TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

München, 15./16.06.2016

Das Passwort im Kontext von Multifaktor-Authentifizierung

Claudia Frohnhoff, Detack GmbH

Octav Opaschi, Detack GmbH

Detack GmbH

- Gründung 2001
- Spezialist für Premium IT-Security Audits
  - IT Security Audits
  - Penetration Tests
  - IT Security Consulting
  - Software Development
- Kundenschwerpunkt Banken & Versicherungen
- Security Software-Entwicklung
- Seriosität, Verlässlichkeit & Innovation

Please Change Your Password…

- „Policy compliant“ Passwörter trotz strenger Policy nachweislich schwach (>60%)
- Mehrfachverwendung von Passwörtern
- „Leere“ oder „Default“ Passwörter
- Bestimmte Accounts „Policy Exempt“

→ **Passwörter sind (wieder) ein beliebtes Angriffsziel für Hacker**

→ Empfehlung von BSI & Anderen: Multi-Faktor Authentifizierung

→ **ABER…**

USER 1 – Der Benutzer

„Heartbeat“ User-Accounts
→ Mehrzahl der User
→ Geringe bis mittlere Berechtigungen
→ Schutzbedarf „normal“ / medium

Ausnahme: Systemadministratoren
→ Hohe Berechtigungen
→ Schutzbedarf hoch

USER 2 – Der technische Account

Bildquelle: Fotolia

„Heartbeat“ User-Accounts
→ Mehrzahl der User
→ Geringe bis mittlere Berechtigungen
→ Schutzbedarf „normal“ / medium

Ausnahme: Systemadministratoren
→ Hohe Berechtigungen
→ Schutzbedarf hoch

Technical / System Accounts

→ Anzahl der Accounts geringer
→ Hohe Berechtigungen
→ Schutzbedarf hoch

Herausforderungen

- Vergessen werden die technischen Accounts
- Biometrische Merkmale kann man nicht zurücksetzen!

  (Please change your fingerprint..?)
- 2-Faktor heißt NICHT, dass wir einen Faktor unsicher gestalten dürfen
- Viele 2-Faktor Methoden in der Theorie sicher, aber in der Praxis nicht sicher implementiert

→ gefährlich: vorgetäuschte „Sicherheit“!

Sicherheitstechnische Unterschiede

Authentifizierungs-methode	Heartbeat User Accounts	Technical Accounts	Changeable	Irreversibly Encrypted
Passwörter	X	X	X	X
Tokens	X	nein	X	nein
Smart Cards	X	nein	X	(x)*
Biometrics	X	nein	nein	nein

*in Windows Systemen, die NTLM Hashes verwenden

EMPFEHLUNGEN – zur Diskussion

- Aufklären, Erklären, Awareness schaffen, Beraten (zu Authentifizierungsmethoden und deren „Fallstricke“)
- Das Multitalent „Passwort“ richtig einsetzen und mit Multifaktor, wo sinnvoll, stärken
- Bedarfsanalyse → gezielte (und passende) Maßnahmen
- Maßnahmen RICHTIG und SICHER implementieren

EMPFEHLUNGEN – zur Diskussion

- Integriert agieren (ISMS, IT Sec, Risk, BCM,..)
- Welchen Eigenschaften soll eine Authentifizierungsmethode haben? (z.B. Ableitung aus Risikoanalyse ISO 27001)
- Kosten / Nutzen („Kronjuwelen“/Massentauglichkeit)
- Pro / Kontra Abwägung bei z.B. Biometrie: wer trägt die Verantwortung?
- Warum werden vom Management keine sicheren Passwörter verlangt?