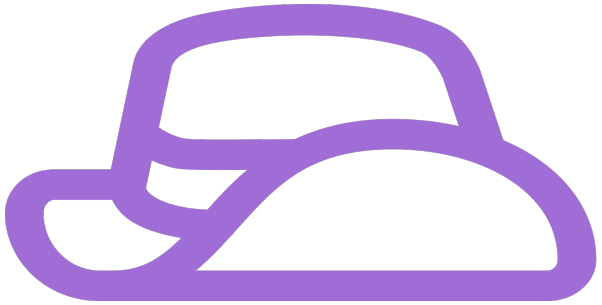
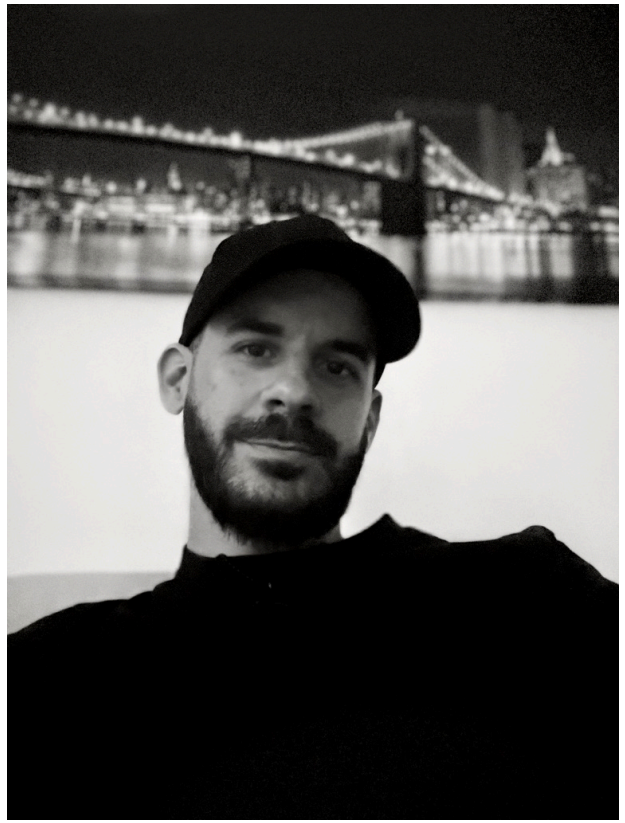
# **Massenhacks**
# Cyberangriffe in Serie – live

purple22 GmbH



Leetcore Cybersecurity GmbH

# Vorstellung Speaker - 2



## Alexander Königstein

Founder & Software Developer

bei **Leetcore Cybersecurity GmbH**

**Ethical Hacking:**

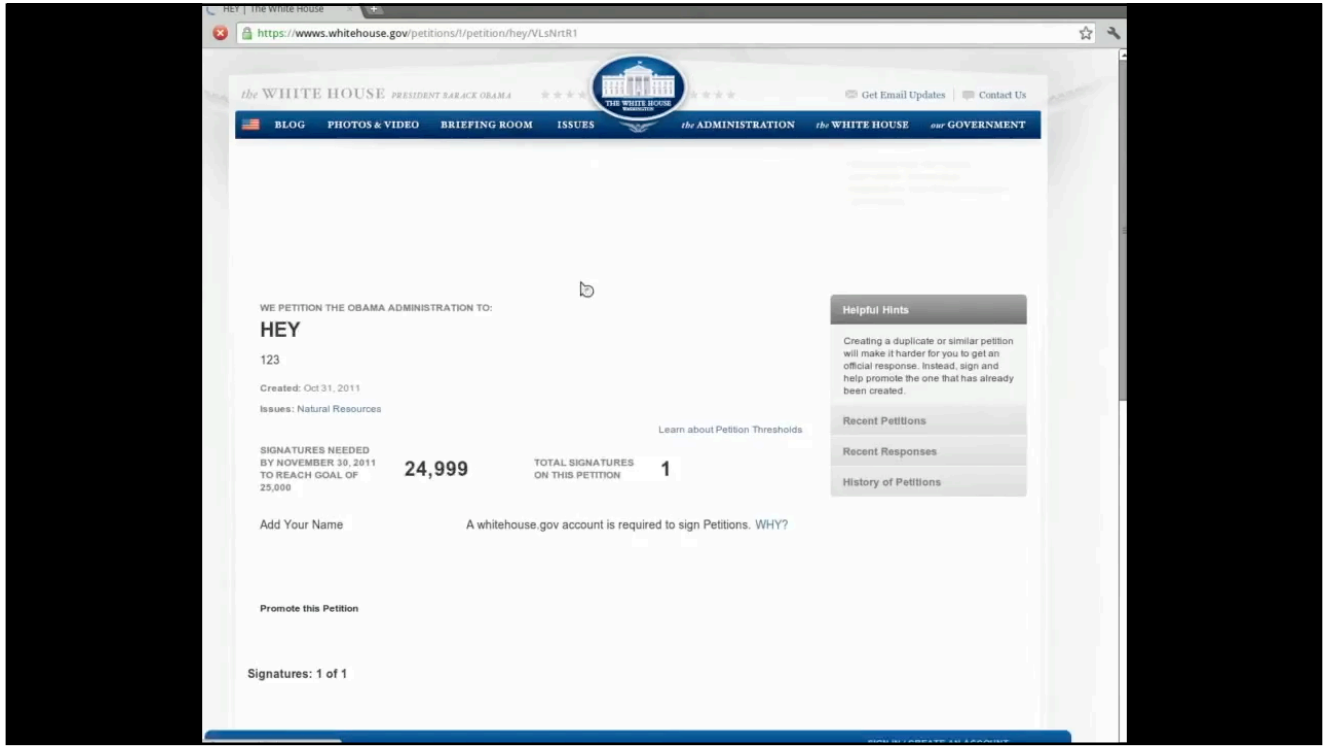
- Microsoft und Apple Security Hall of Fame
- Über 100+ kritische Sicherheitslücken ans BSI gemeldet
- „Hack The Box“ Top 500 weltweit

