Конвергенция физического и логического доступа.

Концепция организации централизованной системы управления доступом

Часть 2.

Алексей МИХАЙЛОВ, директор по развитию направлений «ИТ-решения» и «Безопасность данных» компании TerraLink
Владимир НАРОЖНЫЙ, руководитель направления брендинга и интегрированных маркетинговых коммуникаций компании TerraLink

В статье «Конвергенция физического и логического доступа. Взгляд системного интегратора» (ТЗ, № 5–2014) обозначены предпосылки конвергенции средств доступа на единой карте.
В данном материале подробнее рассмотрим особенности применения единого идентификатора как универсального средства управления доступом для реализации концепции центральной системы управления доступом.

АКТУАЛЬНОСТЬ КОНВЕРГЕНЦИИ

Традиционный подход к вопросам обеспечения безопасности рассматривает поиск решения защиты от определенных типов угроз: СКУД от физического проникновения на объект, логический доступ для защиты информационных ресурсов компании, дополнительные средства идентификации, например одноразовые пароли, для защиты инфраструктуры при работе вне офиса и др. Таким образом, в компании зачастую функционируют несколько систем, обеспечивающих защиту отдельных периметров, которые используют для этого различные средства идентификации.

Наличие нескольких различных средств идентификации для получения доступа к ресурсам компании не только снижает общий уровень безопасности (например, утеря карты или пароля), но и усложняет процессы предоставления и ограничения доступа, так как обязанности предоставления доступа к различным корпоративным ресурсам зачастую разделены между различными подразделениями или разными специалистами в рамках департамента.

Немаловажным является уровень защищенности различных средств идентификации. Традиционно для физического доступа в помещение используют proximity-карты, для доступа к ресурсам – связка «логин-пароль». Оба средства идентификации доступны для копирования и подделки. Для предотвращения угроз и повышения уровня защищенности рекомендуется одновременно применять различные способы идентификации, например, для физического доступа – это карта доступа и pin-code, либо карта доступа и отпечаток пальца. Как правило, описанный вариант применения многофакторной идентификации позволяет локально решить вопрос защищенности отдельного периметра, но не решает вопрос защиты активов компании в целом.

