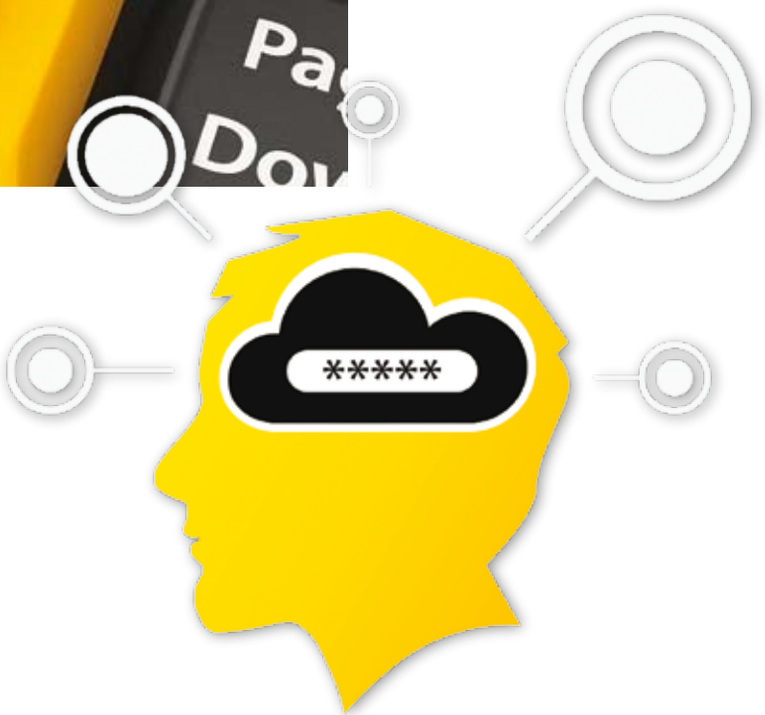
Михаил АШАРИН,
технический консультант TerraLink

Система логического доступа: **удобство или безопасность?**



Проблема выбора

Проблема выбора системы логического доступа к корпоративным информационным ресурсам вызвана, с одной стороны, пониманием недостатков обычного входа по логину и паролю, а с другой — необходимостью самостоятельно разобраться во всем разнообразии предлагаемых методов и технологий аутентификации, не имея должного опыта и компетенции в данной области.

Данный материал поможет составить чек-лист и определить, чем руководствоваться в непростом выборе оптимального решения.

Критерии выбора

Чтобы сразу обрисовать потенциальную сложность правильного выбора новой системы логического доступа, укажем лишь основные факторы:

- уровень защиты доступа к корпоративным ресурсам;
- удобство использования для сотрудников;
- степень нагрузки на службу поддержки;
- необходимость приобретения дополнительных устройств аутентификации;
- возможность применения уже используемых в организации аутентификаторов, например, бесконтактных карт в СКУД;
- возможность использования личных или служебных смартфонов/планшетов сотрудников;
- наличие штата дистанционных сотрудников, для которых требуется защита удаленного доступа;
- возможность развертывания дополнительной инфраструктуры (например, инфраструктуры PKI для контактных смарт-карт);
- необходимость автоматизации доступа к корпоративным ресурсам (приложениям или web-формам) с собственными прикладными учетными данными с помощью функционала однократной сквозной аутентификации (SSO);
- наличие регламентов на доступ в интернет из корпоративной беспроводной сети или возможность публикации в интернет внутренних сервисов аутентификации;
- суммарные затраты на внедрение (стоимость программных лицензий и дополнительного оборудования, например, USB-считывателей карт/отпечатков пальцев для рабочих станций сотрудников или автономных OTP-токенов).

Правильный выбор решения зависит от определения последовательности рассмотрения этих условий.

Удобство или безопасность?

Большинство компаний — разработчиков решений для логического доступа позиционируют себя экспертами в области информационной безопасности, и практически все дистрибьюторы продуктов, справедливо опираясь на основные постулаты информационной безопасности, как правило, предполагают, что интерес конечных клиентов к подобным системам вызван прежде всего желанием усилить защиту аутентификации, подняв тем самым общей уровень безопасности инфраструктуры компании.

Однако на практике нередко оказывается, что для многих организаций важнее в первую очередь именно удобство аутентификации, а проблема повышения безопасности либо не стоит вообще, либо считается решенной на уровне защиты внешнего периметра с помощью СКУД. И нельзя недооценивать такую позицию заказчика.

