Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Weil Sicherheit alles ändert.

Michael Scherzinger
IT Senior Security Engineer | PAM Product Manager
scherzinger@avantec.ch

Agenda

- Begrüssung
- Was ist PAM?
- Angriffe
  - Video: Pass-The-Cookie-Attacke
  - Im Browser gespeicherte Credentials abgreifen
  - Supply-Chain-Attacke
- Wie sieht das PAM Konzept aus?
- Demo
- NSA and CISA Top 10 Misconfiguration
- All-in-One-Lösung
- Fragen

Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Was ist PAM?

AVANTEC
Competence. Security. Trust.

PAM = Privileged Access Management

Quelle:
EA breach – Sophos News: https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass/
Okta Breacht – BeyondTrust Blog: https://www.beyondtrust.com/blog/entry/okta-support-unit-breach

Was ist PAM?

AVANTEC
Competence. Security. Trust.

Was wollen wir mit PAM schützen?

Administrative Sessions
SSH
Browser Cookies
RDP

780 GB

Admin Accounts
Administrative Privilegien

Secrets
Passwörter
SSH Keys
Zertifikaten

okta
Inhouse Administrator Session Cookie

Quelle:
EA breach – Sophos News: https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass/
Okta Breacht – BeyondTrust Blog: https://www.beyondtrust.com/blog/entry/okta-support-unit-breach

AVANTEC
Competence. Security. Trust.

Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Was ist PAM?

AVANTEC
Competence. Security. Trust.

Was wollen wir mit PAM schützen?

Administrative Sessions

SSH

Browser Cookies

RDP

Session Recording

Session Manager

Admin Accounts

Administrative Privilegien

Secrets

Passwörter

SSH Keys

Zertifikaten

Audit Logs

Integrierter Passwort Manager

Quelle:
EA breach – Sophos News: https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass/
Okta Breacht – BeyondTrust Blog: https://www.beyondtrust.com/blog/entry/okta-support-unit-breach

Wie kann eine Pass-The-Cookie-Angriff ablaufen?

AVANTEC
Competence. Security. Trust.

TREND MICRO™

Krypto-Wallets
Sessions

Quelle:
Trend Micro: https://www.inside-it.ch/infostealer-werden-zu-einer-immer-groesseren-bedrohung-20231116

AVANTEC
Competence. Security. Trust.

Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Wie kann eine Pass-The-Cookie-Angriff ablaufen?

AVANTEC
Competence. Security. Trust.

TREND MICRO™

Browser Daten

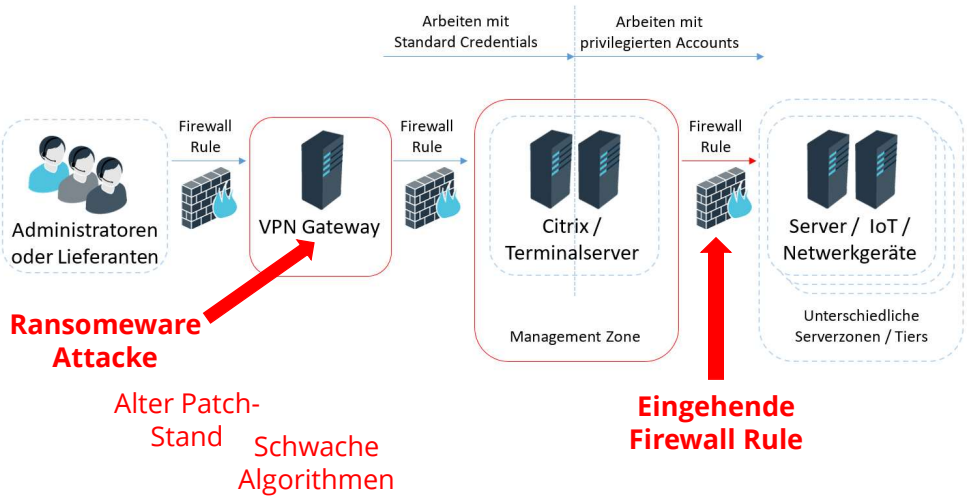
Browser Cookies

Login Daten

Quelle:
Trend Micro: https://www.inside-it.ch/infostealer-werden-zu-einer-immer-groesseren-bedrohung-20231116

