Besuch von Akira

Admin-Stammtisch 11/2024

Prof. Dr. Peter Tröger
Berliner Hochschule für Technik
HRZ-Leiter (2021 - 2024)

BHT
Berliner Hochschule für Technik

Studiere Zukunft

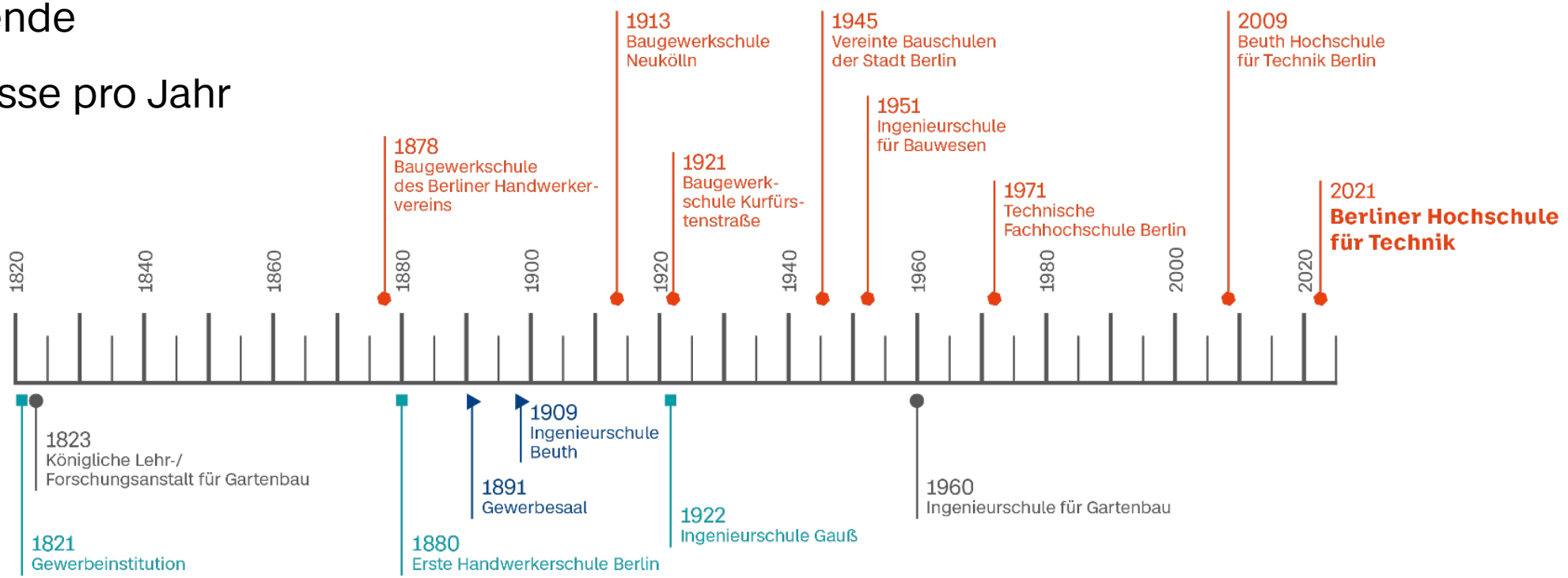
Berliner Hochschule für Technik

8 Fachbereiche

Ca 13.000 Studierende

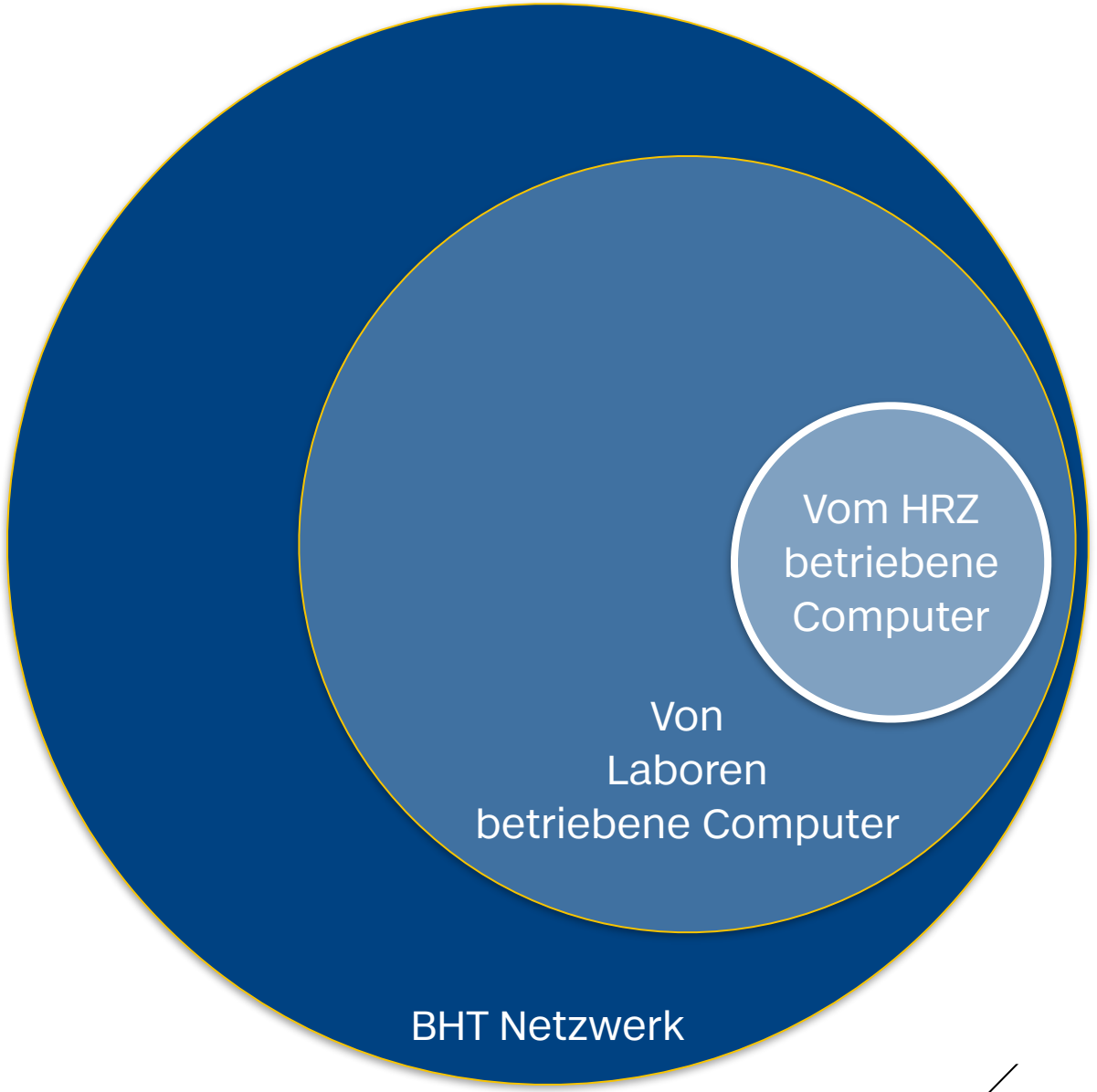
Ca. 840 Mitarbeitende

Ca. 1.000 Abschlüsse pro Jahr



BHT Hochschulrechenzentrum

HRZ Laptops	ca. 550
HRZ Server	ca. 300
AD Accounts	ca. 18.000
Physische Netzwerkgeräte	ca. 800
Standorte	5
HRZ Personal (Wir haben offene Stellen!)	11



