Карта, отпечаток пальца или OTP?

Как избежать необоснованных затрат на внедрение системы логического доступа

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. Во второй – «Как выбрать систему логического доступа. Часть 2. Сценарии усиления защиты доступа к информационным ресурсам и активам компании» («Технологии защиты» № 1 – 2016) подробно рассмотрели сценарии усиления защиты логического доступа с помощью бесконтактных и контактных карт доступа. В третьей части рассмотрим сценарии использования других аутентификаторов и обобщим результаты.

Многофакторная аутентификация: когда третий – не лишний

Способы усиления логического доступа, перечисленные в первых двух частях статьи, подходят для офисных сотрудников компании, которые централизованно подключаются к рабочим станциям через доменные политики, находясь внутри периметра офиса. Рассмотрим еще один сценарий, который будет полезен заказчикам, у которых не организован контроль физического доступа в помещения и которые уже осознали необходимость защиты доступа к корпоративной информации через личные мобильные устройства сотрудников.

Метод Ping Me, или Как проверить присутствие сотрудника в офисе?

Современные программные продукты поддерживают метод Ping Me, который позволяет прозрачно проверить присутствие сотрудников на территории компании.

Алгоритм:

1. В момент пересечения периметра офиса смартфон или планшет сотрудника автоматически подключается к корпоративной беспроводной сети, из которой открыт доступ к серверу аутентификации и в интернет.
2. Для входа на рабочую станцию сотрудник вводит свой обычный системный пароль. Через установленное на смартфоне мобильное приложение следует пройти аутентификацию с помощью входящего Push-сообщения.

В сценарии:

первый фактор – факт присутствия сотрудника в зоне действия корпоративной беспроводной сети (на территории компании);

второй – ввод стандартного доменного пароля;

третий фактор – это наличие личного или рабочего смартфона/планшета с установленным мобильным приложением, которое инициирует запрос на вход в систему через сервис Push-уведомлений от Google (Android) или Apple (iOS).

Если пользователь со своим смартфоном находится вне периметра офиса и попробует войти в систему дистанционно, даже правильно введя свой системный пароль и получив на смартфон запрос на верификацию попытки входа, он не сможет подтвердить его, так как сервер аутентификации не доступен за пределами корпоративной сети.

Достоинство описанного решения многофакторной аутентификации: нет необходимости приобретать дополнительное оборудование – предполагается использование личных или рабочих смартфонов/планшетов сотрудников.

Дистанционный доступ: солдат спит – служба идет

Рассмотрим сценарий усиления удаленного логического доступа к корпоративным ресурсам для дистанционных сотрудников.

Предполагается, что такие пользователи должны проходить безопасную аутентификацию на личных компьютерах, находясь дома, с рабочих лэптопов во время командировок либо пользуясь гостевыми рабочими станциями.

И если для собственных ПК и мобильных устройств можно подключить USB-считыватели для чтения контактных или бесконтактных карт, отпечатков пальцев, инсталлировать клиентское ПО и драйвера, то для гостевого оборудования это будет неуместно и невозможно. Практически единственным выходом в приведенной ситуации является использование инфраструктуры одноразовых паролей (One Time Password – OTP) для безопасной двухфакторной аутентификации по ним.

Одноразовые пароли: эх раз, да еще раз...

Одноразовый пароль валиден только для однократного события ввода в течение ограниченного периода времени (например, одной минуты). Такие пароли могут быть получены на так называемых OTP-генераторах, которые представляют собой аппаратные или программные токены, цифровые идентификаторы которых (сиды) хранятся на серверах аутентификации и логически привязаны к своим владельцам.

Виды токенов

Аппаратные OTP-токены представлены на рынке широким спектром разнообразных устройств – от портативных брелоков с одной кнопкой и дисплеем до настольных моделей с цифровой клавиатурой и поддержкой нескольких сервисов (защита внутренним PIN-кодом, запрос-ответ, OTP-подпись транзакций и т. д.).

Программные генераторы, так называемые софт-токены, в свою очередь, чаще всего представляют собой клиентские мобильные приложения, установленные на смартфоны или планшеты из магазина приложений и активированные через web-сервис серверы аутентификации (через web-портал самообслуживания).

Как это работает?

После запуска приложения для получения OTP и дальнейшего ввода его для доступа к целевому ресурсу может потребоваться сначала правильно ввести PIN-код, заданный владельцем при активации софт-токена и, соответственно, известный только ему.

Весь функционал обслуживания софт-токенов логически разделен на централизованное управление ими со стороны операторов

решения (общая конфигурация, политика безопасности, привязка к пользователям, разблокировка, ресинхронизация и т. п.) и сервисы самообслуживания, доступные для конечных пользователей (активация и смена PIN-кода, самостоятельная разблокировка и ресинхронизация).