Supply-Chain-Attacke

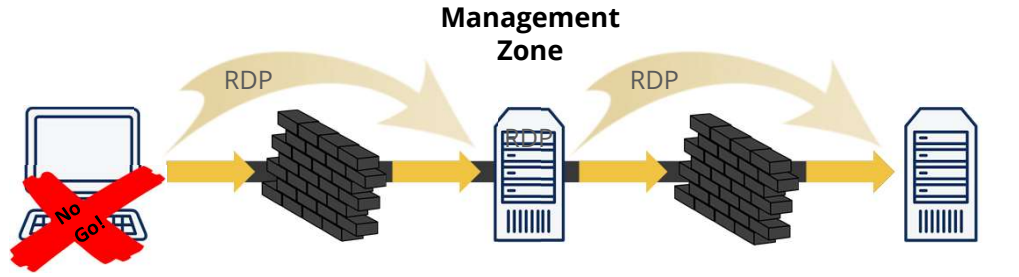
AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Jumphost / Citrix Lösung

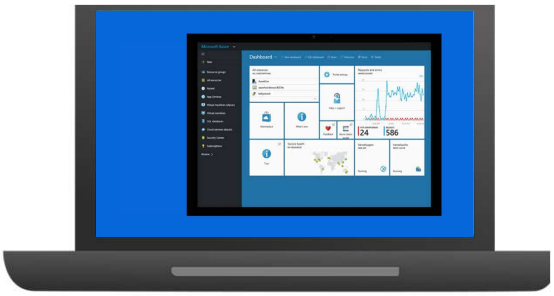


Daily Business Gerät
Email
Web

Jumphost / Citrix Lösung

SQL Server

Challenge – Credential Flow



Password

Credential Extraction

Pass-the-Cookie

AVANTEC
Competence. Security. Trust.

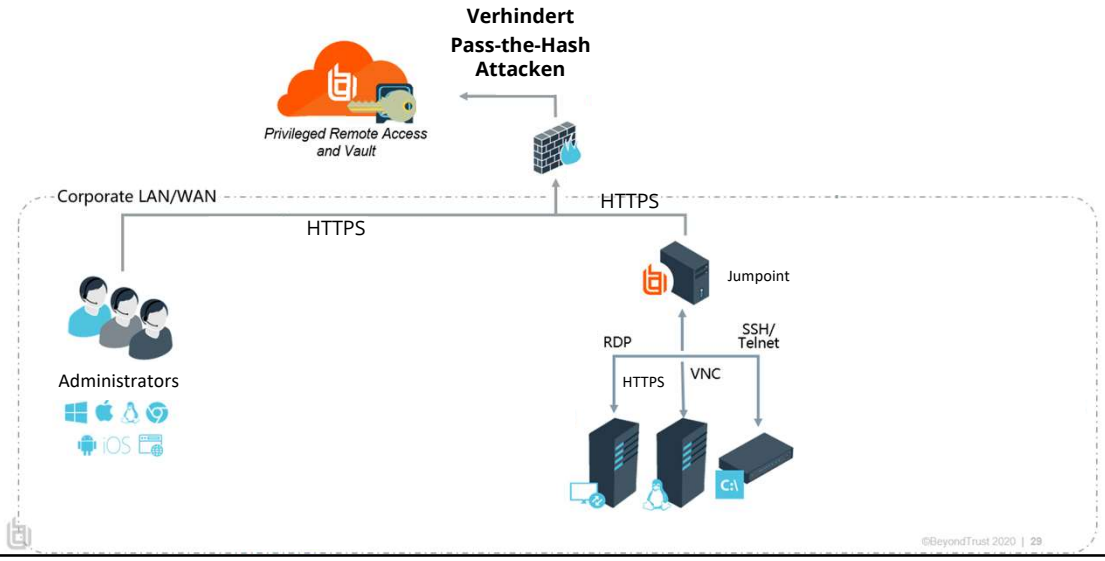
Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Challenge – Credential Flow

AVANTEC
Competence. Security. Trust.