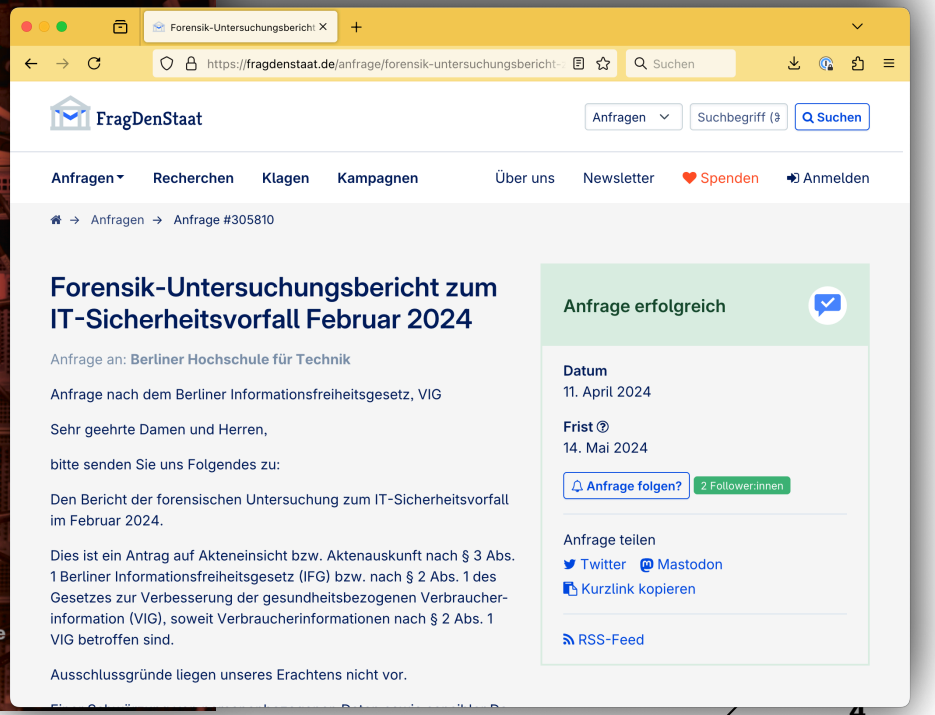
Hack der BHT (02/2024)

Jeder kennt das Problem,
wenige haben es selbst erlebt

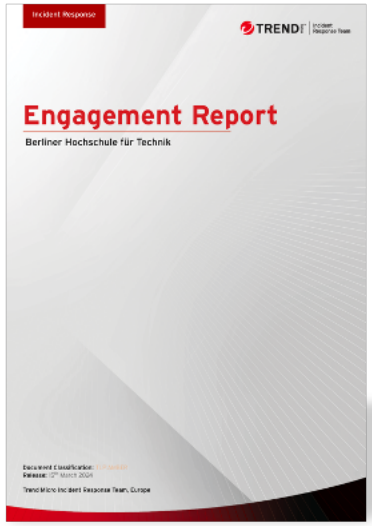
Presse zu diversen gehackten Hochschulen in 2024

Verzweifelter Wunsch nach einfachen Lösungen für „ähnliche“ Probleme (NIS2 😈)

Ungezügelte fachliche Neugier



Post Mortem des Angriffs



Sichtweise der IT-Forensiker
Verlauf des Angriffs, Lücken
Konkrete Campus-Accounts
IP-Adressen spezifischer Systeme
Allgemeine Empfehlungen

Sichtweise des HRZ + Gutachter
Verlauf des Angriffs, Lücken
Anonymisierte Accounts
Anonymisierte IP-Adressen
Spezifische beschlossene Maßnahmen
Schwärzungen nach ISB-Vorgabe

https://www.youtube.com/watch?v=C8Wf7u-Iy8I

Post Mortem

Mittwoch, 14.2.2024
- VPN-Einwahl mit gekaperten studentischen Account
- Brute Force-Angriff auf RDP-Freigabe eines Labors
- Übernahme des lokalen Admin-Accounts
- Auslesen von Passwörtern aus Labor-Backup
- Laterale Bewegung in andere Labore
- Installation von Backdoors und Scan-Tools

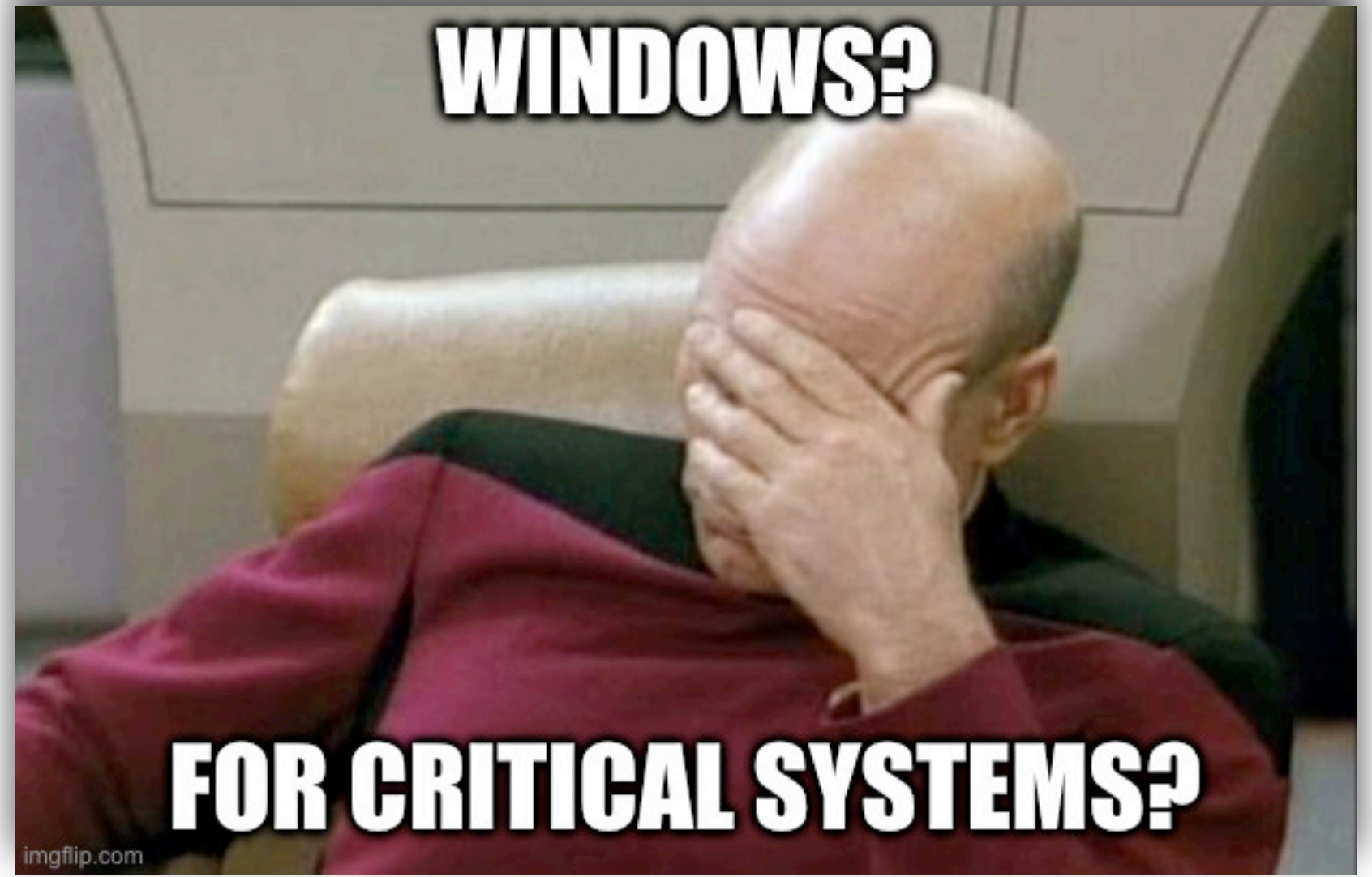
Donnerstag, 15.2.2024
- Testweise Anmeldungen mit ermittelten Account-Daten

Freitag, 16.2.2024
- Brute Force-Angriff auf RDP-Freigabe eines kritischen Systems im HRZ
- Übernahme des lokalen Admin-Accounts
- Übernahme eines administrativen HRZ-Accounts
- Erstellung einer Active Directory - Kopie

Sonntag, 18.2.2024
- unspezifische Warnung des LKA
- Trennung der Backup-Systeme vom Netz durch das HRZ
- Analyse des Monitoring, keine relevanten Erkenntnisse

Montag, 19.2.2024
- CD-ROM mit Daten der BHT aus dem Darknet

Dienstag, 20.2.2025
- Paralleles Herunterfahren der virtuellen Maschinen im ESX-Cluster der BHT (SSH auf ESX-Knoten)
- Verschlüsselung von 252 VM-Festplatten, entsprechende Warnungen im Monitoring
- Auffinden einer Akira-Mitteilung im Storage
- Abschaltung des DFN Uplink
- Beginn der Arbeit des Krisenstabs
- Erfolglose Bitte um Hilfe beim BSI
- Beauftragung des Trend Micro Red Team


WINDOWS?
FOR CRITICAL SYSTEMS?
imgflip.com

Akira Ransomware Gang Extorts

https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html

Suchen

Don't Get Pwned, Get Informed

Followed by 4.50+ million

The Hacker News

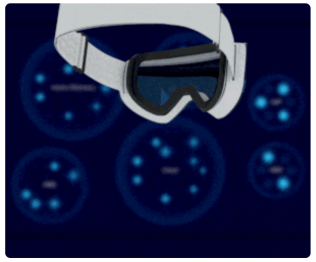
Subscribe – Get Latest News

Home | Data Breaches | Cyber Attacks | Vulnerabilities | Webinars | Expert Insights | Contact

Akira Ransomware Gang Extorts $42 Million; Now Targets Linux Servers

Apr 19, 2024 Ravie Lakshmanan Ransomware / Endpoint Security

SHARE



Threat actors behind the Akira ransomware group have extorted approximately $42 million in illicit proceeds after breaching the networks of more than 250 victims as of January 1, 2024.

