Хороший, плохой… Часть вторая

Владимир Безмалый

Хороший совет: активируйте MFA в своем VPN.

CISA
выпустила специальное предупреждение об использовании VPN в новой среде удаленной работы. Хотя агентство оставляет производителям устранение конкретных уязвимостей, в предупреждении рассматривается, как лучше всего использовать VPN на предприятии.

CISA отмечает, что по мере того, как организации используют виртуальные частные сети для удаленной работы, злонамеренные злоумышленники обнаруживают все больше уязвимостей и становятся их жертвами. Также отмечается, что организации могут иметь ограниченное количество VPN-подключений, после чего ни один другой сотрудник не сможет работать удаленно. Из-за снижения доступности могут пострадать критически важные бизнес-операции, в том числе способность персонала ИТ-безопасности выполнять задачи кибербезопасности.

CISA также рекомендует компаниям внедрять многофакторную авторизацию (MFA) для всех VPN-подключений для повышения безопасности. Если MFA не реализован, то требование к удаленным работникам использовать надежные пароли может обеспечить некоторый — базовый — уровень защиты.

Смешанный совет: в целях безопасности используйте самую последнюю версию «безопасного» основного браузера.

Вопрос: что на самом деле означает ярлык «безопасный» для традиционных браузеров?

Немного, если присмотреться.

Все основные браузеры по-прежнему позволяют — потенциально вредоносному коду из Интернета сохраняться и выполняться на компьютере удаленного работника, откуда он может заразить корпоративную сеть и приложения.

Пока это все еще реальность, мантра «обновите браузер» будет звучать. «Бесплатные» браузеры по своей сути небезопасны, они предназначены для обмена пользовательскими данными и продажи пользовательских данных сетям интернет-рекламы, которые часто также распространяют вредоносную рекламу .

Обновления не могут вылечить основной недуг. Даже если они и сделали — они часто приходят слишком поздно или, если они доступны, откладываются ИТ-отделом, согласно исследованиям: 81% ИТ-директоров и руководителей по информационной безопасности откладывают критические обновления или исправления .

Готова ли ваша команда рискнуть, учитывая возросшую нагрузку на ваш ИТ-отдел в связи с режимом COVID-19?

Плохой совет: расширьте доступ к удаленной работе, разрешив сотрудникам подключаться к собственным ресурсам компании через доступ к удаленному рабочему столу.

Shodan, поисковая система для устройств, подключенных к Интернету, определила, что количество конечных точек RDP подскочило почти до 4,4 миллиона к концу марта по сравнению с 3 миллионами в начале года.

Это примерно 40%-ный скачок в период первоначального роста числа случаев коронавируса COVID-19 на дому. Похоже, что многие организации в значительной степени полагаются на RDP для расширения удаленного доступа.

Одна из проблем заключается в том, что использование мощного протокола RDP в Windows может легко привести к расширению поверхности атаки организации, поскольку его сложно развернуть, управлять и масштабировать даже в лучших условиях.

Хотя клиенты RDP доступны практически для всех операционных систем, устройств и браузеров, новоиспеченные удаленные сотрудники не могут настраивать их самостоятельно.

Сможет ли ваша ИТ-служба поддерживать потребности в конфигурации большинства решений RDP?

Плохой совет: обратите внимание на замок в браузере, он защитит вас.

Замок в окне URL-адреса пользователя показывает либо «заблокировано», либо «разблокировано». Что это на самом деле означает?

Все, что указывает на то, что какой-то сертификат использовался или нет во время обмена данными между веб-сайтом и браузером.

Проблема здесь в том, что браузер не знает, были ли базовые сертификаты правильно проверены или выпущены.

Плохой совет: «Не волнуйтесь, на нас не стоит ориентироваться».

Организация может подумать, что она слишком мала или незначительна, чтобы привлечь внимание злоумышленника. Заблуждение здесь состоит в том, что считается, что целью может быть только ваша организация.

А как насчет ваших клиентов / клиентов, поставщиков и подрядчиков? А как насчет их деловых партнеров?

Сосредоточившись только на наиболее очевидном сценарии, вы рискуете упустить из виду влияние цифровой цепочки поставок, к которой подключена ваша организация.

Полезный совет: помните, что вы — часть сети. Истинной целью злоумышленника могут быть ваши клиенты или поставщики.

Атаки на цепочки поставок не новы. Не позволяйте атакующим, которые могут выполнять более широкую миссию, получить точку опоры. Внедрите дополнительные барьеры, такие как двухфакторная аутентификация для входа в систему, и потребуйте проверки учетных данных при переключении между ресурсами.

Плохой совет: «IT сейчас завален COVID-19, поэтому звоните на горячую линию Microsoft».

Что может пойти не так? Слишком часто встречается то, что пользователи ищут в Интернете «Службу поддержки» и в конечном итоге набирают мошеннический номер горячей линии.

Или всплывающее окно в браузере предлагает им позвонить по поддельному номеру «службы экстренной помощи». Это редко заканчивается хорошо, особенно когда мошенникам удается получить удаленный доступ к компьютеру пользователя.

Полезный совет: расскажите сотрудникам о мошенниках на горячей линии и о том, как они охотятся на своих жертв.

Плохой совет: часто меняйте пароль.

Национальный институт стандартов и технологий (NIST) выпустил официальные рекомендации NIST Special Publication 800-63-3 на 2019 год.

Хотя в исходных рекомендациях по паролям NIST 800-63, опубликованных в 2017 году, существенных изменений не произошло, одно отличие бросается в глаза, поскольку оно отражает явное изменение мышления.

Основное изменение заключается в том, что NIST теперь рекомендует, чтобы правильно сформированные пароли не «уходили в прошлое», что означает, что их изменение больше не является требованием (для пользователей из федерального правительства). Было обнаружено, что частая смена паролей приводит к обратным результатам из-за ненужного увеличения общей сложности.

Хороший совет: используйте 2FA / MultiFactorAuthorization.

2FA может быть очень эффективным методом повышения безопасности. Но способ его использования может быть не менее важным, чем его включение. Например, ответами на вызовы 2FA могут быть полные предложения, которые можно легко запомнить, не сохраняя их где-либо еще. Короче говоря, их следует использовать регулярно.

Удаленная работа существует уже давно. Но недавние события значительно увеличили число тех, кому нужно быстро освоить его использование. В спешке не упускайте из виду принципы, которые хорошо работали для организаций в прошлом и могут быть изменены, чтобы соответствовать «новой норме».

https://ib-bank.ru/bisjournal/news/14683