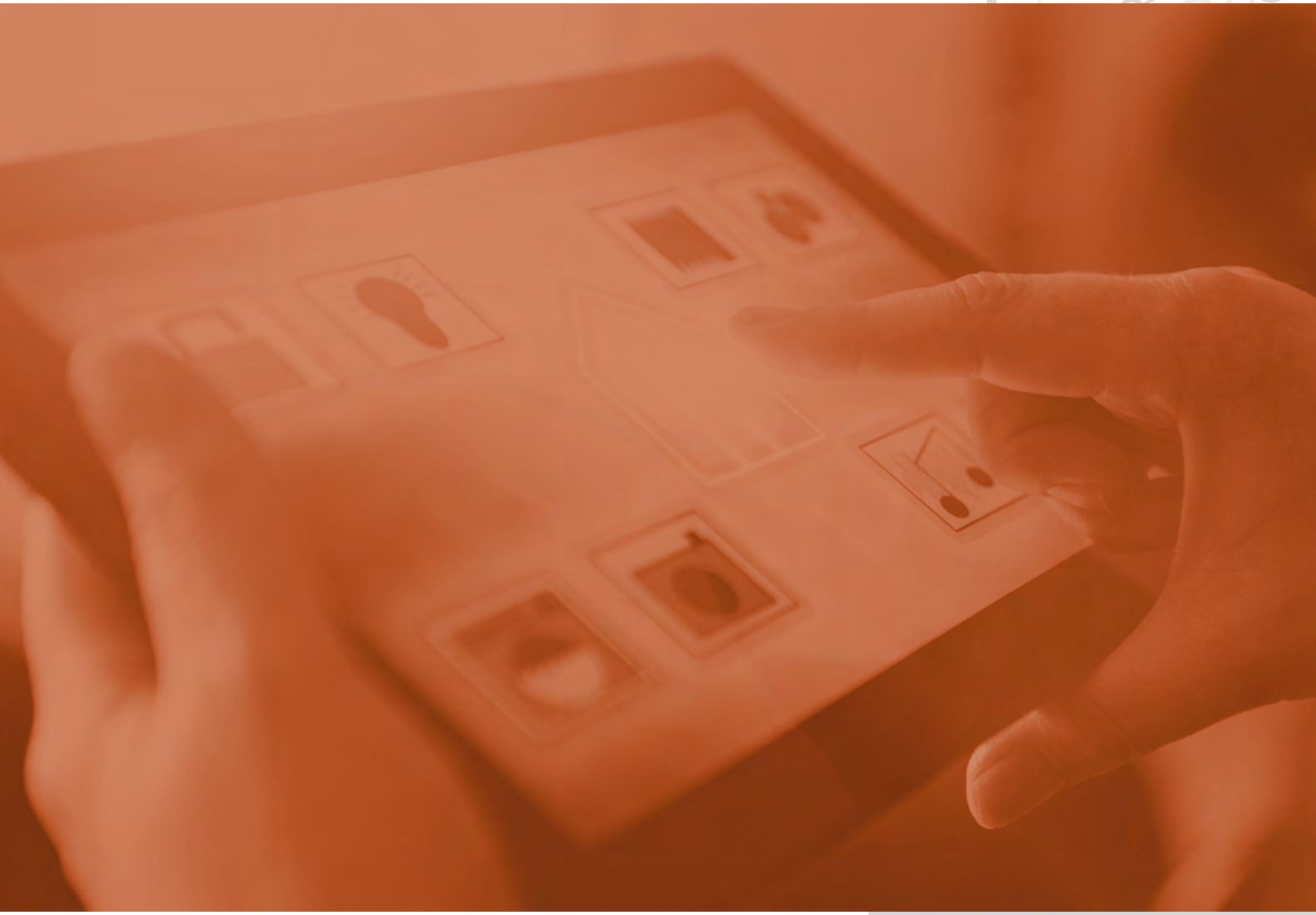
ЭВОЛЮЦИЯ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ ДОСТУПОМ К СЕТИ (NAC)

Как устройства IoT и BYOD изменили решения NAC



АННОТАЦИЯ

Распространение политики использования сотрудниками собственных устройств (BYOD) и Интернета вещей (IoT) привело к трансформации структуры сетей и появлению новых требований к их безопасности. Технологии управления доступом к сети (NAC) предыдущего поколения неспособны обеспечить эффективную защиту конечных точек. Они не поддерживают функции, необходимые для защиты корпоративных устройств IoT и BYOD: комплексное отслеживание, управление и автоматическое реагирование. Такие недостатки системы безопасности не только ставят под угрозу корпоративные данные, пользователей и бизнес-операции, но и могут обернуться штрафами за нарушение требований и другими карательными убытками.

