

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)



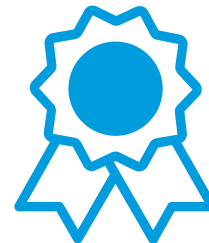
2.000+
Cybersecurity-Projekte



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**

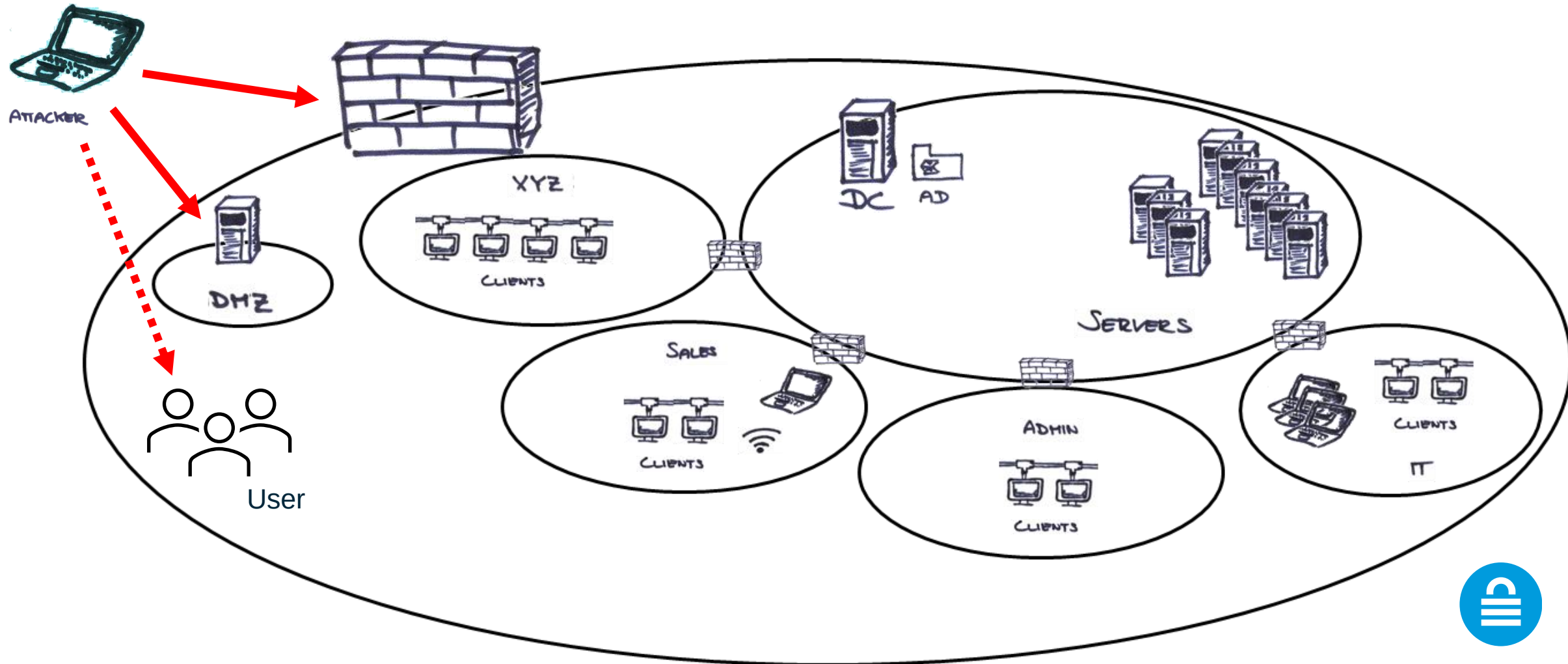


Motivation

Alte Welten und neue Phänomene



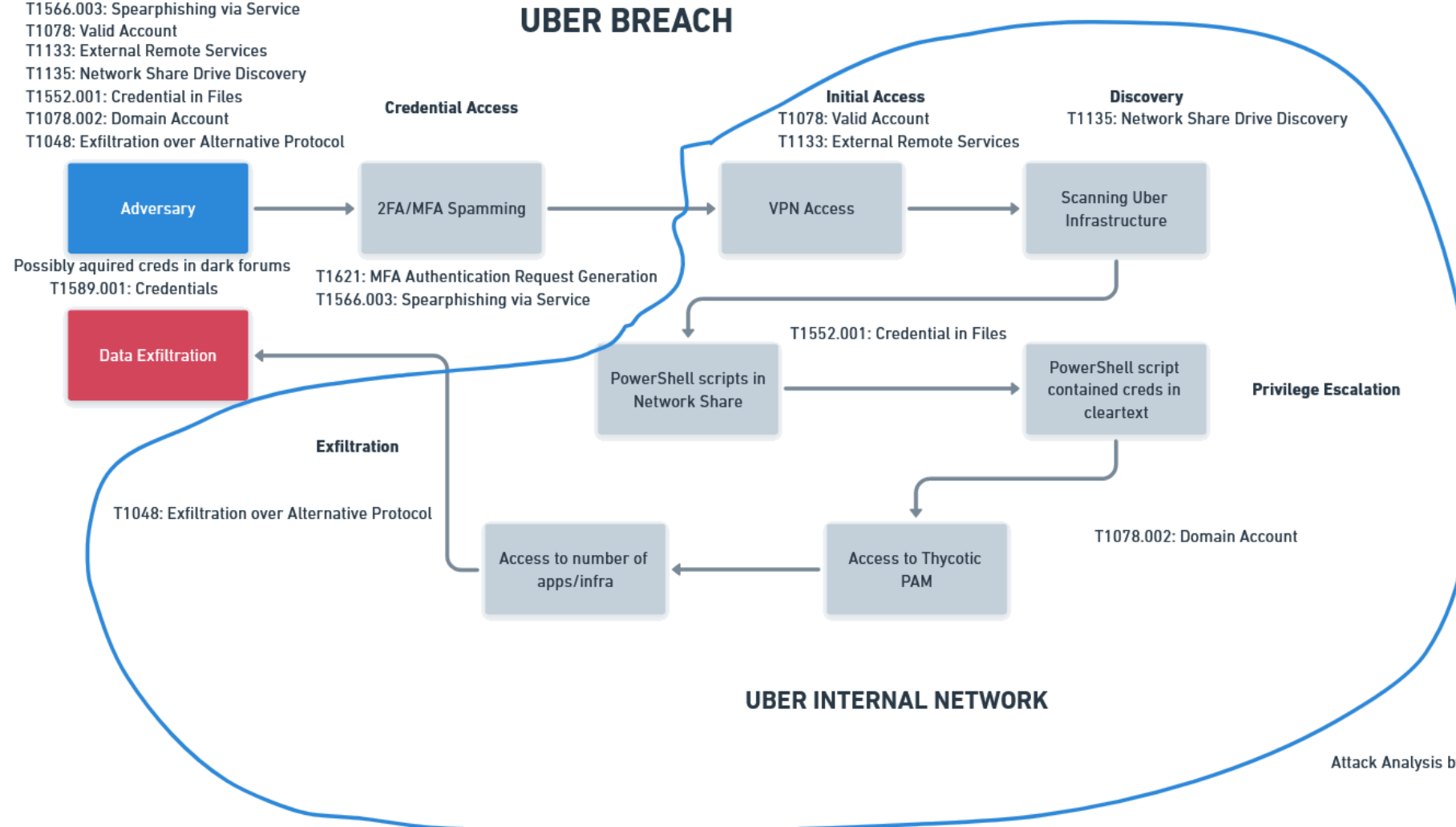
Die „gute“ alte Zeit



Bekannte Fälle – UBER-Hack

MITRE ATT&CK Mapping

T1589.001: Credentials
T1621: MFA Authentication Request Generation
T1566.003: Spearphishing via Service
T1078: Valid Account
T1133: External Remote Services
T1135: Network Share Drive Discovery
T1552.001: Credential in Files
T1078.002: Domain Account
T1048: Exfiltration over Alternative Protocol