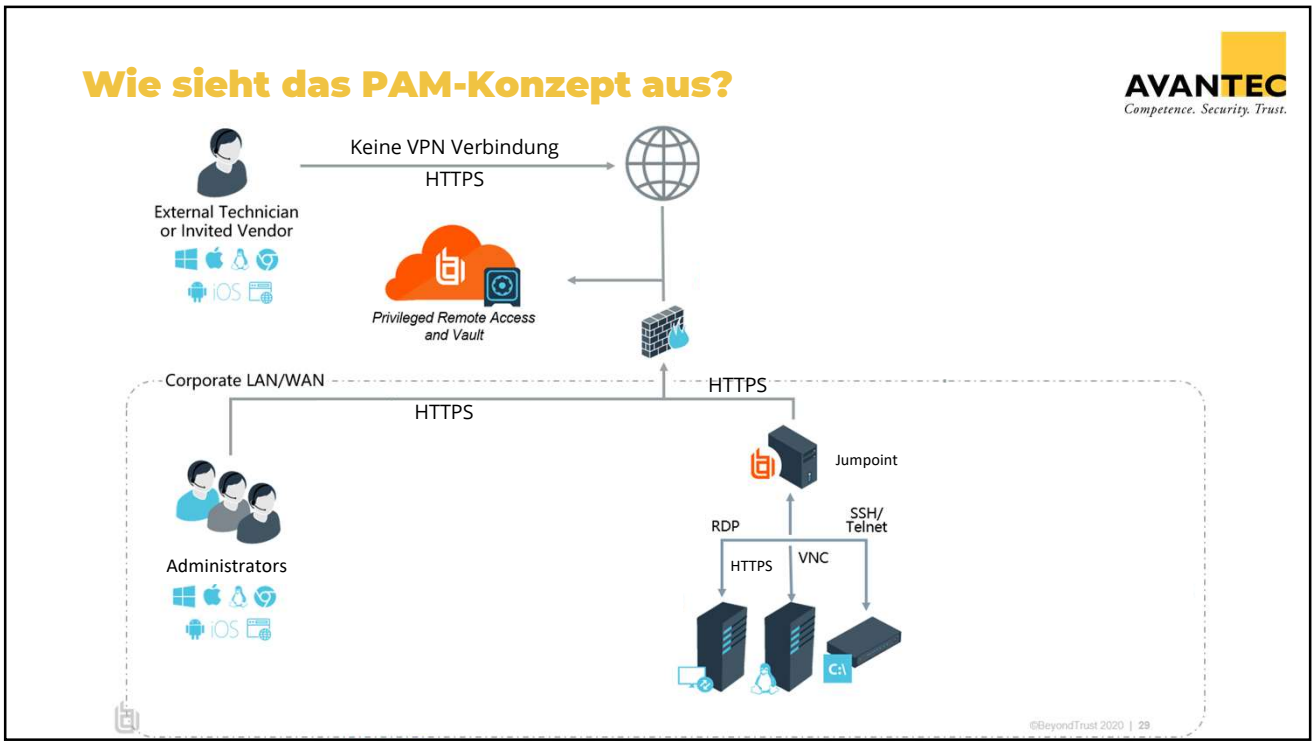
Wie sieht das PAM-Konzept aus?

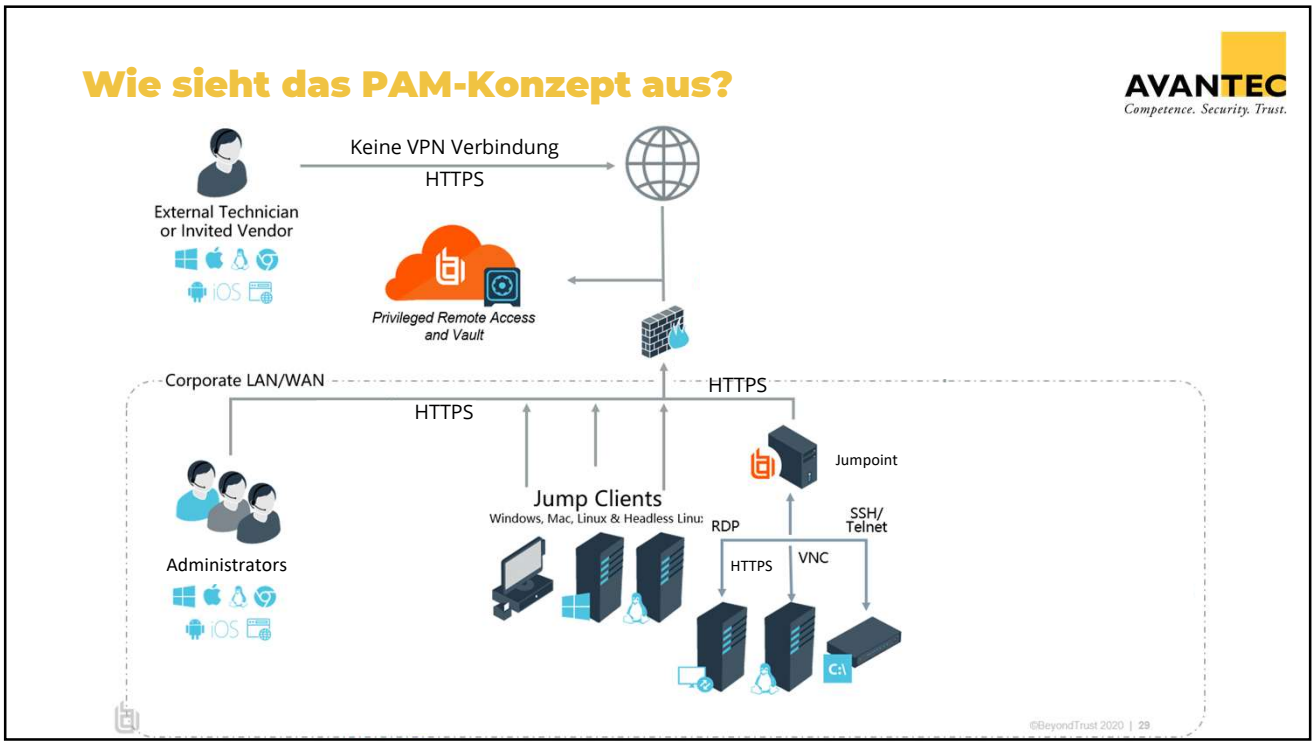
AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

