Как выбрать систему логического доступа. Часть 2

Сценарии усиления защиты доступа к информационным ресурсам и активам компании

Михаил АШАРИН, технический консультант TerraLink

В первой части статьи «Как выбрать систему логического доступа. Удобство или безопасность?» («Технологии защиты», № 6 – 2015) мы затронули проблематику выбора заказчиком между удобством эксплуатации системы и уровнем ее безопасности. Теперь поговорим о возможных сценариях усиления защиты логического доступа к информационным ресурсам компании, когда заказчик ясно понимает низкую безопасность входа только по системному паролю.

БЕЗОПАСНЫЙ ДОСТУП

Пришел, увидел и... не вошел

Ранее озвучено, что используемые по умолчанию статические пароли обладают существенными недостатками, в первую очередь с точки зрения информационной безопасности. Действительно, простые пароли легко могут быть скомпрометированы – подсмотрены при вводе или подобраны злоумышленником. Сложные же пароли (когда в организации применяется строгая политика) трудно запоминать, в результате сотрудники оставляют записки с паролями в доступных для чтения местах или используют легко подбираемые комбинации, например клавиатурные последовательности.

Ввод сложных паролей и их периодическая смена вызывают очевидные трудности у пользователей, что приводит к блокировкам их учетных записей и дополнительной нагрузке на службу технической поддержки. Низкая безопасность, нерациональное использование людских ресурсов в компании – предпосылки принятия решения заказчиков пересмотреть подход к организации управления доступом.

Самое правильное направление поиска решения в данном случае – это надежная двухфакторная аутентификация.

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Один в поле не воин

Два разнородных фактора аутентификации предотвращают несанкционированный доступ к информационным ресурсам в случае компрометации одного из них. Эта пара, как правило, представляет собой некоторую информацию, известную только пользователю, – «то, что он знает» (пароль, PIN-код, контрольные вопросы), и исключительное владение пользователем некоторым аутентификатором – «то, что он имеет» (смарт-карта, токен, палец и т. п.).

КРИТЕРИИ ВЫБОРА МЕТОДОВ

Правильный выбор методов и устройств для двухфакторной аутентификации, в частности программного обеспечения, лучше всего начинать с анализа и расстановки приоритетов из следующих критериев:

- Уровень безопасности (защита от несанкционированного входа в информационные ресурсы).
- Инфраструктурные предпосылки (наличие в корпоративной среде заказчика аутентификаторов для других систем доступа, например, бесконтактных карт СКУД, а также доменных служб сертификации, например, удостоверяющего центра от Microsoft).
- Категории персонала (наличие в штате компании работающих дистанционно сотрудников, для которых требуется усилить удаленный доступ к корпоративным) ресурсам.
- Стоимость владения (включает не только программные лицензии, но также и затраты на дополнительное оборудование, например USB-считыватели, внедрение и эксплуатацию решения).

КОГДА БЕЗОПАСНОСТЬ НА ПЕРВОМ МЕСТЕ

Если разделить уровни безопасности от нуля до десяти, самую строгую защиту способна обеспечить только инфраструктура смарт-карт. Все остальные методы двухфакторной аутентификации – бесконтактная карта, одноразовый пароль, отпечаток пальца и т. п., используемые вместе с PIN-кодом в качестве второго фактора, – будучи в той или иной степени более надежными, чем один парольный фактор, все-таки предполагают использование доменного пароля на уровне системного функционирования Windows, даже если пользователь явно его не вводит.

Поэтому, если не перевести инфраструктуру логического доступа на контактные смарт-карты или PKI-токены, то всегда в той или иной мере будет существовать потенциальная угроза атаки на пользовательские системные пароли или манипуляций с ними со стороны, например, доменного администратора.

КОГДА КОМПРОМИСС ОПРАВДАН

Компромисс с точки зрения информационной безопасности вполне оправдан, в случае если внешний периметр инфраструктуры компании защищен с помощью бесконтактных карт СКУД и заказчик, взвесив вышеупомянутые критерии (безопасность, наличие карт и совокупная стоимость), принял решение использовать карты в качестве аутентификаторов для логического доступа к корпоративным ресурсам.

Практический пример: системный пароль вместо PIN-кода как второй фактор аутентификации

Реализация двухфакторной аутентификации по бесконтактным картам в продукте 2FA one, в котором можно настроить конфигурацию, когда в качестве второго фактора вместо обычного PIN-кода будет использоваться стандартный системный пароль сотрудника в домене.

Достоинства решения:

• Пользователям не надо запоминать и вводить новые статичные данные (PIN-код), что наиболее правильно с точки зрения логики функционирования системы: доменные пароли все равно будут проверяться на системном уровне в процессе входа в Windows.

