Защита опубликованных корпоративных приложений

Публикуя свои ресурсы для удаленного доступа, компании значительно увеличивают риск несанкционированного доступа к бизнес-критичной информации. Обеспечить необходимый уровень защиты возможно только с использованием современных способов аутентификации пользователей.

Решение **Indeed Access Manager (Indeed AM)** позволяет применять методы двухфакторной аутентификации (2FA) для широкого спектра корпоративных приложений, позволяя построить единую систему 2FA при доступе к ресурсам, доступным из-за пределов сети компании.

Описание задачи

1. Обеспечить двухфакторную аутентификацию с применением одноразовых паролей в опубликованных корпоративных сервисах:
    - Web-приложения
    - VPN-сервер
    - VDI
2. Реализовать Web Single Sign-On для сквозного доступа в web-приложения.

2FA в web-приложениях IIS

Для аутентификации в web-приложениях, использующих Internet Information Services (IIS), нами разработан специализированный модуль интеграции IIS Extension. Данный модуль позволяет обеспечить двухфакторную аутентификацию в приложениях без вмешательства в их программный код. После ввода имени и пароля, пользователь перенаправляется на отдельную страницу аутентификации, где должен подтвердить себя с помощью одноразового пароля. IIS Extension может использоваться для любых web-приложений, например Outlook Web Access, Sharepoint, Skype for Business, RD Web Access и др. Для приложений, не использующих IIS, возможна интеграция с применением программного интерфейса (web API).

2FA в VPN

Интеграция со службами VPN выполняется с применением протокола RADIUS, поддерживаемого абсолютным большинством производителей VPN-решений, таких как Cisco ISE, Citrix Netscaler и др. Двухфакторная аутентификация реализуется с помощью механизма Challenge-Response, встроенного в RADIUS: на первом шаге пользователь вводит имя и пароль, после чего RADIUS сервер проверяет пользовательские данные и, в случае их верности, дозапрашивает у пользователя VPN сервиса второй фактор аутентификации - одноразовый пароль. RADIUS сервер выполнен на базе Microsoft Network Policy Server (служба доступна в составе Windows Server) и специализированного расширения для 2FA.

2FA в VDI

Для интеграции с системами виртуальных рабочих столов также применяется двухшаговая RADIUS-аутентификация по механизму Challenge-Response, которая поддерживается во многих VDI продуктах, например VMWare Horizon и Citrix XenDesktop. В случае использования технологий Microsoft, двухфакторная аутентификация может быть добавлена к службе удаленного доступа на сервере Remote Desktop Web Access (с использованием IIS Extension).

2FA в WebSSO (SAML IdP)

Организация сквозного доступа в web-приложения (web single sign-on) позволяет значительно повысить эффективность работы пользователей, позволяя прозрачно получать доступ в web-приложения после однократной аутентификации. Применение 2FA дает возможность сохранить высокий уровень информационной безопасности без снижения удобства использования. Для интеграции с целевыми решениями используется международный стандарт аутентификации SAML 2.0, что гарантирует совместимость с широким спектром систем. В контур WebSSO и 2FA могут быть включены не только корпоративные on-premise приложения, но и облачные сервисы, такие как Office 365 и G Suite (ранее Google Apps).

2FA в ADFS

Поддержка аутентификации пользователей по протоколу ADFS позволяет не только усилить безопасность целевых систем с применением 2FA, но и построить Single Sign-On (SSO) решение, избавив пользователей от необходимости многократно аутентифицироваться в рамках одной сессии. Сочетание 2FA и SSO подходов одновременно значительно усиливает уровень информационной безопасности компании и повышает эффективность работы ее сотрудников.

Ниже приведена общая схема решения.