Attack Analysis by Michael Koczwara





Jake Williams
@MalwareJake

"Active Directory is king. Offline backups are critical, even in very large networks." Maersk CISO #BHEU

The damage

IT Services	End User Devices
• DHCP and Active Directory badly damaged • DHCP gives your computer an address • A.D. is the phone book • Enterprise Service Bus destroyed • vCenter (the thing that controls the cloud) damaged and unstable	• 49,000 laptops destroyed • All print capability destroyed • File shares unavailable

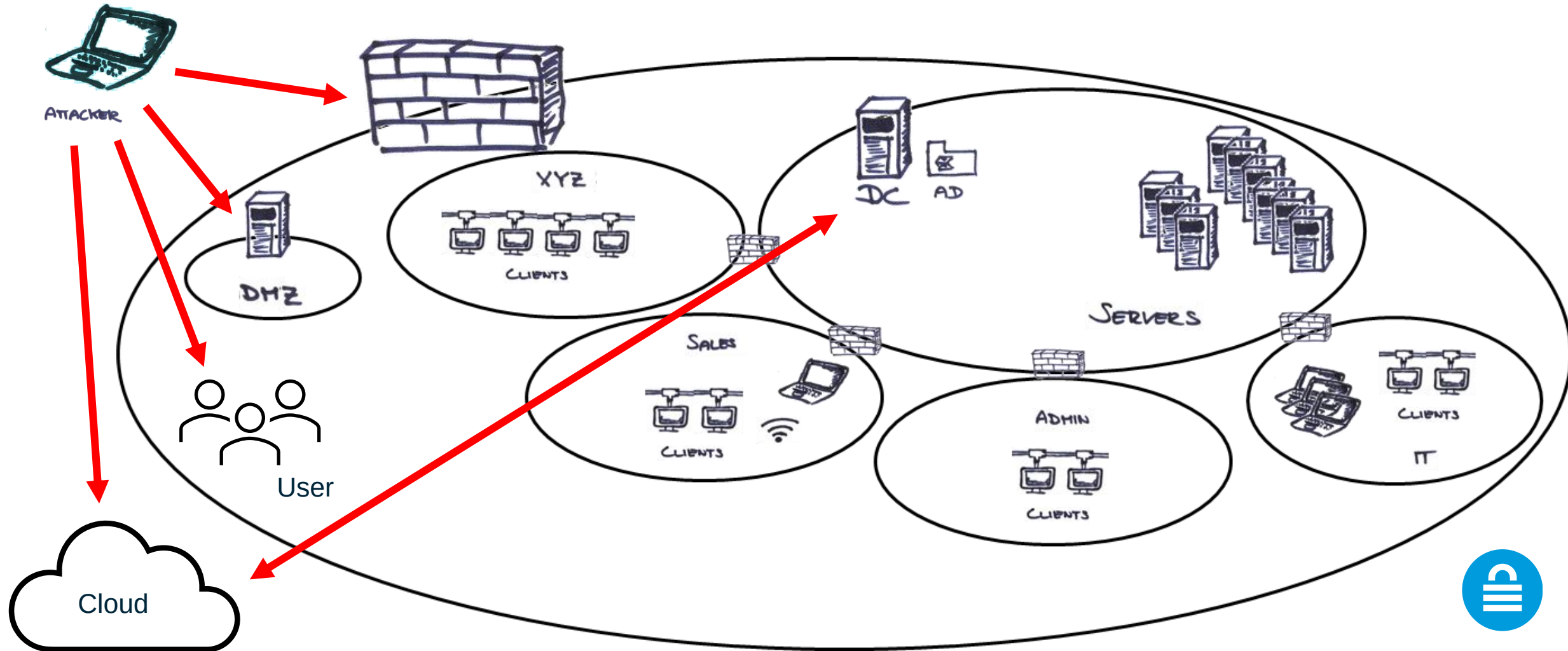
Applications and Servers

All our 1200 applications were inaccessible and approximately 1000 were destroyed. Data was preserved through backup but the applications themselves couldn't be restored from backup as they would immediately have been reinfected.

The impact on servers was that 3,500 out of 6,200 servers were destroyed. Again they couldn't be restored from backup due to reinfected.



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.*

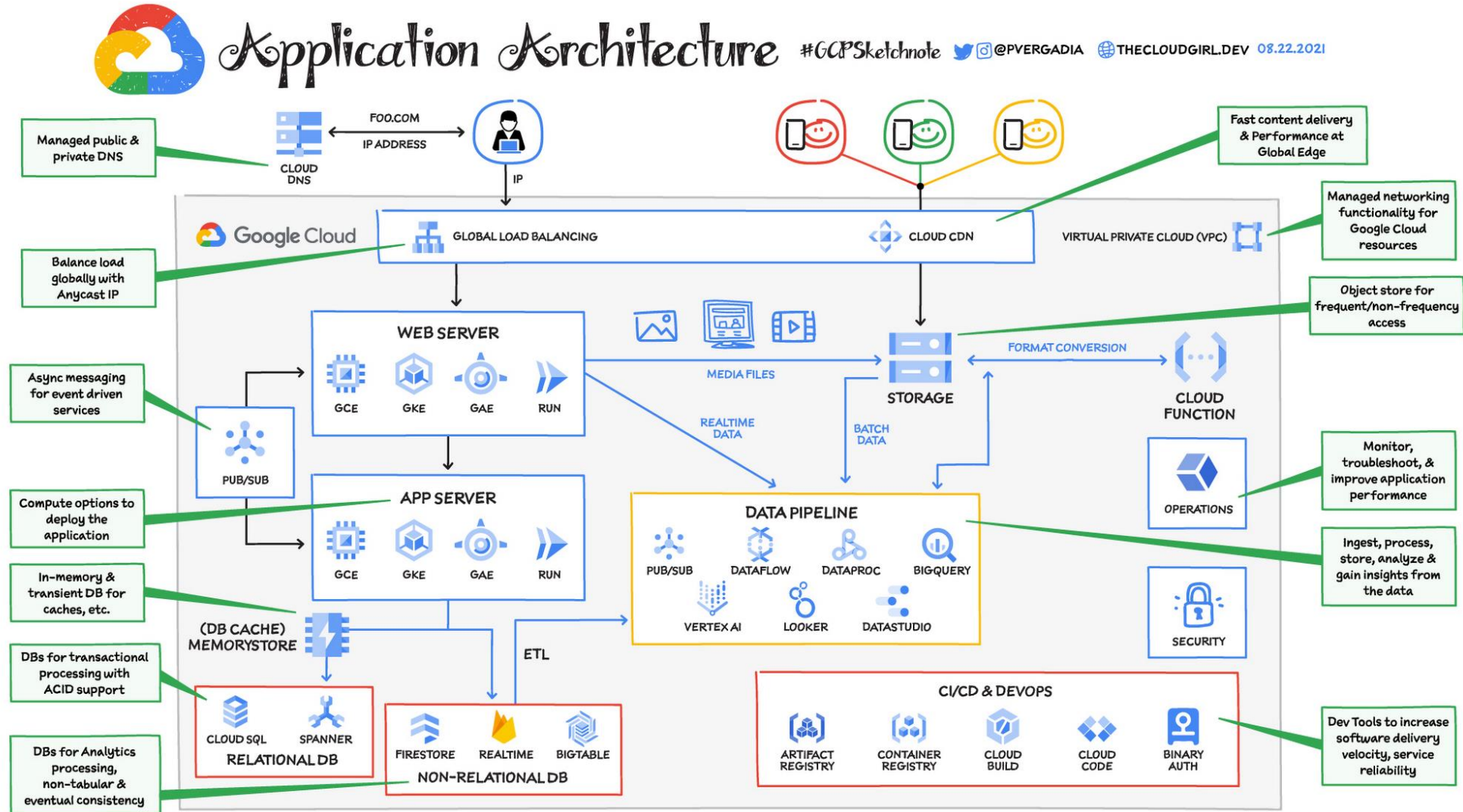
This cloud model is composed of five essential characteristics, three service models, and four deployment models.”



