RSA

OWN YOUR IDENTITY.

Odporúčania pri nasadení MFA

Marek Ledecký
Sr. Territory Sales Manager, CEE, SEE, CIS

RSA

OWN YOUR IDENTITY.

Využívanie 2FA/ MFA sa zvyšuje

Organizations using MFA*
(up from 28% in 2017)

An Increasing Attack Surface

Hybrid Work

Digital Experiences

IT Modernization

Increasing Sophisticated and Automated Cyberattacks

Unifikovaný holistický prístup k manažovaniu bezpečnosti identít

KTO
je užívateľ?

Authentication

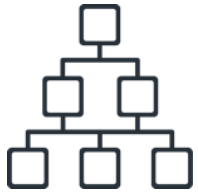
- Multi-factor
- Passwordless
- Behavioral

K ČOMU
Má prístup a ako ho môže využiť ?

Access

Least privilege
Single Sign-on
Privileged users
Shared accounts

KDE
sú identity uložené a ako sú manažované?



Directory

ID Proofing
Password reset
Credential recovery

KEDY
by mal byť prístup pridaný, zmenený alebo odstránený?

Lifecycle

Birthright entitlements
Role management
J-M-L automation

PREČO
má prístup práve k daným aplikaciam a má mať k ním prístup

Governance

- Reviews
- Relevancy
- Policy
- Orphaned accounts

OWN YOUR IDENTITY.

Klasické statické heslá sú obrovský hazard

80% Útokov je spôsobených ukradnutými alebo zneužitými heslami*

** Verizon Data Breach Investigations Report 2020*

RSA

Nasadená 2FA - MFA je stále lepšia ako len klasické statické heslo

Príklady útokov na získanie hesiel

Social Engineering	Eavesdropping	Exploiting the Odds
• Phishing • Spear phishing • Credential stuffing	• Man-in-the-middle • Keyloggers • Shoulder surfing	• Brute force • Password spray • Rainbow tables

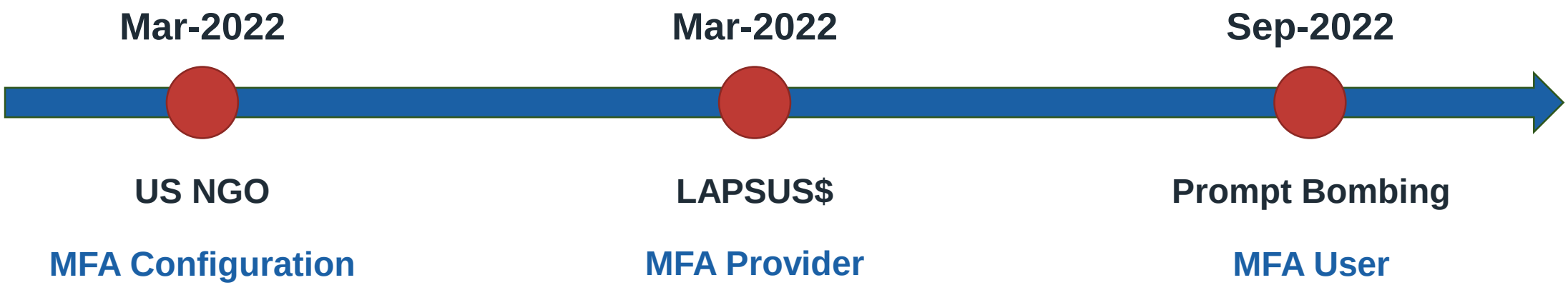
82% of attacks involve the human element*

OWN YOUR IDENTITY.

