Безпека без компромісів:

сучасні виклики автентифікації та рішення від RSA

Захищений і контрольований доступ користувачів до корпоративних систем — наріжний камінь захисту цих систем. Єлизавета КОСТІНА, Cybersecurity Engineer компанії Seeton, пояснює, як тут може прислужитися рішення RSA SecurID.

Парадокс сучасної автентифікації: чим більше захисту, тим менше безпеки?

Цікавий феномен останніх років – парадокс «втоми від безпеки». Що складнішими стають вимоги до паролів і що більше факторів автентифікації додається, то частіше користувачі намагаються їх обійти. Наслідки – записки з паролями на моніторах, використання одного пароля для всіх сервісів та навіть передача токенів між співробітниками «для зручності». З іншого боку, служба інформаційної безпеки не може дозволити собі компромісів: атак стає більше, методи – складнішими, облікові дані – головна ціль зловмисників.

Скільки коштує компрометація?

За даними дослідження IBM Cost of a Data Breach Report 2024, середня вартість одного скомпрометованого запису становить $165, а повне відновлення після серйозного інциденту займає в середньому 277 днів.

Попри це, у багатьох компаніях досі відсутня прозора картина того, хто до чого має доступ і чому.

Саме тут постає питання не лише автентифікації, а й управління обліковими даними та доступами (IAM – Identity & Access Management). Але з чого починати цей складний шлях, щоб не втратити контроль над користувачами і не порушити бізнес-процеси?

Відповідь — RSA SecurID

RSA SecurID – це не просто система багатофакторної автентифікації. Це перший і фундаментальний крок на шляху до побудови повноцінної IAM-стратегії в компанії.

Рішення дозволяє:

- захистити вхід до будь-яких систем — локальних, хмарних, VPN, веб-застосунків;
- використовувати різні фактори підтвердження (мобільний застосунок, апаратний токен, біометрію, push-повідомлення);
- впроваджувати адаптивну автентифікацію – вимагати додаткові підтвердження лише в ризикованих ситуаціях;
- забезпечити єдиний центр управління всіма політиками доступу та контролю над автентифікаціями.

Від культового брелока до сучасної платформи

Ще з 2000-х років багато IT-фахівців пам'ятають культові брелоки RSA з шістьма цифрами, що змінюються щохвилини. Ці брелоки виступали фактором «щось, що ви маєте» при автентифікації **(рис. 1)**. З роками платформа суттєво розширилася: з'явились мобільні токени, інтеграція з біометрією, push-автентифікація, FIDO-ключі, а також адаптивна автентифікація на основі ризику. Цей функціонал реалізується через **RSA Cloud Authentication Service** – хмарну платформу автентифікації з адаптивною логікою.

Можливості RSA SecurID включають:

- сертифіковану інтеграцію з понад 500 технологічними партнерами;
- підтримку відкритих стандартів: SAML, RADIUS, OAuth тощо;
- гнучку інтеграцію в складні середовища (через REST API, агенти, SDK);
- модуль RSA My Page – портал для верифікації особи та безпечного самообслуговування співробітників.

Крім того, процес переходу між різними методами автентифікації – з апаратних токенів на мобільні, з SMS на push-повідомлення тощо – є поетапним і не потребує складної перебудови системи. Міграція виконується просто та без порушення бізнес-процесів.

Надійність RSA підтверджується довірою 94% компаній зі списку Fortune 500 – загалом рішення SecurID захищає понад 50 мільйонів користувачів у всьому світі.

Міф про вкрадений токен: чому цього недостатньо для доступу

Поширене хибне уявлення: якщо зловмисник заволодіє токеном, він автоматично отримає

Рис. 1. Апаратний токен RSA SecurID SID700

доступ до системи. Насправді – ні. Код, який генерує токен RSA SecurID, називається tokencode і сам по собі не є паролем.

Tokencode створюється за допомогою алгоритму, який використовує унікальний для кожного пристрою 128-бітний seed і поточний час. Код оновлюється щохвилини і є дійсним лише протягом обмеженого періоду. Користувач автентифікується у два етапи: спочатку вводить свій логін і основний пароль, після чого система запитує одноразовий пароль (passcode), який складається з двох частин – відомого лише користувачеві PIN-коду та змінного коду токена (tokencode).

Навіть якщо зловмисник фізично викрав токен і має облікові дані для входу, без PIN-коду, який знає лише власник, вхід неможливий. Цей принцип забезпечує подвійний рівень захисту: *«щось, що ви маєте» (токен) + «щось, що ви знаєте» (PIN).*