Microsoft Azure – Service Overview

AI + Machine Learning	Analytics	Compute	Databases	Development	Identity + Security	IoT + MR	Integration	Management + Governance	Media + Comms	Migration	Networking	Storage
 AI Bot Service	 Analysis Services	 App Service	 Apache Cassandra MI	 App Configuration	 Azure AD EI	 Azure Maps	 API Center	 Automation	 Azure CDN	 Azure Migrate	 Application Gateway	 Avere vFXT
 Azure AI Search	 Azure Purview	 Azure Batch	 Cosmos DB	 Azure Chaos Studio	 Azure Key Vault	 Azure Sphere	 API Management	 Azure Advisor	 Azure Comms. Gateway	 Data Box	 Azure Bastion	 Azure Elastic SAN
 Azure AI Services	 Data Explorer	 Azure Functions	 Database for MariaDB	 Azure DevOps	 Copilot for Security	 Defender for IoT	 Energy Data Manager	 Azure Arc	 Comm. Services	 DB Migration Service	 Azure DNS	 Azure NetApp Files
 Azure AI Studio	 Data Factory	 Azure Quantum	 Database for MySQL	 Azure Spring Apps	 DDoS Protection	 Digital Twins	 Event Grid	 Azure Automanage		 Resource Mover	 Azure Firewall	 Azure Storage
 Machine Learning	 Databricks	 Azure Red Hat OpenShift	 Database for PostgreSQL	 Deployment Environments	 Dedicated HSM	 IoT Central	 Health Data Services	 Azure Backup		 Site Recovery	 Azure Front Door	 Confidential Ledger
 Microsoft Genomics	 Event Hubs	 Azure VMware Solution	 Redis Cache	 DevTest Labs	 Defender EASM	 IoT Edge	 Logic Apps	 Azure Blueprints			 Azure Orbital	 Container Storage
 Open Datasets	 Graph Data Connect	 Cloud Services	 SQL Database	 Lab Services	 Defender for Cloud	 IoT Hub	 Notification Hubs	 Azure Lighthouse			 ExpressRoute	 Data Lake Storage
	 HDInsight	 Compute Fleet		 Load Testing	 Information Protection	 Remote Rendering	 Service Bus	 Azure Monitor			 Load Balancer	 Data Share

Google Cloud Platform – Application Architecture



“Sensitive US military emails spill online”

TechCrunch

Join TechCrunch+

Login

Search Q

TechCrunch+

Startups

Venture

Security

Crypto

Apps

Events

Advertise

More

Sensitive US military emails spill

+

←

↺

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

23

⚙

☆

👤

⋮

TC

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



✕

Twitter

f

in

Reddit

✉

🔗

TechCrunch

Early Stage

April 20, 2023

Boston, MA

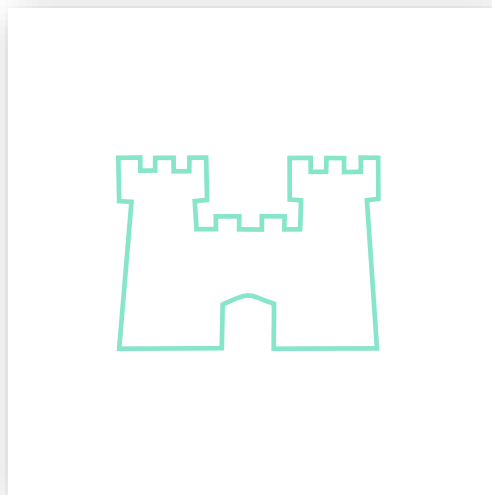
Register Now

Identität als neuer Perimeter

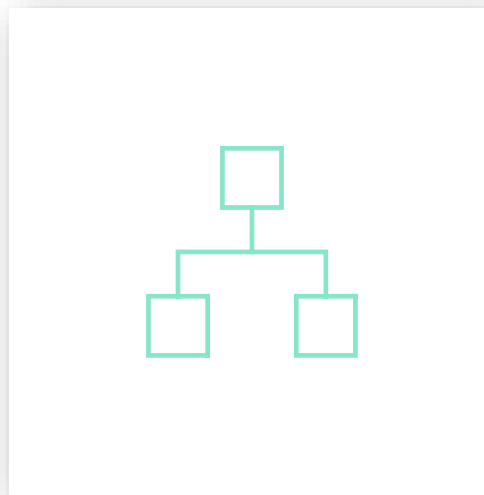
Die Renaissance der Passwortangriffe



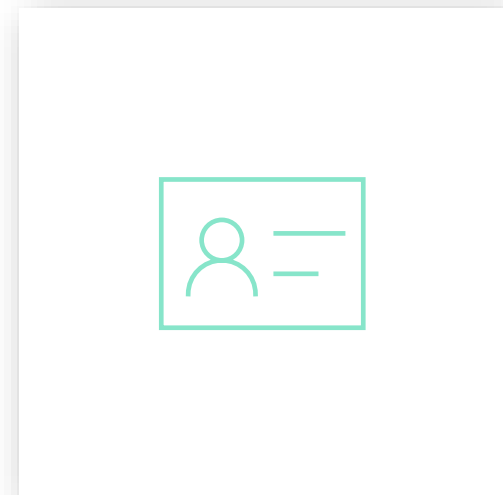
Evolution der Sicherheitsperimeter – Identität als neuer Perimeter



Physisch



Netzwerk



Identität



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

Microsoft

Tech Community

Community Hubs

Blogs

Events

Microsoft Learn

Lounge

Search

Sign In

Home

Security, Compliance, and Identity

Microsoft Entra (Azure AD) Blog

Your Pa\$\$word doesn't matter

Your Pa\$\$word doesn't matter

By  Alex Weinert

Published Jul 09 2019 08:58 AM

405K Views

(to learn about other credential attacks, see <https://aka.ms/allyourcredsarebelongtous>)

Every week I have at least one conversation with a security decision maker explaining why a lot of the hyperbole about passwords – “never use a password that has ever been seen in a breach,” “use really long passwords”, “passphrases-will-save-us”, and so on – is inconsistent with our [research](#) and with the reality our team sees as we defend against 100s of millions of password-based attacks every day. Focusing on password rules, rather than things that can really help – like multi-factor authentication (MFA), or great threat detection – is just a distraction.

Because here’s the thing: When it comes to composition and length, your password (mostly) doesn’t matter.

To understand why, let’s look at what the major attacks on passwords are and how the password itself factors into the equation for an attacker. Remember that all your attacker cares about is stealing passwords so they, or others, can access accounts. That’s a key difference between hypothetical and practical security – your attacker will only do really wacky, creative stuff you hear about at conferences (or wherever) when there’s no easier way and the target of the attack justifies the extra effort.

