

ДВОХФАКТОРНА АВТЕНТИФІКАЦІЯ ЯК МЕТОД ДЛЯ НАДІЙНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Коли мова йде про захист інформації, одним з найважливіших аспектів є захист від несанкціонованого доступу до ресурсів нашої мережі. Зрозуміло, вкрай важливим питанням є забезпечення процедури безпечної автентифікації. Цілком очевидно, що будь-яке розмежування повноважень, настройка прав доступу на ресурси системи має сенс тільки в тому випадку, якщо ми впевнені в тому, що той, хто намагається отримати доступ до наших ресурсів, є легальним користувачем.

Двохфакторна автентифікація або 2FA - це метод ідентифікації користувача в будь-якому сервісі, де використовуються два різних типи автентифікаційних даних. Введення додаткового рівня безпеки забезпечує більш ефективний захист акаунта від несанкціонованого доступу.

Двохфакторна автентифікація вимагає, щоб користувач мав два з трьох типів ідентифікаційних даних: щось йому відоме, щось у нього наявне, щось йому притаманне (біометрія). Очевидно, що до першого пункту належать різні паролі, пін-коди, секретні фрази і так далі, тобто щось, що користувач запам'ятовує і вводить в систему при запиті. Другий пункт - це токен, тобто компактний пристрій, який знаходиться у власності користувача. Найпростіші токени не вимагають фізичного підключення до комп'ютера - у них є дисплей, де відображається число, яке користувач вводить в систему для здійснення входу - складніші підключаються до комп'ютерів за допомогою USB і Bluetooth-інтерфейсів. Сьогодні в якості токенів можуть виступати смартфони, тому що вони стали невід'ємною частиною нашого життя. У цьому випадку так званий одноразовий пароль генерується або за допомогою спеціального додатку (наприклад Google Authenticator), або приходить по SMS - це максимально простий і дружній для користувача метод, який деякі експерти оцінюють як менш надійний.

Щоб користувач міг здійснити вхід, між токеном клієнта і сервером автентифікації повинна існувати синхронізація. Головна проблема полягає в тому, що з часом вони здатні розсинхронізуватися, проте деякі системи, такі як SecurID компанії RSA, дають можливість повторно синхронізувати токен з сервером шляхом введення декількох кодів доступу. Більш того, більшість з цих пристроїв не мають змінних батарей, тому мають обмежений термін служби.

Методам захисту, заснованим на методиках багатфакторної автентифікації, сьогодні довіряє велика кількість компаній, серед яких організації зі сфери інформаційних технологій, фінансового і страхового секторів ринку, великі банківські установи та підприємства державного сектору, незалежні експертні організації, а також дослідницькі фірми.