Хороший, плохой...

Владимир Безмалый

Разговоры, как правило, не стоят ничего, а веб-советов о том, как обезопасить свои ИТ-ресурсы и

цифровые активы, когда сотрудники работают из дома из-за пандемии COVID-19, предостаточно и бесплатно. Но чего стоит эта «мудрость» на практике?

В конечном итоге, если что-то пойдет не так, виноватыми будут ИТ-директор, технический директор, директор по информационной безопасности и служба безопасности. Итак, прежде чем спешить с предоставлением сотрудникам удаленного доступа, давайте рассмотрим тонкие моменты.

Плохой совет: просто расширьте существующую ИТ-инфраструктуру, и все будет в порядке.

Когда унаследованная инфраструктура рассматривается руководством, уровни мощности обычно оцениваются в совокупности. Общая структура сети может иметь пропускную способность и время отклика, которые кажутся достаточными для ведения бизнеса.

Но такое рассмотрение игнорирует любую сегментацию, которая может происходить внутри унаследованного ресурса.

Хороший совет: не предполагайте, что устаревшая инфраструктура в достаточной степени обеспечит и поддержит удаленную работу.

Грегг Зигфрид, директор Gartner по исследованиям в области облачных технологий и ИТ-операций, недавно был процитирован Diginomica . Он напомнил нам, что «многие организации используют традиционные корпоративные приложения с «толстыми клиентами», которые никогда не были предназначены для работы с локальной сетью со скоростью ниже 100 Мбит/с между клиентами и серверами». Они не смогут работать через удаленные соединения с высокой задержкой и «могут просто быть непригодными для удаленного использования».

Плохой совет: пока вы убеждены, что у удаленных сотрудников установлена последняя версия антивирусного программного обеспечения, ваш бизнес будет защищен.

Антивирусное программное обеспечение ищет статические данные, связанные с файлом или процессом, чтобы определить, является он вредоносным или нет. Эти статические данные обновляются в последних версиях AV, чтобы отразить характеристики кода вредоносного ПО, которое было изменено или обнаружено с момента предыдущих обновлений.

Такое ПО может поймать атаки, а может и нет, и в этом случае будет слишком поздно предотвратить дальнейший ущерб. Вредоносный код, возможно, уже проник в периметр защиты организации и распространяется по сети.

Отсутствие надежности и эффективности — не единственные проблемы, с которыми приходится полагаться на AV-инструменты для обеспечения безопасности удаленных сотрудников. Знаете ли вы, что ведущие антивирусные пакеты, благодаря их тесной интеграции с операционной системой, действительно были указаны исследователями как привносящие дополнительные риски?

Хороший совет: не полагайтесь только на антивирусное программное обеспечение. Это всего лишь одно точечное решение среди многих, направленных на защиту уязвимых конечных точек.

Вместо этого запланируйте, чтобы веб-эксплойты не доходили даже до устройств, выданных работодателем или BYOD. Программное обеспечение AV, например, рассматривает лишь небольшую часть возможных угроз, с которыми можно столкнуться. Модель угроз для конкретной ситуации всегда будет более сложной, чем просто (задокументированные) угрозы, исходящие от вредоносных файлов.

Опора только на один механизм, например, VPN, веб-фильтрация, CASB, менеджеры паролей — часто создает ложное ощущение безопасности и оставляет более сложные угрозы, которые могут причинить системный ущерб.

Плохой совет: ключом к защите ваших цифровых активов является политика удаленной работы (RWP) для сотрудников.

Большинство политик удаленной работы уже были функционально нарушены еще до того, как разразилась пандемия COVID-19. По разным причинам компании сохраняют их ограниченные и высокоуровневые, без особого учета конкретных ситуаций.

Компании, которые создают RWP впервые, склонны переоценивать влияние этого положительного контроля. Действительно ли он эффективен как инструмент для обеспечения комплексной безопасности и защиты данных, когда удаленные сотрудники выходят в Интернет? Нет.

Но понадобится RWP в любом случае — если в основном в качестве документа, который корпоративный советник может предоставить страховщикам, судебным органам или регулирующим органам после утечки данных.

Хороший совет: не полагайтесь на RWP для предотвращения утечки данных.

Предотвратите попадание эксплойтов в конечную точку в первую очередь, приняв активные меры предотвращения. Подход и метод могут быть разными в зависимости от модели угроз ситуации, но требуется прямой метод, а не просто общая политика.

Кроме того, могут потребоваться возможности централизованного аудита онлайн-деятельности удаленных сотрудников, например, для обеспечения соответствия в регулируемых секторах.

Плохой совет: «Разверните VPN, и ваши данные и удаленные сотрудники будут в безопасности».

Многие руководства по удаленной работе рекомендуют «использовать VPN» для защиты вашей организации и ее удаленных сотрудников. В одном

недавнем отчете указывается, что использование VPN в США и Канаде увеличилось на 36% во время пандемии коронавируса.

Хотя VPN может быть полезен для защиты сотрудников, работающих на дому, от случайного подслушивания, сам по себе он не обеспечивает действительно безопасный доступ.

В 2019 году различные поставщики VPN, такие как SSL VPN Palo-Alto, FortiGate VPN и PulseSecure VPN, выпустили рекомендации и обновления из-за критических уязвимостей в своих устройствах.

Эти предупреждения и исправления были вызваны обнаружением нескольких уязвимостей в этих продуктах VPN исследователями безопасности OrangeTsai и MehChang из команды DEVCORE.

Исследователи в области безопасности сообщили, что более 14000 конечных точек PulseSecure VPN все еще оставались уязвимыми более чем через три месяца после выпуска исправления поставщика для обнаруженной уязвимости (CVE-2019-11510). Такие задержки часто связаны с тем, как обновляются VPN.

Кажется, что VPN редко обновляются, так как ожидается (и необходимо), чтобы они всегда были в рабочем состоянии для обеспечения доступности связи.

И это только с точки зрения ИТ. Теперь рассмотрим последствия того, что подавляющее большинство новоиспеченных удаленных сотрудников настраивают своих VPN-клиентов дома, буквально оставив их на своих (BYOD) устройствах.

Короче говоря, VPN — это не панацея от всех проблем, которую делают многие руководства по удаленной работе. Как пишет в своем блоге технолог и эксперт по безопасности Брюс Шнайер, «предоставление людям программного обеспечения VPN для установки и использования без обучения — это рецепт ошибок безопасности, но отказ от VPN — еще хуже».

Итог: VPN без комплексной стратегии развертывания и ресурсов для ее выполнения вполне может повысить риск для вашей организации.

23 ноября, 2020

https://ib-bank.ru/bisjournal/news/14674