Here are some ways passwords are broken today (stats are only from Azure Active Directory connected accounts, whether hybrid or cloud only; on-premises only environments are not visible to our team):

Attack	Also known as . .	Frequency	Difficulty: Mechanism	User assists attacker by . . .	Does your password matter?
--------	-------------------	-----------	-----------------------	--------------------------------	----------------------------

Version history

Last update:

Aug 19 2021 04:21 PM

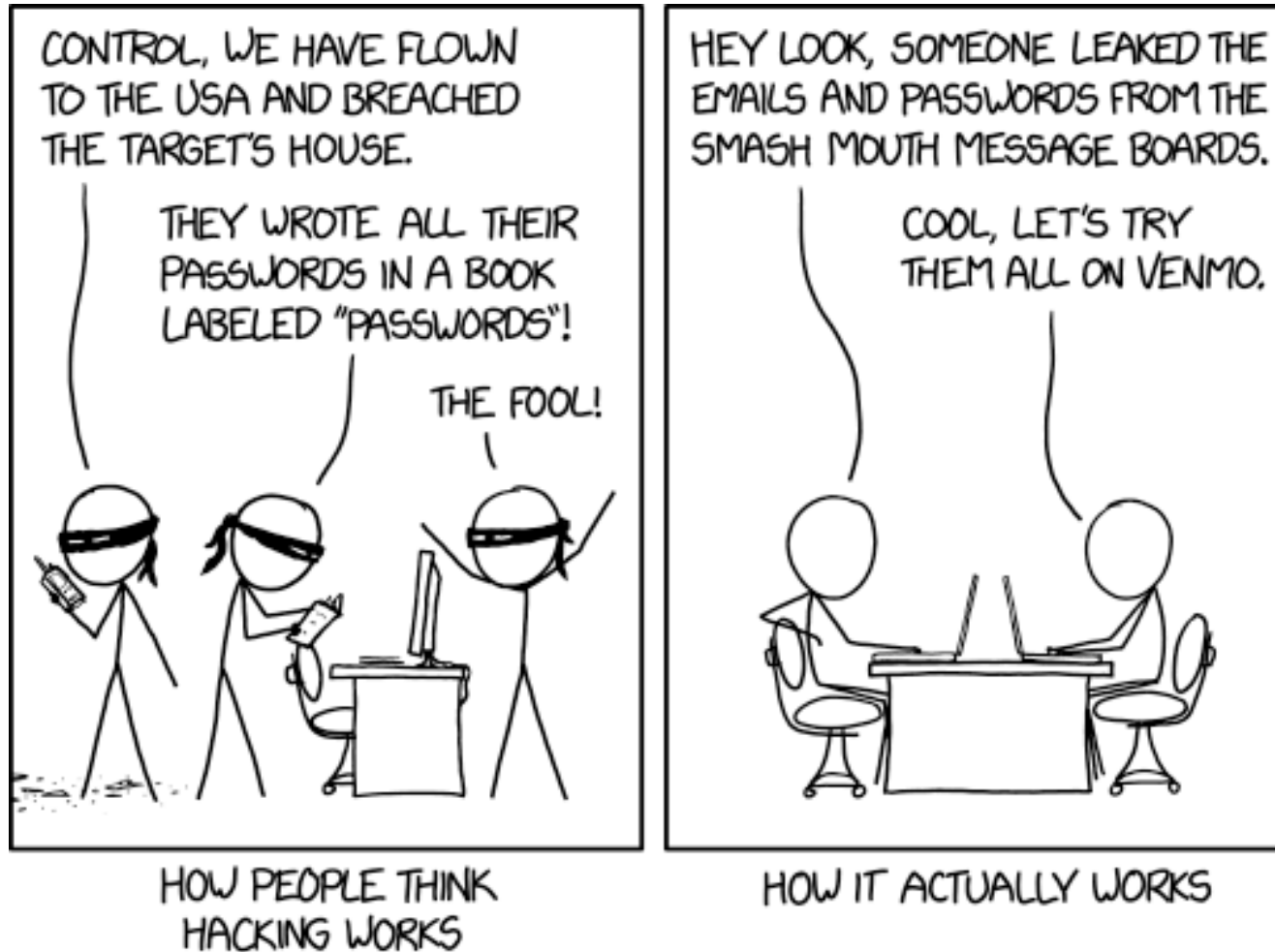
Updated by:

