Безопасный доступ при удаленной работе требует перестройки сетевой инфраструктуры

В связи с массовым переходом на удаленную работу в 2020 г. многим компаниям пришлось оперативно решать задачи, связанные с защитой данных. Какие угрозы наиболее актуальны и как их минимизировать, рассказывает эксперт в этой статье

Сергей Петренко
Директор продуктового направления "Защищенные носители информации" компании "Аладдин Р.Д."

Двухфакторная аутентификация является надежным методом защиты доступа как при локальной, так и при удаленной аутентификации. Она может быть либо строгой на основе цифровых сертификатов, либо усиленной на базе сложного автоматически сгенерированного и неизвестного пользователю пароля

Для безопасности данных при удаленной работе, во-первых, остаются актуальными все угрозы, которые были в корпоративной сети. Во-вторых, усиливается угроза доступности. Когда пользователь работает удаленно, задача наличия устойчивого сетевого соединения с корпоративной сетью переходит с ИТ-службы непосредственно на пользователя. И естественно, проблем будет больше. Даже самый дорогой высокоскоростной доступ в сеть "Интернет" не сравнится с сетевым взаимодействием в рамках корпоративной локальной вычислительной сети (ЛВС). В-третьих, добавляются угрозы со стороны недоверенного окружения. И это как раз самое интересное. Легитимный пользователь, имеющий доступ к многочисленным корпоративным ресурсам, содержащим в том числе и конфиденциальную информацию, перемещается из контролируемой офисной зоны в неизвестное недоверенное окружение (квартира, дача и т.д.). Соответственно, кратно увеличиваются риски доступа третьих лиц к ПК пользователя и, как следствие, к корпоративной инфраструктуре.

Оптимальный набор технологий

Самым эффективным способом минимизации угроз безопасности при удаленной работе является применение специализированных средств защиты информации (СЗИ), специально разработанных для обеспечения безопасного удаленного доступа. Приказом ФСТЭК России от 16 февраля 2021 г. № 32 утверждены Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах. В них изложена основная требуемая функциональность таких специализированных СЗИ, в том числе перечислены такие функции, как:

- доверенная загрузка;
- аутентификация пользователя до загрузки операционных систем (ОС);
- авторизация личных средств вычислительной техники пользователя администратором безопасности;
- использование сертифицированных ОС и VPN и др.

Трудности организации удаленных рабочих мест

Руководители и специалисты служб безопасности, которые должны обеспечить безопасность удаленных рабочих мест, обычно сталкиваются со следующими трудностями:

1. Недостаток бюджета.

Весьма проблематично при массовом переводе сотрудников на удаленный режим работы обеспечить каждого корпоративным ноутбуком с набором необходимых средств защиты.

2. Необходимость приобретать и эксплуатировать новые для компании средства защиты.

Допустим, крупная компания имела один большой офис в Москве и не испытывала необходимости в организации защищенного сетевого взаимодействия, так как все рабочие места располагались в одной ЛВС. При удаленном подключении сотрудников службе безопасности, скорее всего, придется "осваивать" VPN. А если это государственное учреждение, то еще и обязательно отечественный сертифицированный VPN. Стоит отметить, что в России сертифицированные решения в силу жестких требований регуляторов зачастую гораздо сложнее в настройке и эксплуатации, чем их иностранные и/или бесплатные аналоги.

3. Перестройка сетевой инфраструктуры.

Аналогично примеру выше, не все организации в силу специфики своей структуры и бизнес-процессов имеют зрелую современную сетевую инфраструктуру, готовую к появлению большого количества удаленных клиентов.

Двухфакторная аутентификация – надежная защита

Безусловно, двухфакторная аутентификация является надежным методом защиты доступа, собственно, как и при локальной аутентификации. Двухфакторная аутентификация может быть либо строгой на основе цифровых сертификатов, либо усиленной на базе сложного автоматически сгенерированного и неизвестного пользователю пароля. Простая аутентификация (по логину/паролю) уже давно не соответствует текущему уровню угроз информационной безопасности. К слову, сейчас уже ведется системная работа по изменению руководящих документов ФСТЭК России, в частности 17-го приказа, в сторону усиления требований к аутентификации.

Скажи, кто твой провайдер...

Для безопасности удаленной работы очень важна надежность провайдера. И не только сама надежность, но и вообще параметры Интернета. Надо понимать, что доступ в сеть "Интернет" для личных нужд и использование этой же сети для доступа к корпоративным ресурсам и полноценной работе – это совершенно разные вещи. Радует, что как минимум в крупных городах сейчас нет проблем с высокоскоростным доступом в Интернет. Но многим пользователем придется сменить тарифы, а может и провайдера, чтобы обеспечить дома приемлемый для работы уровень связи. А это потребует дополнительных затрат, что, естественно, многим не понравится, возможны конфликты сотрудников с компанией на этой почве. У меня, например, был такой кейс. VPN Cisco AnyConnect не работал через сеть GPON от МГТС. Чтобы VPN-соединение могло устанавливаться, необходимо было за дополнительные ~150 руб/мес подключить услугу статического IP. Да, вроде мелочь, но неприятная. Подобных примеров с возникающими сложностями доступа из "домашнего" Интернета в корпоративную сеть, наверное, можно найти очень много.

ЭКСПЕРТИЗА, МНЕНИЯ