"Since March 2023, Akira ransomware has impacted a wide range of businesses and critical infrastructure entities in North America, Europe, and Australia," cybersecurity agencies from the Netherlands and the U.S., along with Europol's European Cybercrime Centre (EC3), said in a joint alert.

— Trending News

#StopRansomware: Akira Ransc

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

Suchen

An official website of the United States government Here's how you know

FREE CYBER SERVICES | ELECTION THREAT UPDATES | #PROTECT2024 | SECURE OUR WORLD | SHIELDS UP | REPORT A CYBER ISSUE

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

SHARE:

CYBERSECURITY ADVISORY

#StopRansomware: Akira Ransomware

Release Date: April 18, 2024 **Alert Code:** AA24-109A

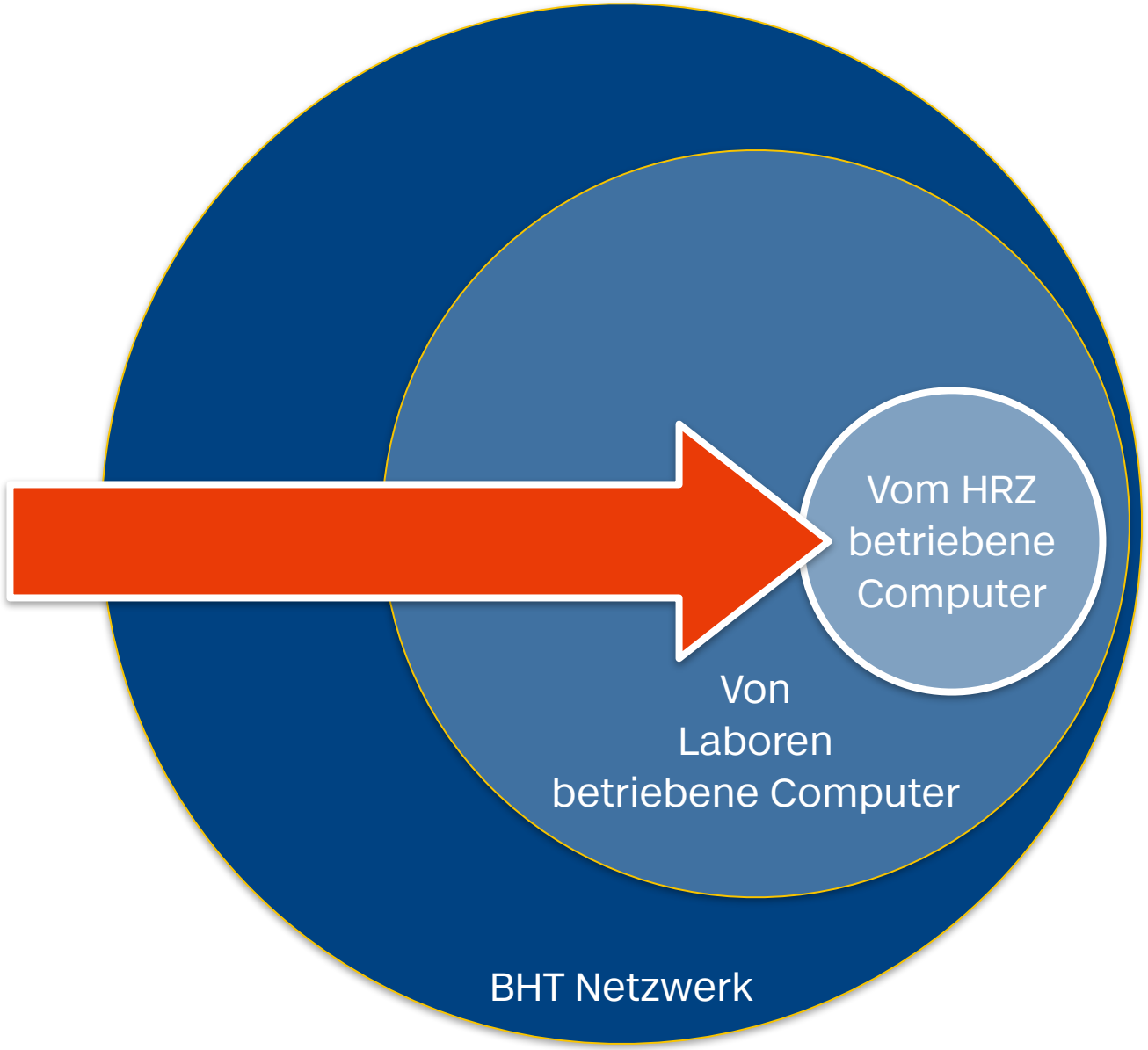
RELATED TOPICS: CYBERSECURITY BEST PRACTICES, CYBER THREATS AND ADVISORIES, INCIDENT DETECTION, RESPONSE, AND PREVENTION

ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM AKIRA RANSOMWARE:

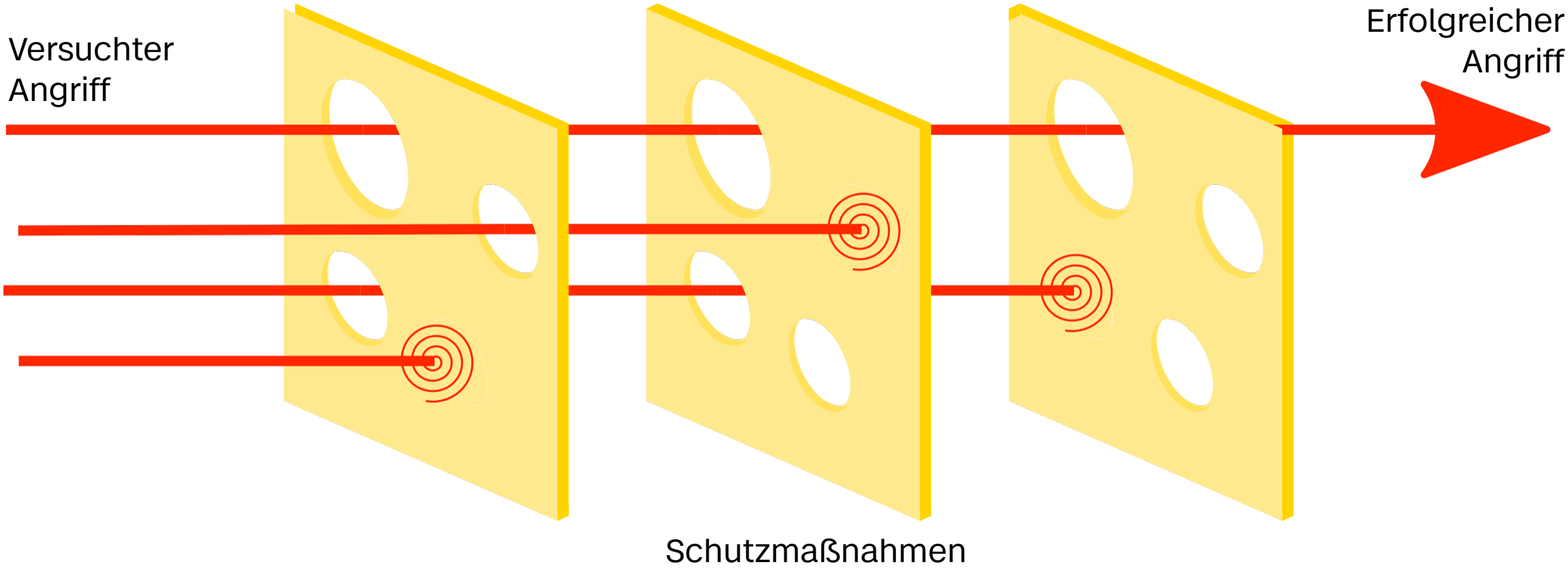
1. Prioritize remediating known exploited vulnerabilities.
2. Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
3. Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

