в системах кибербезопасности),» SANS Institute, January 26, 2018.

www.fotinet.com/ru

414260-0-0-EN

14 июня 2019 21.59

eb-retailers-security-architecture