# Ethik Disclaimer

- Aufklärung und Forschung
- „Was-wäre-wenn“ Angriffe simulieren, um sie zu verstehen
- Perspektive des Angreifers einnehmen – ohne Täter zu werden
- Schwachstellen verantwortungsvoll an Hersteller/Betreiber weitergeben
- IT-Systeme respektvoll behandeln – keine Ausnutzen zum Schaden
- Menschen und Privatsphäre schützen
- Sicherheitslücken sichtbar machen, damit andere sie schließen können

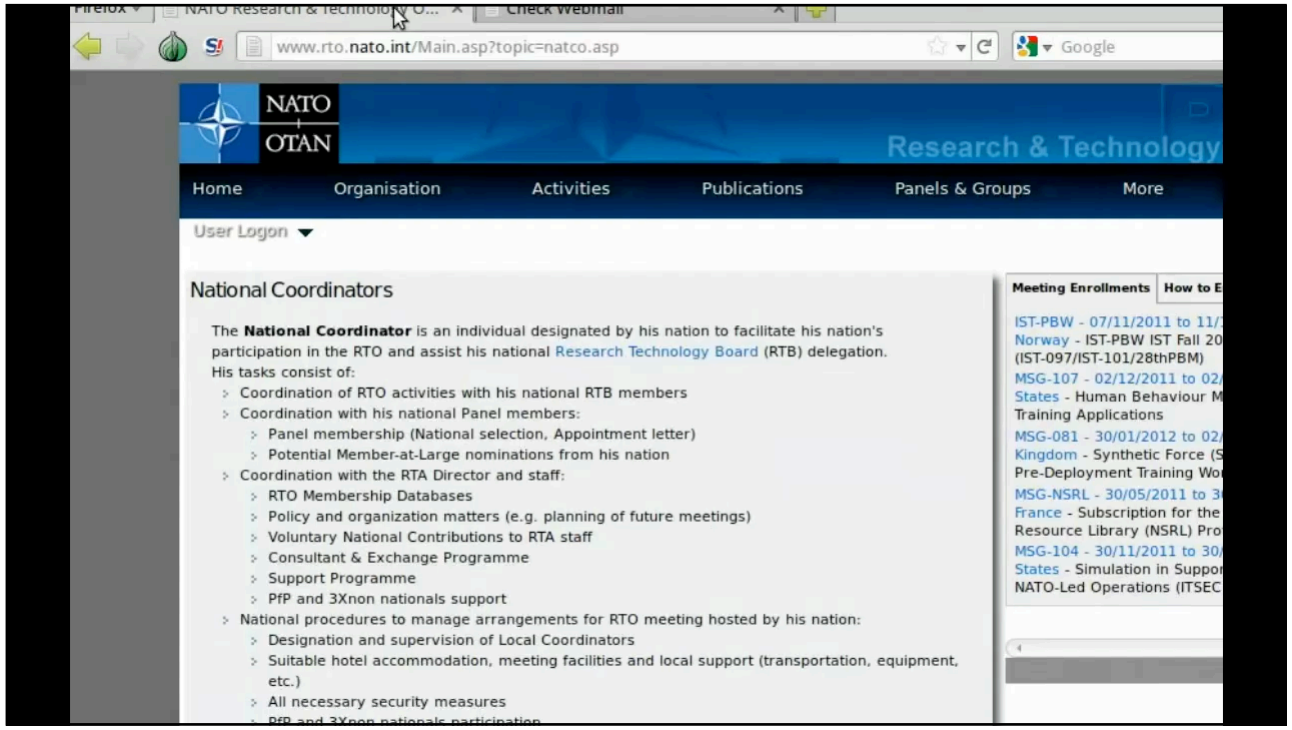
# White House Petition Platform

- Responsible Disclosure
- **Art der Lücke:** Persistent Cross-Site-Scripting (XSS)
- **Bedingung:** Nur beim ersten Anmelden auslösbar
- **Auswirkung:** Eingeschleuster JavaScript-Code lief bei jeder Petition
- **Reichweite:** Rund 250.000 betroffene Nutzer



