УДК 004.56

М.І. Ганченко, О.Л. Яковенко
(Національний авіаційний університет, Україна.

Автентифікація як захист інформаційних ресурсів при віддаленому доступі.

Актуальний сучасний підхід до здійснення автентифікації користувачів при віддаленій роботі та доступі до корпоративних ресурсів, сервісів, додатків.

Сервер автентифікації.

Найбільшу цінність у роботі та просуванні продукції, послуг для будь-якої компанії являють: дані, інформація, повноваження та людські ресурси. Ситуація, що склалась у світі з поширенням пандемії коронавірусу створює та диктує нові умови і правила при яких виникає необхідність у створенні та організації дистанційної форми роботи працівників. Це сприяє виникненню та реалізації загроз інформаційної безпеки, а витік будь-яких критично важливих для організації даних несе за собою збитки, втрату довіри клієнтів та конкурентних переваг.

Так як додатки та сервіси компаній призначені лише для співробітників, то забезпечення безпечного входу та доступу до корпоративних ресурсів - пріоритетне завдання. Тож перше з чим зіштовхується користувач та зловмисник локально, або ж віддалено при спробі доступу до робочого облікового запису, системи, інформаційного ресурсу - це автентифікація. Саме ця процедура, за наявності доказів (введеного дійсного паролю, парольної фрази, біометрії та інших методів), дозволяє визначити, що користувач, котрий здійснює вхід у систему є тим за кого намагається себе видати. І як відомо, всі методи розпізнавання та підтвердження справжності особи лише фіксують факт, що автентифікатор відповідає його ідентифікатору і не автентифікують конкретного суб′єкта. Тобто без перевірки справжності користувача має бути відсутня можливість здійснити авторизацію та надати доступ та права у інформаційній системі. До прикладу: повинна бути мінімізована ймовірність компрометації облікового запису користувача, що здійснює вхід до електронної пошти з використанням логіну та паролю без використання протоколу HTTPS, або ж перевірка справжності користувача при використанні смарт-карти за сертифікатом – суттєво ускладнена.

Основною метою автентифікації є потужне зменшення можливостей використання чужих, вкрадених, підроблених облікових даних. При цьому для користувача процес входу має залишатися простим та зручним, що дещо ускладнює задачу. Зазвичай, в компаніях використовуються різні методи автентифікації для різних систем, що не пов′язані між собою (корпоративний портал, електронна пошта, віддалений VPN доступ, Wi-Fi), і що суперечить основам забезпечення інформаційної безпеки. Так як, використання різних, не пов′язаних між собою систем автентифікації вимагають великих та об′ємних ресурсів для підтримання та не відповідають вимогам гнучкості для їх

реалізації. Адже користувачам необхідний доступ до багатьох сервісів, а на системних адміністраторів при цьому покладається завдання розповсюдження інформації для реєстрації та входження до кожного серверу.

Для вирішення проблеми пропонується сучасний спосіб реалізації одноразового входу (запиту на проходження ідентифікації та автентифікації користувача) - серверу автентифікації. Єдиного центру адміністрування всіх процесів для перевірки автентичності як користувача, так і всіх додатків, сервісів та ресурсів. Такі сервери повинні підтримувати набори методів автентифікації, таких як: звичайний, одноразовий пароль, апаратний або програмний токен, смарт-карта, сертифікат та інші. Кожному ресурсу, що використовуватиме подібний сервер, забезпечується можливість вибору необхідного для себе методу автентифікації та висування вимог до методів перевірки користувачів будь-якими додатками та сервісами, що підключатимуться та обслуговуватимуться. Також передбачається можливість вбудовування нових методів, видалення, або модифікація старих. Це значно спрощує та усуває необхідність розробок для кожного додатку окремо. Відповідно зменшується час для виконання цих завдань, а швидкість введення продукту в експлуатацію містить конкурентні переваги у розгортанні бізнесу та виходу на перші позиції ринку. Інформаційні системи, що не підтримують сувору автентифікацію також можуть використовувати подібні сервери для підключення власних користувачів. Значне забезпечення збереження інформації реалізується шляхом підтримання серверами апаратних модулів, котрі додатково шифрують інформацію, що зберігається та обробляється у них. Таким чином досягається вищий рівень захищеності даних автентифікації.