TechCommunityAPIAdmin

Share

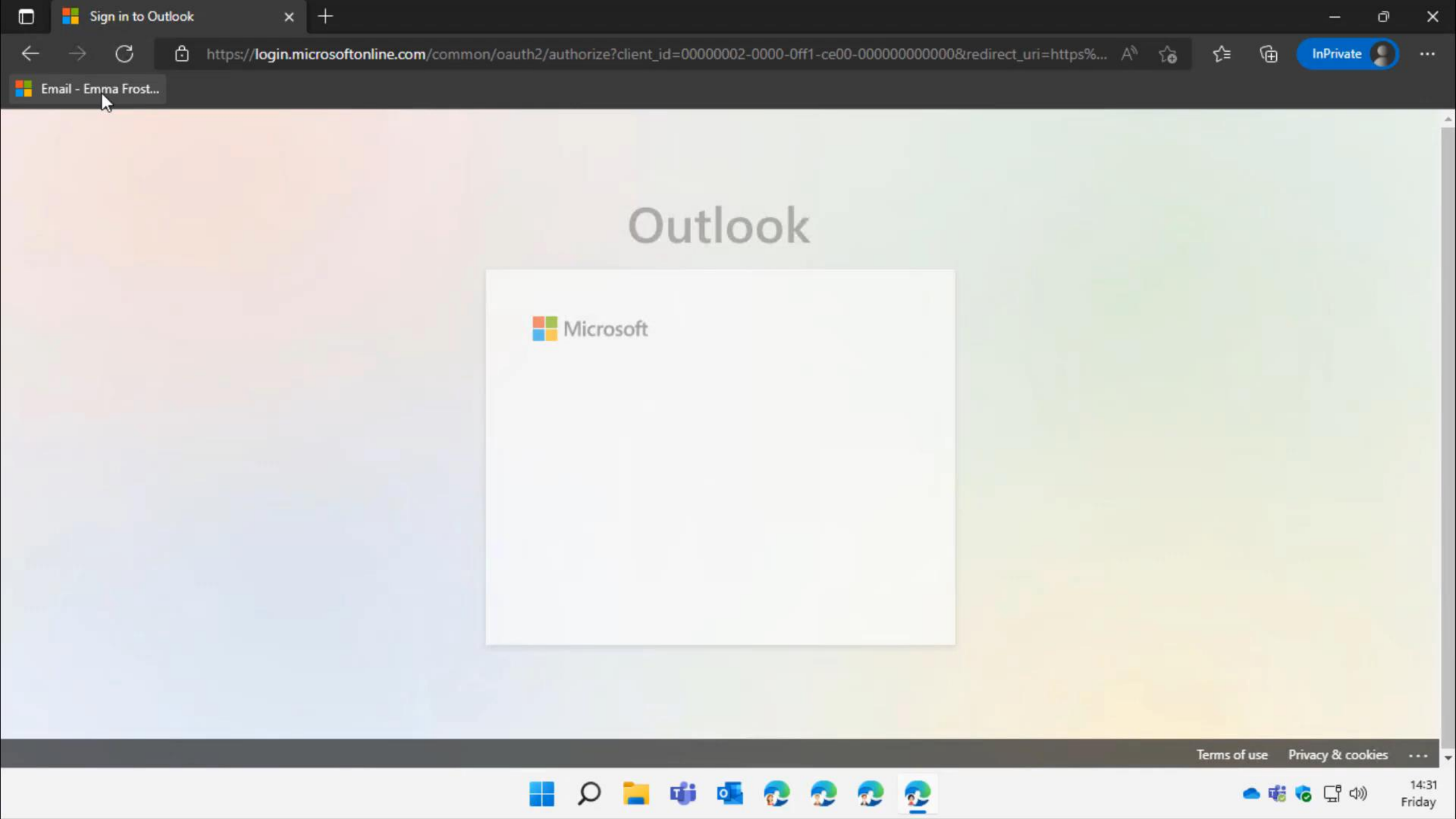


Passwortangriffe – Credential Stuffing

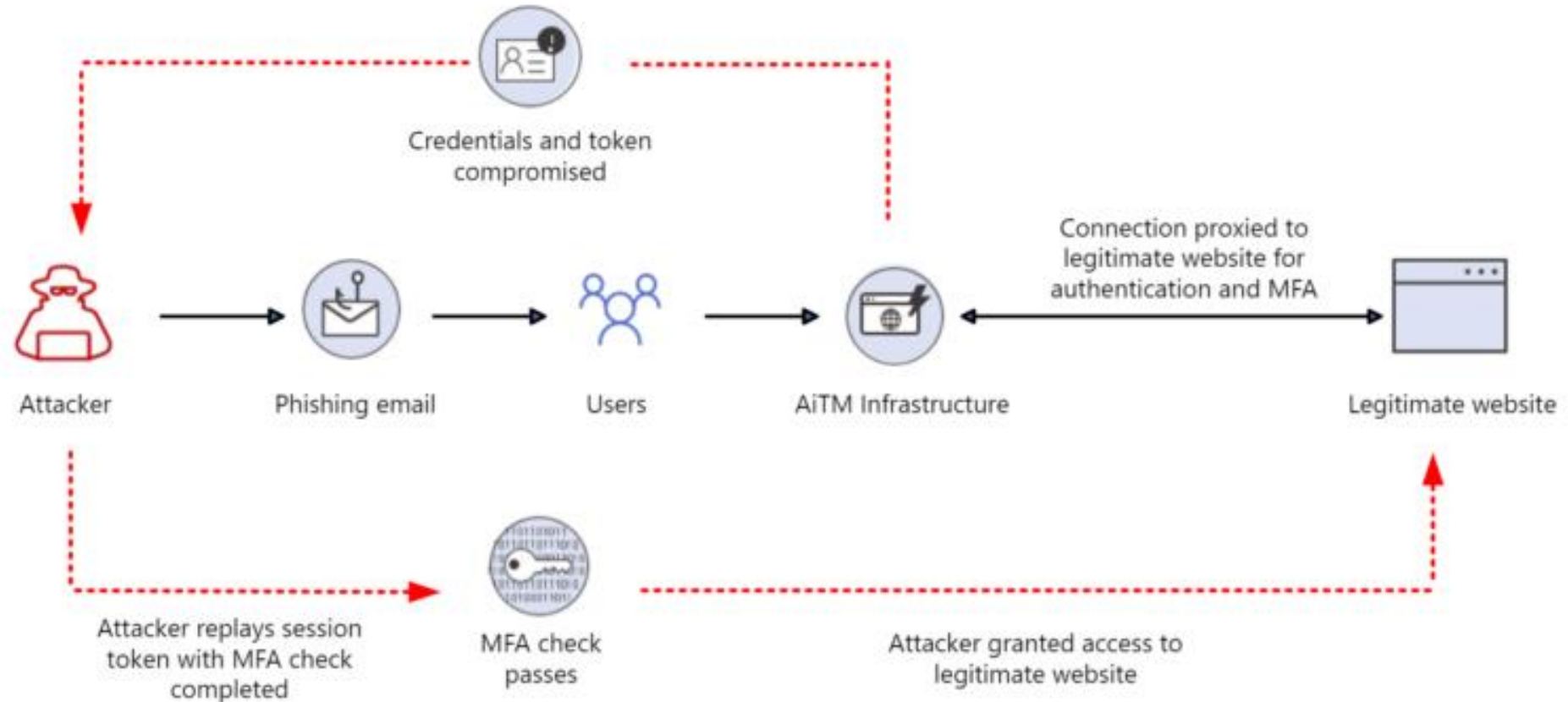


Starke Authentifizierung – Das Ende der Passwörter

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



Adversary-in-the-Middle (AitM) Phishing

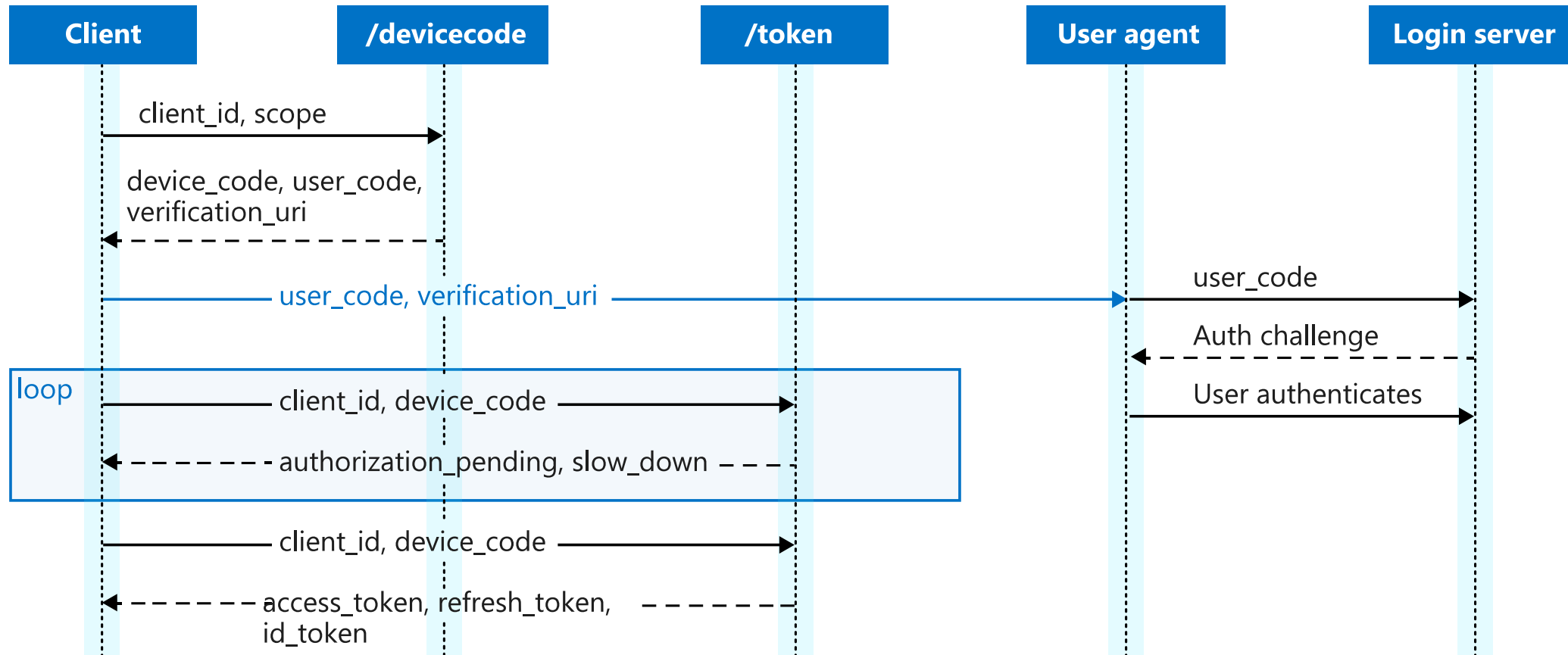


The new Phish in Town

Device Code Phishing und mehr



Device Code Flow



Demo

Device Code Sign-in Authentication Flow

This technique can be leveraged for phishing.

