



Souverän, sicher, resilient: Identity Security für den öffentlichen Sektor

Ingo Schubert

Field CTO International

RSA Security



Viele neue Anforderungen an IAM

- Absicherung moderner und historischer Infrastruktur
- Moderne Authentifizierungsmethoden
 - FIDO Passkeys
 - QR Code
 - ...
- Sichere und bequeme Registrierung
- Teil von Zero Trust Umgebungen
- Passwordlose Anmeldung
- Absicherung Help Desk
- ...

IAM aus der Cloud ist großartig!

- Cloud IAM hat Vorteile für die Kunden
 - Eine IAM Infrastruktur sicher zu betreiben ist nicht einfach.
 - SaaS Anbieter können das in vielen Fällen einfach besser.
 - Die üblichen Vorteilen z.B. einfache Updates, niedrigere Betriebskosten
 - Neue Features tauchen magisch auf
 - ...
- Identity & Access Management und speziell MFA werden immer mehr in die Cloud verlagert.
 - Viele Funktionen sind nur noch dort verfügbar
 - ggf. keine Option wegen Datenhoheit
 - die Sache mit der Resilienz...

NIS2 (... und DORA) verlangen Antworten



Organisationen müssen ihr Risk Management ausbauen

- “Was passiert falls XYZ ausfällt?”
- “Wie lange geht das gut?”
- “Wie kann das behoben werden?”



IAM muss dafür bereit sein

- Teil der Kern-Infrastruktur
- Falls “IAM” ausfällt... fällt alles aus!

Es geht nicht nur um Verfügbarkeit

- Ein Cloud-IAM Ausfall kann zu Sicherheitsproblemen führen
- Angreifer können daraus einen Vorteil ziehen
 - Das Chaos während eines Disasters ist perfekt!
- Angreifer haben ggf. das Disaster (z.B. MFA Outage) selbst verursacht.



MFA ist weg! Was jetzt?

- Ein Cloud-MFA Ausfall kann mehrere Gründe haben
 - “Echter” Ausfall der MFA Lösung beim Anbieter
 - Ausfall des zugrundeliegenden Cloud Providers
 - Verbindung zur Cloud ist gestört
 - Vertrauensverlust durch kompromittierten MFA Anbieter
 - ...
- Möglicherweise sind alle (On-premise oder Cloud) Applikationen nicht mehr verfügbar.
 - Email
 - VPN
 - ...

Die Cloud ist perfekt... bis sie es nicht mehr ist.

- Der Plan für ein IAM Ausfall sollte nicht sein:
 - “Wir können eh nichts dagegen machen, ist halt die Cloud.”
 - “Wird schon wieder!”
- Resilientes IAM ist essenziell um
 - Dienste verfügbar zu halten
 - sicher zu genesen.
- Ein komplett separates MFA System “für Resilienz” zu betreiben ist
 - nicht kosteneffizient,
 - oft nicht möglich und
 - unsicher.

RSA ID Plus Deploy Anywhere Optionen

ID Plus SaaS

- Seit Jahren verfügbar: Run by RSA
 - Inkl. Hybrid HA
- PII bleibt in der EU

ID Plus Sovereign

- Kunden betreiben ID Plus on-premise
- Identischer Funktionsumfang
 - Benötigt Internetverbindung

ID Plus Sovereign *Air-gapped*

- Kunden betreiben ID Plus on-premise air-gapped
 - Keinerlei Internetverbindung
- Funktionseinschränkungen

Wer "A" sagt muss auch "B(etrieb)" sagen

- Infrastruktur
 - Hardware: CPU, RAM, Disk
 - DNS, Firewalls
 - ...
- Betrieb
 - Updates
 - Technische und betriebliche Sicherheit
 - ...



Modernes IAM und Resilienz

- Dringend notwendige Modernisierung sind möglich...
 - Konsistente Absicherung neuer und vorhandener Infrastruktur
 - Passwortlose Anmeldung
 - Moderne Authentifizierungsmethoden
 - Sichere Registrierung
 - Etc.
- ... ohne bei der Resilienz Abstriche machen zu müssen!



- **Keine Angst vor der Frage
“Was passiert, falls die
IAM/MFA Cloud ausfällt?”**
- **Auf dieses Szenario
vorbereiten!**
- **RSA hat die Technologie
und Wissen um Sie zu
unterstützen.**