Подібний сервер автентифікації можна налаштувати на контроль доступу користувачів у відповідності до прийнятої в організації політики безпеки. Передбачається можливість задання правил та умов, вимог до автентифікації користувачів різних рівнів. До правил можуть додаватись параметри навколишнього середовища та атрибути користувачів (час, адреса мережі користувача, тип пристрою з якого відбувається вхід). До прикладу: при вході у деякі додатки за певних умов буде вимагатись повторна або багатофакторна автентифікація.

Доступне налаштування та здійснення аудиту на сервері автентифікації. Реєстрація спроб входу користувача, як всіх успішних так і неуспішних та доступу до додатків. Здійснення моніторингу всіх невдалих спроб входу дозволяє виявити атаки (підбору паролів до облікових записів) та своєчасно відреагувати на них.

В загальному вигляді сервер автентифікації працює наступним чином:

- додаток хоче ідентифікувати користувача, котрий бажає ним скористатись та спрямовує користувача на зазначений сервер;

- сервер відображає сторінку входу, куди браузер надсилає дані автентифікації на перевірку;

- сервер автентифікації здійснює перевірку і через браузер передає спеціальний проміжний маркер безпеки.

- отримавши даний маркер додаток ідентифікує користувача. У разі, якщо програма намагається визвати сервіси іншого додатку, вона отримує від серверу автентифікації маркер доступу – токен, на право звернутись до іншого додатку від імені визначеного користувача. При цьому токен видається лише у тому разі, якщо користувач самостійно дозволив отримувати про нього дані у деякому сервісі.

Тож використання спеціалізованих серверів автентифікації дозволяє підвищити підхід до процедур перевірок автентичності в організації та дистанційно. Підвищення вимог до автентифікації, як окремого напрямку безпеки, забезпечить підвищений рівень доступу до ресурсів компанії та зменшить витрати на адміністрування, експлуатацію та аудит. Адміністратори отримують єдиний зручний інтерфейс для керування обліковими даними, та можливості для зміни або додавання нових методів перевірки автентичності. Авторизовані користувачі отримують змогу доступу та зручного використання корпоративних ресурсів з будь-якого віддаленого місця. А підприємство, у свою чергу, матиме надійний захист у вигляді, як мінімум, двухфакторної автентифікації (спершу на сервері, згодом при доступі до необхідного ресурсу, додатку).

Список літератури

1. Зачем нужен сервер аутентификации [електронний ресурс]. - Режим доступу: https://www.itweek.ru/security/article/detail.php?ID=171502
2. Обзор способов и протоколов аутентификации в веб-приложениях / Habr [електронний ресурс]. - Режим доступу: https://m.habr.com/ru/amp/post/262817/
3. Ричард Э. Смит Аутентификация: от паролей до открытых ключей. : Пер. с англ. – М. : Издательский дом ”Вильямс”, 2002. – 432 с. : ил. – Парал. тит. англ.
4. Enterprise Single Sign-On без установки на ПК программ-агентов [електронний ресурс]. - Режим доступу: https://identityblitz.ru/no-agent-esso/
5. Мартынова Л. Е., Умницын М. Ю., Назарова К. Е., Пересыпкин И. П. Исследование и сравнительный анализ методов аутентификации // Молодой ученый. — 2016. — №19. — С. 90-93.
6. Сервер аутентификации Kerberos [електронний ресурс]. - Режим доступу: https://www.osp.ru/os/1996/01/178793
7. Класифікація механізмів автентифікації користувачів і їх огляд [Електронний ресурс]. – Режим доступу: http://ed.kpi.ua/wp-content/uploads/conferences/2017/2017-178-185.pdf