Was ist Privileged Access Management?
29. November & 05. Dezember 2023





AVANTEC
Competence. Security. Trust.

Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Demo

AVANTEC
Competence. Security. Trust.

T

Quelle:
NSA: https://www.nsa.gov/
CISA: https://www.cisa.gov/

Quelle: https://pixabay.com/photos/tree-park-autumn-fall-foliage-99852/

AVANTEC
Competence. Security. Trust.

Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Top 10 Misconfiguration

AVANTEC
Competence. Security. Trust.

Legende:
Kann mit der PRA abgesichert werden

1. Einsatz von Standardkonfigurationen
2. Unzureichende Trennung von Benutzer- und Administratorenprivilegien ✓
3. Unzureichende interne Netzwerküberwachung
4. Fehlende Segmentierung von Netzwerken ✓
5. Mangelhaftes Patch-Management
6. Mögliche Umgehung von Systemzugangskontrollen ✓
7. Schwache oder falsch konfigurierte 2FA Methoden ✓
8. Unzureichende Zugriffskontrolllisten für Netzwerkfreigaben und Dienste
9. Mangelhafter Umgang mit Anmeldeinformationen (Bsp. Passwörtern) ✓
10. Uneingeschränkte Codeausführung

Quelle:
English Original: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a
Deutscher Blog: https://www.golem.de/news/nsa-und-cisa-10-fehler-die-cyberkriminellen-am-haeufigsten-die-tuer-oeffnen-2310-178298.html

All-in-One Solution.

AVANTEC
Competence. Security. Trust.

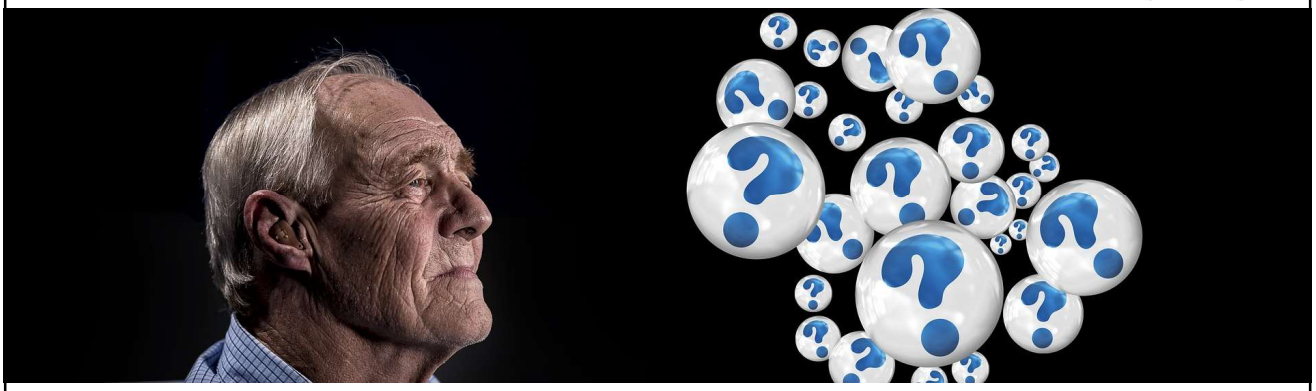
Lösung
- Privileged Access Workstation (PAW)
  - Kontentrennung
- VPN-Less Access
- Protocol Change
- Account Management
- Complete Session Management
- Credential Management

Ersetzt
- Citrix / Terminalserver / Jumphosts
- VPN Gateways
- Reverse Proxy
- IAM Lösung für Externe
- Session Recording Solution
- Passwort Speicher Lösung

AVANTEC
Competence. Security. Trust.

Was ist Privileged Access Management?
29. November & 05. Dezember 2023

Fragen



AVANTEC
Competence. Security. Trust.