oneconsult
together against cyberattacks

Cyberrisiken identifizieren: Einblicke aus der Praxis

Tim Mittermeier | Oldenburg, 23. Oktober 2024

Vorstellung Referent

Tim Mittermeier

Head of RT&PT, Oneconsult Deutschland AG

Studium Luft & Raumfahrttechnik mit Schwerpunkt Autonome Systeme, M.Sc. UniBwM

Forschungsinstitut Cyber Defence CODE, UniBwM

- Aufbau Cyber Range Labor
- Netzsicherheit & IT-Sicherheit
- Verschiedene Forschungsprojekte

Offensive Security Certified Professional (OSCP)

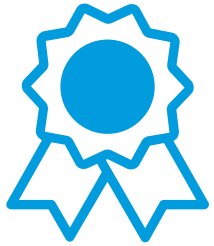
Oneconsult
Über uns

2.000+
Cybersecurity-Projekte

Oneconsult-Unternehmensgruppe:
Oneconsult International AG (Holding),
Oneconsult AG,
Oneconsult Deutschland AG,
Oneconsult New Zealand Limited

100+
Red-Teaming-Projekte

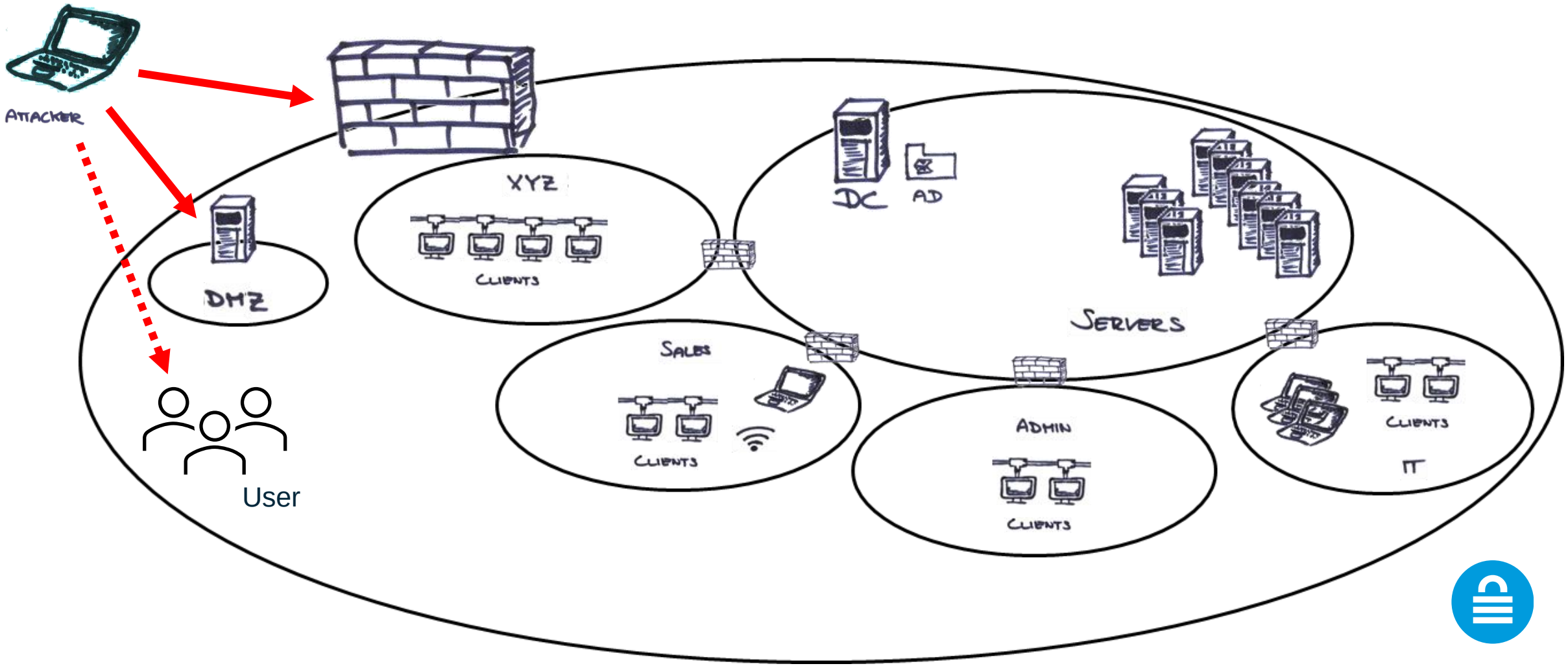
250+
Incident-Response-Einsätze



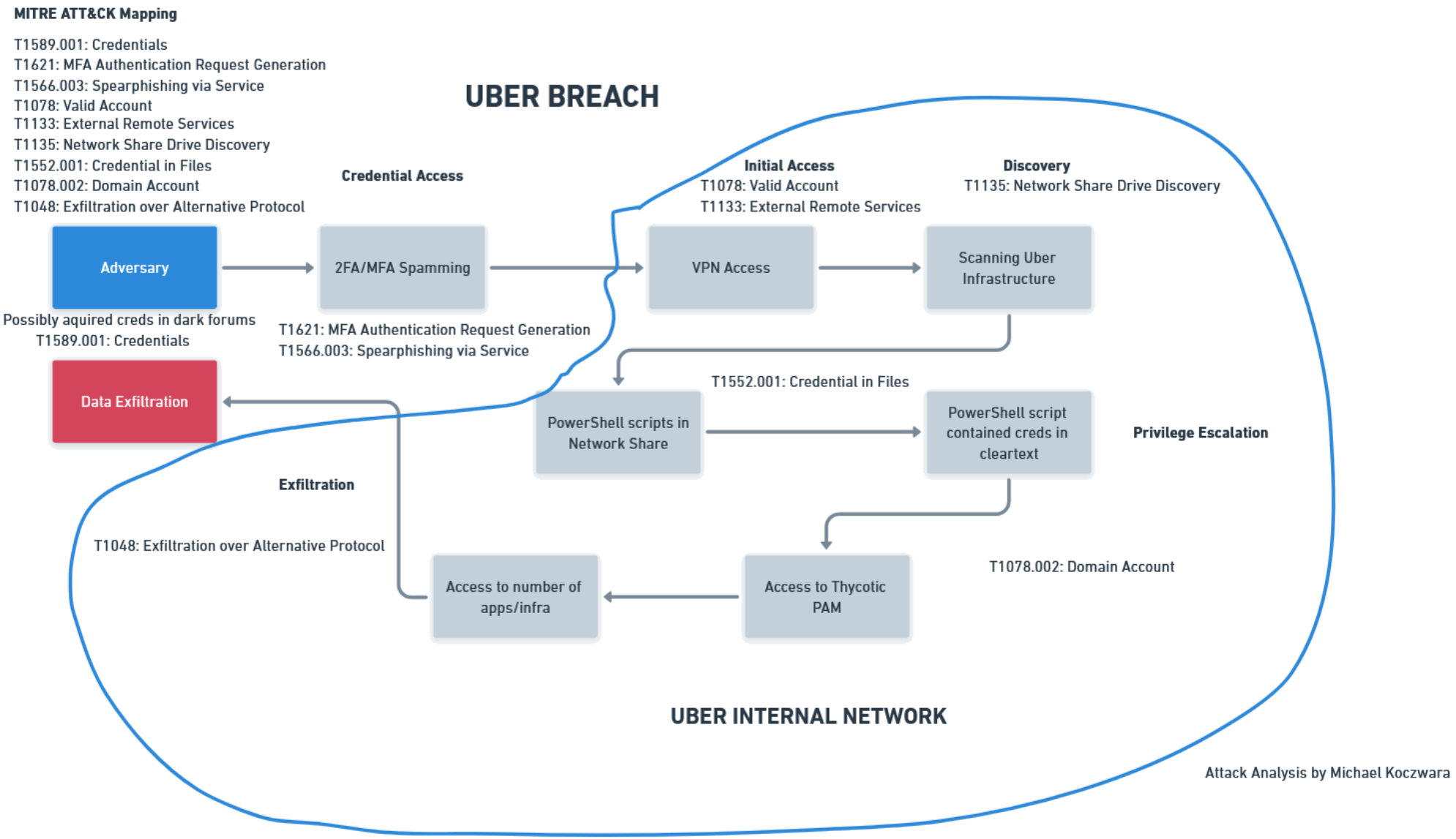
Inhabergeführt seit 2003

Motivation
Alte Welten und neue Phänomene

Die „gute“ alte Zeit

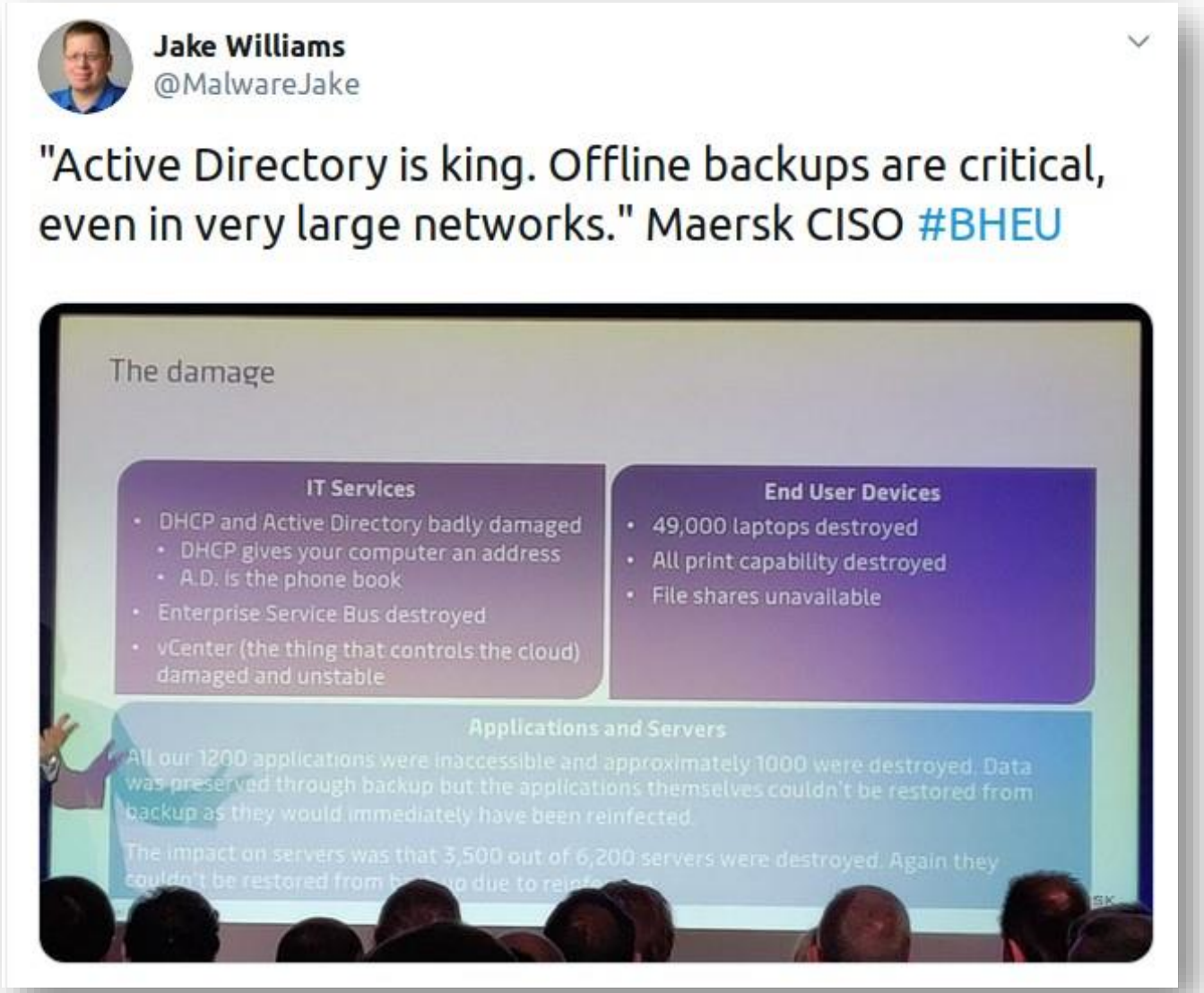


Bekannte Fälle – UBER-Hack

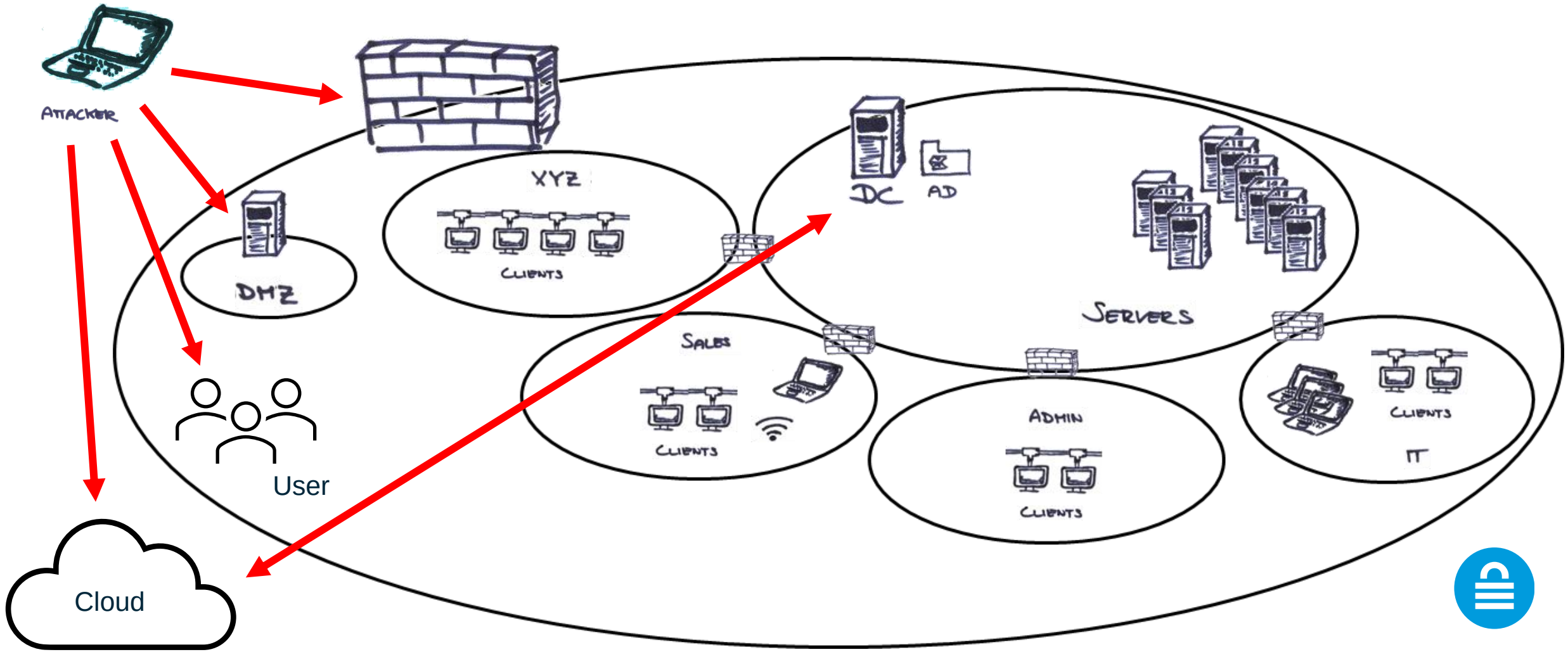


Quelle: https://twitter.com/MichalKoczwara/status/1571432800787759104/photo/1

Bekannte Fälle – Maersk



Die neue Welt – Hybride Infrastrukturen



Definition Cloud Computing nach NIST

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

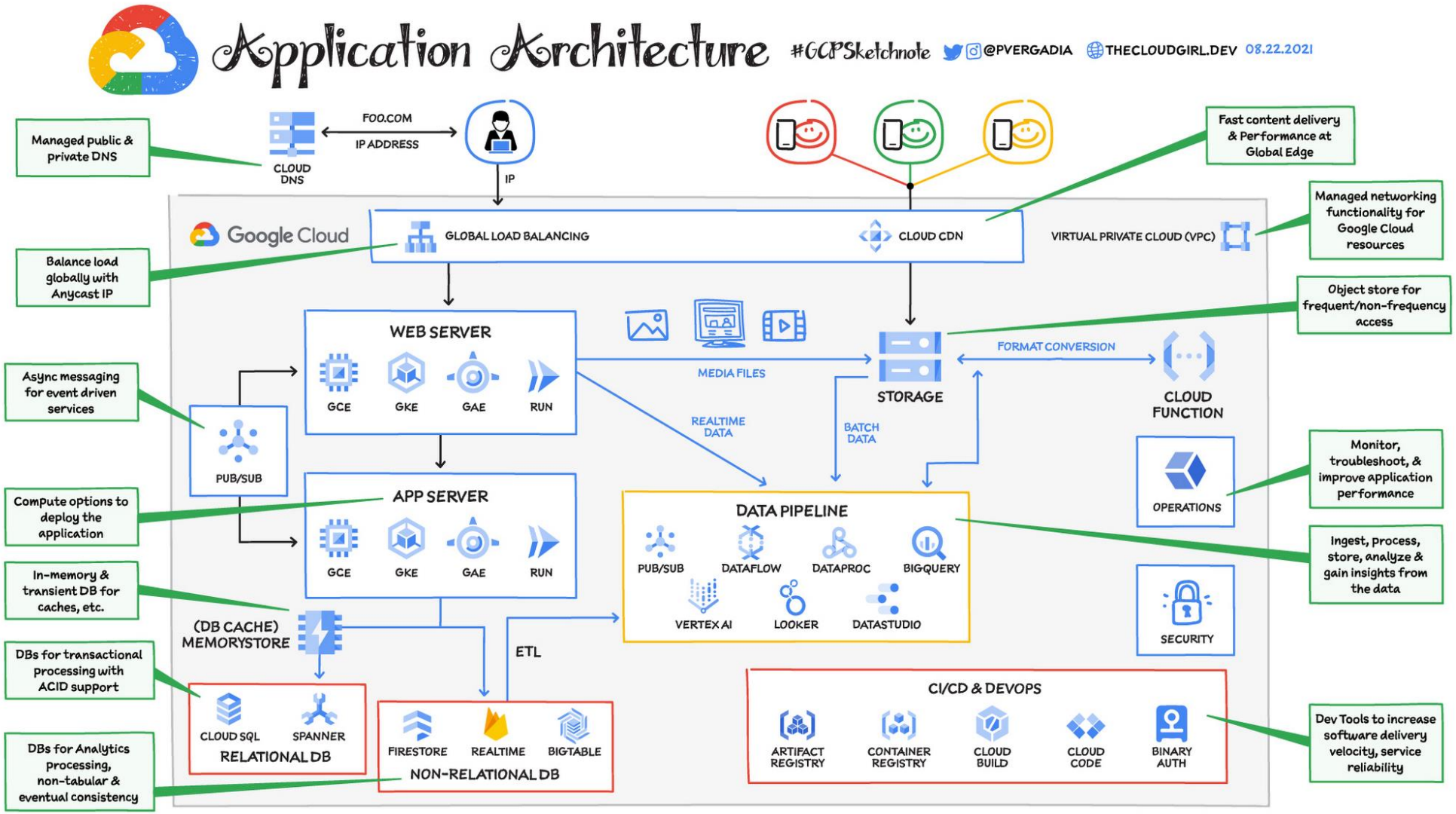
This cloud model is composed of five essential characteristics, three service models, and four deployment models.”