# NATO Research & Technology Webmailer

- **Art der Lücke:** Local File Inclusion (LFI)
- LFI über URL-Parameter (?topic=…)
- Manipulation des Parameters erlaubte Zugriff auf interne Dateipfade
- **Beispiel:** ?topic=/etc/passwd -> lokale Systemdatei erreichbar



# Öffentliche Verwaltung und ProxyShell

- **Was:** Ketten-Exploit („ProxyShell“) gegen on-premises Exchange -> RCE über OWA/ Autodiscover.
- RCE = **Remote Code Execution** (Code aus der Ferne ausführen) Ferne = Internet
- **Betroffene Bereiche**: viele Domains öffentlicher Stellen - Länder, Landkreise, Städte und Behörden.
- Domains aller Bundesländer, über 200 Landkreise, etlicher Bundesbehörden und über 2.000 Städte, Gemeinden, Orte, …
- 59.000 Hostnames

Quelle: https://www.heise.de/news/Verwundbare-Exchange-Server-der-oeffentlichen-Verwaltung-6320504.html

## Verwundbare Exchange-Server der öffentlichen Verwaltung

20 Exchange-Server in öffentlicher Hand waren für eine Sicherheitslücke anfällig. Kriminelle hätten die Kontrolle übernehmen können.

198



(Bild: VideoFlow/Shutterstock.com)

**14.01.2022, 06:00 Uhr** **Lesezeit: 7 Min.** | **c't Magazin**

*Von Alexander Königstein*

# Öffentliche Verwaltung

- **Endpunkt:** https://autodiscover.ihredomain.de/
- **Kettenschwachstelle**: CVE-2021-34473, CVE-2021-34523, CVE-2021-31207
- „Unser Testskript filterte daraus 460 öffentlich erreichbare Exchange-Server-Webapps, die am Pfad /owa/ zu erkennen sind, und analysierte sie, wonach 20 Server angreifbar waren.“
- **Konsequenzen:** Web-Shells, persistenter Zugriff, Daten-/Credential-Diebstahl.

Quelle: https://www.heise.de/news/Verwundbare-Exchange-Server-der-oeffentlichen-Verwaltung-6320504.html

## Verwundbare Exchange-Server der öffentlichen Verwaltung

20 Exchange-Server in öffentlicher Hand waren für eine Sicherheitslücke anfällig. Kriminelle hätten die Kontrolle übernehmen können.

198

(Bild: VideoFlow/Shutterstock.com)

**14.01.2022, 06:00 Uhr** **Lesezeit: 7 Min.** | **c't Magazin**

*Von Alexander Königstein*

# Öffentliche Verwaltung bereits gehackt

- Der Mailserver mindestens einer Verwaltung wurde bereits gehackt.
- Woher wissen wir das?
- Die Angreifer antworten auf meine E-Mail, die ich an die Verwaltung geschickt habe und zitieren meine Nachricht
- „Bitte stellen Sie sicher, dass alle Dokumentationen über den nächsten Link gefunden werden können.“
- Ich sollte doch bitte diesen Trojaner ausführen! ;)

ANTWORT VOM UNGEBETENEN BESUCH

Ein paar Wochen, nachdem wir den Betreiber eines Exchange-Servers mit offener Sicherheitslücke per E-Mail gewarnt hatten, erhielten wir eine ungewöhnliche Antwort: "Guten Tag! Bitte stellen Sie sicher, dass alle Dokumentationen über den nächsten Link gefunden werden können." – der Link führte auf eine Website, die nichts mit der betroffenen Stadtverwaltung oder uns zu tun hatte. Die E-Mail selbst kam nicht von der Stadtverwaltung, sondern wurde über eine gehackte Wordpress-Website versendet, nur im Absendername stand die Stadt. Als vorangegangene Konversation zitierte die E-Mail unsere Warnung zum verwundbaren Exchange-Server. Wie die Stadtverwaltung uns mitteilte, wurde unsere E-Mail bei einem Befall des Mailservers kopiert. Wir können uns vorstellen, durch welche Sicherheitslücke das passiert ist. Man arbeite daran, dass dies in Zukunft nicht mehr vorkommt.