• Послабление политики сложности системных паролей, поскольку некоторое снижение безопасности будет компенсировано дополнительным фактором аутентификации — приложенной к считывателю картой.

• Отключение принудительной периодической смены доменных паролей.

Как это работает?

Использование системных паролей в качестве PIN-кода от бесконтактных карт доступа и их выпуск можно организовать полностью на стороне оператора без физического присутствия владельца карты. Последовательность операций выпуска исключает возможный несанкционированный доступ к PIN-коду сотрудника со стороны недобросовестного оператора.

• Оператор выпуска привязывает карту к конкретному сотруднику на административном портале и персонализирует ее без ввода PIN-кода или пароля, приложив карту к подключенному USB-считывателю. Выпущенная карта может быть доставлена владельцу любым способом.

• Для входа на рабочую станцию сотрудник должен будет приложить свою карту к считывателю и ввести свой обычный пароль. Дополнительная настройка: при удалении карты с считывателя происходит блокировка сеанса пользователя, разблокировка рабочей станции происходит после повторного прикосновения карт с вводом PIN-кода/пароля.

В качестве экстренного входа в систему (или разблокирования заблокированной карты на этом этапе) в решении предусмотрена резервная аутентификация по контрольным вопросам.

ДРУГИЕ МЕТОДЫ И УСТРОЙСТВА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

В этой статье мы привели практический пример использования карт доступа как одного из самых распространенных способов организации системы с двухфакторной аутентификацией. В следующей статье постараемся раскрыть особенности организации двухфакторной аутентификации по одноразовым паролям (OTP) для усиления дистанционного доступа через генерацию OTP с

помощью мобильных приложений на личных или корпоративных смартфонах/планшетах сотрудников, а также функционал однократной сквозной аутентификации (SSO), который обеспечивает автоматизированный вход в корпоративные приложения или web-порталы по прикладным учетным данным после входа в систему с помощью основного метода,

СМАРТ-КАРТЫ

О строгой аутентификации

Среди экспертов в области двухфакторной аутентификации есть довольно распространенное бескомпромиссное мнение: по-настоящему строгим методом является исключительно инфраструктура контактных смарт-карт, когда владение картой рассматривается в качестве первого фактора, а известный только пользователю PIN-код от нее – в качестве второго.

Поэтому если для заказчика вопрос безопасности стоит на первом месте, то выбор решения практически ограничен областью контактных смарт-карт и USB-токенов с криптографическим чипом. Принцип их работы основан на надежных алгоритмах шифрования в контексте так называемой инфраструктуры открытых ключей (PKI), которая обеспечивает взаимодействие между центрами сертификации (CA), цифровыми сертификатами и секретными ключами на контактных смарт-картах.

В отличие от остальных методов двухфакторной аутентификации (по бесконтактным картам, одноразовым паролям, отпечаткам пальцев и др.) только инфраструктура контактных смарт-карт позволяет полностью уйти от использования системных паролей для доступа на рабочие станции в корпоративной сети, построенной на службе каталогов от Microsoft.

Критерии выбора системы строгой аутентификации:

- Наличие тесной интеграции со смежной инфраструктурой – доменными службами сертификации и корпоративной службой каталогов.
- Высокая оптимизация и автоматизация процессов обслуживания смарт-карт или PKI-токенов – их предельное эффективное централизованное управление: выпуск, персонализация, замена, разблокировка, обновление, отзыв, очистка и др.
- Система обслуживания устройств максимально защищена от несанкционированного захвата управления и внутреннего взлома со стороны злоумышленников.

КОМБИНИРОВАННЫЕ КАРТЫ ДОСТУПА

Наиболее интересным расширением инфраструктуры смарт-карт может стать так называемый конвергированный доступ, при котором подразумевается объединение физического (в помещения компании) и логического (в ее информационные ресурсы) доступа с помощью единой унифицированной карты, которая в этом случае будет одновременно являться и пропуском в офис, и аутентификатором в систему.

Отчасти такая реализация была нами рассмотрена выше, когда речь шла о построении логического доступа на базе уже применяемых в СКУД бесконтактных картах. Но если говорить о бескомпромиссном уровне защите доступа, а именно передовых бесконтактных технологиях для защиты периметра и контактных смарт-картах для аутентификации в ресурсы, в случае, когда внедрение инфраструктуры планируется «с нуля», решение может базироваться на комбинированных смарт-картах, которые совмещают в себе две или более разнородные технологии, например, со встроенным контактным PKI-чипом и разными комбинациями нескольких стандартов RFID (iCLASS, MIFARE, HID Prox/Indala и т. п.). Это тема для следующей части статьи.