Quelle: The NIST Definition of Cloud Computing, Mell & Grance, NIST Special Publication 800-145

Microsoft Azure – Service Overview

Oneconsult AG
Tim Mittermeier
23. Oktober 2024

Google Cloud Platform – Application Architecture



Quelle: https://cloud.google.com/blog/topics/developers-practitioners/introduction-google-cloud?hl=en

“Sensitive US military emails spill online”

Sensitive US military emails spill

https://techcrunch.com/2023/02/21/sensitive-united-states-military-emails-spill-online/

Join TechCrunch+

Login

Search

TechCrunch+
Startups
Venture
Security
Crypto
Apps
Events
Advertise
More

Featured Article

Sensitive US military emails spill online

A government cloud email server was connected to the internet without a password

Zack Whittaker @zackwhittaker / 3:40 PM GMT+1 • February 21, 2023

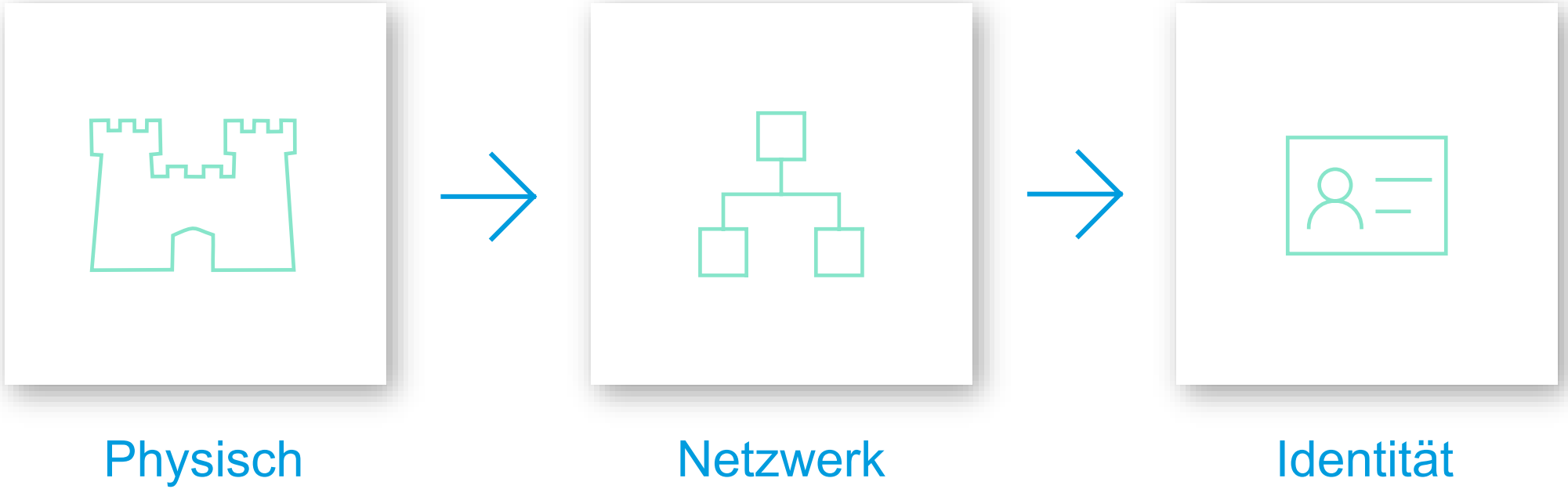
Comment

Oneconsult AG
Tim Mittermeier
23. Oktober 2024

Identität als neuer Perimeter
Die Renaissance der Passwortangriffe

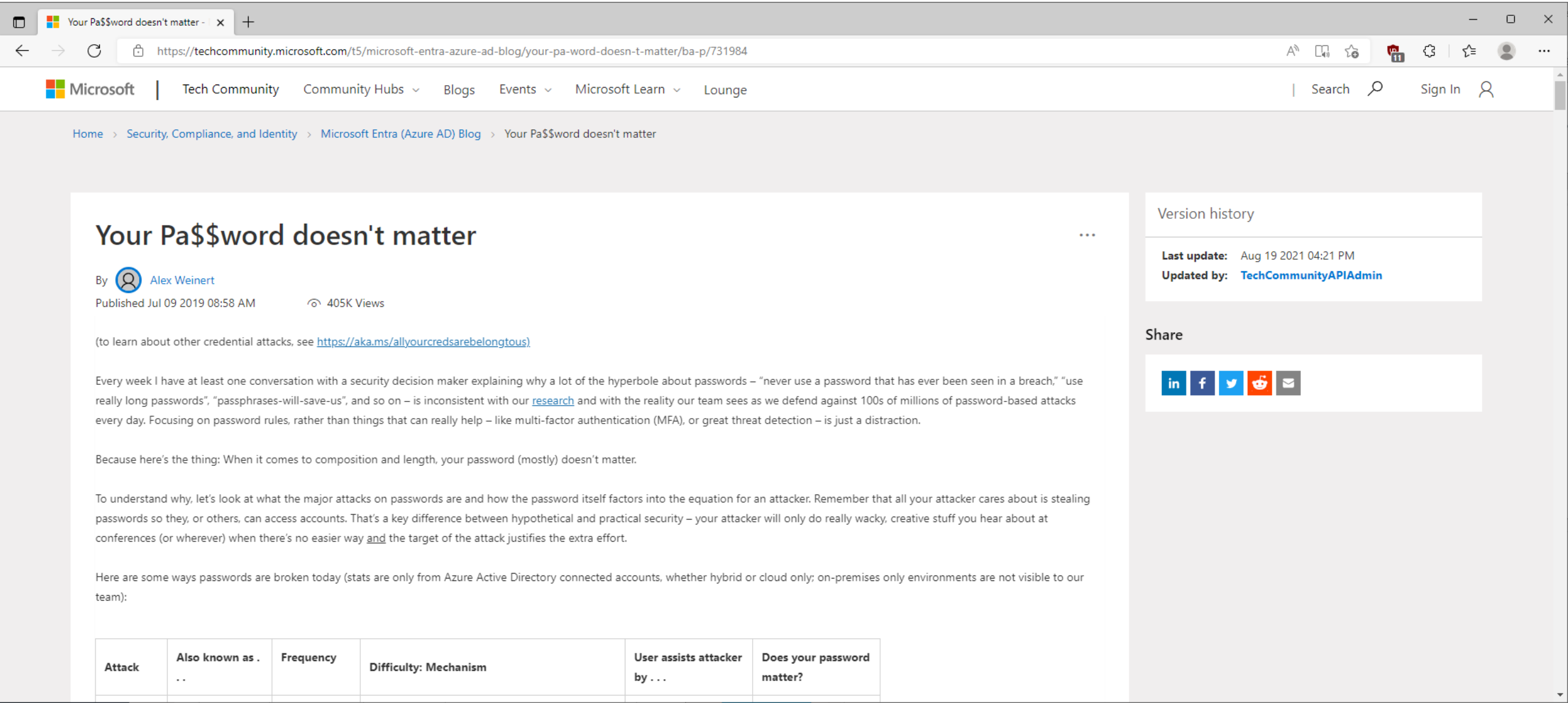
Evolution der Sicherheitsperimeter – Identität als neuer Perimeter

