Zwei-Faktor-Authentisierung in der betrieblichen Praxis

Übersicht

- Zwei-Faktor ? Multi-Faktor ?
  - Ein paar Beispiele
- Anforderungen einer ‘kleinen Organisation’ …
- Optionen & Entscheidungen
  - Auslagern, ganz oder in teilen
  - Standards – SSO
- Dies ist ein Bericht über den Weg soweit, das Ziel ist noch nicht erreicht

Einführung 2FA

- Passwörter alleine sind seit langem als Schwachstelle bekannt
- Weitere “Faktoren” werden genutzt um Zugang zu kontrollieren

⇒Multi-Faktor-Authentisierung (MFA), oder auch

⇒Zwei-Faktor-Authentisierung (2FA)

Kategorien an Faktoren:

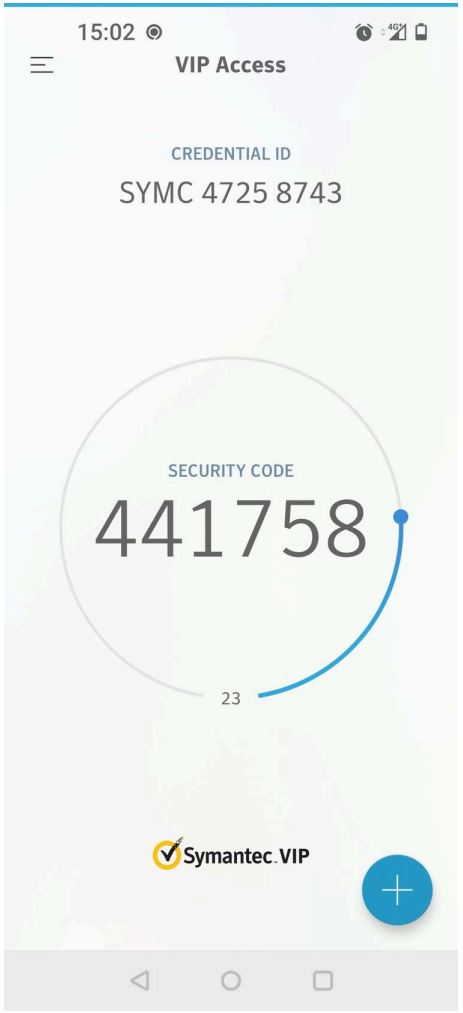
- Besitz: Schlüssel, Token, Karte etc.
- Wissen: Passwort, PIN, Sicherheitsfragen
- Biometrie: Fingerabdruck, Gesichtserkennung etc.
- Kontext: Zugang nur von bestimmten Orten oder Netzen

Einführung 2FA

- Einmal-Passwörter (OTP) sind am geläufigsten, TANs gehören dazu
  - Vorteil: Oft leicht zu integrieren (kann an ein PW angehängt werden) und viele Wege die OTPs zu generieren: Token, SMS, Mobil-App, Papier …
  - Nachteil: Der Nutzer muss es manuell eingeben …

- Aber heute ist ein Mobiltelefon fast immer im Bild
  - Es ist praktisch bereits ein MFA System: Besitz wird mit PIN oder Biometrie verknüpft und oft Identitäts-checks (Mobilnummer erfordert Ausweis)
  - Es ist ‘immer dabei’.
  - Erlaubt ‘out-of-band’ Authentisierung bei der die Kommunikation ausserhalb von client und server geschieht.

Einführung 2FA



Anforderungen

- Als “Kunde eines Anbieters” wird oft nur eine Anwendung genutzt
  - Online-Banking, Shopping, Bahn-Portal usw.
- Dies vereinfacht die Integration auf Anbieterseite
  - Nur eine Anwendung muss angepasst werden, z.B.
    “Danke für das korrekte Login, ich sehe dieses Gerät/Browser ist neu, daher warte ich noch auf einen Klick in der email”
  - Als zweiten Faktor gibt es mehr einfache Optionen, z.B.
    Email-validierung und Sicherheitsfragen
- Für eine Organisation die Ihre Mitglieder authentisiert ist es anders
  - Es gibt dutzende an Diensten und Anwendungen
    (email, wiki, chat, crm, file-sharing, git und noch viel mehr)
  - Der klassische Weg das zu vereinheitlichen ist ‘login via LDAP/AD’

Anforderungen Betrieb

- Die vielen Anwendungen
  - Implizieren dass oft Authentisiert wird im laufe eine Tages
  - Integration wird knifflig – wer bringt der ‘XY-App’ die email-frage bei ?
  - Nicht bei allen Anwendungen sitzt der Nutzer davor, z.B.
    email (IMAP), chat usw die kontinuierlich in eigenen Anwendungen laufen
- Nicht immer ist die Nutzergruppe rein intern
  - Besonders hart: Gemischte Anwendungen sowohl für Mitarbeiter als auch Kunden, Partner und anderen ‘externe’.

Das (meiner Meinung nach) wichtigste Thema: Frust Vermeiden !

