

СЕКЦІЯ 8

ЗАСОБИ АВТОМАТИЗАЦІЇ І КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ АПВ

ЧИННИК ВОЛОДІННЯ ПРИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ.

Чалий І.В., к.т.н., доцент, Балак С.О., студент
(ДБТУ, м. Харків, Україна)

Many cybersecurity experts believe that password authentication will gradually be replaced by passwordless authentication. Therefore, attention should be paid to the issue of using security keys.

Застосування у якості методу доступу класичної паролльної автентифікації потроху йде у минуле, так як має низку суттєвих недоліків. Зараз дуже популярними є двофакторна автентифікація (2FA), а ще більш перспективна дуже схожа на неї безпарольна автентифікація.

Взагалі розрізняють 3 чинники двофакторної автентифікації: знання, властивості та володіння. Перший чинник простий, не потребує наявності додаткових пристроїв, але не найнадійніший. Чинник властивості (біометрія) - це використання біометричних датчиків та сканерів. Якщо для мобільних пристроїв відбитки пальців та датчики голосу зараз доволі розповсюджені, то для офісної роботи застосовуються мало. Інші способи біометрії поки зазвичай занадто дорогі і громіздкі. Чинник володіння передбачає наявність у власності користувача якогось пристрою.

До останнього чинника відносяться дуже відомий такий засіб двофакторної автентифікації як автентифікація по телефону. Вона має декілька способів з яких найбільш відомими є банери із кнопкою підтвердження та посилка через SMS одноразового паролю. Однак фахівці з кібербезпеки мають багато застережень до цих способів, тому якщо вимагається високий ступінь безпеки, то цими способами користуватися не рекомендується.

Тому зараз все ширше застосування знаходять виносні пристрої - токени або ключі безпеки. Найбільш відомими та розповсюдженим у нас є токени для зберігання кваліфікованого електронного підпису (ЕЦП), які використовуються для віддаленого доступу до інформації та для ідентифікації його власника. Зовні вони схожі на звичайну флешку.

Ми звернули увагу на серію ключів безпеки YubiKey американської компанії Yubico. Вони дуже зручні у використанні, компактні, стійкі до механічних ушкоджень і головне надійні. Оскільки це фізичний фактор, злодіє не зможе зламати ваш обліковий запис, не маючи в наявності вашого ключа. Ключі використовуються співробітниками Google, Facebook, взагалі провідними ІТ-компаніями та державними структурами в багатьох країнах світу для автентифікації з метою запобігання витоку даних.

Серед недоліків ключів безпеки виділімо два основних: вони відносно дорогі і їх можна загубити. Але це притаманно більшості пристроїв, які реалізують чинники володіння, причому ситуація з ціною потроху покращується.

Висновки. Багато фахівців з кібербезпеки вважає, що паролльна автентифікація буде поступово замінюватися на безпарольну. Тому питанням застосування ключів безпеки (наприклад YubiKey), треба приділити більшу увагу при підготовці спеціалістів з кібербезпеки.