Oneconsult AG
Tim Mittermeier
23. Oktober 2024

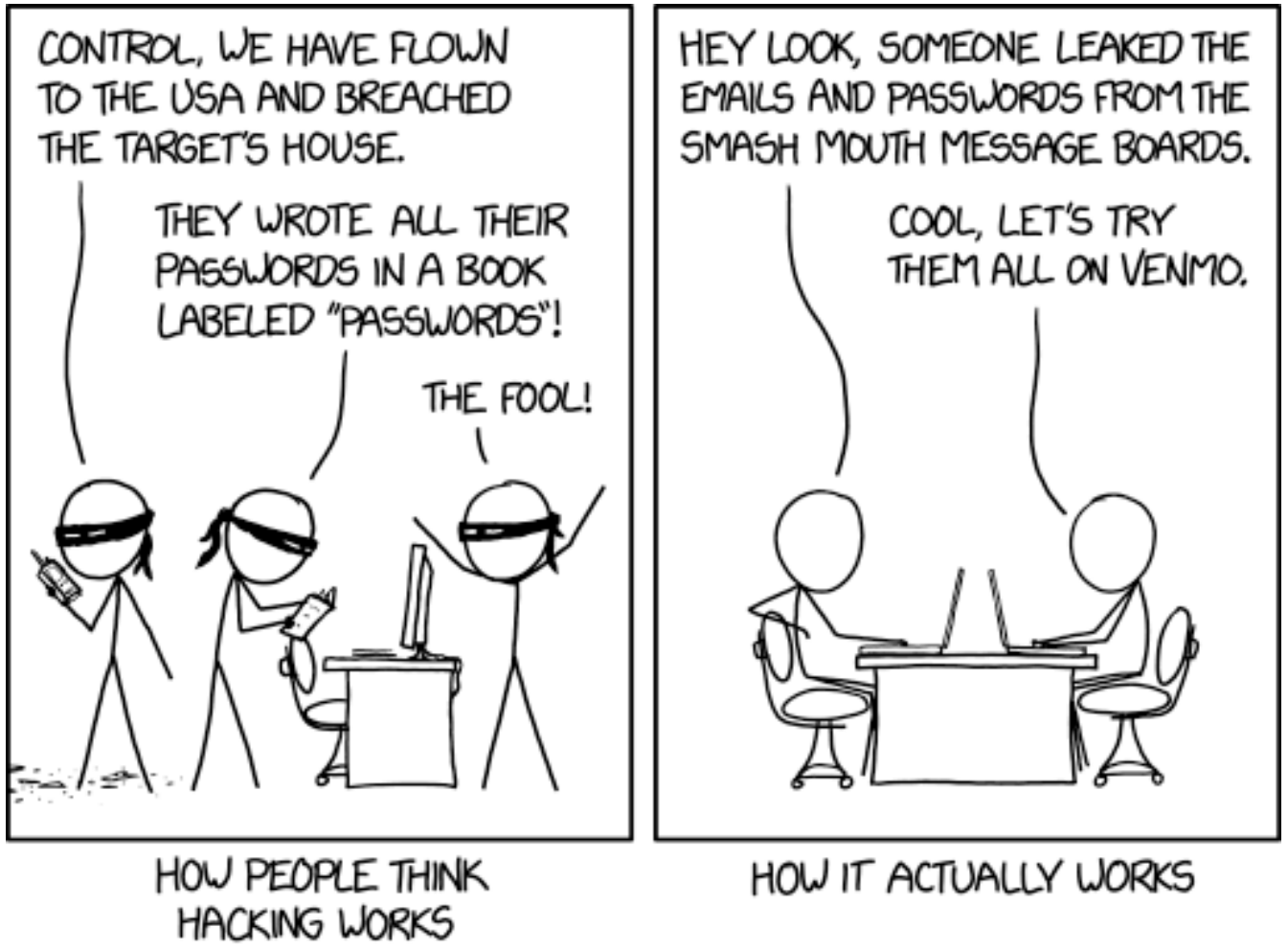


Quelle: https://learn.microsoft.com/de-de/security/ciso-workshop/ciso-workshop

Your Pa$$word doesn't matter – Password Spraying, Credential Stuffing, Phishing ...



Passwortangriffe – Credential Stuffing

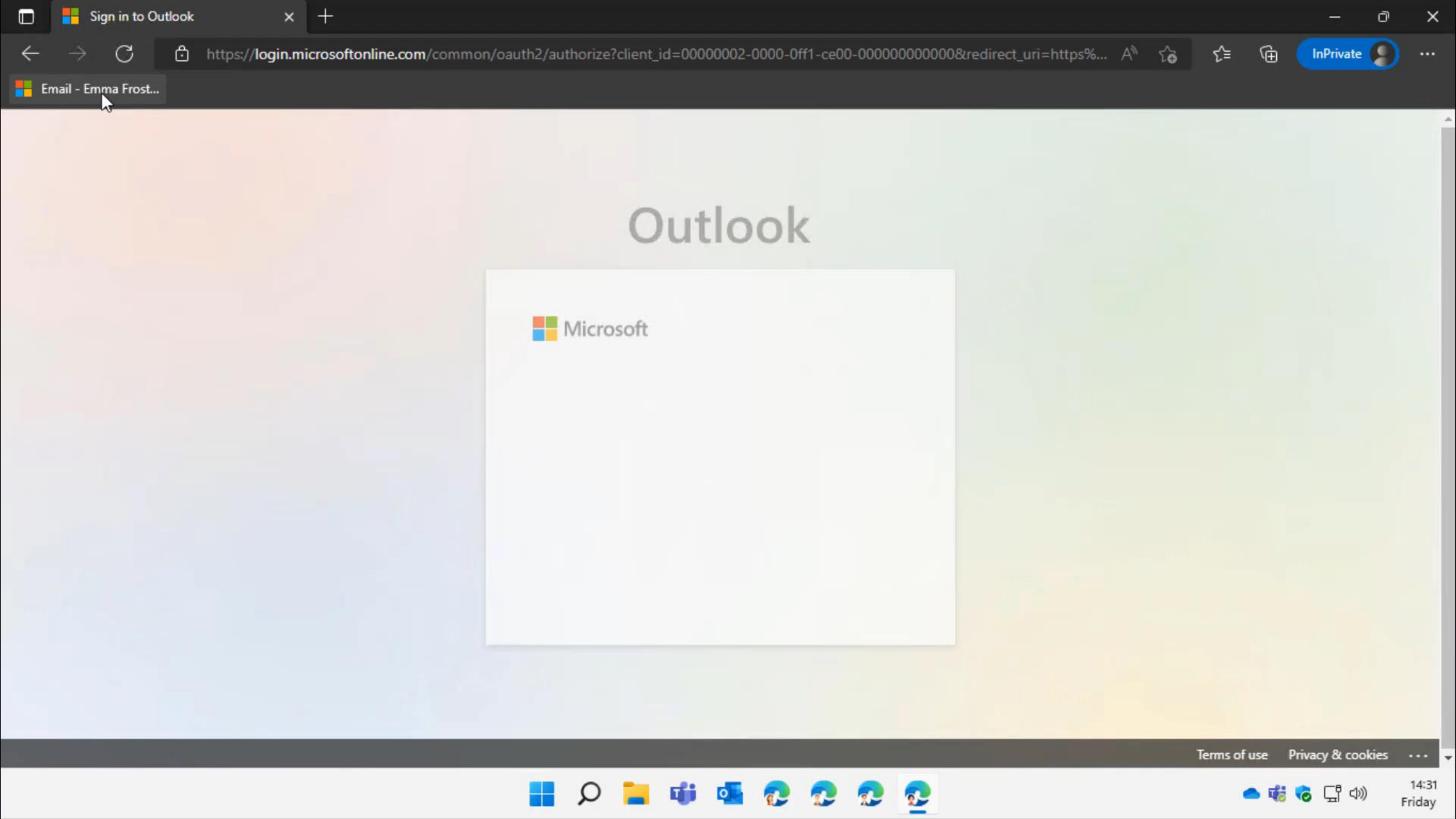


Quelle: https://xkcd.com/2176/

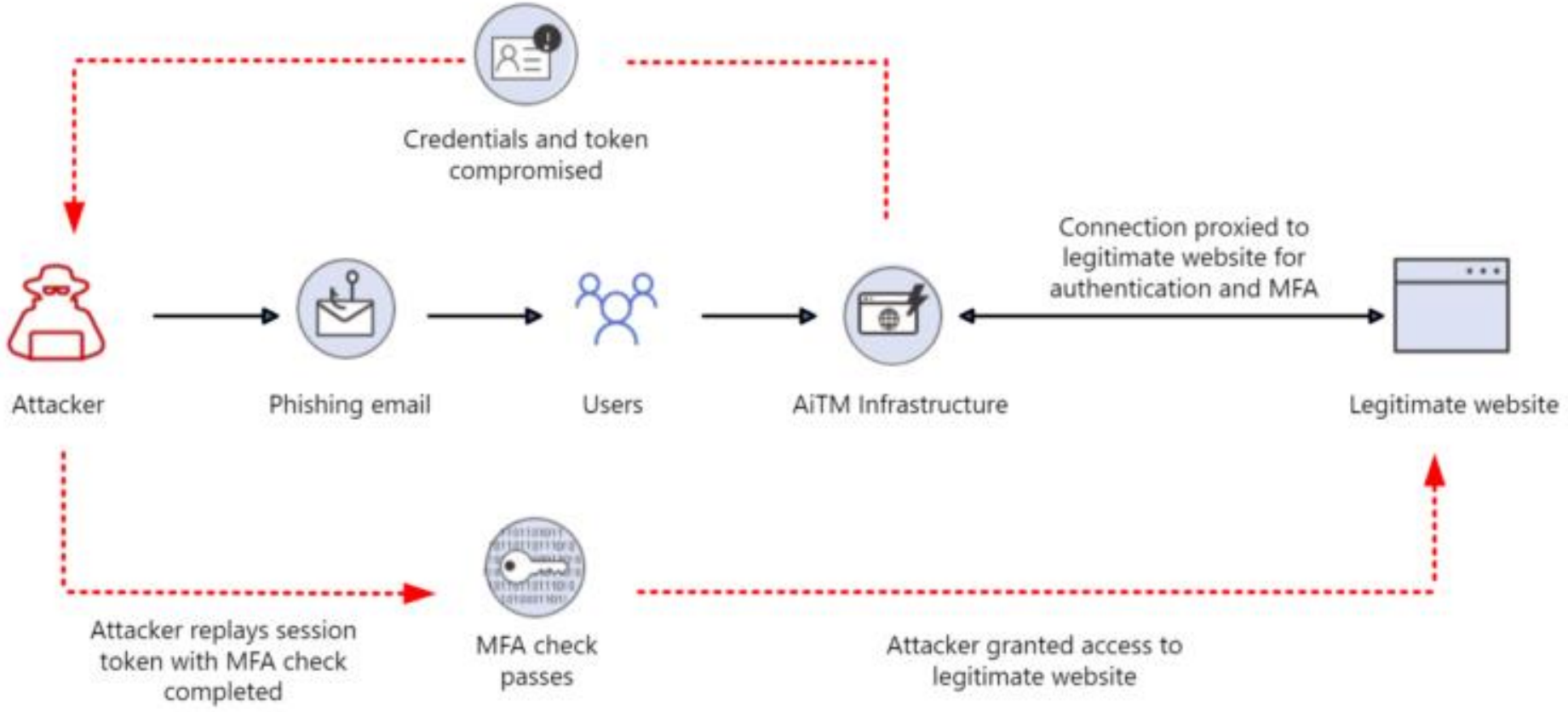
Starke Authentifizierung – Das Ende der Passwörter

Oneconsult AG
Tim Mittermeier
23. Oktober 2024

Methode	Sicherheit	Benutzer-freundlichkeit	Primäre Authentifizierung	Sekundäre Authentifizierung
Microsoft Authenticator-App	hoch	hoch	ja **Phishing-resistent**	MFA und SSPR
FIDO2-Sicherheitsschlüssel	hoch	hoch	ja	MFA
Windows Hello for Business	hoch	hoch	ja	MFA*
Zertifikatbasierte Authentifizierung	hoch	hoch	ja	nein
SMS	mittel	hoch	ja	MFA und SSPR
OATH-Softwaretoken	mittel	mittel	nein	MFA und SSPR
OATH-Hardwaretoken	mittel	mittel	nein	MFA und SSPR
Sprachanruf	mittel	mittel	nein	MFA und SSPR
Passwort	niedrig	hoch	ja	nein