Согласно прогнозу IDC, в условиях цифровой трансформации расходы на **IoT по всему миру достигнут 772,5 млрд долл. США** в 2018 г. и превысят отметку в **1 трлн долл. США** к 2021 г.[1]

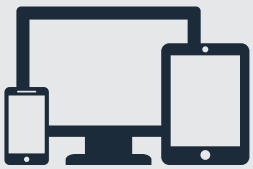
ИССЛЕДОВАНИЕ

ОТ МОБИЛЬНЫХ КОНЕЧНЫХ ТОЧЕК К УСТРОЙСТВАМ IOT

Компании продолжают испытывать сложности в процессе обеспечения безопасности мобильных конечных точек. Работающие по временному договору сотрудники, посетители, обслуживающий персонал и другие «сторонние» пользователи нуждаются в доступе к сети. На помощь могут прийти технологии управления корпоративными мобильными устройствами (EMM) и межсетевые экраны, однако эти решения лишены таких важных функций, как комплексное отслеживание состояния устройств и пользователей в целях определения полномочий доступа к сети и ограничения этого доступа.

В то же время устройства IoT в силу своей принадлежности к числу слабейших точек сети нередко становятся целью киберпреступников. К примеру, многие устройства IoT не имеют средств управления: они не поддерживают установку даже простых исправлений и лишены встроенных компонентов безопасности.

Нормативные требования в отношении устройств IoT находятся в процессе разработки. Тем не менее даже на этом этапе стратегии защиты IoT должны соответствовать существующим стандартам и требованиям. Перед большинством организаций стоит задача обеспечения соответствия нормативным документам, требующим строгого контроля за доступом к сети и наличия средств защиты данных: это Общие положения о защите данных (GDPR), Закон об унификации и учете в области медицинского страхования (HIPAA), акты Комиссии по ценным бумагам и биржам США (SEC), Закон Сарбейнза-Оксли (SOX) и стандарт безопасности данных индустрии платежных карт (PCI DSS). В целях обеспечения соответствия организации должны внедрить средства защиты конечных устройств. Неисполнение требований может повлечь за собой миллионные штрафы.



Продолжается и распространение концепции BYOD — численность мобильных работников превысила 1,76 млрд человек, что составляет около 59,4 % от общего количества работающих по всему миру.[2]

По данным одного исследования, 63 % организаций не могут контролировать мобильные устройства за пределами корпоративной сети, а 53 % респондентов отметили, что за последние 12 месяцев увеличилось количество конечных точек, зараженных вредоносным ПО.[3]

Такие общемировые тенденции, как внедрение виртуальных/облачных сервисов, коммутаторов и маршрутизаторов, а также рост числа подключенных к сети филиалов, обменивающихся между собой информацией, превращают задачу обнаружения угроз и обеспечения безопасности конечных точек в неподъемное бремя. Отдельные средства защиты могут успешно предотвращать атаки определенного типа, однако они, как правило, лишены интегрированных функций комплексного отслеживания истории и сбора аналитических данных. Между тем, эти функции играют важнейшую роль в процессе предотвращения, выявления и устранения угроз сотрудниками отделов реагирования на угрозы и обеспечения соответствия требованиям законодательства.

Ключевой проблемой является уязвимость сетей для атак (к примеру, распространения вредоносного ПО зараженными устройствами или несанкционированного доступа с помощью украденных учетных данных) вследствие использования устаревших средств управления доступом. Решения NAC первого поколения для проверки подлинности и авторизации конечных точек (главным образом управляемых ПК) использовали простую технологию сканирования и блокирования. Переход к решениям NAC второго поколения был обусловлен ростом потребности в управлении гостевым доступом к корпоративным сетям. Средства управления доступом второго поколения предоставляют ограниченный интернет-доступ внешним пользователям — посетителям, деловым партнерам и сотрудникам, работающим по временному договору.

