Конвергенция физического и логического доступа. Взгляд системного интегратора

Алексей МИХАЙЛОВ, директор по развитию направлений «ИТ-решения» и «Безопасность данных» компании TerraLink

Владимир НАРОЖНЫЙ, руководитель направления брендинга и интегрированных маркетинговых коммуникаций компании TerraLink

Использование единого идентификатора для предоставления доступа к различным ресурсам компании – тренд последних лет (одни из первых упоминаний: круглые столы «СКУД + ИТ: интеграция неизбежна» в журналах «Системы безопасности» (№ 5 2010) и ТЗ (№ 2 2011).

На наш взгляд, сегодня достаточно оснований перевода теории в практическую область. Цель данного материала – на практическом примере продемонстрировать возможности карты, которую каждый из нас применяет для входа в офисное помещение.

Предпосылки конвергенции средств доступа на единой карте

ВОЗВРАТ ИНВЕСТИЦИЙ И ПРОЗРАЧНОСТЬ УПРАВЛЕНИЯ ИБ КОМПАНИИ

Очевидно, что это удобно. Капитализировать вложенные инвестиции в организацию контроля доступа компании в создание единой системы управления доступом: к дверям, к корпоративным информационным ресурсам, оргтехнике и рабочим терминалам сотрудников. Очевидно, что целью создания такой системы является не только оптимизация операционных расходов. Ключевыми предпосылками конвергенции с позиции топ-менеджмента и ИТ-директоров является решение задач повышения прозрачности и гибкости управления информационной безопасностью компании.

Очевидно, что реализация такой системы возможна только в случае достаточной защищенности идентификаторов системы СКУД. Как правило, это отказ от стандартных технологий идентификации, таких как proximity-карты в пользу защищенных технологий 13,56 МГц, например, смарт-карт с технологией шифрования на базе модели SIO. Смарт-карта может также использоваться для хранения ключей шифрации почтовых или файловых данных, выписанных для пользователя. Безусловно, что использование одной универсальной карты для всех задач информационной безопасности упрощает работу сотрудников со средствами обеспечения безопасности и повышает эффективность ее обеспечения для службы безопасности компании.

ОБЩАЯ КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПАНИИ

Повсеместное применение сетевых технологий в сегменте физической безопасности способствует разработке единой стратегии обеспечения безопасности, которая подразумевает тесное со-

трудничество двух традиционно разделенных подразделений: ИТ и физической безопасности, их естественное объединение в один департамент. Отсутствие единой стратегии в области безопасности способствует «лоскутной» защите и, как правило, утечке информации.

УЧЕТ РАБОЧЕГО ВРЕМЕНИ

Конвергенция физического и логического доступа расширяет возможности ведения учета рабочего времени. Гибкость настроек модулей УРВ системы физического доступа дополняется возможностью фиксации фактического учета времени, проведенного сотрудником на рабочем месте и непосредственно за рабочим терминалом, в журнале событий.

ЦЕНТРАЛИЗАЦИЯ УПРАВЛЕНИЯ ДОСТУПОМ

Знания, опыт, ноу-хау часто являются самым ценным, что есть в компании. Это цифровая информация, доступ к которой предоставляется только авторизованным сотрудникам. Для этого физическое рабочее место сотрудника традиционно оснащено ПК или ноутбуком. В большинстве случаев доступ к корпоративным ресурсам осуществляется по логину и паролю (однофакторная аутентификация).

При этом существует дилемма безопасности: если проводить строгую политику назначения пароля с требованиями наличия букв в разных регистрах, цифр и специальных символов, то, скорее всего, данные для входа в систему сотрудники будут хранить на стикере, наклеенном на корпус монитора. Однако если не назначать такую политику, то, скорее всего, будут использоваться простые однотипные пароли, обеспечивая быстрый доступ злоумышленника к корпоративным данным. При этом так называемые шпионы, отслеживающие запущенные программы и нажатия клавиш, даже в случае строгой политики оставляют шанс злоумышленнику завладеть идентификатором сотрудника.