Высокий уровень защиты от компрометации основан на специальных алгоритмах их генерации, которые практически исключают вычисление или подбор следующего значения OTP из любого количества предыдущих. Функции вычисления OTP работают только «в одну сторону», обратных алгоритмов не существует, а данные во внутренней памяти OTP-генераторов надежно защищены строгой криптографией, а в случае аппаратных токенов – дополнительной защитой от механического вскрытия.

OTP для дистанционных и офисных сотрудников

Нет технических ограничений, которые бы ограничивали использование OTP для повышения защиты логического доступа не только дистанционных, но и офисных сотрудников. А в случае использования мобильных софт-токенов на собственных или рабочих смартфонах это позволяет значительно снизить издержки.

С точки зрения информационной безопасности рекомендуем обратить внимание на решения, которые не предусматривают уход от системных паролей при входе в систему, а усиливают его через дополнительный ввод одноразового пароля. Такой сценарий позволяет отключить собственный PIN-код для софт-токенов, имея в виду установленную защиту доступа к смартфону у большинства владельцев с помощью своего кода или графического ключа.

Единая карта: три в одном

В двух первых частях статьи мы уже говорили о так называемом конвергированном доступе, когда объединение логического и физического доступа осуществляется через единую комбинированную карту, которая совмещает в себе несколько различных технологий, например, контактный чип смарт-карты, один или несколько бесконтактных стандартов. Но область применения таких карт может быть расширена также и на инфраструктуру одноразовых паролей для удаленного доступа по ним к корпоративным ресурсам со стороны сотрудников, работающих дистанционно.

Эта концепция в полной мере реализована в картах, в которые могут быть встроены несколько технологий в разных комбинациях. В наиболее полном варианте это контактный чип смарт-карты; совместимая со СКУД бесконтактная метка плюс OTP-генератор с ЖК-дисплеем, обозначенной пьезокнопкой и высококонтрастным ЖК-дисплеем, на который выводится 6-значный одноразовый пароль при нажатии на кнопку.

Унификация доступа в этом сценарии будет выглядеть так: сотрудник использует карту для прохода в офисное помещение. Для входа на рабочую станцию вставляет карту в USB-считыватель на своей рабочей станции и вводит PIN-код для входа на нее. А в случае дистанционной работы для удаленной аутентификации, например к корпоративной почте через web-клиент, использует одноразовый пароль, сгенерированный на той же карте.

Резюме

Чтобы существенно облегчить выбор методов и устройств аутентификации для усиления логического доступа к корпоративным ресурсам, взвесить все «за» и «против», обеспечить должный уровень безопасности и удобства, а также избежать необоснованных затрат на внедрение, обобщим проведенный анализ с помощью условного дерева критериев с указанием дополнительных устройств для их реализации:

Критерий	Метод усиления защиты	Использование аутентификаторов СКУД
Удобство на первом месте	Бесконтактные карты вместо пароля	Уже используются бесконтактные карты для СКУД
Удобство и безопасность	Отпечатки пальцев вместо пароля	Уже используются бесконтактные карты для СКУД
Безопасность важнее	Самый надежный метод	Контактные смарт-карты плюс PIN-код
		USB-PKI-токены плюс PIN-код
	Бесконтактные карты плюс PIN-код или системный пароль	Уже используются бесконтактные карты для СКУД
	Комбинированные смарт-карты (контактный чип + RFID) плюс PIN-код	СКУД не используется, но планируется
	Отпечатки пальцев плюс опционально, PIN-код или системный пароль	СКУД не используется, но планируется
	Одноразовые пароли плюс PIN-код или системный пароль	СКУД не используется, но планируется
Безопасный вход в систему с контролем присутствия в офисе	Вход по системному паролю с подтверждением на смартфоне	СКУД не используется

Дистанционный доступ	Одноразовые пароли плюс PIN-код или системный пароль	Только дистанционные сотрудники
	Для внутреннего доступа — бесконтактные карты плюс PIN-код, для удаленного — одноразовые пароли плюс PIN-код через мобильные софт-токены на смартфонах или планшетах	Для входа в офис используются бесконтактные карты для СКУД
	Комбинированные смарт-карты (PKI + RFID + OTP) плюс PIN-код	СКУД не используется, но планируется
	Комбинированные USB-токены (PKI + OTP) плюс PIN-код	Для входа в офис СКУД не используется и не планируется

Следует учесть, что факторы условны, ситуации у заказчиков различны, а корпоративная среда, как правило, уникальна, поэтому рекомендуем проводить предпроектный анализ. Мы предлагаем рассматривать приведенные критерии как результат общего анализа сегмента логического доступа, как исходные «точки входа» для предварительной ориентации в широком спектре существующих методов, устройств, решений и, главное, аспектов аутентификации в инфраструктуре компании.