Fehlerausbreitung

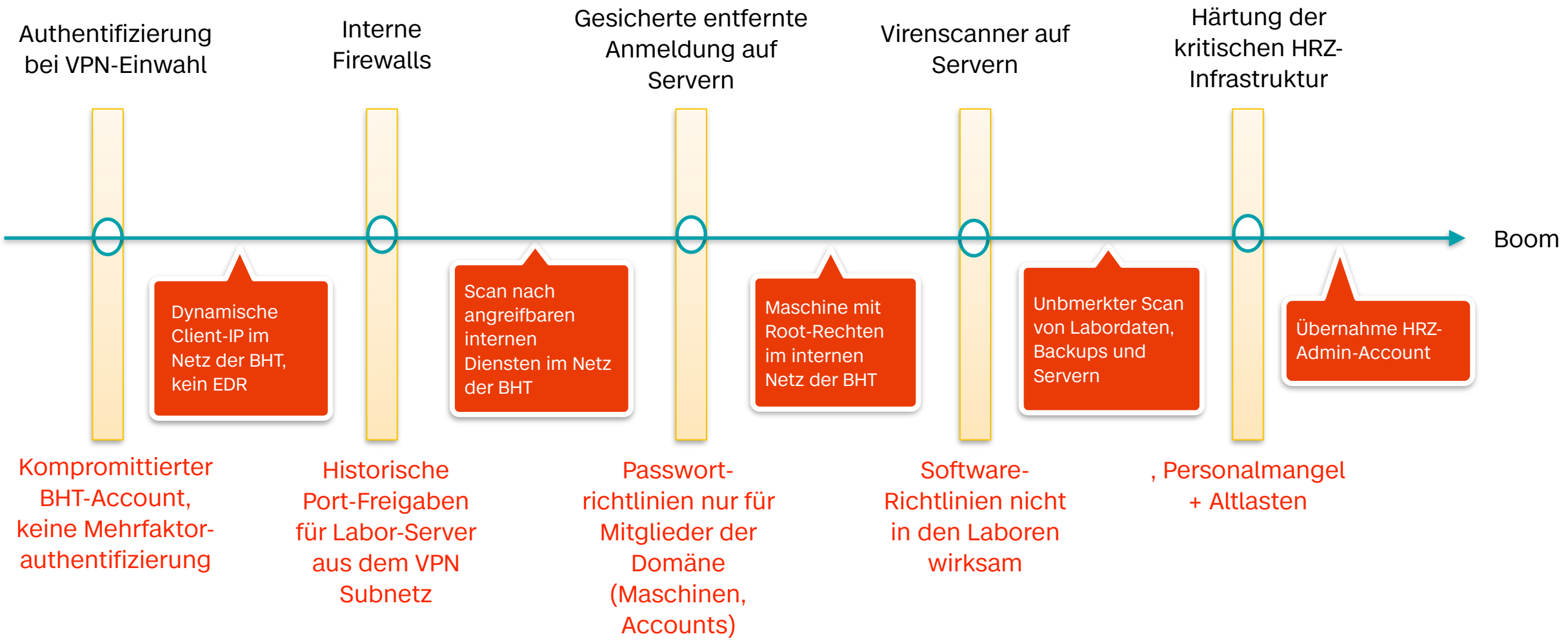
https://www.flaticon.com



Swiss Cheese Model

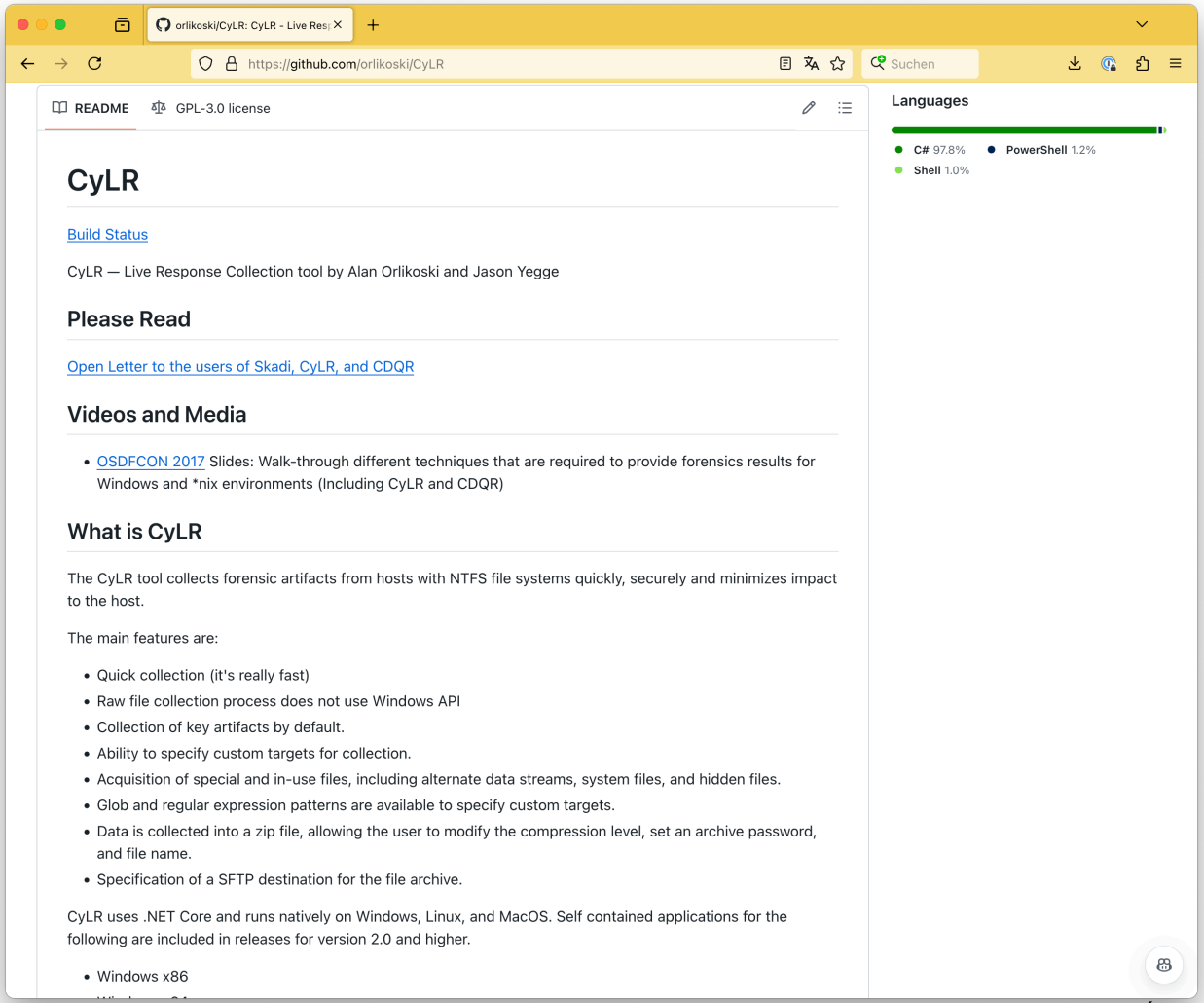


Gescheiterte Schutzvorkehrungen



Forensik

Trend Micro
Deep Discovery Inspector (DDI)