Изменения инфраструктуры сетей (цифровая трансформация) и развитие изощренных целевых атак привели к появлению новых уязвимостей, связанных с доступом к сети, на устранение которых должны быть направлены современные средства безопасности.

1. Отсутствие функций отслеживания и управления. Невозможно защитить компоненты, сведениями о состоянии которых вы не располагаете. Уязвимость организаций связана с отсутствием средств комплексного централизованного отслеживания устройств (как BYOD, так и IoT). Сотрудники отдела безопасности должны иметь возможность отслеживать все компоненты сетевой инфраструктуры во всех локациях, в том числе на периферии сети. Как правило, средства защиты конечных точек изолированы от системы сетевой безопасности, что делает невозможным обмен важными данными в режиме реального времени. Если какое-либо устройство становится целью атаки, остальные подключенные устройства во всех местоположениях (и другие компоненты архитектуры сетевой безопасности) должны немедленно получить сигнал об угрозе и приступить к согласованной реализации мер противодействия. В рамках большинства традиционных подходов к безопасности это невозможно.

2. Отсутствие политик автоматического реагирования на угрозы. Системы безопасности ежедневно создают тысячи предупреждений. Разумеется, сотрудники ИТ-отделов

не могут вручную обрабатывать каждый инцидент. Когда межсетевой экран, система выявления вторжений (IDS), система предотвращения вторжений (IPS) или другая служба выявляет нарушение безопасности по определенному IP-адресу, архитектура безопасности должна автоматически устранить угрозу. Оперативность и эффективность реагирования существенно снижает риск.

3. Отсутствие автоматизированных рабочих процессов. Многие устаревшие процессы, к примеру, связанные с выделением ресурсов, требуют вмешательства ИТ-специалистов. Это замедляет подключение новых сотрудников к сети, повышает риск ошибок, вызванных человеческим фактором, усугубляет нагрузку на ИТ-персонал и снижает общую эффективность операций безопасности.

Существующие решения обеспечивают контроль над устройствами, рассчитанными на традиционную парадигму управления, однако непрерывный рост количества продуктов IoT и BYOD приводит к появлению новых проблем. Наиболее значительной из них является отсутствие стандартов конфигурации устройств BYOD и IoT. На рынке представлено великое множество типов и марок устройств, оснащенных самыми разными операционными системами и компонентами безопасности, причем большинство устройств не соответствует стандартам корпоративной безопасности. С течением времени проблема становится все более серьезной: этому способствует стремительный рост количества роботов, устройств контроля температуры, дозаторов инсулина, датчиков систем отопления, вентиляции и кондиционирования, автоматизированных средств защищенного доступа и других устройств с подключением к IoT.

По оценкам специалистов, приблизительная оценка количества устройств IoT составляет 9 миллиардов. Согласно прогнозам, этот показатель возрастет до 55 миллиардов к 2025 году.[4]

ЭФФЕКТИВНОЕ ПРОТИВОДЕЙСТВИЕ РИСКАМ ОТКРЫТОГО ДОСТУПА ТРЕБУЕТ РАЗВИТИЯ СИСТЕМ БЕЗОПАСНОСТИ

Распространение BYOD и устройств IoT привело к тому, что средства управления доступом предыдущего поколения перестали соответствовать требованиям к безопасности конечных точек. По мере развития и роста количества целевых эксплойтов «нулевого дня» и продвинутых угроз задача устранения этих уязвимостей с каждым днем становится все более актуальной. Разработчики архитектур безопасности должны найти способы модернизации средств управления доступом. Этого требует защита конечных точек, пользователей и организаций от разрушительных последствий атак с использованием корпоративных устройств.

[1] «IDC Forecasts Worldwide Spending on the Internet of Things to Reach $772 Billion in 2018», IDC, 7 декабря 2017 г.

[2] Ник Элиа (Nick Elia), «Mobile Worker Report Announcement», VDC Research, 11 августа 2017 г.

[3] «The Cost of Insecure Endpoints», Ponemon Institute, июнь 2017 г.

[4] Питер Ньюман (Peter Newman), «IoT Report: How Internet of Things technology is now reaching mainstream companies and consumers,», Business Insider, 27 июля 2018 г.

22 мая, 2019 2:00 ПП

271964-A-1-RU

WP-the-evolution-of-NAC-final-A4_RU