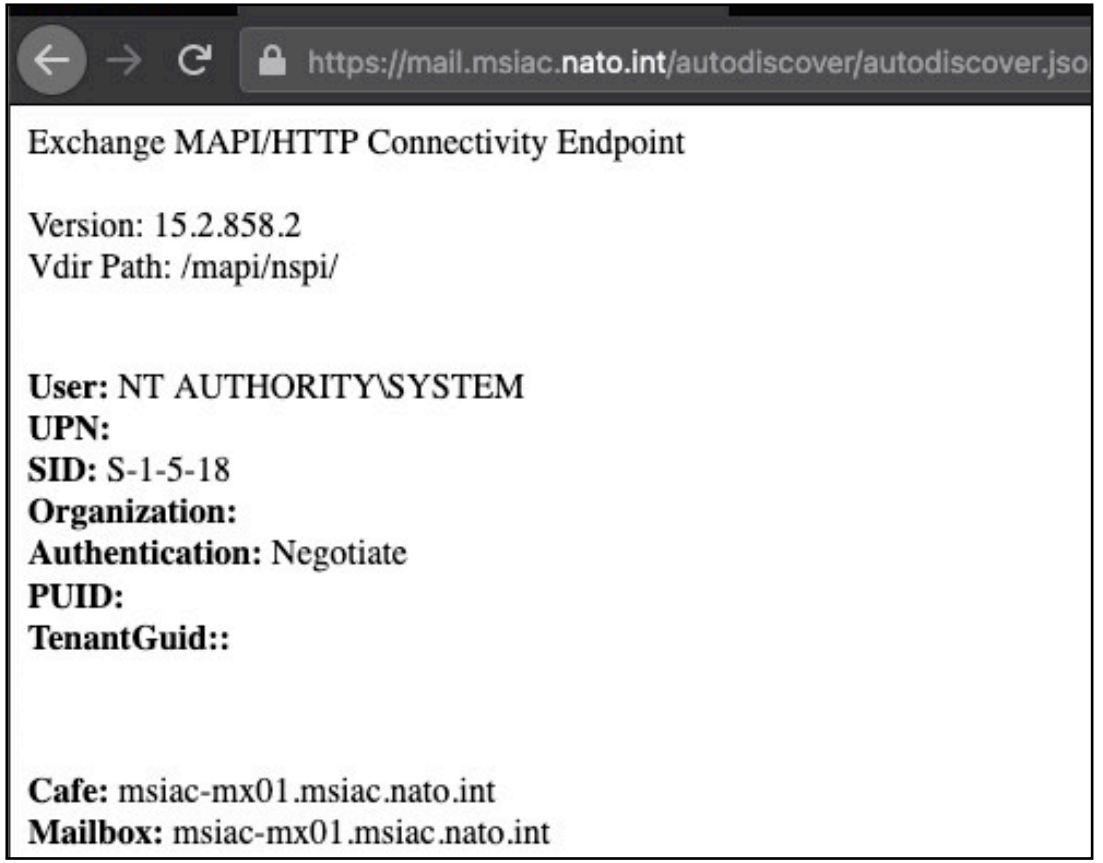
# NATO und Proxyshell

- Mailserver der Munitions Safety Information Analysis Center (MSIAC) könnte über die Exchange-Schwachstelle kompromittiert werden.

Version: 15.2.858.2

User: NT Authority\System

Mailbox: msiac-mx01.msiac.nato.int.



# Massenhacks - Ablauf

- **Zielsetzung:** Fokus auf ganze Branchen – z. B. Energiesektor, Rüstungsindustrie, kritische Infrastrukturen
- **Informationssammlung:** Öffentliche Datenleaks, Unternehmenswebseiten, Subdomains, erreichbare Dienste, …
- **Automatisierte Angriffe:** Viele Systeme gleichzeitig scannen / testen -> schnelle Reichweite / gezielte Exploits
- **Monitoring:** Systeme beobachten, auf Schwachstellen warten
- **Exploit-Bereitschaft:** Angreifer halten ihre Infrastruktur bereit, um bei Auftreten einer Schwachstelle **Zugriff** auf Systeme zu erlangen
- **Netzwerk- und Systemausbreitung:** Lateral Movement, interne Rechteausweitung
- **Monetarisierung & Motivation:** Spionage, Datenklau, Verkauf von Informationen, Ransomware, Mining von Kryptowährungen

# Listen Listen Listen

Öffentliche Quellen: Wikipedia, Vereins- und Verbandslisten, öffentliche Verzeichnisse

**KRITIS-Sektoren** (kritische Infrastrukturen):

- Energie, Wasser, Gesundheit, Transport & Verkehr
- Digitale Infrastruktur, Finanzwesen, Sozialversicherung
- Weltraum, Staat, Ernährung, Entsorgung
- Post & Kurier, Chemie, Verarbeitendes Gewerbe
- Digitale Dienste, Forschung