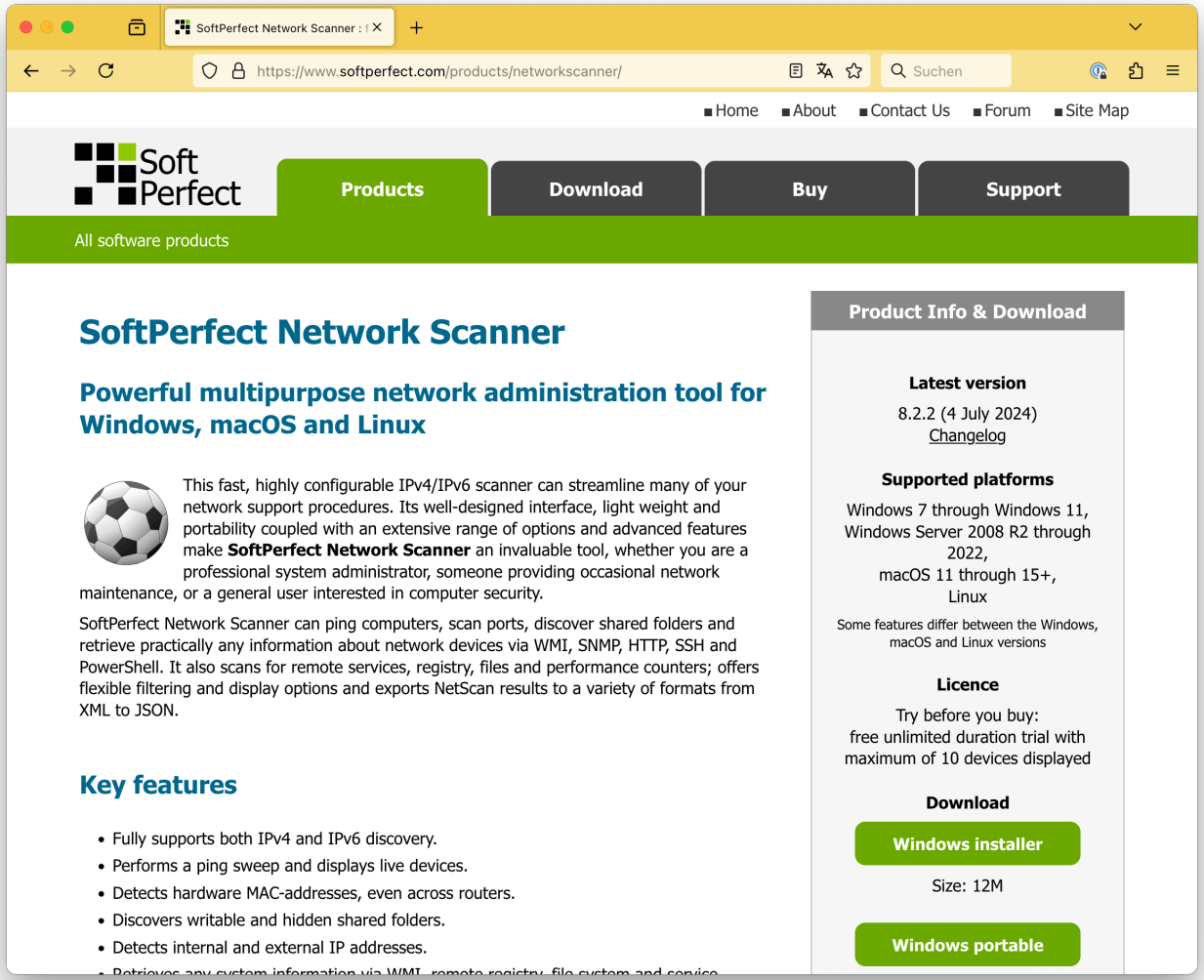
Angreifer: netscan.exe

Regulärer Netzwerk-Scanner, verfügbar als Windows Portable

NMap mit einer Windows GUI

Wird von Windows Defender als „Hack Tool“ klassifiziert

Angreifer richteten entsprechende Ausnahme ein



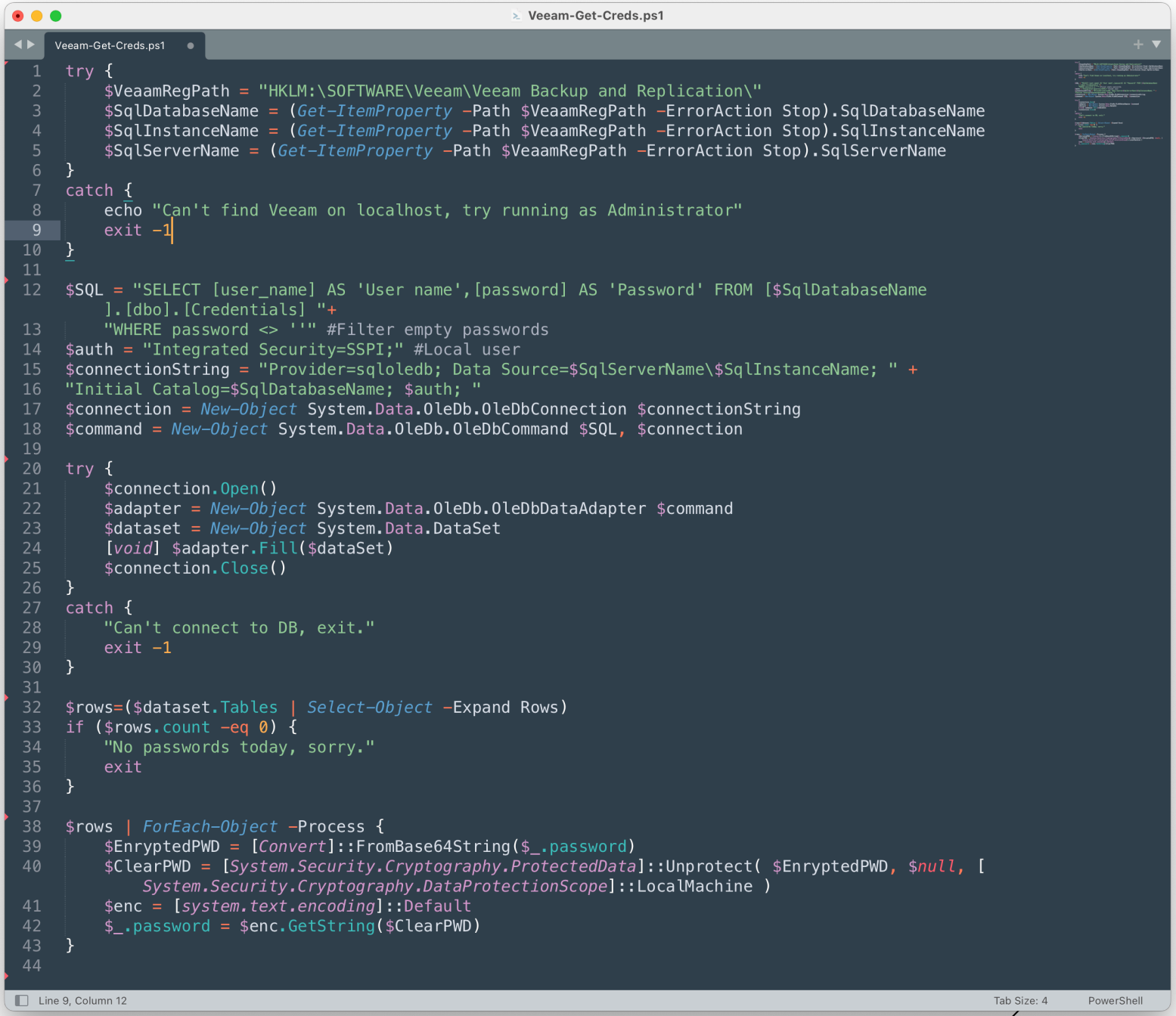
Angreifer: 69 Zeilen PowerShell von GitHub