Sign in to Outlook
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&redirect_uri=https%...
InPrivate
Email - Emma Frost...
Outlook
Microsoft
Terms of use
Privacy & cookies
14:31
Friday

Adversary-in-the-Middle (AitM) Phishing

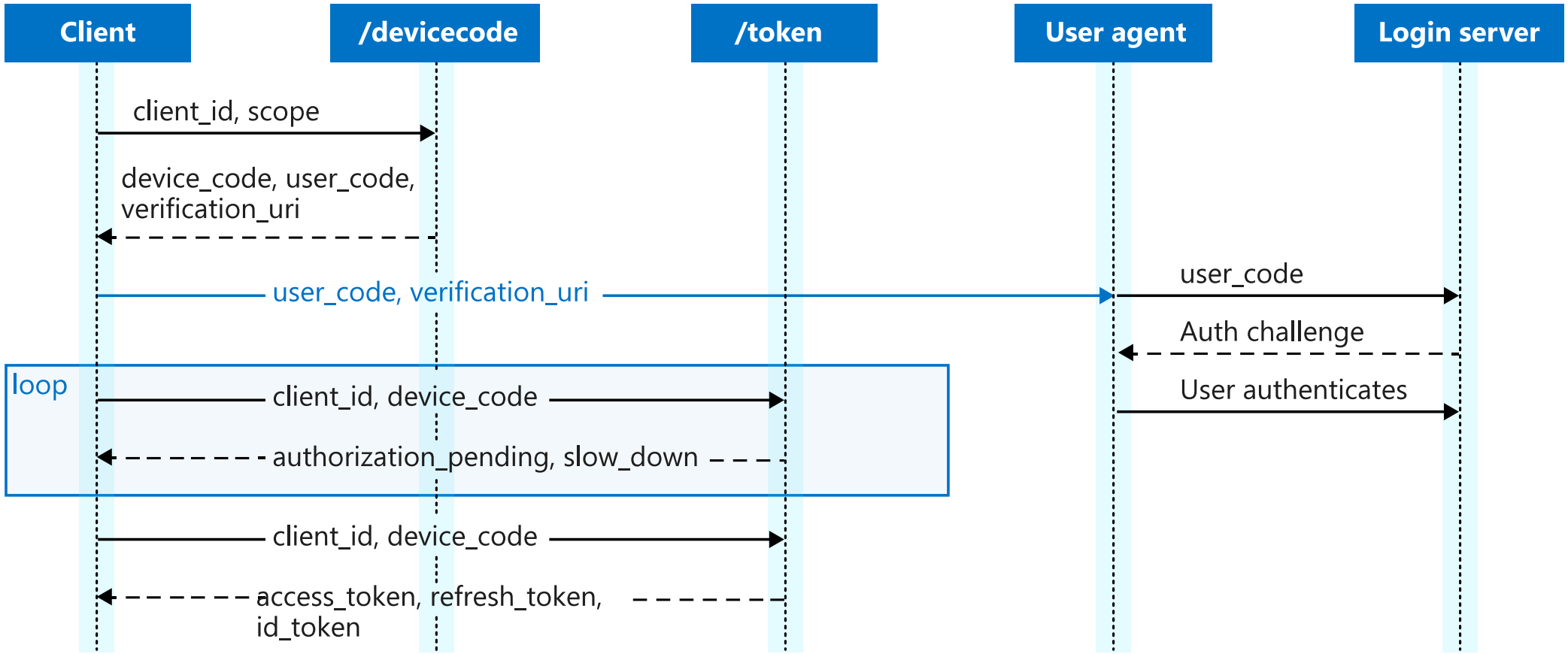


Quelle: https://www.microsoft.com/en-us/security/blog/2022/11/16/token-tactics-how-to-prevent-detect-and-respond-to-cloud-token-theft/

Oneconsult AG
Tim Mittermeier
23. Oktober 2024

The new Phish in Town
Device Code Phishing und mehr

Device Code Flow



Quelle: https://learn.microsoft.com/de-de/azure/active-directory/develop/v2-oauth2-device-code

*Untitled - Notepad

File Edit Format View Help

Demo

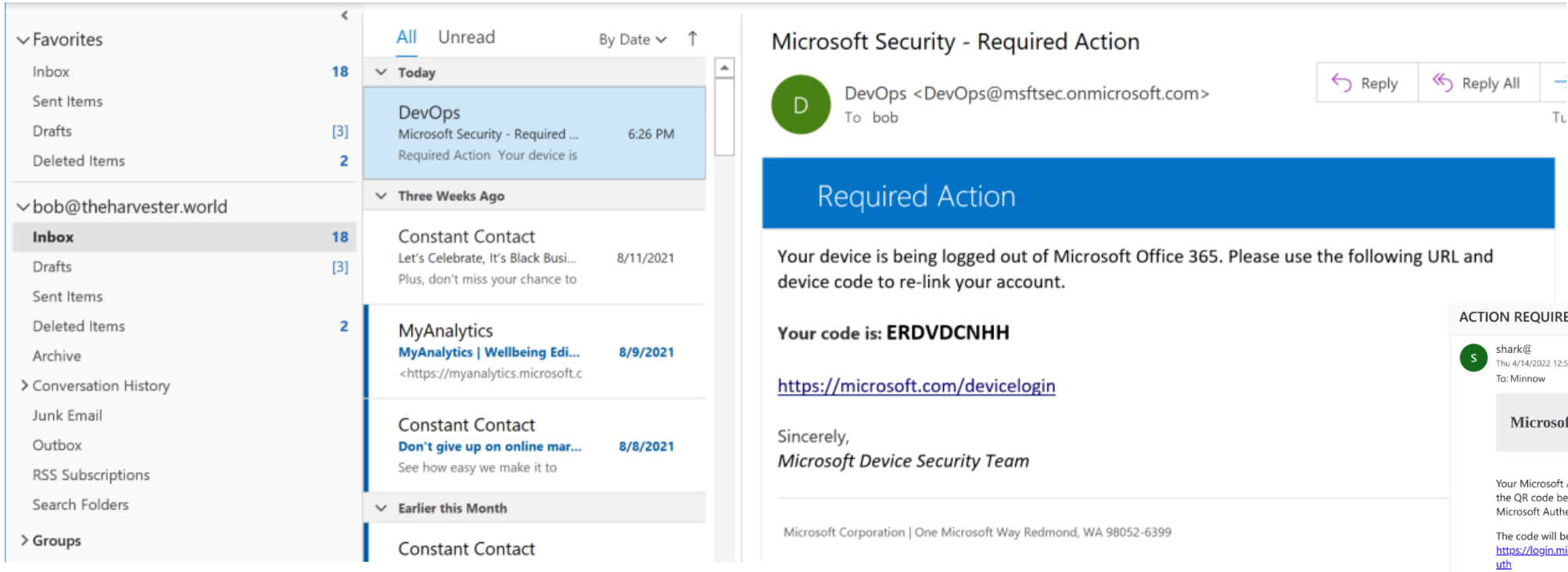
Device Code Sign-in Authentication Flow

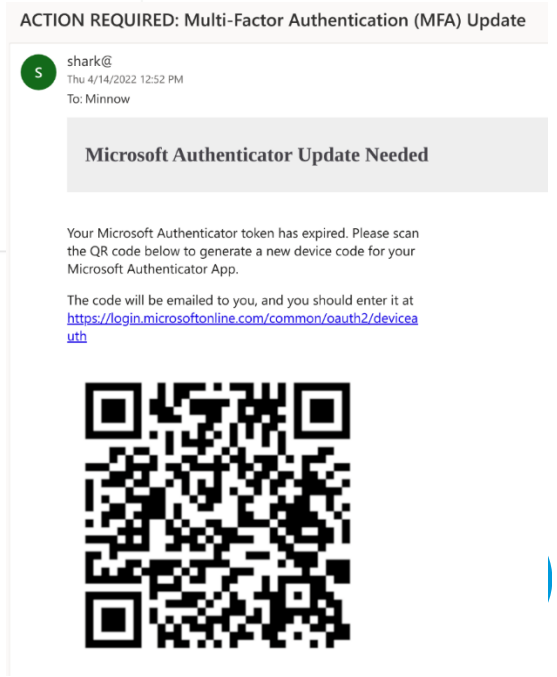
This technique can be leveraged for phishing.