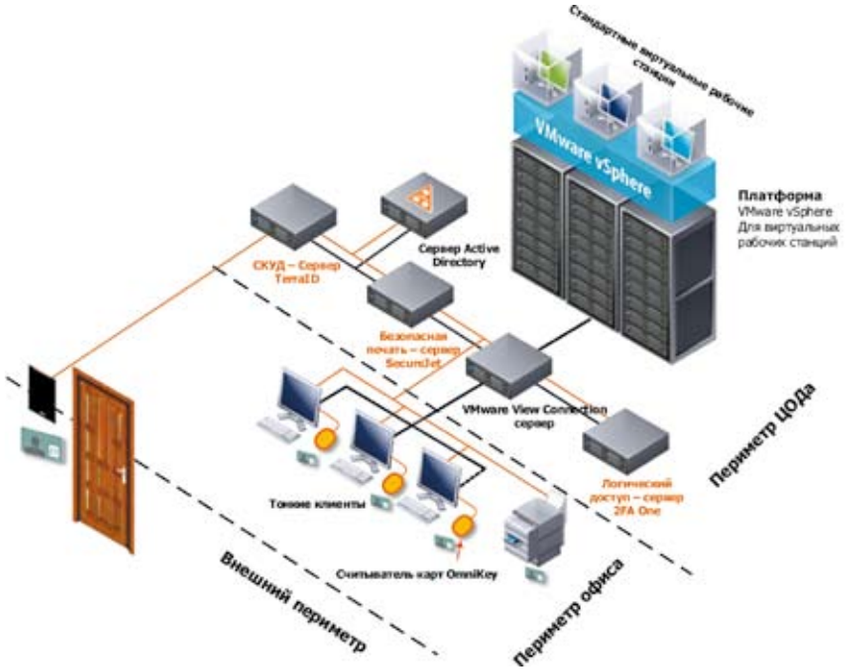
Еще один наиболее частый способ получения доступа к корпоративным данным: достаточно извлечь жесткий диск или физически вынести устройство из офиса компании. Эти примеры наглядно демонстрируют, что отсутствие централизованной системы управления доступом приводит к снижению общего уровня безопасности.

Максимальный уровень безопасности входа в помещение и в информационное пространство компании

ОРГАНИЗАЦИЯ ВИРТУАЛЬНЫХ РАБОЧИХ МЕСТ СОТРУДНИКА

Для предотвращения описанных выше угроз утечки корпоративной информации целесообразно обеспечить рабочие места сотрудников простыми бездисковыми устройствами доступа. Основное назначение тонких клиентов — предоставление интерфейса к удаленным рабочим станциям, с которых запускаются необходимые приложения для работы сотрудников, при этом для сотрудника интерфейс и характер работы остается прежним. Файлы, с которыми работают сотрудники, хранятся в корпоративных центрах обработки данных. Для организации защищенного доступа сотрудника к виртуальному рабочему месту к тонкому клиенту подключается настольный USB-считыватель карт, таким образом, избавляясь от риска физической кражи информации на носителе и удостоверяя личность сотрудника с помощью двухфакторной аутентификации, лишенной недостатков логина и пароля.

Централизация управления физической безопасностью и виртуальной инфраструктурой позволяет максимально защитить конечное



рабочее место, переместив работу с корпоративной информацией в защищенный центр обработки данных. В итоге на рабочем терминале, который находится в эксплуатации сотрудника, не хранится ценная информация, а доступ невозможно подделать без физического изъятия карты.

Использование карты доступа в помещение для идентификации сотрудника на рабочем месте обеспечивает переход от однофакторной идентификации «логин-пароль» к многофакторной «карта доступа и pin code для верификации», что значительно повышает уровень безопасности к информационным ресурсам компании.

Доступ к распечаткам имеет только тот, кто отправил информацию на печать

ИСПОЛЬЗОВАНИЕ ЕДИНОГО ИДЕНТИФИКАТОРА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ ПЕЧАТИ

Решение позволяет осуществлять печать с виртуальных рабочих мест на любое печатающее устройство компании, забирать распечатки после авторизации на устройстве. Таким образом, никто, кроме владельца задания печати, не сможет получить несанкционированный доступ к распечатке. Попутно решается вопрос экономии на печати за счет исключения бесхозных заданий, отправленных на печать и забытых на устройстве. Для авторизации в простом случае необходимо ввести pin code, более защищенный вариант — приложить карту доступа к специальному считывателю.

Дополнительным фактором безопасности при печати конфиденциальных документов является шифрование данных при отправке на печать. Алгоритм следующий: шифрование файла происходит на рабочем терминале сотрудника, до момента дешифрования файл хранится в БД корпоративного сервера. Дешифрование и печать происходят после идентификации пользователя.

Гибкие метрики отчетности, назначение прав доступа для различных пользователей, возможность оценки нагрузки по каждому пользователю и прогнозирование затрат на печать, поддержка различных средств и комбинаций идентификации, форматов и стандартов карт доступа — основные драйверы интереса к системам безопасной печати.

Резюме

Выбор карты доступа 13,56 МГц с технологией шифрования данных SIO в качестве единого идентификатора для доступа к корпоративным ресурсам компании и входа в помещение офиса упрощает процессы организации централизованной системы управления доступом, позволяет сократить затраты на внедрение и обслуживание информационных систем, предотвратить угрозы утечки информации, а также улучшает микроклимат в компании за счет регламентации бизнес-процессов.