Case Study
доступ к Office 365

Как Nexus избавился от паролей и выбрал безопасное решение для входа в Office 365 и в другие системы.

о многих компаниях ИТ процессы зачастую замкнуты на собственные ресурсы и инфраструктуру. Правильным подходом, позволяющим оптимизировать и диджитализировать процессы, является отказ от установки Office вручную на каждом новом компьютере и переход к ИТ решениям следующего поколения, передача на аутсорсинг или, что еще правильнее, покупка облачных сервисов. Сегодня Office 365 является привлекательным вариантом. Но задумайтесь, как вы организуете доступ к облачным сервисам, чтобы работа с ними была одновременно безопасной и простой?

«Будучи компанией, занимающейся информационной безопасностью, Nexus предъявляет высокие требования к защите доступа к системе, чтобы не допустить несанкционированный доступ и защитить клиентов, а так же данные компаний. В то же время все наши сотрудники по всему миру, должны иметь возможность войти в Office 365 в любое время, чтобы работать как обычно. Именно поэтому мы выбрали облачное решение», - говорит Питер Хеллстрем, ИТ-директор Nexus Group.

Задача для ИТ-отдела Nexus была масштабной. Являясь компанией, занимающейся вопросами идентификации и безопасности, Nexus предъявляет очень высокие требования к безопасности. У компании Nexus есть много клиентов с критическими с точки зрения безопасности данными и приложениями, что приводит к огромному множеству вопросов, поскольку эта область запутана и сложна. «Многие по-прежнему сомневаются, что можно «уйти в облако» без ущерба для безопасности. Существует большой скептицизм в отношении того, можно ли защитить данные так, чтобы пользователи могли работать как обычно», - говорит Хеллстрем.

Самая большая проблема заключается в выборе решения для входа в систему, которое может обслуживать не только обычных пользователей, но и администраторов, обладающих привилегированными правами доступа, а также является простым в использовании и, в то же время, безопасным. Еще два требования были обязательными. «Первым требованием было иметь одно решение для аутентификации для всех систем, то есть все сотрудники должны иметь возможность входа в систему с мобильным телефоном, и то же самое касается администраторов, которые должны иметь возможность использовать смарт-карту для еще более высокого уровня безопасности. Второе требование состояло в том, чтобы решение могло работать как с внешними, так и с внутренними системами», - говорит Хеллстрем.

ООО “Пауэр Секьюрити”
Тел.: 7 (495) 518-2229
7 (495) 518-0767
e-mail: info@powersecurity.org

Адрес: 107140, Москва, ул. Верхняя Красносельская, д.3 стр.1
ИНН/КПП: 7708753879/770801001
ОГРН: 5117746069502 от 29.12.2011

Хватит использовать пароли - выберите мобильное решение

Были приняты решения: прекратить использование паролей при входе и использовать одинаковый метод аутентификации для всех систем и приложений. Nexus необходимо было согласовать и настроить безопасный вход в локальные системы и в облаке и в то же время найти решение, которое также можно использовать для электронной подписи. Кроме того, новый способ работы должен упростить повседневную жизнь сотрудников. «Сегодня мы используем решение единого входа (SSO) для всех систем через шлюз доступа Hybrid Access Gateway (HAG). Шлюз доступа управляет всеми системами и приложениями, включая облачные сервисы, такие как Office 365 и Nexus GO Signing», - говорит Хеллстрем.

Существует несколько различных решений для аутентификации на мировом рынке, но большинство решений работают или только для аутентификации или только для подписи. Nexus нуждался в двух типах сильных аутентификаторов на базе мобильного телефона: простой метод на основе push, когда пользователь одобряет логин с помощью отпечатка пальца, лица или PIN-кода; и метод, основанный на одноразовых паролях (OTP). Одноразовый пароль (OTP) требуется, когда пользователь находится в среде без мобильного интернета, но тем не менее нуждается в строгой аутентификации. Этот метод основан на использовании одноразового пароля, который действителен в течение 30 секунд и который позволяет пользователю получать доступ к определенным ресурсам компании. «Оба Эти метода находятся в одном мобильном приложении Nexus Personal Mobile. Тот факт, что это одно и то же приложение, позволяет нашим пользователям и нашим администраторам поддерживать всего одно решение. Например, сотрудники Nexus могут дополнительно использовать Nexus Personal Mobile для защиты своих личных учетных записей Google, Microsoft или Facebook. Мы призываем их заботиться о безопасности даже в нерабочее время». Nexus сертифицирован по ISO в соответствии со стандартом безопасности 27001, который предъявляет высокие требования к процессам и безопасности. Кроме того, нам понадобилось мобильное решение, которое работает для тех, кто находится в движении или работает дома. Mobile First - наш девиз для всех систем, как собственных, так и аутсорсинговых», - говорит Хеллстрем.

Один идентификатор для всего

«Нашей основной целью во время реализации были наши собственные сотрудники, но также клиенты должны иметь доступ к объектам в нашей среде простым и безопасным способом. Смарт-карты безопасны и помогают нам предоставить правильный доступ нужному человеку», - говорит Хеллстрём.

Nexus основывает все свои продукты и решения на проверенных и стандартизированных технологиях. Все, что было реализовано, должно было основываться на безопасной проверке подлинности, которую можно использовать без проблем. Инфраструктура клиентов обычно сложная, как и в Nexus, а это означает, что решения должны быть как интегрированными, так и совместимыми с облачными и легаси решениями. «Мы в Nexus можем предложить комплексное

решение на основе единого идентификатора - это наше преимущество, и клиенты отмечают это, когда тестируют наши решения, - вот когда мы выигрываем», - говорит Питер Хеллстрем.

Сотрудники Nexus находятся в 17 офисах в 11 разных странах. В дополнение к мобильному идентификатору, все сотрудники всегда носят удостоверение личности в виде смарт-карты с визуальным идентификатором (фото). С помощью смарт-карты пользователи входят в свои офисы, регистрируются на компьютерах, печатают (печать follow-me) и подписывают документы. Поскольку в некоторых офисах Nexus есть отделы разработки, на картах также есть информация о том, в каких зонах люди могут получить доступ.