Wenn ‘die vorgesehene Technik’ zu umständlich ist, weichen Nutzer aus.
Dabei wird Sicherheit nicht selten schwerer ‘beschädigt’ als eine unvollständige Integration. (Beispiele, aber nichts schriftliches hier …)

Optionen

- ALLES wird ausgelagert – Anwendungen und Authentisierung
  - Man landet bei Microsoft oder Google in der Cloud
  - Diese bieten auch MFA Dienste
  - Integration ist ein “Problem anderer Leute”
- Authentisierung wird ausgelagert
  - Neben den ‘Cloud Giganten’ gibt es dedizierte Anbieter von Authentisierungsdiensten mit offenen Schnittstellen (dazu später mehr)
- Eigene MFA Platform, ebenfalls mit offenen Schnittstellen
  - Software dafür ist zunehmend einfacher / billiger verfügbar
- Anwendungsintegration vermeiden durch Netz-zugang mit 2FA/MFA
  - Mit anderen Worten: Ein VPN das 2FA praktiziert, dahinter reicht ein klassisches Passwort.
- Diese Optionen sind nicht exklusiv - Mischformen sind möglich

Offene Schnittstellen

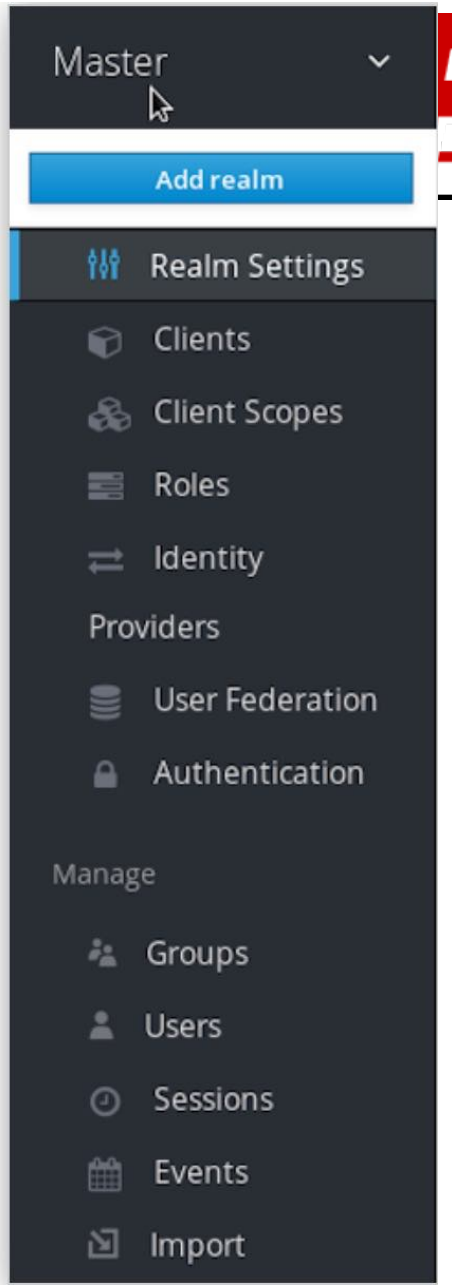
- Klassische Methoden: LDAP, RADIUS, Kerberos
- Neuere Protokolle/Methoden:
  - OpenID (obsolete), OpenID Connect (OIDC) (nutzt Oauth)
  - CAS v1/v2/v3
  - Oauth (in verschiedenen Versionen)
  - Fido2, SAML und noch mehr
- Oft gibt es nicht die gleichen Funktionen und es werden verschiedene Ebenen vermischt.
- Am Ende zählt ob (fast) alle Anwendungen integriert werden können

Aggregatoren / Broker

- Eine ‘Quelle’ von Nutzern reicht oft nicht: Mitarbeiter vs Kunden
- Eine Schnittstelle (OIDC vs …) reicht oft auch nicht
- Daher gibt es ’Broker’ die beides verbinden
  - Verschiedene Nutzer-repositories können integriert werden
  - Verstehen nicht nur verschiedene Protokolle sondern auch Anwendungen
  - Ort um Authorisierung zu konfigurieren
    Welche Nutzer dürfen was in welcher Anwendung
  - Logging & Audit: Wer hat sich wann/wo angemeldet ?
    gibt es wiederholte Fehlversuche ?

Broker II

- Aus der Vergangenheit: Crowd (Atlassian)
- Neu: KeyCloak (RedHat)
- Oder als externer Dienst …



2FA Gedanken

- Als neuen ”Faktor” zähle ich etwas das nicht gleichzeitig mit vorhandenen Faktoren kompromitiert wird.
  - Beispiel: Der verlorene Laptop
    Solange er verschlüsselt und mit Zugangsschutz (Passwort, Fingerabruck) versehen ist, reicht der ‘Besitz’ alleine nicht.
  - Auf einem solchen Gerät sehe ich einen ssh private key oder ein client-key+cert für ein VPN als “2FA” – man braucht Gerät UND Login.
- Zu erzwingen dass Geräte (Laptop, Handy) ausreichend gesichert sind ist ein weiteres, nicht-triviales Problem
- Gleicher Login (z.B. LDAP) ist nicht ‘Single-Sign-On’ (SSO)
  Einmal authentisieren, dann in mehreren Anwendungen nutzen.

2FA Gedanken II

- Mit einem VPN kann man nicht wirklich alles erledigen
  - Zugriff von fremden Geräten, ohne VPN client, ist (fast) nicht möglich
  - Kunden/Partner wollen kein extra VPN

- Immer weiter verbreitet und mein persönlicher Favorit:
  - Out-of-band validierung mit Mobile-App
  - Allerdings braucht es einen Plan B für die gelegentlichen Fälle ohne Netzzugang des Mobiltelefons.

Fazit

- Die Suche ist bei uns noch nicht am Ende
  - An verschiedenen Ecken kommt 2FA zum Einsatz, aber noch zu viele wichtige Dienste brauchen ‘nur ein Passwort’.
- Ich habe Vertrauensprobleme bei den grossen Anbietern
  - Der Anbieter hat die ’Schlüssel’ zu ALLEM
  - Deren Sicherheitsprozesse mögen gut sein, aber Anbieter sind auch ein fantastisch attraktives Ziel für Angriffe
- In meinem Fall
  - Tiefere Tests mit Keycloak
  - Insbesondere welche Integrationen leicht sind – oder auch nicht

Vielen Dank!

Gibt es noch Fragen ?