ChannelPartner

Themen ChannelPartner Events

**Rangliste der 25 größten Systemhäuser Deutschlands 2025**

| Rang | Unternehmen | 2024 Inlandsumsatz (in Millionen Euro) | 2023 Inlandsumsatz (in Millionen Euro) |
|---|---|---|---|
| 1 | Bechtle AG | 3.722,0 | 3.996,0 |
| 2 | Computacenter AG & Co. oHG | 3.282,0 | 3.301,0 |
| 3 | T-Systems International GmbH 3) | 3.000,0 | 2.950,0 |
| 4 | NTT Data 3) | 2.300,0 | 2.380,0 |
| 5 | SoftwareOne Deutschland GmbH | 2.237,2 | 2.084,2 |

# Praxisbeispiel - Informationssammlung

- IHK Verzeichnis von Unternehmen im Saarland
- Übersicht über Firmen-Domains erstellen - mit Google
- ZF, Saarstahl, Dillinger Hütte, Bosch, …
- **Wir präsentieren nur öffentlich erreichbare Informationen!**

MENÜ | SUCHE | A-Z

IHK Saarland

## DIE 50 GRÖSSTEN PRIVATWIRTSCHAFTLICHEN UNTERNEHMEN DER SAARWIRTSCHAFT

*(bezogen auf die Anzahl der Beschäftigten im Saarland)*

Stand: August 2025

| | Betrieb | Beschäftigtenzahl im Saarland |
|---|---|---|
| 1 | ZF Friedrichshafen AG | 9.000 |
| 2 | Saarstahl Konzern | 4.300 |
| 3 | AG der Dillinger Hüttenwerke | 3.600 |
| 4 | Robert Bosch GmbH | 2.800 |
| 5 | Ford Werke GmbH | 2.300 |
| 6 | Schaeffler Technologies GmbH & Co. KG | 2.000 |
| 7 | Fresenius Medical Care | 2.000 |
| 8 | Villeroy & Boch AG | 1.800 |
| 9 | Globus Holding GmbH & Co. KG | 1.800 |
| 10 | Festo AG & Co. KG | 1.600 |
| 11 | HYDAC International GmbH | 1.600 |
| 12 | Original Wagner Pizza GmbH | 1.600 |
| 13 | Hager Electro GmbH | 1.500 |
| 14 | Ludwig Schokolade GmbH & Co. KG | 1.100 |
| 15 | Gebrüder Meiser GmbH | 1.100 |

# Analyse öffentlich erreichbarer IT-Systeme

**Quellen und Methoden:**

- Öffentliche Zertifikate
- Suchmaschinen (Google, Wayback Machine)
- Reverse DNS -> Hostnamen von IP herausfinden

**Ergebnisse der Analyse:**

- 12.200 Hostnames insgesamt
- 4.291 öffentlich erreichbare Systeme
- Erreichbare Dienste analysieren (nur Websites)

- zf.com
- saarstahl.com
- ford.de
- dillinger.de
- bosch.de
- festo.com
- schaeffler.de
- freseniusmedicalcare.com
- original-wagner.de
- hydac.com
- villeroy-boch.de
- hager.com
- globus.de
- unimed.de
- gross-bau.de
- karlsberg.de
- orbis.de
- klima-becker.de
- woll-maschinenbau.com
- matfoundrygroup.com

# IT-Infrastruktur - 4.291 Systeme

| Hostname | IP-Adresse | Organisation |
|---|---|---|
| login.stg.hager.com | 65.9.66.87 | Amazon.com,Inc.(AMAZO-4) |
| guest-confirm.hager.com | 194.99.48.55 | HagerElectroGmbH&Co.KG |
| postman1.villeroy-boch.de | 193.169.73.20 | Villeroy&BochAG |
| carhi-gp01.freseniusmedicalcare.com | 207.219.215.81 | TELUSCommunicationsInc.(TACE) |
| nsb01.fe.bosch.de | 194.39.219.2 | RobertBoschGesellschaftmitBeschraenkterHaftung |

Angreifer analysieren öffentlich erreichbare Server, um mögliche Zugänge zu internen Netzwerken zu erkennen.

**Diese Beispiele zeigen nur, wie sich die IT-Infrastruktur über öffentliche Daten analysieren lässt.**

- zf.com
- saarstahl.com
- ford.de
- dillinger.de
- bosch.de
- festo.com
- schaeffler.de
- freseniusmedicalcare.com
- original-wagner.de
- hydac.com
- villeroy-boch.de
- hager.com
- michelin.de
- globus.de
- unimed.de

