ТЕХНОЛОГИИ ЗАЩИТЫ
НОМЕР 05, 2015

Достоинства и недостатки применения бесконтактных карт для усиления логического доступа к корпоративным ресурсам

Михаил АШАРИН, технический консультант TerraLink
Владимир НАРОЖНЫЙ, технический маркетолог TerraLink

В этой статье хотелось бы раскрыть достоинства и недостатки использования таких традиционных для каждого из нас «ключей», как бесконтактные карты для усиления логического доступа к рабочим станциям, корпоративным ресурсам и активам компании.
О том, почему это экономически целесообразно использовать карты СКУД для логического доступа, рассказано в статье «Конвергенция физического и логического доступа. Взгляд системного интегратора» (ТЗ № 5–2014).

Проблематика. Почему ответ «НЕТ» статическим паролям

Ежедневно для входа на рабочую станцию мы вводим статические (доменные) пароли, которые принято классифицировать как простые и сложные. Простые пароли обеспечивают быстрый и легкий вход для пользователей, пригодны только для слабозащищаемых и контролируемых систем, несанкционированный доступ к которым не приведет к ощутимому ущербу для компании. Сложные статические пароли, как правило, должны быть строго регламентированы корпоративной политикой, обеспечивают более высокую безопасность по сравнению с простыми, однако недостатки нивелируют преимущества: в первую очередь их трудно создавать (придумывать), вводить и менять (запоминать), а разблокировка после нескольких попыток неверного ввода и трудности с периодической сменой значительно повышает нагрузку на службу поддержки. Сложные пароли нередко хранятся пользователями в легкодоступных местах, например, на стикерах, что может привести к несанкционированному доступу.

Бесконтактные карты. Как просто перейти к двухфакторной аутентификации

Применение бесконтактных карт и RFID-меток для доступа к рабочему месту сотрудника и ресурсам компании значительно снижает нагрузку на службу поддержки (отсутствие обращений на разблокировку и смену паролей), обеспечивает быстрый и легкий вход для пользователей, позволяет унифицировать доступ по единой карте. Однако использование только карты без дополнительных средств аутентификации сопряжено с серьезным риском – для входа в домен достаточно украсть карту. Данный способ усиления безопасности рекомендован исключительно для организации локального доступа (внутри организации).

Таким образом, использование универсальных карт без дополнительного фактора аутентификации с точки зрения безопасности мало чем отличается от использования доменных паролей, однако среди достоинств следует отметить возможность снижения нагрузки на техническую поддержку и автоматизации внутренних процессов управления доступом.

Бесконтактные карты + PIN-код

Наиболее взвешенным по соотношению удобства/безопасность и поэтому рекомендован для большинства заказчиков с уже развернутой СКУД по бесконтактным картам – метод двухфакторной аутентификации по бесконтактной карте с вводом PIN-кода.

Данный метод двухфакторной аутентификации снижает риски несанкционированного доступа в систему в случае утери или кражи карты, а также предпочтителен для усиления внутреннего доступа.

Бесконтактные карты + доменный пароль

Аутентификация по бесконтактной карте и системному паролю является оптимальным методом доступа к системе для большинства заказчиков с уже развернутой СКУД по бесконтактным картам. Рекомендован для усиления внутреннего доступа. Из достоинств отметим возможность безопасного выпуска карт для пользователей полностью на стороне оператора и возможность использовать привычные, уже известные сотрудникам системные пароли вместо нового PIN-кода.

О применении карт с магнитной полосой для усиления безопасности

Несмотря на то что использование карт данного типа принято считать нерациональным с точки зрения удобства, физической инфраструктуры и безопасности, аутентификация по картам с магнитной полосой может рассматриваться в качестве более безопасной альтернативы статическим паролям для усиления внутреннего доступа только для заказчиков с уже развернутой системой СКУД по этим картам в случае, если отказ от карт данного типа не планируется. Карты могут использоваться для организации простейших систем двухфакторной аутентификации в качестве дополнительного способа к системным паролям по причине ограниченного срока службы карт, вызванного постоянным механическим контактом с устройством считывания.

Контактные смарт-карты и PKI-токены. Организация системы строгой двухфакторной аутентификации

Логический доступ с использованием инфраструктуры открытых ключей PKI является подлинно строгим методом двухфакторной аутентификации и рекомендуется организациям с повышенными требованиями к защите доступа к корпоративным ресурсам. Переход на систему строгой аутентификации обеспечивает полный отказ от системных паролей на уровне инфраструктуры Windows.

При строгой аутентификации используется двухфакторная аутентификация двух типов: использование токенов или смарт-карт с вводом PIN-кода для выполнения криптографических операций внутри устройства. Недостаток использования смарт-карт по сравнению с PKI-токенами – традиционный для всех видов карт – необходимость приобретения считывателей и, возможно, инсталляция клиентского ПО для каждого рабочего места. Применение смарт-карт рекомендовано для заказчиков, которые планируют организовать унифицированный доступ по единой комбинированной карте (контактный PKI-чип плюс бесконтактная технология) физического и логического доступа, а также для дополнительной защиты данных с помощью цифровой подписи и/или шифрования на смарт-картах.

Организация системы строгой аутентификации сопряжена также с необходимостью развертывания в организации инфраструктуры PKI, например, на базе популярных служб сертификации от Microsoft.

Не картой единой

Не менее востребованы на сегодняшний день OTP-токены. Аутентификация по аппаратным генераторам одноразовых паролей (OTP) или через мобильные приложения (софт-токены) на смартфонах/планшетах сотрудников рекомендуется для организаций, которые планируют усилить безопасность доступа с помощью токенов, не требующих подключения к рабочим местам пользователей, что особенно актуально при наличии в компании штата дистанционных сотрудников.

В случае готовности заказчика к приобретению биометрических USB-считывателей на каждое рабочее место метод двухфакторной аутентификации по отпечаткам пальцев и PIN-коду является достаточно удобным и безопасным методом доступа для организаций с высокими требованиями к защите корпоративных ресурсов. Рассматривается предпочтительно для внутреннего доступа.

Инновационный метод аутентификации по Push-уведомлениям (Ping Me) с помощью подтверждения доступа на личных или служебных смартфонах/планшетах является особенно привлекательным как по общей стоимости реализации, так и по возможности использования присутствия сотрудника в корпоративной беспроводной сети в качестве дополнительного фактора безопасности. Подробно этот метод описан в статье «Доступ к корпоративным ресурсам. Новые методы двухфакторной аутентификации» (ТЗ № 5–2015).

В дополнение

Как получить доступ к рабочей станции в случае блокировки или временной недоступности аутентификаторов? Эффективным дополнением практически к любому основному методу усиления аутентификации для реализации самостоятельного обслуживания сотрудниками своих аутентификаторов в случае их блокировки или временной недоступности является резервный доступ по контрольным вопросам, ответы на которые пользователь дал заблаговременно.

Во многих случаях также требуется однократная сквозная аутентификация (Single sign-on), которая обеспечивает автоматизированный единый вход в приложения после аутентификации в систему через основной метод.

Резюме

Каждый из предложенных способов расширения области применения уже используемых на предприятиях бесконтактных карт для физического доступа (СКУД) до безопасной двухфакторной аутентификации по ним в системы компании имеет свои, присущие только ему достоинства и недостатки, объективно оценить которые предпочтительно в процессе детализации бизнес-задачи и знания существующей инфраструктуры компании.