В первую очередь, на наш взгляд, заказчику необходимо определиться, чем его не устраивает простая аутентификация по системному паролю — соображениями безопасности или неудобством такого метода.

Неудобство входа по паролю

Итак, чем может быть неудобен обычный доступ на рабочую станцию по статическому (как правило, доменному) паролю? Ответ только один: пользователь должен помнить и, возможно, периодически менять свой пароль, а также каждый раз для входа в систему правильно его вводить, учитывая раскладку клавиатуры.

Чтобы избежать неразумных упрощений, сразу следует отметить, что реализация автоматического входа в систему без ввода системного пароля:

- во-первых, неприемлема с точки зрения элементарной безопасности;
- во-вторых, сильно ограничивает работу нескольких пользователей за одним компьютером;
- в-третьих, затруднена через обычный функционал Windows в доменной инфраструктуре без специальных настроек в реестре.

Также конфигурация с очень простыми паролями, например, «1234», может применяться только, когда эти пароли нужны исключительно для идентификации пользователя в системе без какой-либо защиты от несанкционированного входа в нее. В остальных случаях, где должны быть соблюдены базовые требования защиты доступа, нужно

использовать замену парольного фактора аутентификации на более удобный с помощью стороннего решения.

Удобство и безопасность

В качестве альтернатив системному паролю, которые бы удовлетворяли и требованиям удобства эксплуатации, и политикам безопасности, рекомендуем обратить внимание на следующие методы:

- доступ по бесконтактной карте (или по устаревшей технологии с магнитной полосой);
- доступ по отпечатку пальца (или аналогичная биометрическая технология).

Бесконтактная карта вместо пароля

Первый метод с использованием бесконтактных карт вместо ввода паролей особенно привлекателен для компаний, в которых карты уже используются в системах защиты физического доступа (СКУД). Основной недостаток метода: необходимость установки USB-считывателей бесконтактных карт по числу рабочих станций. На рынке представлен достаточно широкий ассортимент моделей считывателей бесконтактных карт в разнообразных форм-факторах и с поддержкой различных технологий.

Если ориентироваться на перспективу и последующий переход на более защищенные технологии при выборе считывателя, рекомендуем обратить внимание на универсальные устройства, которые совместимы практически со всеми стандартами. Сразу оговоримся, что не стоит ожидать низкой стоимости таких считывателей — в любом случае в силу технологических особенностей цена будет выше по сравнению с ценой USB-считывателей контактных смарт-карт.

Что касается самого решения для реализации этого подхода, рекомендуем обратить внимание на продукты, архитектура и целевое назначение которых изначально ориентированы на организацию системы логического доступа с централизованным управлением жизненным циклом бесконтактных карт с ролевой моделью и полнофункциональным аудитом.

Биометрия вместо пароля

В случае если карты не используются в инфраструктуре заказчика, для повышения удобства логического доступа имеет смысл обратить внимание на второй упомянутый метод — по отпечаткам пальцев. При выборе этого метода требуется установка биометрических USB-считывателей (сканеров) отпечатков пальцев для каждой рабочей станции. С точки зрения удобства вход по отпечаткам пальцев более предпочтителен, чем по бесконтактным картам, так как такой аутентификатор — палец — невозможно потерять или забыть, следовательно, значительно снижается нагрузка на службу поддержки. Несмотря на то что в данном материале мы рассматриваем методы с точки зрения удобства использования, отметим, что логический доступ по отпечаткам пальцев из-за своей технологической особенности выделяется довольно высоким уровнем безопасности, особенно на фоне статических паролей и бесконтактных карт.

Резюме

Общее слабое место приведенных методов доступа — необходимость дополнительного приобретения считывателей карт или отпечатков пальцев, особенно если в организации много рабочих станций. Однако если заказчик планирует в перспективе модернизировать бесконтактную технологию в картах для усиления защиты физического входа в помещения путем замены устройств СКУД, в том числе самих карт, разумно будет изначально инвестировать в инсталляцию мультиформатных считывателей с одновременной поддержкой основных бесконтактных технологий, включая защищенные, например, iCLASS SE и Seos с SIO.

Если для заказчика удобство определенно выше безопасности, выбор методов и устройств аутентификации на этом можно остановить. Но очень рекомендуем даже в этом случае ознакомиться с остальными вариантами логического доступа, важными в первую очередь с точки зрения уровня информационной безопасности, которые мы рассмотрим во второй части материала.