Ln 6, Col 1 150% Windows (CRLF) UTF-8

12:38 PM
8/26/2022

Device Code Phishing aus Opfersicht – Linkziel: https://microsoft.com/devicelogin

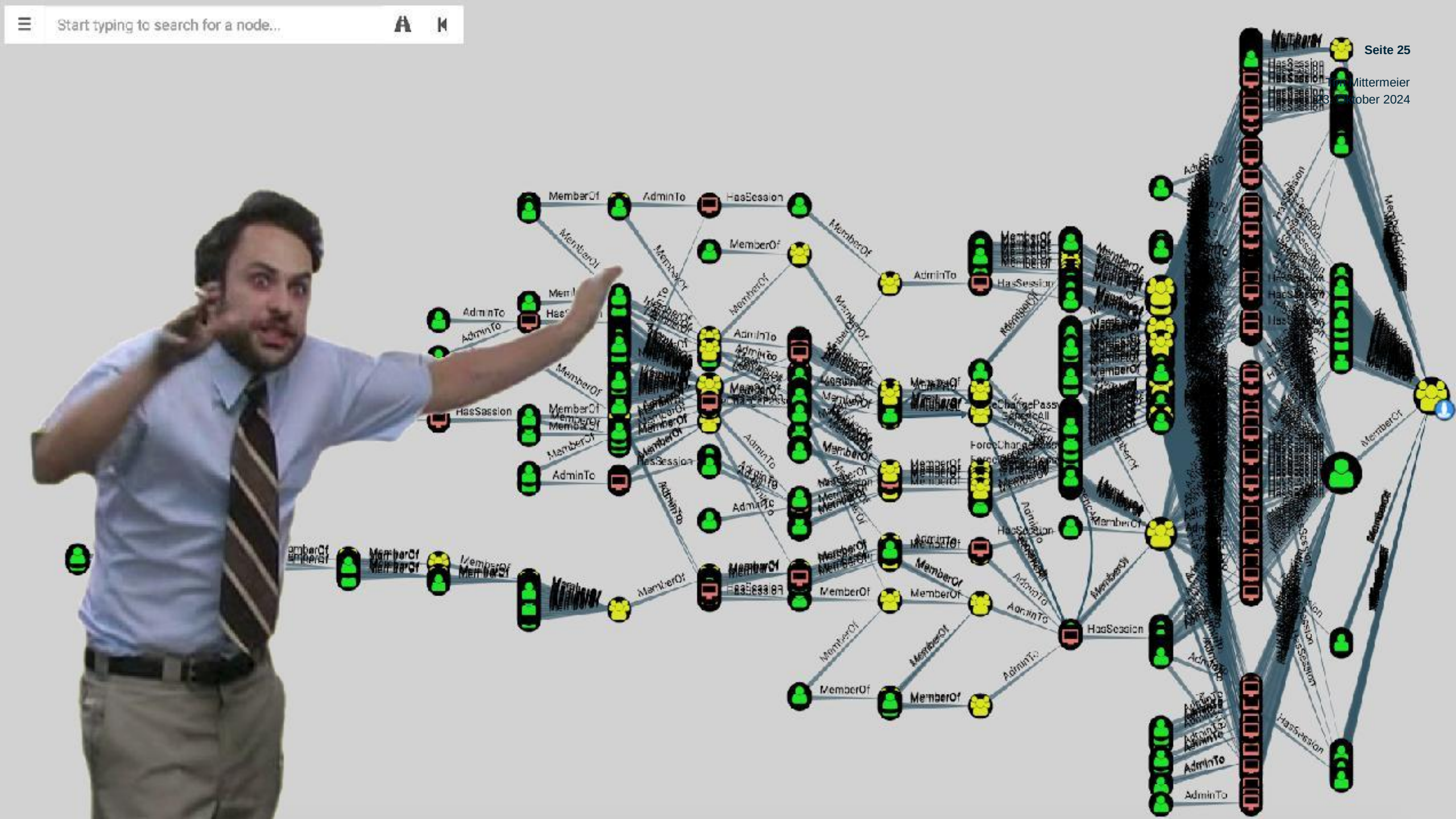




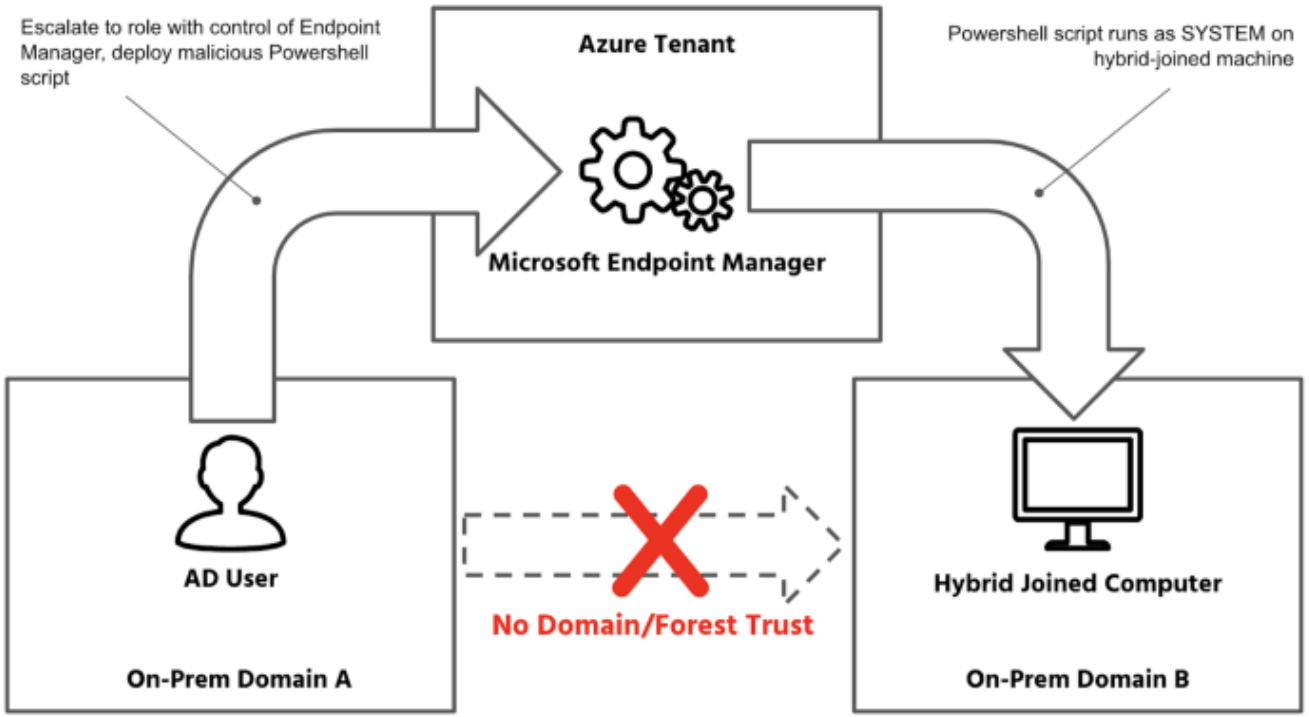
Quelle: https://0xboku.com/2021/07/12/ArtOfDeviceCodePhish.html