Datenbank des Veeam Backup Server enthält Secrets zur Durchführung von Backups

DB Credentials in der Registry des Backup-Servers

Verschlüsselung der Secrets mit Key der lokalen Maschine

Lokaler Admin des Backup-Servers kann alle Secrets dekodieren



https://github.com/sadshade/veeam-creds/blob/main/Veeam-Get-Creds.ps1

Angreifer: DWAgent

Agent einer regulären Software für Fernwartung

Nimmt Verbindung zu „DWService“ Servern der Firma auf

Fernsteuerung aus einem Web Browser heraus möglich

Analyse der Netflow-Daten des DFN, um Datenabfluss zu recherchieren

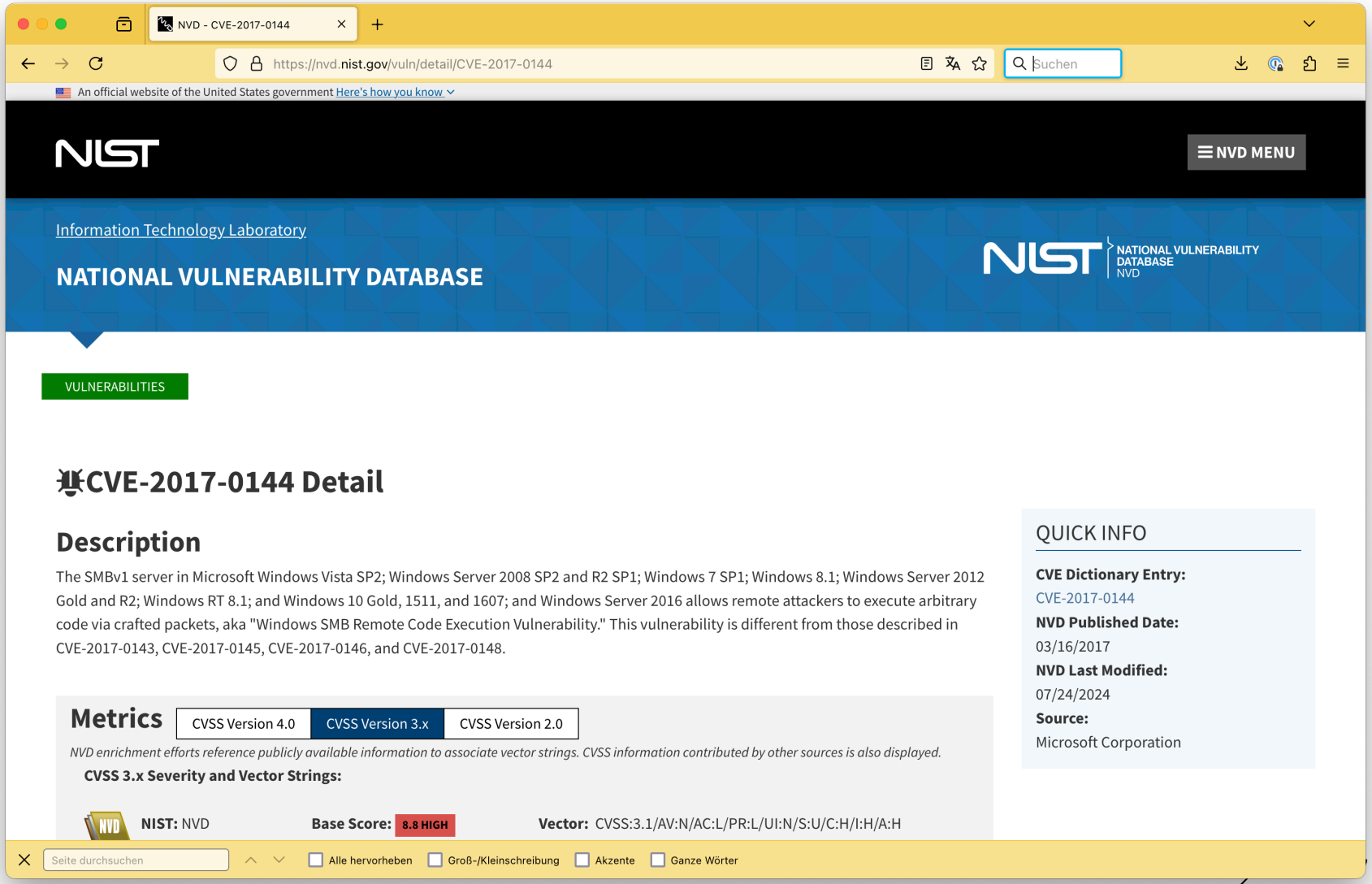
Angreifer: CVE-2017-0144

EternalBlue

Schwäche in SMBv1

Windows 95 - Server 2016

Erkennung des Angriffs durch Trend Micro Virenscanner bei lateraler Bewegung

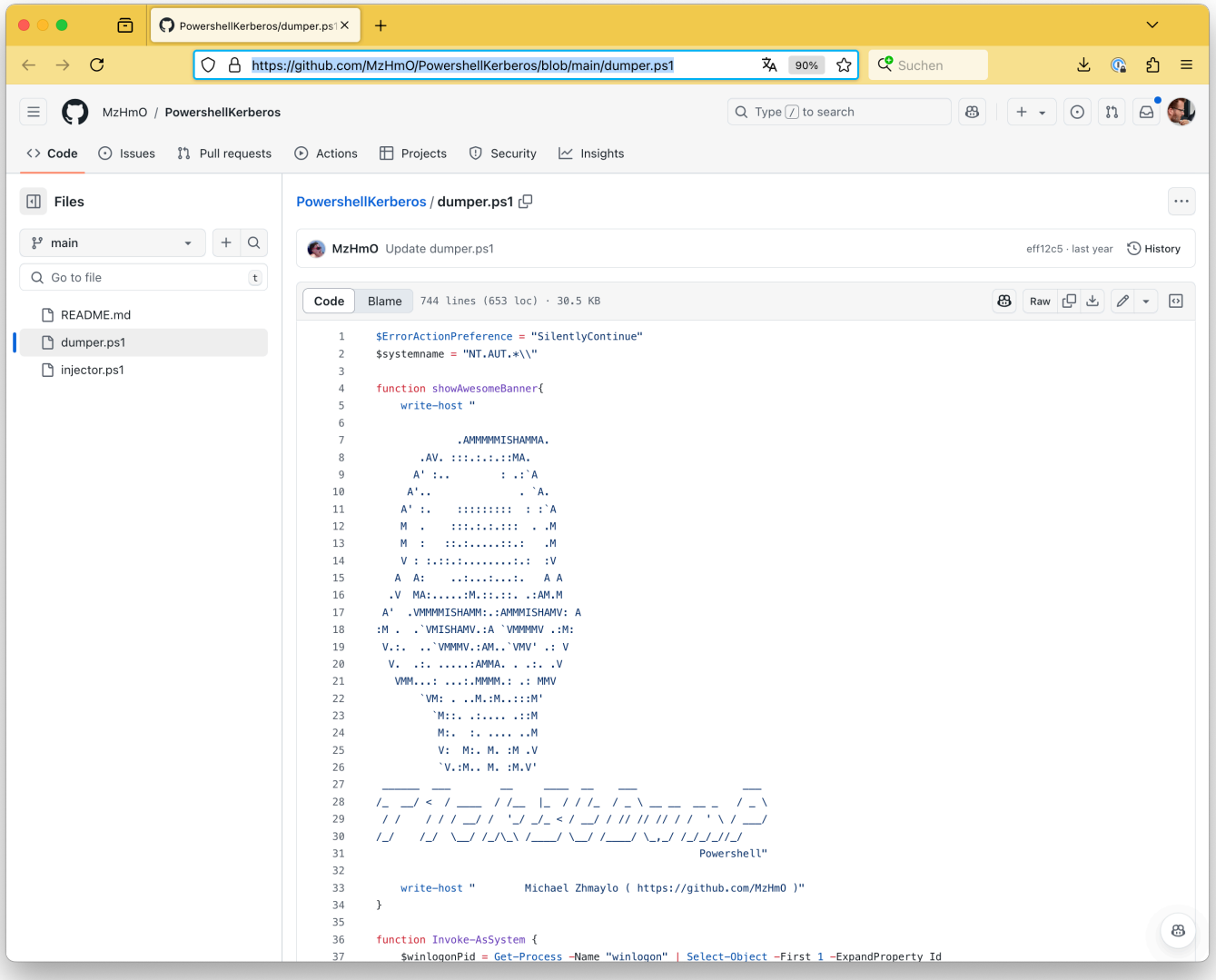


Angreifer: dumper.ps1

Dump von Kerberos Tickets aus dem LSA Cache (Linux: kcc)

Mit Admin-Account alle Tickets, sonst nur des aktiven Accounts

Kerberos Ticket erlaubt Authentifizierung gegen andere Systeme ohne ein Passwort



https://github.com/MzHmO/PowershellKerberos/blob/main/dumper.ps1

Angreifer: Kerberoasting

Windows Dienst-Account

- regulärer AD-Account, hat einen *Service Principle Name (SPN)* gesetzt
- Bindung eines Windows-Dienstes an ein Nutzerkonto im AD (Bsp. File Server)
- typischerweise kein ablaufendes Passwort, meist umfangreiche Berechtigungen

Angreifer fordert Kerberos Service-Ticket für alle SPN-Accounts beim Domain Controller an

