


Мультифакторная аутентификация в ЕВРАЗ: критерии выбора

 Нуйкин Андрей

 05.2023



ЕВРАЗ является вертикально-интегрированной металлургической и горнодобывающей компанией с активами в России, США, Канаде и Казахстане. Компания входит в число крупнейших производителей стали в мире. Собственная база железной руды и коксующегося угля практически полностью обеспечивает внутренние потребности ЕВРАЗа.

Позволяет подтвердить подлинность пользователя

Используется с древних времен

- Замок и ключ
- Сургучная печать на письме
- Сказка Али-Баба и 40 разбойников
- ПИН код

Факторы аутентификации:

- Нечто, что нам известно, например, какая-либо секретная информация.
- Нечто, чем мы обладаем, например, какой-либо уникальный физический объект.
- Нечто, что является неотъемлемой частью нас самих — биометрия.

Многофакторная аутентификация – использование двух и более факторов

Обычно используется один фактор - пароль

На примере с Али-Бабой видим уязвимость такого подхода

Вывод:

Нужно использовать многофакторную аутентификацию.

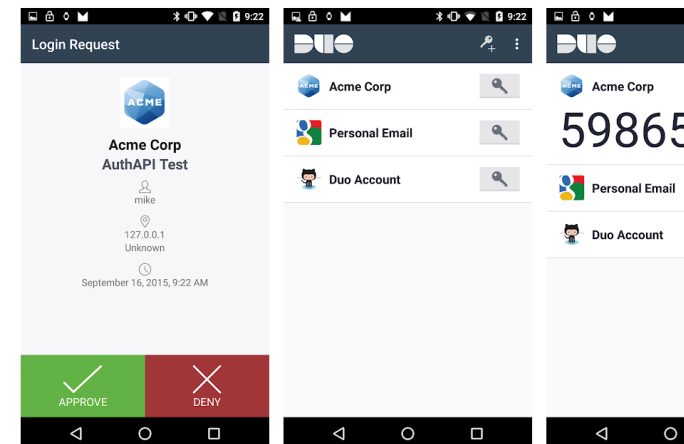
В зависимости от критичности защищаемого ресурса могут быть разные варианты по количеству факторов.

В большинстве случаев достаточно 2-х факторов.

Первый фактор обычно – пароль.

Второй фактор:

- OneTime Password (OTP)
- PUSH уведомления на смартфон
- SMS
- Токен\карта
- Биометрия



Требования:

- Надежность
- Удобство использование
- Простота подключения
- Интеграция в существующую инфраструктуру
- Наличие интеграции с альтернативными провайдерами (ГосУслуги, Я.Ключ, VK.ID, СберID и т.д.)

Ограничения:

- Не у всех есть смартфон
- Не все готовы ставить программное обеспечение
- Стоимость спец.устройств

1. Основной режим PUSH-уведомления

Ставим программное обеспечение на смартфон. Обычно имеет функцию OTP и PUSH

2. Запасной режим SMS

Для пользователей без смартфона или не желающих ставить программное обеспечение

3. Для привилегированных пользователей спец.устройство генерации OTP

4. Для пользователей не имеющих доменной учетной записи, интеграция с внешними провайдерами

- Multifactor (<https://multifactor.ru/>)
Быстрое внедрение. Пока не очень много интеграций. Хорошо развивается.
- Аванпост FAM (<https://www.avanpost.ru/products/avanpost-fam/>)
Чуть сложнее внедрение. Объявлено наличие интеграций с внешними провайдерами (ГосУслуги, Я.Ключ, СберID и т.д.)
- Индид (<https://indeed-company.ru/indeed-access-manager>)
Наличие в штатной поставки большого количества вариантов 2 фактора.

Спасибо за внимание



+7(495) 363-19-60



Andrey.nuykin@evraz.com



www.evraz.com



Андрей Нуйкин
CISA, CISM, CRISK
APСИБ
RuSCADASec Coin #29