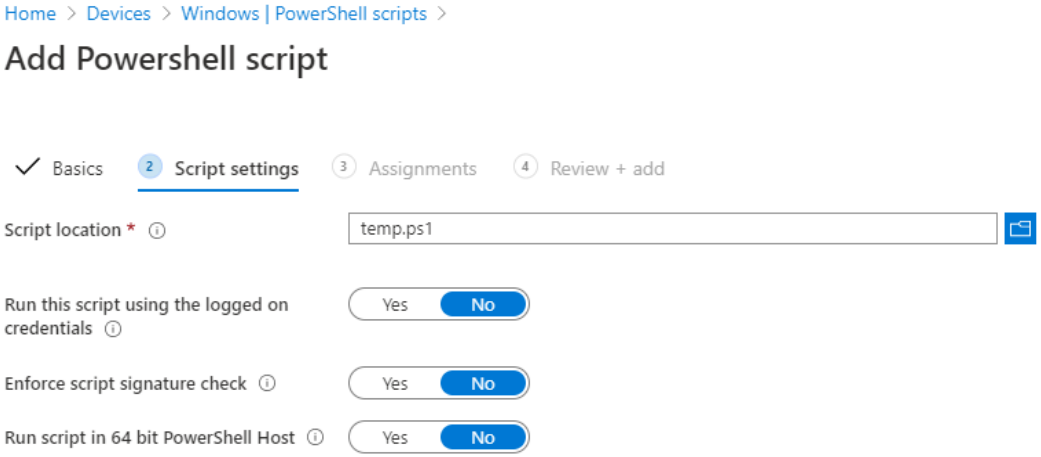
Angriffspfade
Hybride Infrastrukturen

Tim Mittermeier
03. Oktober 2024



Death from above – Cloud-managed Device zur OnPrem Administration





Quelle: https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d

Laterale Bewegung – Viele Wege führen zum Ziel

Credential Stuffing & MFA Spamming

Synchronisierung von Identitäten

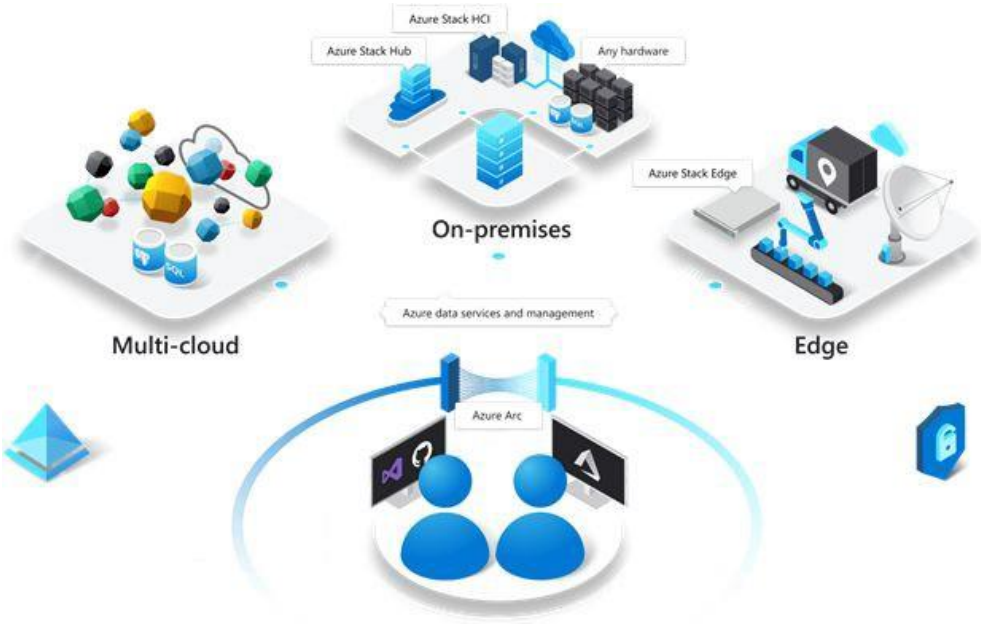
Device Code Phishing

Domain-joined Server als VM

Hybrid-joined Device zur Administration

Hybride Identität mit privilegierter Rolle

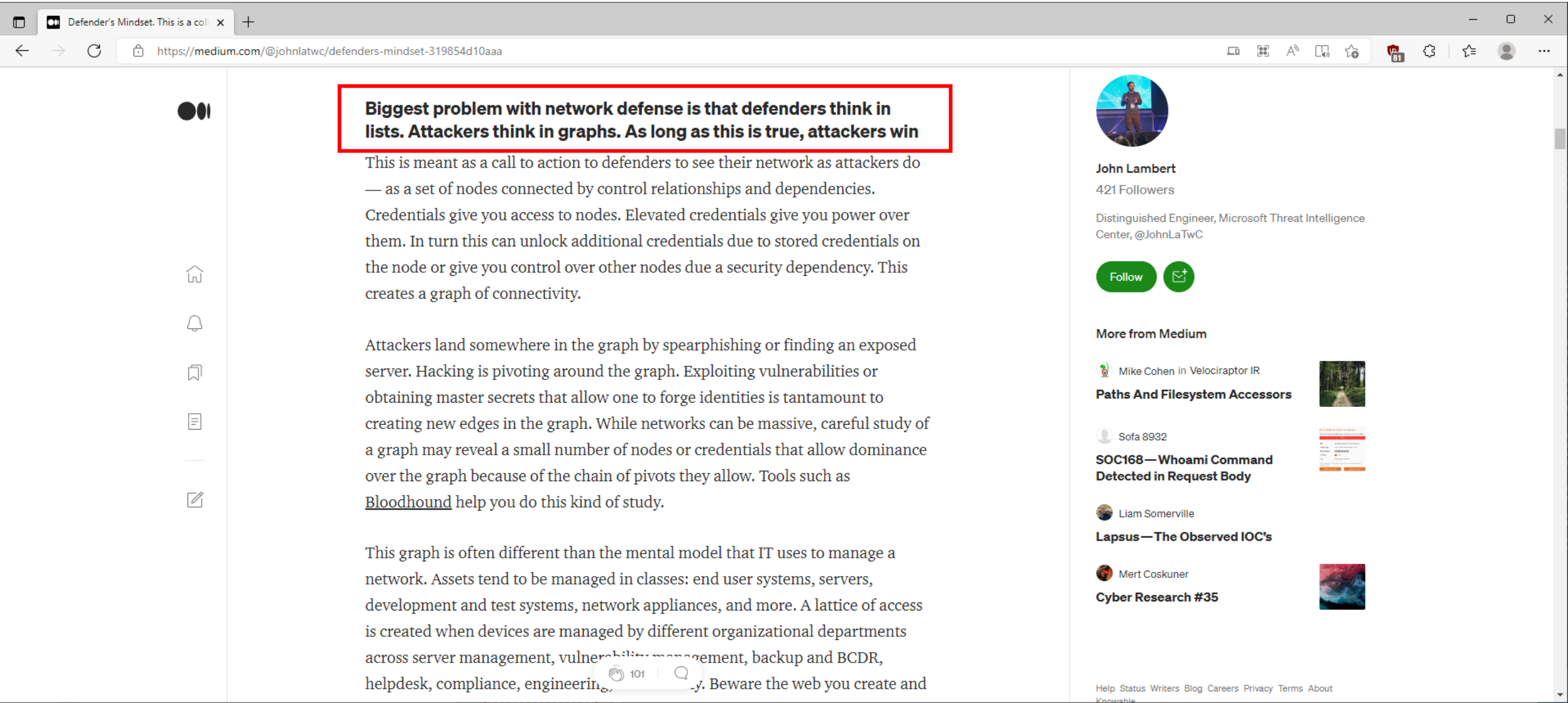
Phishing & Malware



Oneconsult AG
Tim Mittermeier
23. Oktober 2024

Penetrationstests
Planung & Durchführung

Warum Penetrationstests?
John Lambert: Defender‘s Mindset



Planung, Durchführung und Auswertung einer technischen Sicherheitsanalyse

Oneconsult AG
Tim Mittermeier
23. Oktober 2024

Scoping

- Was ist das Worst-Case-Szenario für meine Organisation?
- Welches Ziel möchte ich erreichen?
- Welche Systeme sollen getestet werden?

Kick-off Meeting

- Wie wird der Test ablaufen?
- Welche Vorbereitungen sind zu treffen?
- Wer ist zu informieren?

Vor-bereitung

- Muss eine Testumgebung bereitgestellt werden?
- Müssen Endgeräte bereitgestellt werden?
- Welche Benutzerkonten sind anzulegen?

Durch-führung

- Wie werden kritische Schwachstellen gemeldet?
- Welches Personal muss verfügbar sein?
- Was passiert bei einer Beeinträchtigung produktiver Systeme?

Planung, Durchführung und Auswertung einer technischen Sicherheitsanalyse

Oneconsult AG
Tim Mittermeier
23. Oktober 2024

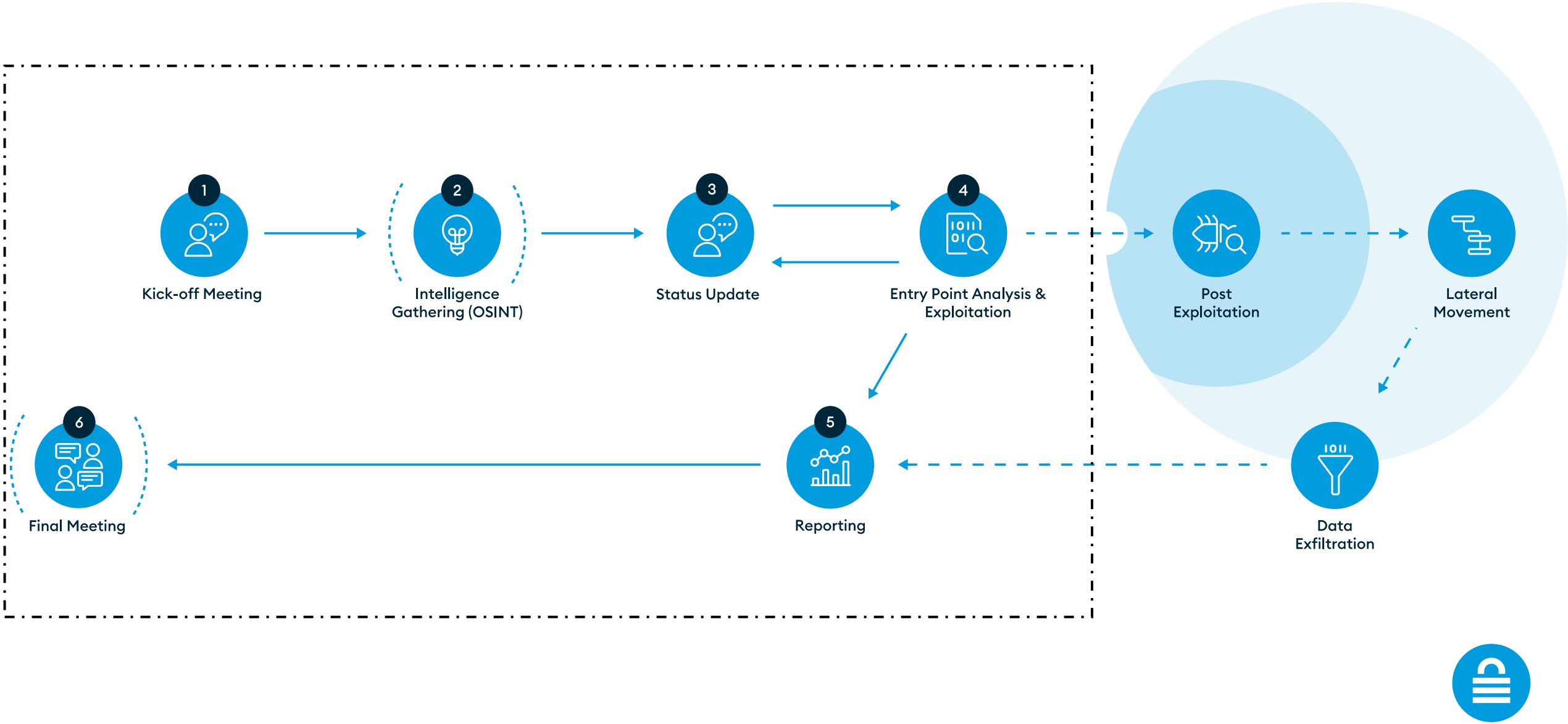
Clean-up
- Hinterlassenschaften entfernen
- Benutzerkonten & Zugänge deaktivieren
- Ggf. Systeme zurücksetzen

Schluss-bericht
- Sofortmaßnahmen einleiten
- Befunde auswerten & priorisieren
- Maßnahmen planen

Diskussion
- Teilnehmerkreis festlegen
- Offene Fragen klären
- Empfehlungen zum weiteren Vorgehen

Maß-nahmen
- Kommunikation mit Dienstleistern & Anbietern, ggf. Disclosure
- Löschung von Projektdaten
- Planung weiterer Testaktivitäten

Technische Testmethode



Scope – Beispiel

Scope: Penetrationstest der sicherheitsrelevanten Komponenten der Webapplikation Snakeoil.io aus Sicht eines externen Angreifers, der bereits einen Standardbenutzer kompromittiert hat.

Details: Die Webapplikation des Kunden wird einer gründlichen, technischen, privilegierten und unprivilegierten Sicherheitsüberprüfung unterzogen. Hierbei werden manuelle und automatisierte Testverfahren verwendet, angelehnt an den OWASP Application Security Verification Standard (ASVS), um Schwachstellen in der Webapplikation zu identifizieren. Die Analyse hat einen hohen manuellen Test- und Verifikationsanteil.