Device Code Phishing aus Opfersicht –

Linkziel: <https://microsoft.com/devicelogin>

▼ Favorites

Inbox 18

Sent Items

Drafts [3]

Deleted Items 2

▼ bob@theharvester.world

Inbox 18

Drafts [3]

Sent Items

Deleted Items 2

Archive

► Conversation History

Junk Email

Outbox

RSS Subscriptions

Search Folders

► Groups

All Unread By Date ▼ ↑

▼ Today

DevOps
Microsoft Security - Required ... 6:26 PM
Required Action Your device is

▼ Three Weeks Ago

Constant Contact
Let's Celebrate, It's Black Busi... 8/11/2021
Plus, don't miss your chance to

MyAnalytics
MyAnalytics | Wellbeing Edi... 8/9/2021
<https://myanalytics.microsoft.c

Constant Contact
Don't give up on online mar... 8/8/2021
See how easy we make it to

▼ Earlier this Month

Constant Contact

Microsoft Security - Required Action

D

DevOps <DevOps@mstfsec.onmicrosoft.com>
To bob

↩ Reply ↩ Reply All

Tu

Required Action

Your device is being logged out of Microsoft Office 365. Please use the following URL and device code to re-link your account.

Your code is: **ERDVDCNHH**

<https://microsoft.com/devicelogin>

Sincerely,
Microsoft Device Security Team

Microsoft Corporation | One Microsoft Way Redmond, WA 98052-6399

ACTION REQUIRED: Multi-Factor Authentication (MFA) Update

S

shark@
Thu 4/14/2022 12:52 PM
To: Minnow

Microsoft Authenticator Update Needed

Your Microsoft Authenticator token has expired. Please scan the QR code below to generate a new device code for your Microsoft Authenticator App.

The code will be emailed to you, and you should enter it at <https://login.microsoftonline.com/common/oauth2/deviceauth>