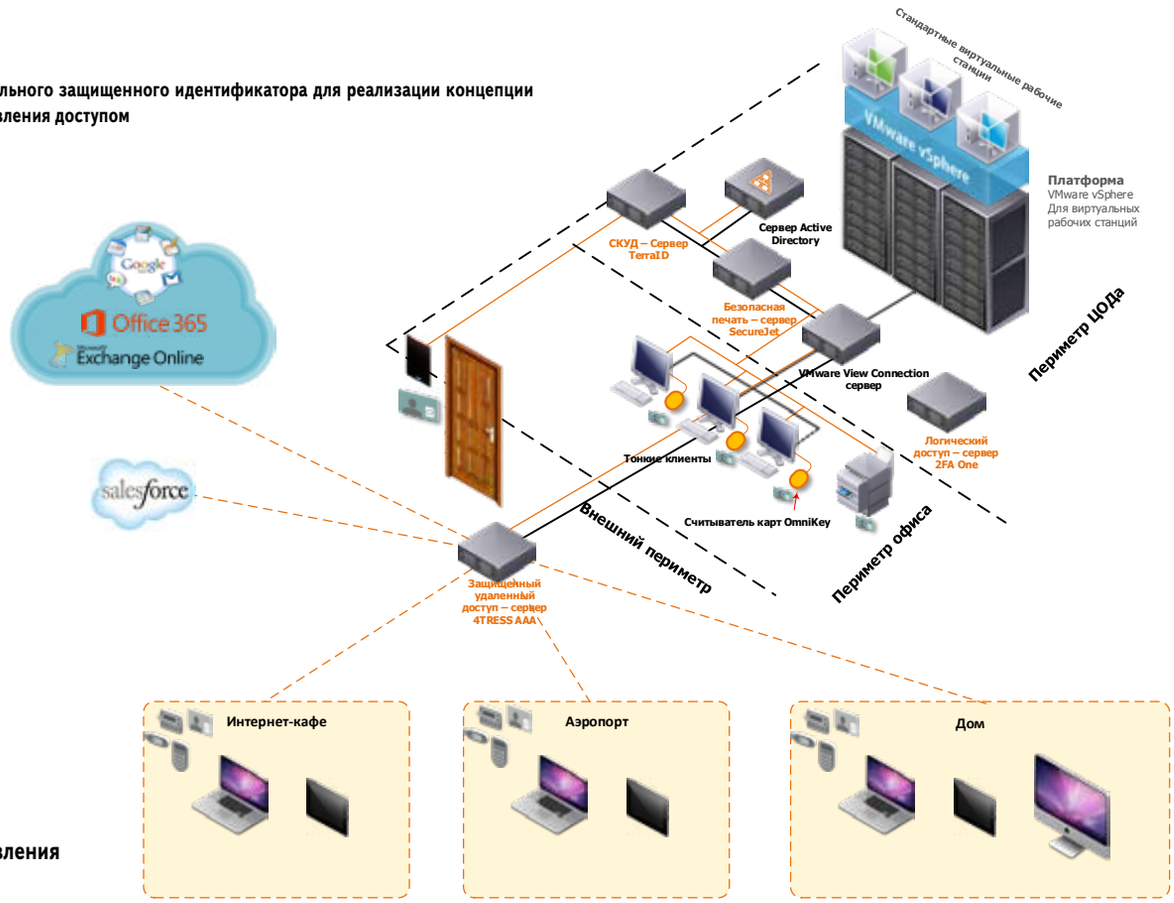
ДРАЙВЕР ПЕРЕХОДА К ЕДИНОЙ ПОЛИТИКЕ БЕЗОПАСНОСТИ

Технологический драйвер конвергенции – полный отказ от автономных систем в пользу сетевых технологий в области физического доступа. Это позволяет делегировать обслуживание системы СКУД в ИТ-департамент компании и сократить издержки на внедрение нескольких решений в инфраструктуру компании. Что, в свою очередь, позволит оптимизировать с точки зрения бизнес-процессов и технологий организацию комплексной системы управления доступом.

Основным критерием зрелости комплексной системы управления является реализация единой политики безопасности, которая определяет уровни доступа и использования корпоративных ресурсов.

Выработка единой политики безопасности подразумевает проработку вопросов администрирования выдачи прав и средств доступа, а также аудита защищенности идентификаторов. Целесообразным с точки зрения бизнес-процессов является не только консолидация управления доступом в одной службе, но и выпуск универсального защищенного идентификатора для сотрудников, что позволит отказаться от использования в работе нескольких устройств, снизит трудозатраты на их перепрограммирование и обеспечит сильную аутентификацию по всей инфраструктуре.

Использование универсального защищенного идентификатора для реализации концепции централизованного управления доступом



Традиционная концепция комплексной системы управления доступом

Защита доступа в периметр офиса	физический доступ
Защита доступа к информационным активам организации внутри периметра	логический доступ
Защита доступа к информационным активам организации вне периметра организации	решение по защите удаленного доступа с помощью одноразовых паролей
Защита доступа к информационным активам организации с личных устройств (BYOD)	конвергенция защиты доступа с помощью универсальных идентификаторов со встроенными генераторами одноразовых паролей

ДОСТУП К КОРПОРАТИВНЫМ РЕСУРСАМ С МОБИЛЬНЫХ УСТРОЙСТВ

Мобильность сотрудников можно рассматривать не только как дополнительную угрозу с точки зрения утечки информации, но и в качестве платформы или идентификаторов для средств физического и логического доступа. Первые наработки в этой области уже представлены на рынке в виде решения HID Mobile Access, в котором смартфон используется в качестве идентификатора физического доступа. Технология SIO, применяемая для защиты ключей, предусматривает хранение нескольких объектов, открывая потенциальную возможность встраивания мобильных устройств в общую централизованную систему управления доступом. Среди возможных юридических барьеров использования мобильных устройств — смартфоны не принадлежат организации, как следствие, не могут без должного согласия сотрудника быть «ключом» для доступа к корпоративной информации в рамках единой политики безопасности.

ЗАЩИТА УДАЛЕННОГО ДОСТУПА К КОРПОРАТИВНЫМ РЕСУРСАМ

В случае если пользователь находится в защищенном периметре, например в офисном помещении компании, и подключен по локальной сети к корпоративным ресурсам, достаточно простой двухфакторной аутентификации с помощью RFID-карты и ПИН-кода к ней. Однако все больше пользователей для большей мобильности используют более одного устройства для работы с корпоративными ресурсами. Как правило, дополнительные устройства являются личными. Многие компании поддерживают инициативу BYOD (использования личных устройств). Подключение с дополнительных устройств в большинстве случаев происходит по беспроводным сетям, часто для гостевого доступа, что подразумевает либо частичную защиту трафика, либо полное отсутствие защиты.

Все современные средства тестирования на проникновение позволяют перехватывать беспроводной трафик и извлекать из него данные, такие как логин и пароль, в том числе из SSL пакетов. В таких случаях крайне важно обеспечить строгую аутентификацию для доступа к активам компании. Целесообразно использовать OTP (генератор одноразовых паролей), который в случае встраивания в карту RFID или чип метки позволяет создать унифицированное средство защиты от входа в офисное помещение до аутентификации на рабочий компьютер или доступ к корпоративным данным с планшета в аэропорту или из дома.

КОНЦЕПЦИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ АКТИВОВ КОМПАНИИ

Переход от традиционного деления на уровни и периметры безопасности к единой политике безопасности позволяет уйти от концепции «лоскутной» защиты от конкретного типа угроз к внедрению централизованного управления защитой активов компании. Предложенная концепция предусматривает пересмотр представлений о составляющих элементах системы с точки зрения решения одной узкой задачи по защите отдельного периметра (например, физический доступ в помещение) в сторону ее адаптивности и простоты интеграции в единое решение для обеспечения безопасности доступа ко всем ресурсам с любых зарегистрированных в системе устройств, в том числе и с мобильных.