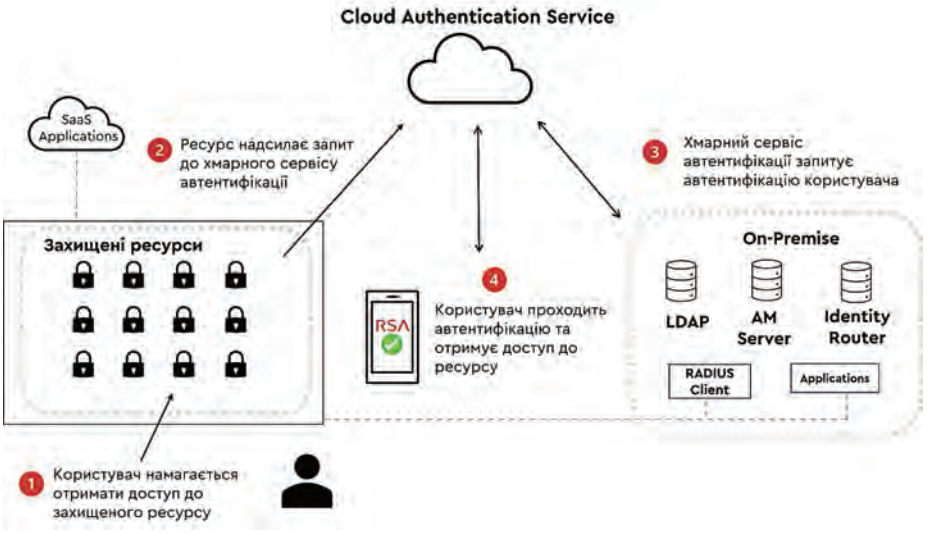

Рис. 2. Варіант архітектури автентифікації за допомогою RSA SecurID

Без хмари? Реалізуємо! Тільки хмара? Без проблем

RSA SecurID підтримує гнучкі варіанти розгортання, що дозволяє адаптувати рішення до конкретних потреб компанії.

- **On-Premises (локальне розгортання)** – класичне розгортання у власному датацентрі. Підходить для організацій, які прагнуть повного контролю над усіма компонентами системи автентифікації.
- **Cloud (хмарне розгортання)** – ідеальне для компаній, які вже працюють у хмарі або рухаються в цьому напрямку. Серед основних переваг – автоматичне оновлення та спрощене адміністрування.
- **Hybrid (гібридна модель)** – поєднує можливості хмари з наявною локальною інфраструктурою. У такому сценарії автентифікація відбувається через хмарний сервіс RSA, водночас захищені ресурси можуть залишатися в локальному середовищі (**рис. 2**). Для зв'язку між локальними системами та хмарною платформою використовуються спеціальні агенти (Identity Routers).

Безпека в дії: 6 бізнес-сценаріїв використання RSA SecurID

1. Захист привілейованих облікових записів. Використання RSA SecurID для входу адміністраторів дозволяє реалізувати окремі посилені політики безпеки та виключити ризик доступу лише по паролю.

2. Безпечний доступ до VPN і корпоративних ресурсів. Захистіть доступ до віртуальної приватної мережі, вимагаючи від користувачів автентифікацію за допомогою токенів RSA SecurID. Це гарантує, що лише авторизовані особи можуть підключатися віддалено.

3. Автономна автентифікація на Windows. RSA SecurID підтримує офлайн-доступ до робочої станції через локальні агенти, що синхронізуються з токенами. Це забезпечує автентифікацію навіть за відсутності мережевого з'єднання.

4. Захист хмарних сервісів. Розширте багатофакторну автентифікацію на хмарні програми та сервіси, такі як Microsoft 365, AWS та Google Workspace, забезпечивши захищений доступ до критичних сервісів.

5. Безпечні транзакції в фінансових системах. Доступ до внутрішньої CRM або електронного банкінгу можна зробити безпечним за допомогою одноразових кодів, які не зберігаються та не можуть бути використані повторно.

6. Відповідність вимогам аудиту та стандартів (GDPR, PCI DSS, ISO 27001).

Алгоритм підозри: що відбувається, коли ваші дії змінюються

Однією з ключових інновацій RSA SecurID останніх років є технологія автентифікації на основі ризику (**Risk-Based Authentication, RBA**). Уявіть собі систему, яка знає, що ви зазвичай працюєте з 9-ї до 18-ї, використовуєте конкретний пристрій, підключаєтесь з певної IP-адреси. Якщо запит на доступ відповідає звичному шаблону – автентифікація відбувається без додаткових дій з боку користувача. Але якщо система фіксує відхилення – наприклад, спробу входу вночі, з незнайомого пристрою або незвичної локації, – вона автоматично вимагає додаткової перевірки (наприклад, повторної MFA або блокування запиту).

Масштабування RSA SecurID до повноцінної IAM-системи

Платформа RSA Identity Governance & Lifecycle (IGL) розширює функціональність RSA SecurID, надаючи засоби для управління життєвим циклом облікових записів і правами доступу. Крім того, IGL забезпечує централізоване керування ролями користувачів і контроль доступу для цілей аудиту та відповідності нормативним вимогам.

Таким чином, впровадження багатофакторної автентифікації через RSA SecurID – це лише перший крок. Надалі організація може поступово масштабувати рішення до повноцінної IAM-системи, активуючи можливості RSA IGL без зміни базової архітектури. Комплексний підхід до IAM на базі рішень RSA забезпечує не лише надійну автентифікацію, але й централізований повноцінний контроль над обліковими записами, доступами та дотриманням вимог безпеки.