- Analyse
- Application Tests, z.B.:
  - Unsichere Speicherung sensitiver Daten
  - Client-Side Injection
  - Fehler bei der Authentifizierung und Autorisierung
  - Fehlerhafte Kryptographie
  - Funktions- und Rollenmissbrauch
- Manuelle Verifikation detektierter Sicherheitslücken
- Erarbeitung von Gegenmaßnahmen

Scope – Beispiel

Testart

Prüfobjekt

Scope: Penetrationstest der sicherheitsrelevanten Komponenten der Webapplikation Snakeoil.io aus Sicht eines externen Angreifers, der bereits einen Standardbenutzer kompromittiert hat.

Vektor

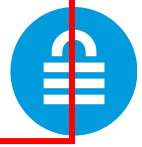
Ausprägung

Details: Die Webapplikation des Kunden wird einer gründlichen, technischen, privilegierten und unprivilegierten Sicherheitsüberprüfung unterzogen. Hierbei werden manuelle und automatisierte Testverfahren verwendet, angelehnt an den OWASP Application Security Verification Standard (ASVS), um Schwachstellen in der Webapplikation zu identifizieren. Die Analyse hat einen hohen manuellen Test- und Verifikationsanteil.

Methodik

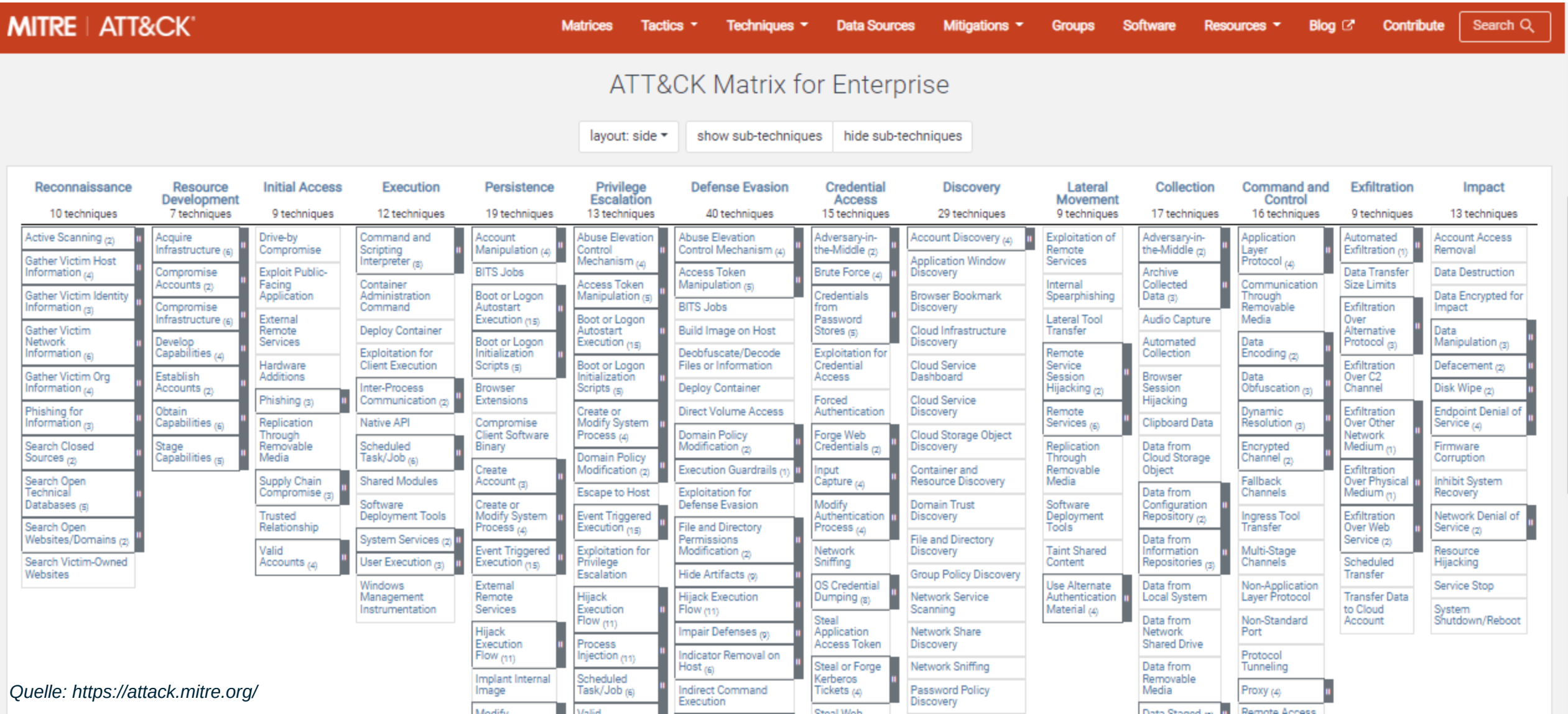
- Analyse
- Application Tests, z.B.:
  - Unsichere Speicherung sensitiver Daten
  - Client-Side Injection
  - Fehler bei der Authentifizierung und Autorisierung
  - Fehlerhafte Kryptographie
  - Funktions- und Rollenmissbrauch
- Manuelle Verifikation detektierter Sicherheitslücken
- Erarbeitung von Gegenmaßnahmen

Prüfumfang



MITRE ATT&CK® – ATT&CK Matrix for Enterprise

Oneconsult AG
Tim Mittermeier
23. Oktober 2024



Quelle: https://attack.mitre.org/

Durchführung – Zertifizierungen wie Sand am Meer

- Keine Berufsausbildung „Pentester“
- Zertifizierungen zum Nachweis der Befähigung
  - Aktuelle Inhalte?
  - Spezialisierung?
  - Anerkennung?
  - Hands-on-Anteil?
- Referenzprojekte?
- Kerngeschäft?
- Veröffentlichungen, z.B. Artikel und CVEs?

Quellen:
https://www.sans.org/emea/
https://www.offsec.com/courses/pen-200/
https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/

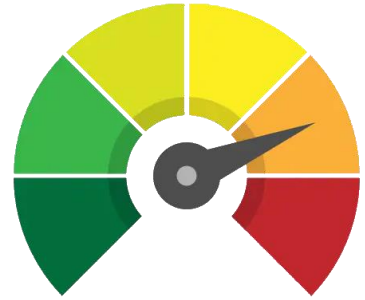
Schlussbericht

Wesentliche Bestandteile eines Schlussberichts:

- Einleitung
  - Ausgangslage & Rahmenbedingungen
  - Ziele & Scope
- Management Summary
  - Übersicht über Befunden
  - Zusammenfassung (Fließtext)
- Methodik der Durchführung
- Befunde in tabellarischer Form
- Ergänzende Informationen zu Befunden und Durchführung
- Anhänge

Schlussbericht – Bewertung der Befunde
Common Vulnerability Scoring System (CVSS)

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0



Quelle: https://www.first.org/cvss/

Schlussbericht – Befunde und Maßnahmen

5.1 Application Penetration Test – External REST API

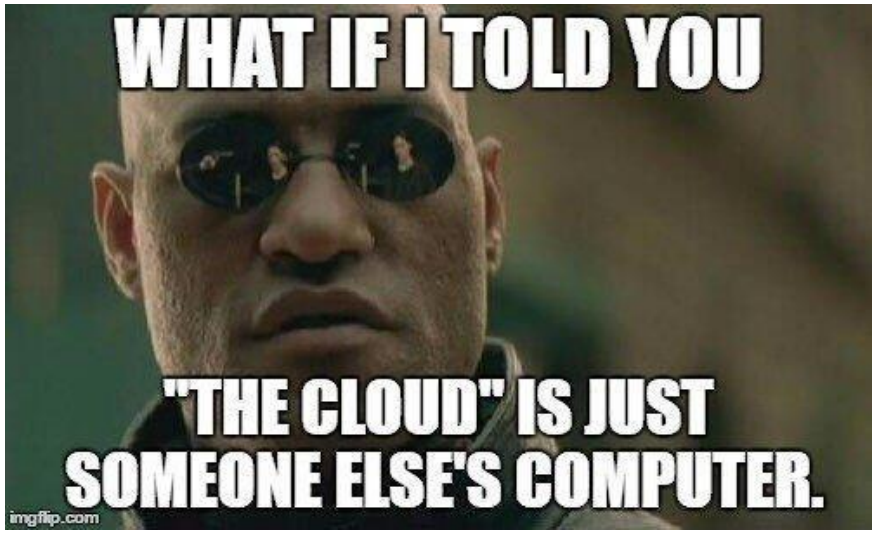
The following risks have been identified and categorized in the audit:

System	ID	Risk	Measure	Assessment
api.sps-company.com (198.51.100.250) 8820/tcp	c1	**SQL Injection in Login Form** Legitimate SQL database queries of the application can be manipulated by sending prepared requests to the server. These requests can be used to read information from the database or to manipulate data sets. As a result, this can lead to compromised user accounts, manipulated business processes or the compromise of the server itself. Affected page: → https://api.sps-company.com:8820/login More details in chapter 6.1. **Re-Test 03-Nov-2020**: Risk not resolved.	Database queries should be implemented such that user input is only ever used as data and never interpreted as code. For example, this can be achieved when using prepared statements. Further information: → https://owasp.org/www-community/attacks/SQL_Injection	**Rating:** Critical (9) **Risk remediation effort**: Medium **OSSTMM**: Vulnerability

Zusammenfassung & Fazit
Wie schützen wir uns?

Zusammenfassung & Fazit

- Cloud-Umgebungen und hybride Infrastrukturen müssen aktiv administriert werden
- Netzwerk und Systeme müssen ganzheitlich und kontinuierlich evaluiert werden
- Privilegierter Zugriff ist kritisch
- Anzahl möglicher Angriffspfade steigt mit der Komplexität
- 100% Sicherheit gibt es nicht
- **Aber:** Wir können Angreifer verlangsamen und deren Kosten erhöhen



Let's connect

www.oneconsult.com

/oneconsult-ag

/OneconsultAG

/oneconsult

Monatliche Cyber Security News abonnieren:

Oneconsult Newsletter