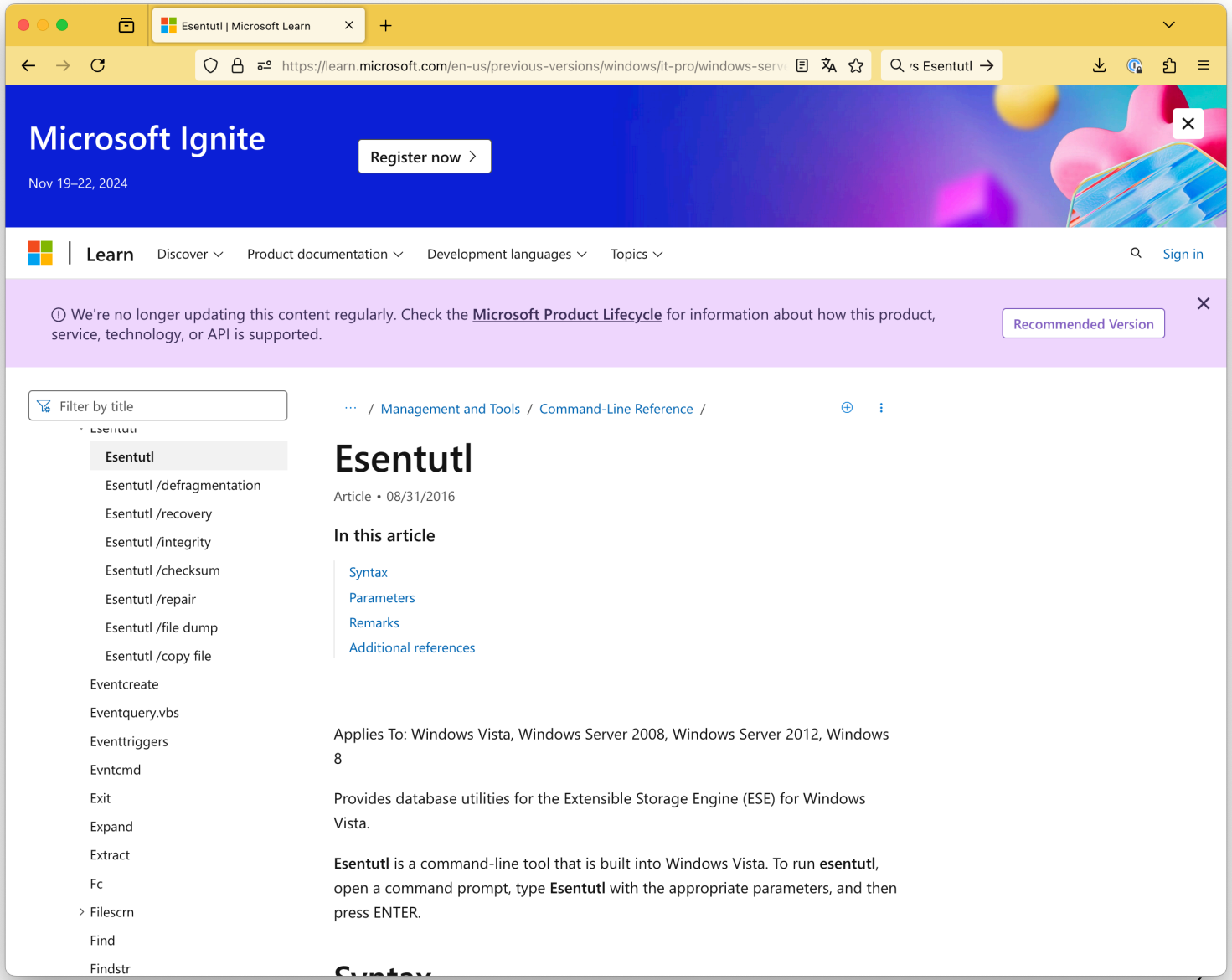
- zurückgegebenes Ticket wird mit NTLM-Hash des Accounts verschlüsselt
- Offline-Dekodierung, um Passwort-Hash zu ermitteln (RC4: 500 Millionen Versuche/s pro GPU)
- *Pass-the-Hash* Angriffe bei NTLM im nächsten Schritt problemlos möglich

Angreifer: Esentutl

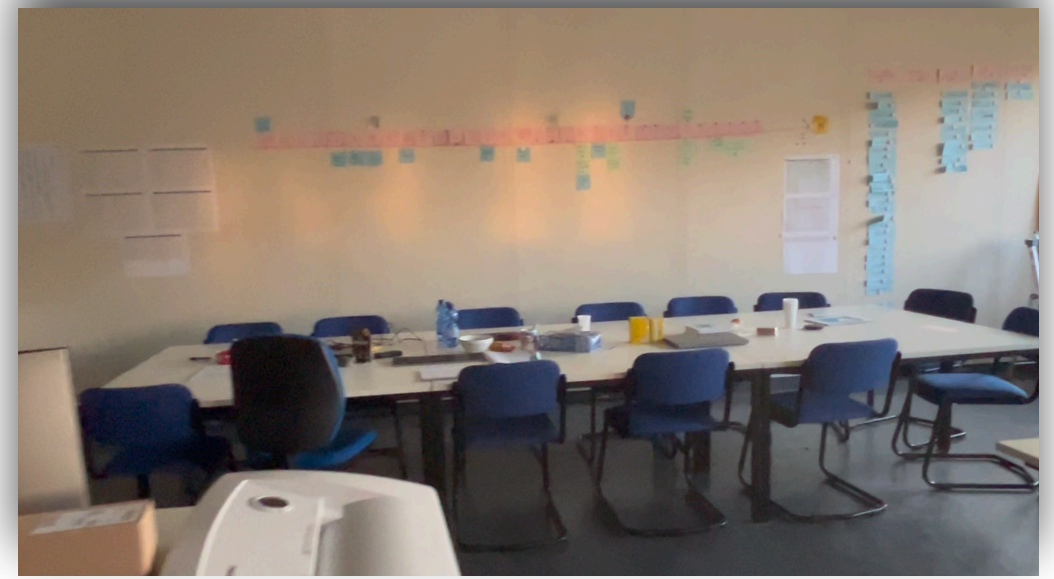
Extensible Storage Engine (ESE) Datenbanken for Exchange / AD / Windows Search

Kommandozeilenwerkzeug zur Reparatur solcher Datenbanken

Anfertigung einer Kopie von NTDS.dit = komplettes AD



Auswirkungen



<u>Februar / März 2024</u>

Forensische Untersuchung mit Trend Micro

Ausfall aller HRZ IT-Dienste (Semesterferien!)

Gekappte Anbindung an den Zahlungsdienstleister

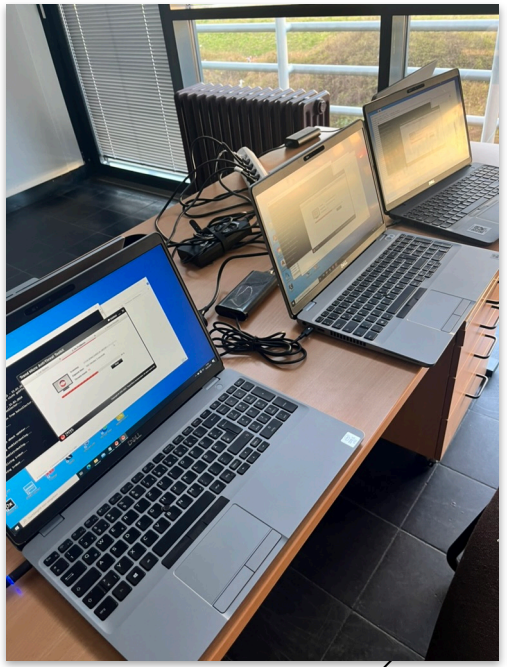
Gekappte Anbindung an Hochschulstart

Notbetrieb der Hochschule in allen Referaten

<u>Bis Sommer 2024</u>

Abschaltung des VPN-Angebots bis zur Umstellung auf 2FA

Verbot der Nutzung von Endgeräten, die noch nicht gescannt wurden



Maßnahmen

<u>Koordination</u>

- Kurzes tägliches Meeting
  (HRZ, Präsidium, beratende Nerds)
- Einigung auf Sprachregelungen
- "Essen reinwerfen, in Ruhe lassen“
  - Präsidium koordiniert um das HRZ herum
  - Abfrage (nicht Vorgabe) von Deadlines
- Notfall-Webseite
- Telefon Hotline
- Konstruktive Zusammenarbeit aller Einheiten … leider schon wieder vorbei

Maßnahmen

<u>Reset der Domäne</u>

Wiederherstellung eines AD-Backups

KRBTGT Passwort Rollover („Golden Ticket“)