2022: Rok útokov na MFA

RSA

‘Top 3’ MFA útoky 2022



Prompt Bombing

September 2022

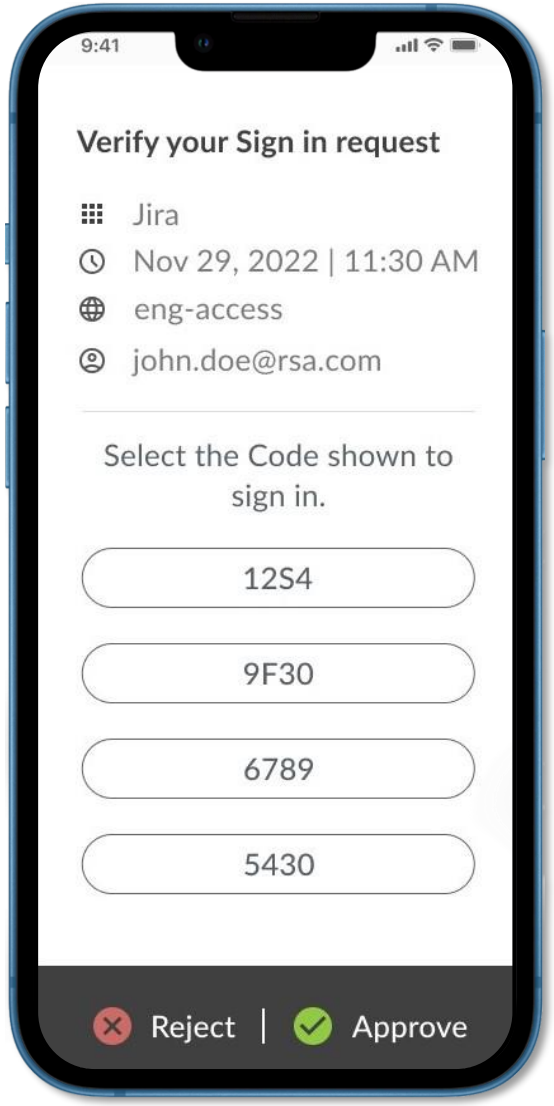
Prompt Bombing

Štruktúra útoku

1. Útočník sa zmocnil hesla do AD
2. Užívateľ bol zahltený požiadavkami na MFA (MFA fatigue / prompt bombing)
3. Útočník sa vydával za Uber IT admina, presdvedčil zamestnanca aby MFA potvrdil
4. Potvrdené MFA, použité na login do VPN and získal plný prístup do siete
5. Útočník ziskal prístup do Microsoft Powershell scriptu, ktorý obsahoval admin heslá do PAM
6. Získal prístup ku číslam vodičským preukazov, emailové adresy, rodné čisla, databázu customer support a informácie o interných novo zistených zraniteľnostach v systéme Uber

Odporúčania

1. Vzdelávanie užívateľov
2. Aplikácia Zero Trust princípov
   - IGA: Limitovanie prístupov k aplikáciam
   - Access: risk-based vs. network-based
3. Vylepšená “Push-to-Approve”
   - Code matching
   - Lockout po niekoľkých odmietnutých autent. požiadavkách
4. Využívanie FIDO štandardov



2.

MFA je stále vaša najlepšia prvá obranná línia

- Nasaďte MFA všade
- Neobetujte bezpečnosť kvôli pohodliu
- Využitie tzv. autentifikačných metód založených na riziku na dosiahnutie aj bezpečnosti aj užívateľského komfortu.
- Využite moderné možnosti autentifikácie, ako sú mobilné push a FIDO, ale pochopte ich limity
- Dajte si pozor na defaultné predvolené nastavenia – out of the box
- Majte back up plán v prípade “odstrihnutia od internetu” - tzv. offline autentifikácia

OWN YOUR IDENTITY.

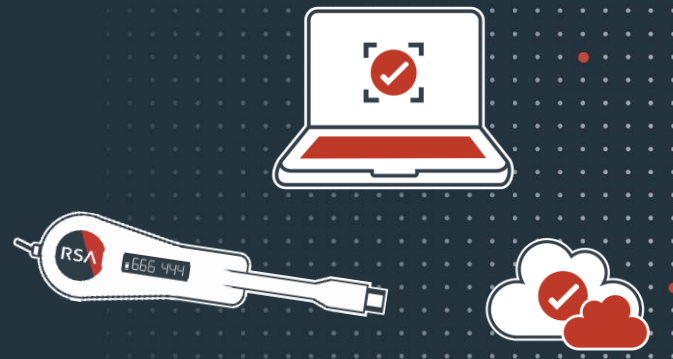
Complete Unified Identity Platform

RSA

On-premise

Cloud

Hybrid



Authentication

- Modern MFA
- Unified Authenticators
- Integrations

Access

- Hybrid H/A
- RBA
- Single Sign-On
- Self-service Portal

Identity Governance & Administration

- Governance & Lifecycle
- Cloud managed hosted, on-prem

RSA

OWN YOUR IDENTITY.

Ďakujem

Vizitka

Marek Ledecký

Sr. Teritorry Sales Manager, CEE, SEE, CIS

Marek.Ledecky@rsa.com

RSA