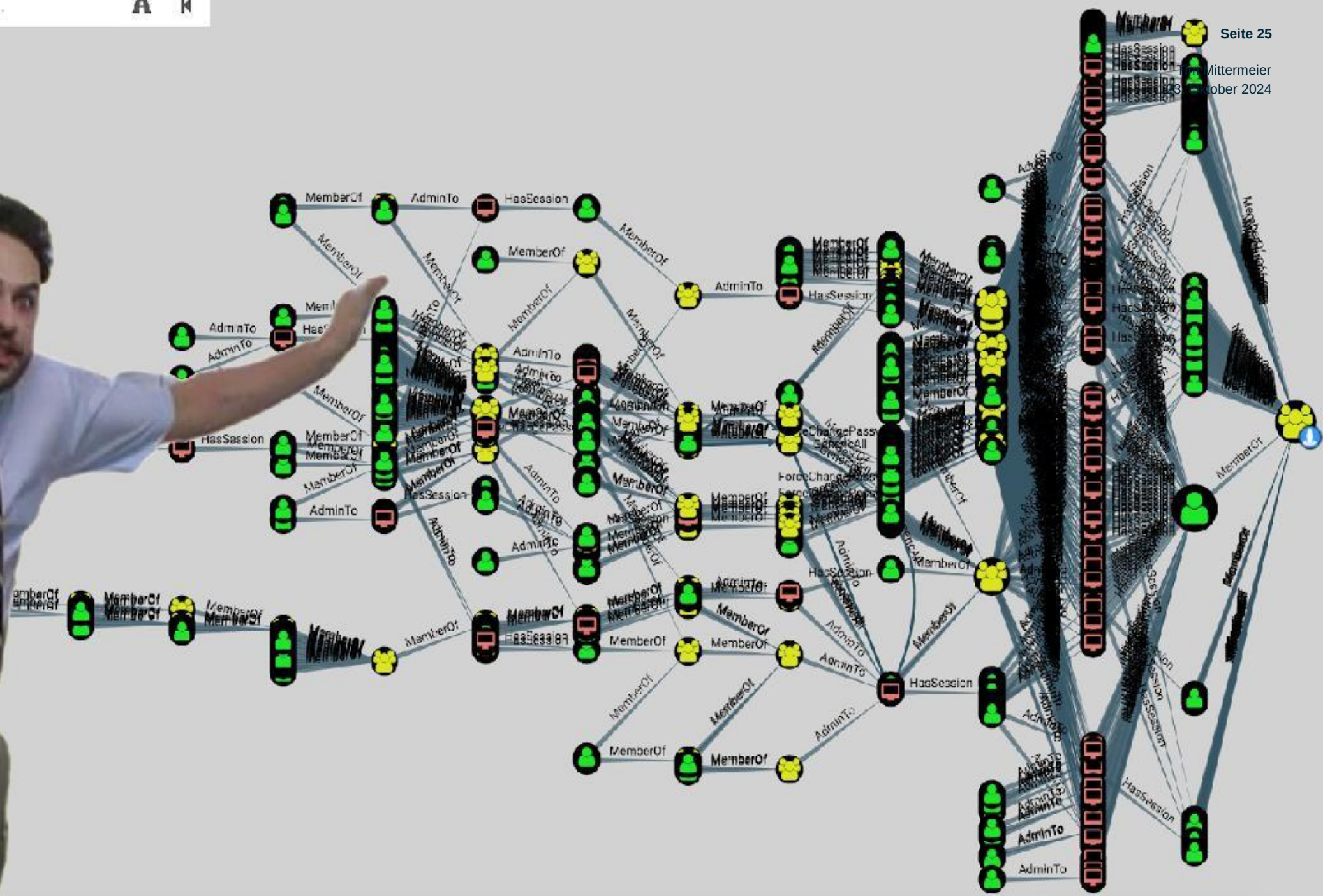


Angriffspfade Hybride Infrastrukturen

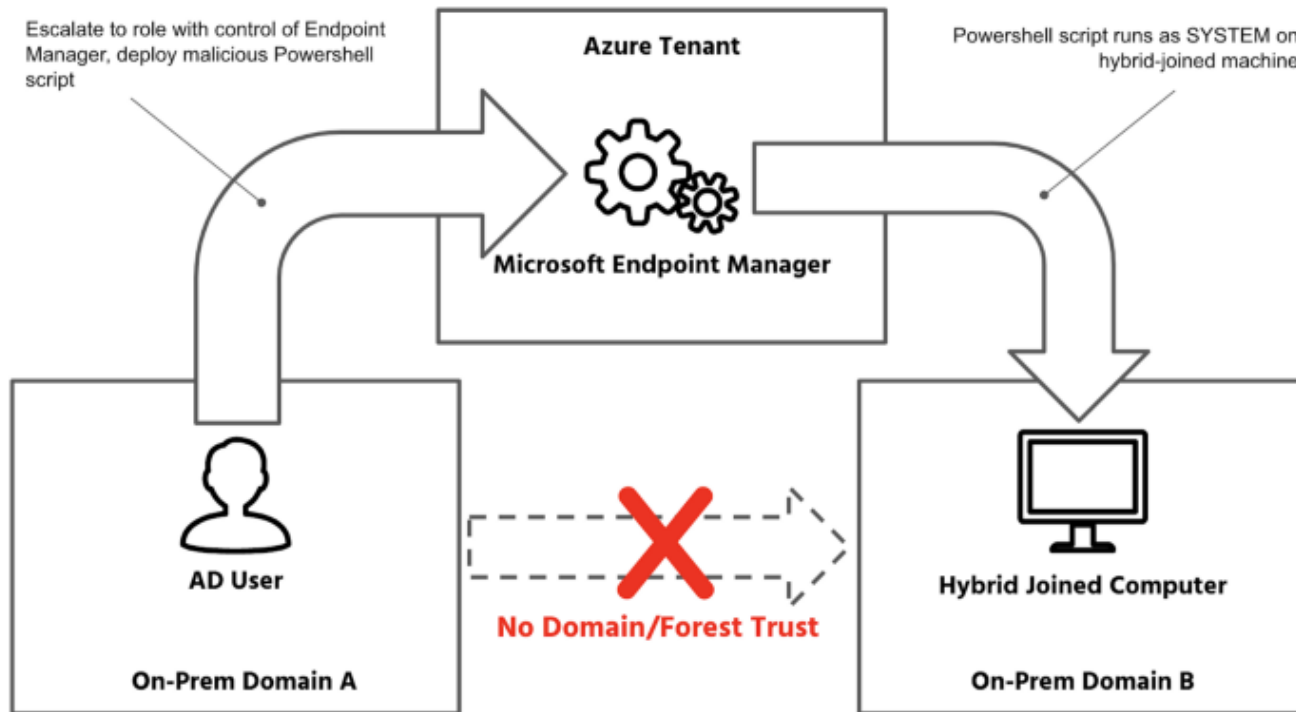




Start typing to search for a node...



Death from above – Cloud-managed Device zur OnPrem Administration



[Home](#) > [Devices](#) > [Windows | PowerShell scripts](#) >

Add Powershell script

✓ Basics 2 Script settings 3 Assignments 4 Review + add

Script location * ⓘ

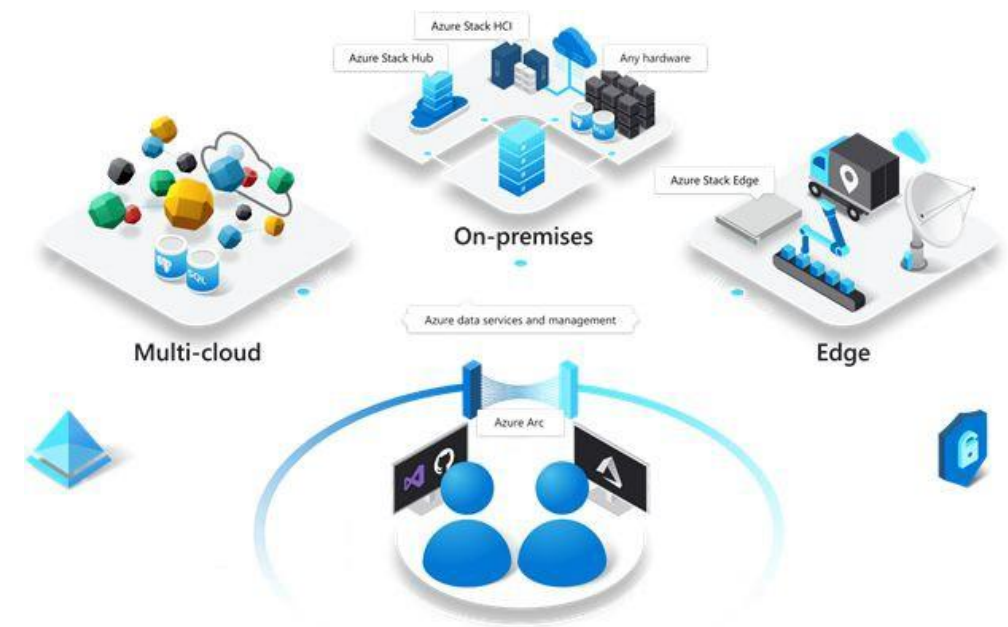
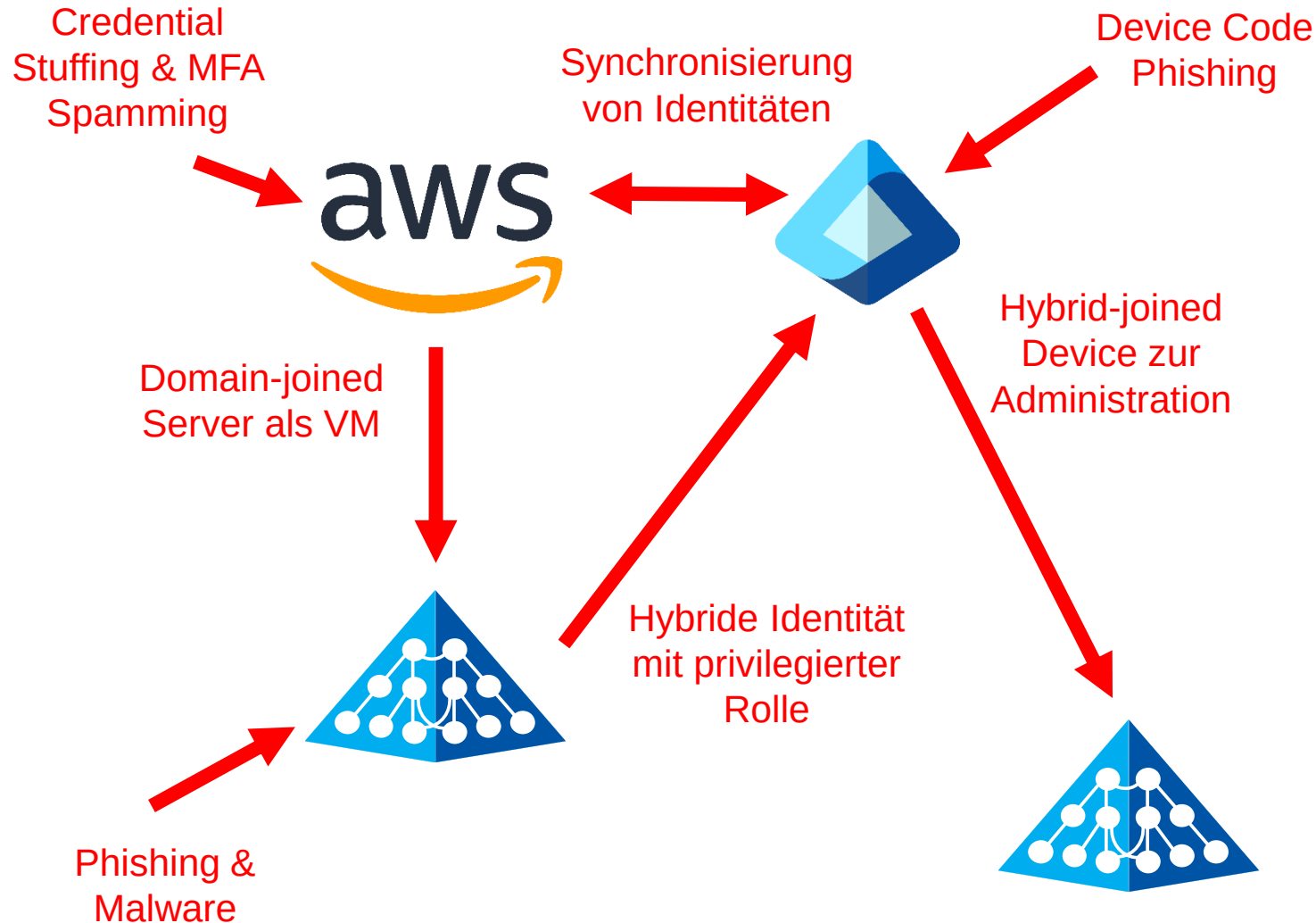
Run this script using the logged on credentials ⓘ Yes ☒ No ☐