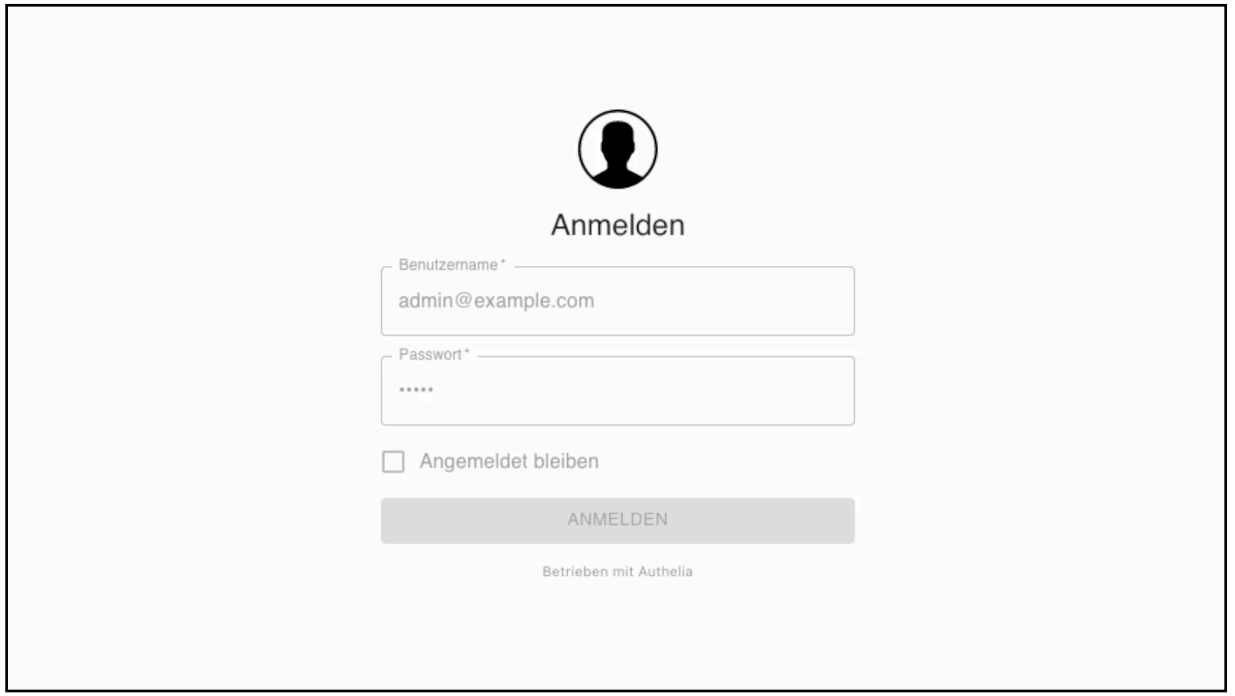
# Passwortleaks - Sensibilisierung

- Sammlung und Filterung von Passwortleaks **basierend auf Unternehmensdomains** (nur öffentlich zugänglich)
- **Analysierte Daten:** ca. 32.000 Datensätze im Format:
  E-Mail:Passwort
- **Strukturanalyse:** E-Mail in Vorname.Nachname -> Raten von Benutzernamen!
- **Disclaimer:** Awareness für Passwortsicherheit, kein Zugriff auf gelistete Zugangsdaten!

- k****@ford.de:kimberley
- jr*******@dillinger.de:Huette
- dieter.******@bosch.de:*****baum
- ***.mueller@hager.com:****nik
- ****.theo@villeroy-boch.de:vb061**
- mit*****@thyssenkrupp.com:FV3BN***
- shr*********@sap.com:**ena123
- *****baptista@sap.com:Jas***2001
- colleen******@infor.com:Hawaii62***
- ***.dominici@treofan.com:****1fcf
- jen*****@infor.com:disney

# Risiken kompromittierter Accounts

- Eingehende E-Mails könnten **mitgelesen** werden
- Angreifer könnten **auf E-Mails antworten** und Trojaner verteilen
- Unternehmen A selbst ist sicher, kommuniziert jedoch mit Unternehmen B, das gehackt wurde
- **Zugriff auf verbundene Dienste:** Webseiten, VPN, interne Applikationen, weitere Services



# Versionsnummer <> Proof of Concept

**Versionsnummer:**

- Schwachstellenscans basierend auf Versionsnummer mit CVE-Datenbank (CVE-2021-34473)
- Ergebnisse sind **theoretisch**: Sicherheitslücken wurden bereits gepatcht (durch Backports)
- **Backports**: Übernahme einer Sicherheitskorrektur in eine alte Softwareversion - die Versionsnummer bleibt gleich!
- Hohe Rate an **False Positives** – nicht jedes gefundene System ist tatsächlich verwundbar

