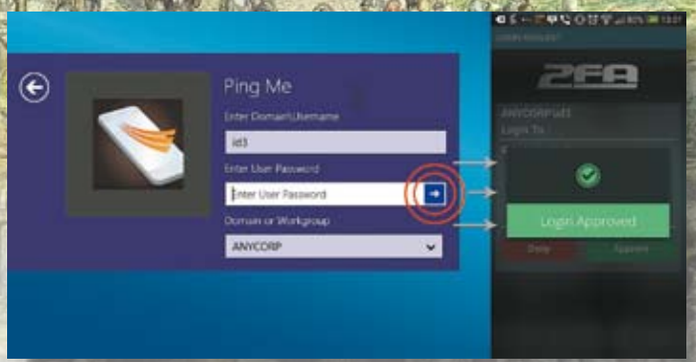
Михаил АШАРИН,
технический консультант TerraLink



Доступ к корпоративным ресурсам: новые методы двухфакторной аутентификации

Многие организации в последнее время обращают внимание на необходимость повышения безопасности доступа к корпоративным ресурсам. Но, как правило, большая часть ограничивается организацией системы контроля физического доступа, а логический доступ к корпоративным системам по-прежнему остается на уровне аутентификации по статическим паролям. Уязвимость такого метода вполне очевидна и давно известна — простые пароли могут быть легко подсмотрены или подобраны, а строгая политика сложности паролей приводит к трудности их создания и замены: пользователи их часто забывают — и это приводит к увеличению нагрузки на ИТ-департамент.

Что такое двухфакторная аутентификация

Поэтому все чаще перед компаниями встает вопрос повышения защиты логического доступа к своим ресурсам — доменным рабочим станциям, корпоративным порталам, файловым серверам, VPN-туннелям и т. п. Самым распространенным и эффективным способом усиления логического доступа, как известно, является внедрение двухфакторной аутентификации, которая предполагает применение для доступа двух разнородных факторов. Это может быть, например, известное исключительно пользователю (ПИН-код или тот же пароль) и аутентификатор, которым пользователь владеет (смарт-карта или токен, отпечаток пальца, смартфон и т. д.).

В ранее опубликованных материалах «Конвергенция физического и логического доступа. Взгляд системного интегратора» (ТЗ № 5–2014) и «Концепция организации централизованной системы управления доступом» (ТЗ № 1–2015) авторы обозначили, что одним из самых привлекательных способов перехода на усиленную аутентификацию к активам компании является применение уже используемых на предприятиях бесконтактных карт для физического доступа (СКУД).

Отметим, что современные сервер-клиентские системы логического доступа поддерживают сразу несколько методов и устройств: бесконтактные карты и карты с магнитной полосой, контактные смарт-карты и PKI-токены, биометрию по отпечаткам пальцев и одноразовые пароли на аппаратных токенах, а также резервную аутентификацию по контрольным вопросам.

Такой подход позволяет предотвратить несанкционированный доступ к ресурсам в случае получения злоумышленниками контроля над одним из факторов (например, утеря или кража смарт-карты, подбор ПИН-кода). Это особенно актуально для компаний, в которых для удаленных сотрудников уже организован доступ к внутренним ресурсам или же планируется такая организация.

One-Time-Password (OTP) для смартфонов и планшетов

Наряду с широко распространенными методами аутентификации по бесконтактным и контактным смарт-картам, контрольным вопросам и отпечаткам пальцев необходимо отметить методы, которые ранее не поддерживались в ПО для логического доступа.

Широко известная инфраструктура одноразовых паролей (OTP) позволяет использовать для логического доступа пароль, валидный только для однократного события аутентификации. При следующем доступе к тому же ресурсу требуется новый одноразовый пароль. В некоторых решениях, например 2FA one, сотрудники смогут сгенерировать такой пароль на предварительно установленном из магазина

приложений и активированном через сервер на мобильном клиенте ПО после ввода ПИН-кода, известного только самому пользователю. После получения значения OTP пользователь вводит его для доступа к корпоративным ресурсам. По сути, мобильный клиент представляет собой программный OTP-токен, предварительная конфигурация которого настраивается оператором на административном WEB-портале. По умолчанию срок службы жизни пароля, полученного через мобильный клиент, составляет 30 секунд, после истечения которых автоматически генерируется новое значение.

Push-уведомления через мобильное приложение для смартфонов и планшетов

В отличие от метода аутентификации по одноразовым паролям новый метод подтверждения доступа через Push-уведомления на мобильных устройствах является достаточно уникальной и инновационной функцией в системах аутентификации, в том числе если рассматривать метод в качестве сценария для входа в систему (Windows Logon). Для этого, кроме развернутой и соответствующим образом настроенной в корпоративной инфраструктуре системы логического доступа, на рабочей станции пользователя (или на терминальном сервере, если используется RDP-соединение) должно быть инсталлировано клиентское ПО, а на его смартфоне или планшете (iOS, Android, Windows Phone) установлен и активирован мобильный клиент. В таком сценарии пользователь выбирает для аутентификации в Windows этот метод, вводит свой логин и доменный пароль.

Новый функционал известных методов аутентификации

Наряду с внедрением новых методов аутентификации постоянно расширяется функционал поддерживаемых методов. Например, прекрасным дополнением к применяемому в компании методу аутентификации по бесконтактным картам станет использование функции Password as PIN (системный пароль вместо ПИН-кода). Функционал особенно удобен при переходе от простой аутентификации по системным паролям к безопасному логическому доступу. Сотрудникам в этом случае не потребуется задавать и запоминать новые статические данные в качестве ПИН-кода, а использовать вместо него уже известные свои системные пароли.

Резюме

Оба вышеописанных метода – OTP и Push-уведомления для мобильных устройств являются эффективными вариантами реализации безопасной двухфакторной аутентификации, которая может быть внедрена в корпоративную инфраструктуру организации для усиления логического доступа к ресурсам.

Настройки системы позволяют использовать оба новых метода одновременно для всех сотрудников сразу либо только для выделенных групп пользователей или доменных компьютеров.

Внедрение Push-уведомлений в качестве нового метода аутентификации будет очень интересно компаниям, которые не планируют использовать дополнительные устройства аутентификации для своих сотрудников, такие как смарт-карты, PKI-токены, аппаратные OTP-токены, а готовы ограничиться уже имеющимися у них личными или корпоративными смартфонами и планшетами.