Hersteller, Hacker, Geheimdienste?
Die eigene Identität unter eigener Kontrolle!

Wie Sie Ihre Identität schützen und Ihre Zugänge und Daten besser absichern.

Linux Solution Day 2014
23.10.2014, Bad Iburg

Cornelius Kölbel
cornelius.koelbel@netknights.it

NetKnights
securing your identity

NetKnights GmbH

- gegründet Juni 2014 mit Sitz in Kassel
- Beratung, Integration und Support für
  - Identitäten und Authentisierung
  - Einmal-Passwörter, X509
  - Public Key Infrastruktur
  - Hardware-Sicherheits-Module
  - Verschlüsselung

Cornelius Kölbel
cornelius.koelbel@netknights.it

NetKnights
securing your identity

Identität

- Person oder Account
- Nachweis der Identität
  - Persönlich bekannt
  - Personalausweis oder Reisepass
  - Mitgliedsausweis
  - Hausschlüssel
  - Passwort (Wissen)
  - Fingerabdruck und sonstige Biometrie
  - Token (Token)

Cornelius Kölbel
cornelius.koelbel@netknights.it

Hersteller, Hacker, Geheimdienste

- Hersteller hat Seeds von OTP-Token
- Fingerabdruck gehackt
- Geheimdienste müssten sich über Biometrie freuen (Stimmerkennung, Tippverhalten, Gangerkennung)
  - Person ist „bis ans Lebensende“ identifizierbar
- Die Identität droht meiner Kontrolle zu entgleiten:
  - Sie kann kopiert werden (Seed)
  - oder für andere Dinge missbraucht werden (Biometrie)
- Identität am Computersystem sicher feststellen!

Cornelius Kölbel
cornelius.koelbel@netknights.it

Das Passwort

- Password strength https://xkcd.com/936
- „Ax%t0$7.“
  - ~67 verschiedene Zeichen, 8 Stellen => 67^8 Permutationen = $4{,}1*10^{14}$ ~ 48 Bit
  - Brute Force Raten bei 1000/s: $1{,}3*10^4$ Jahre
- Bitcoin sei Dank.
  - 800GH/s (sha256)

Cornelius Kölbel
cornelius.koelbel@netknights.it

Hash me

- Hash Angriff bei 800GH/s: 110h (4 Tage)
- 4 HE, $700
- Neues Passwort: „Auto Platzer Bratpfanne“
  - 26 verschiedene Zeichen, 23 Stellen => 26^{23} Permutationen = $3{,}6*10^{32}$ ~ 108 Bit
  - Brute Force Raten bei 1000/s: $1{,}1*10^{22}$ Jahre
  - Hash Angriff bei 800GH/s: $1{,}1*10^{16}$ Jahre
- Size matters!

Cornelius Kölbel
cornelius.koelbel@netknights.it

Ein Passwort bleibt ein Passwort

- Sniffing
- Keylogger
- Shouldersurfing
- Passwort-Datenbank
- Wiederverwendung

Cornelius Kölbel
cornelius.koelbel@netknights.it

Zwei-Faktor-Authentisierung

- 1. Faktor Wissen
  - Passwort
- 2. Faktor Besitz
  - Zertifikate
  - Smartcards/Token → PKI
  - Besitz eines anderen Gerätes
    - OTP
    - SMS
    - Email

Cornelius Kölbel
cornelius.koelbel@netknights.it

Qual der Wahl

- Entscheidungsgrundlagen
  - Hersteller wollen Hardware verkaufen (noch lieber Software)
  - Proprietäre Systeme und Algorithmen
  - Vendor-Lock
  - Lizenzkosten
  - Token-Hardware mit Seed-Problemen
- Net**Knights** kennt sich mit verschiedenen Systemen aus

Cornelius Kölbel
cornelius.koelbel@netknights.it

privacyIDEA

- Open Source
  - Transparenz auf Github
- System ohne Vendor-Lock
  - OTP, SMS, Email, Remote, RADIUS, SSH Keys, (Zertifikate),
- Offline-Funktionalität mit Maschinenverwaltung
- Null-Invasiv
  - Anbindung an LDAP, AD, SQL, SCIM, Flatfile

Cornelius Kölbel
cornelius.koelbel@netknights.it

NetKnights
securing your identity

Szenarien

- VPN, Remotezugang
- Webapplikationen (Shops, Portale)
- Server/Desktop (Linux und Windows)
- SSO in der Cloud
- SSO im Unternehmen
- Verwaltung von Maschinen/Notebooks (SSH, LUKS)
- Geeignet für Service Provider (Leichtgewicht)
- TAN-Verfahren und andere Signaturen

Cornelius Kölbel
cornelius.koelbel@netknights.it

Details in den Szenarien

- Zeitlich beschränkter Zugriff
  - Dienstleister, „Zeitarbeiter“, beschränkter Zugriff auf Resourcen
- Einfache Migratonsszenrien (RADIUS Token)
- Gewaltenteilung (Remote Token)
- Einfaches Rollout (auto assignment)

- Beratung und Support durch die NetKnights GmbH

Cornelius Kölbel
cornelius.koelbel@netknights.it

Ein kleiner Schritt...

- Überdenken Sie Ihre Authentisierung.

Cornelius Kölbel
cornelius.koelbel@netknights.it