**Proof of Concept:**

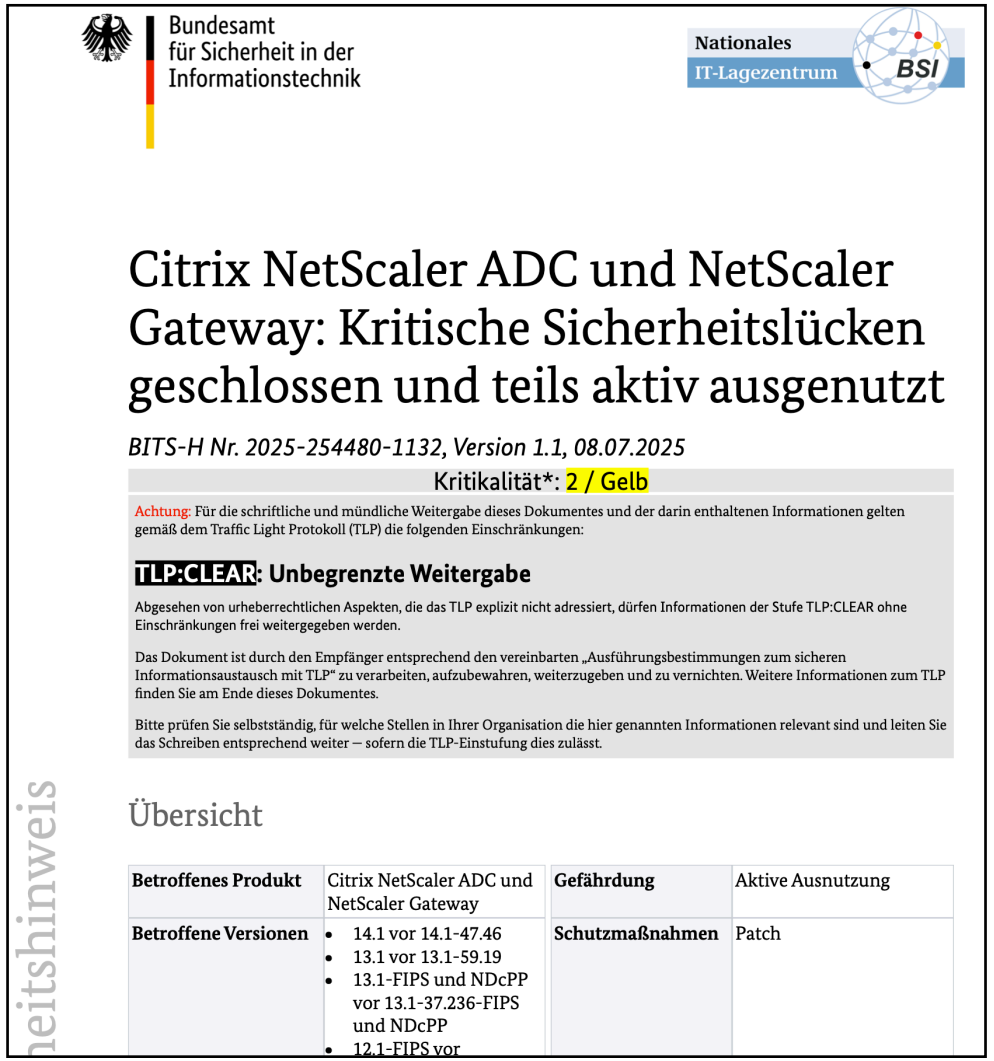
- Realistische Verwundbarkeit
- Nutzung von bekannten Exploits zur Verifikation
- Testet, ob eine Schwachstelle **praktisch ausnutzbar** ist
- Sicherheitslücke nachvollziehbar erkennen, nicht missbrauchen
- Liefert **kaum False Positives** – zeigt tatsächliche Risiken

# Realistische Angriffe

- Citrix NetScaler ADC & NetScaler Gateway
- Kritische Sicherheitslücke wurde gepacht - wurde aber bereits aktiv ausgenutzt

„Aufgrund der Medienberichte zu Ausnutzungen der kritischen Schwachstelle CVE-2025-5777, die bereits seit Mitte Juni ausgenutzt werden soll, sollten Betreiber ihre NetScaler auf eine mögliche Kompromittierung mit vorhandenen Indikatoren prüfen, auch dann, wenn zeitnah gepatcht wurde.“

Quelle: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2025/2025-254480-1032.html



Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

Citrix NetScaler ADC und NetScaler Gateway: Kritische Sicherheitslücken geschlossen und teils aktiv ausgenutzt