Enforce script signature check ⓘ Yes ☐ No ☒

Run script in 64 bit PowerShell Host ⓘ Yes ☐ No ☒



Laterale Bewegung – Viele Wege führen zum Ziel



Penetrationstests

Planung & Durchführung



Planung, Durchführung und Auswertung einer technischen Sicherheitsanalyse

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

Clean-up

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

Schlussbericht

- Sofortmaßnahmen einleiten
- Befunde auswerten & priorisieren
- Maßnahmen planen

Diskussion

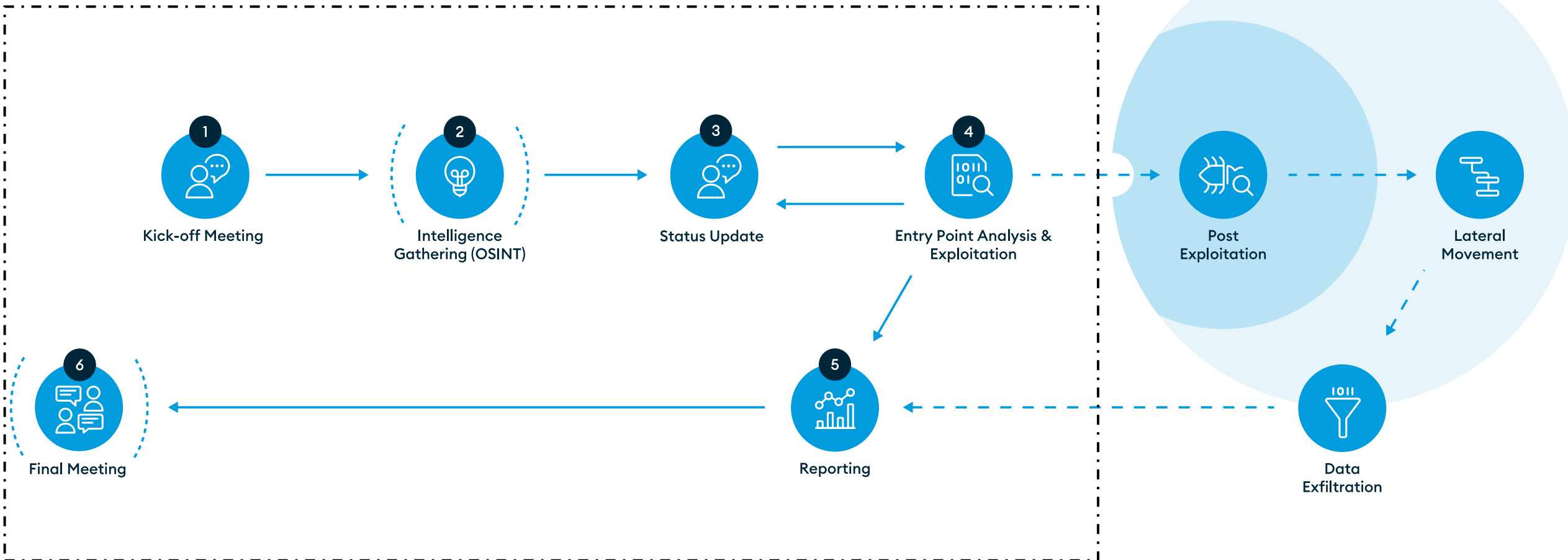
- Teilnehmerkreis festlegen
- Offene Fragen klären
- Empfehlungen zum weiteren Vorgehen

Maßnahmen

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



Technische Testmethode



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 sensibler 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 sensibler 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

ATT&CK Matrix for Enterprise

layout: side show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (5)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (5)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Data from Cloud Storage Object	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Container and Resource Discovery	Data from Configuration Repository (2)	Data from Information Repositories (3)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	Domain Trust Discovery	Data from Local System	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	File and Directory Discovery	Data from Network Shared Drive	Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Hide Artifacts (9)	Group Policy Discovery	Proxy (4)	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Hijack Execution Flow (11)	Network Service Scanning		Protocol Tunneling		Service Stop
				Modify	Valid	Impair Defenses (9)	Steal Web	Indicator Removal on Host (6)	Network Share Discovery		Remote Access		System Shutdown/Reboot
						Indirect Command Execution		Indirect Command Execution	Network Sniffing				
								Password Policy Discovery					

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/>

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

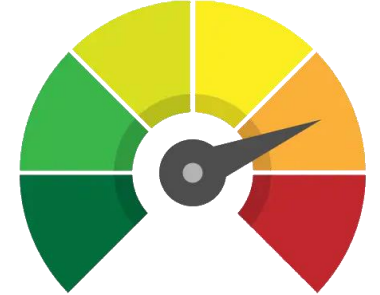
1	Introduction	3
1.1	Overview	3
1.2	Initial Situation and Audit Objectives	3
2	Executive Summary	4
2.1	Application Penetration Test – External REST API	4
2.2	Host Discovery and Network Segmentation Test	5
2.3	Conclusion	6
3	Approach	7
3.1	Methodology	7
3.2	Risk Assessment and Rating	7
3.3	Estimate of Risk Remediation Effort	9
3.4	Risk Categorisation by OSSTMM	9
3.5	Example Table "Risk and Measures"	10
3.6	Project Organization	10
3.7	Generic Process	11
3.8	Tasks and Schedule	11
4	Scope	12
4.1	Application Penetration Test – External REST API	12
4.2	Host Discovery and Network Segmentation	12
5	Risks and Measures	13
5.1	Application Penetration Test – External REST API	13
5.2	Host Discovery and Network Segmentation Test	16
6	Test Details	19
6.1	SQL Injection Vulnerability on Login Form	19
6.2	Password Policy	20
7	Appendix.....	22
7.1	RAV Calculation – Application Penetration Test – External REST API	22
7.2	Figures	23

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



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

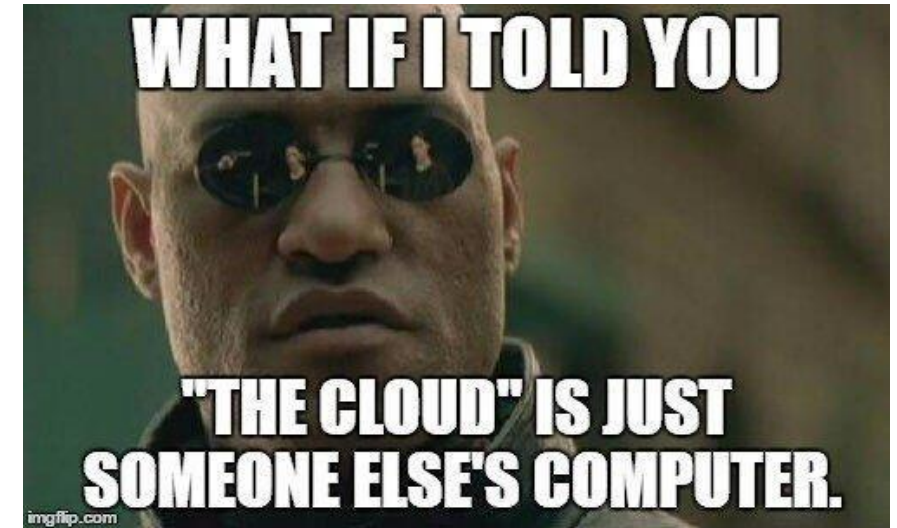


Zusammenfassung & Fazit

Wie schützen wir uns?



- ▶ 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](https://www.linkedin.com/company/oneconsult-ag)



[/OneconsultAG](https://twitter.com/OneconsultAG)



[/oneconsult](https://www.youtube.com/channel/UC...)



Monatliche Cyber Security News abonnieren:
[Oneconsult Newsletter](#)