*BITS-H Nr. 2025-254480-1132, Version 1.1, 08.07.2025*

Kritikalität*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

**TLP:CLEAR: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

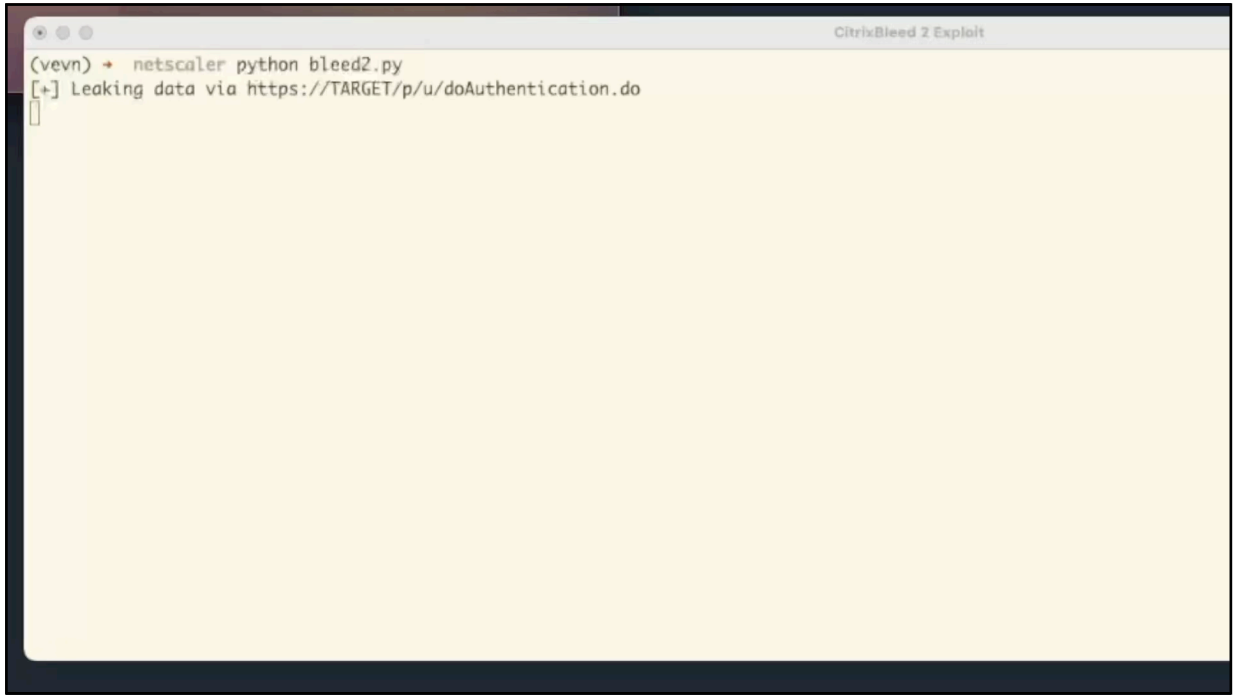
Bitte prüfen Sie selbstständig, für welche Stellen in Ihrer Organisation die hier genannten Informationen relevant sind und leiten Sie das Schreiben entsprechend weiter – sofern die TLP-Einstufung dies zulässt.

Übersicht

| | | | |
|---|---|---|---|
| **Betroffenes Produkt** | Citrix NetScaler ADC und NetScaler Gateway | **Gefährdung** | Aktive Ausnutzung |
| **Betroffene Versionen** | • 14.1 vor 14.1-47.46<br>• 13.1 vor 13.1-59.19<br>• 13.1-FIPS und NDcPP vor 13.1-37.236-FIPS und NDcPP<br>• 12.1-FIPS vor | **Schutzmaßnahmen** | Patch |

# Citrix NetScaler ADC & NetScaler Gateway

- Memory Disclosure Vulnerability
- Schwachstelle am Login-Endpunkt: /p/u/doAuthentication.do
- Angreifer können den **Arbeitsspeicher des Servers mitlesen** und finden dort zum Beispiel die Session-IDs von gerade eingeloggten Mitarbeitern
- Diese Session-ID kann ein Angreifer mitlesen und kopieren. **Danach kann er sich als Mitarbeiter einloggen!**

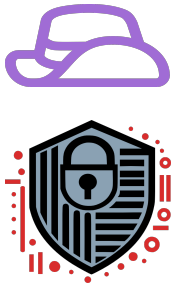



Quelle: https://horizon3.ai/attack-research/attack-blogs/cve-2025-5777-citrixbleed-2-write-up-maybe/

# Wettrennen gegen die Zeit

- Öffentlicher Patch kann Angreifer zu schnellerem Exploit motivieren
- Zeitnahes Patchen ist entscheidend – **kann aber trotzdem zu spät sein**
- **Zero-Day-Schwachstellen:** Keine Patches verfügbar, Systeme sind sofort anfällig
- **Automatisierte Angriffe:** Nach Patch-Veröffentlichung können Exploit-Skripte innerhalb von Stunden online sein
- Systeme sollten regelmäßig geprüft werden, ob sie bereits kompromittiert wurden

# Praxisbeispiel - NetScaler Gateway/AAA



- https://aad.**zf.com**, NetScaler AAA
- https://ag-mfa.emea.**zf.com**, NetScaler AAA
- https://jumphost.access-emea.**sap.com**, NetScaler AAA
- https://cag.**diehl.com**, NetScaler Gateway
- https://gateway.ast.**hoermann.de**, NetScaler Gateway

**Disclaimer: Wir zeigen, welche Systeme aus unserem Beispiel von bekannten Schwachstellen betroffen sein könnten!**

# Besuchen Sie uns gerne an unserem Stand

Purple22 & Leetcore Cybersecurity

- Stand: 56
- Sector: Cybersecurity


**Live-Demo am Stand**

Danke für Ihre Aufmerksamkeit