Rücksetzung aller Passwörter

Aktivierung von LAPS

- automatische Rotation der lokalen Admin-Konten

- per GPO auf Rechnern der Domäne aktiviert

Teilweise Deaktivierung der Admin-Shares

<u>Reset von Maschinen</u>

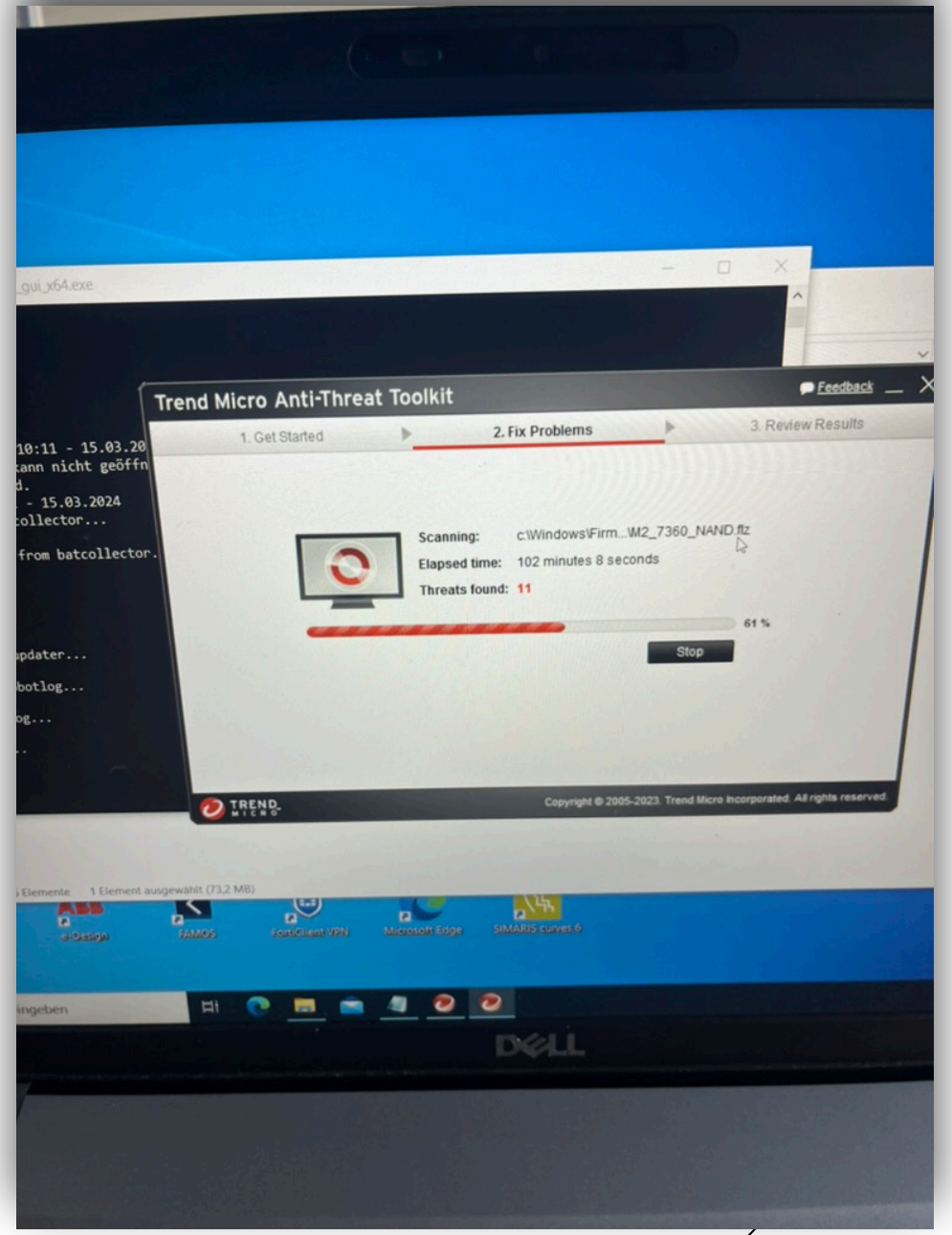
Batch Restore von VMs aus dem Backup nach Priorität

Größtes Problem: Zurückgesetzte gespeicherte Passwörter

Maßnahmen

<u>Scan der Endgeräte</u>

- Per Dienstanweisung verpflichtend für alle HRZ-Endgeräte
- „Der grüne Aufkleber“
- Nutzung von Multiplikatoren aus den Laboren
- Trend Micro stellte angepasste Signaturen auf Basis der Forensik bereit



Maßnahmen

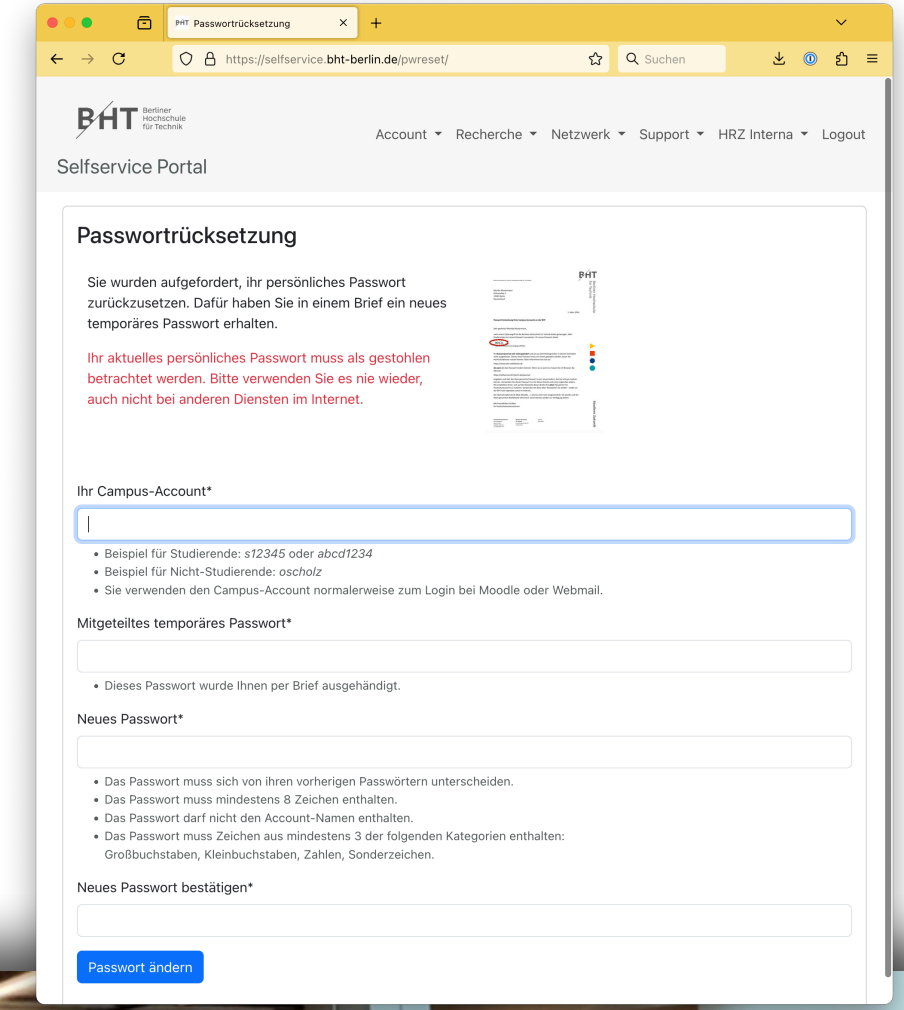
Umstrukturierung der gesamten Firewall-Architektur

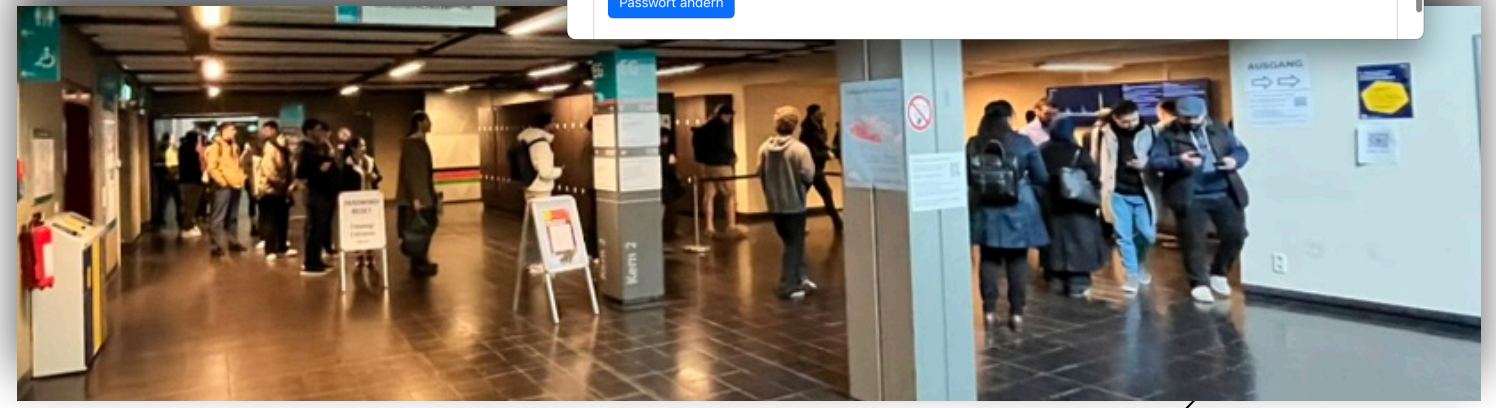
- Konkret(er) definierte Sicherheitszonen, Einordnung der vorhandenen VLANs
- Abräumen von Altlasten bei abgeschalteter Hochschule (Regeln, Core)
- Vereinheitlichung der Einbruchserkennung (IDS) durch Umzug von Routing Interfaces
- Massive Einschränkung der Port-Freigaben für Labore
  - Umzug von Labor-Servern aus Büro-Netzen in separates Subnetz
  - Aggressive „Vermarktung“ der Domänen-Mitgliedschaft (GPOs), inkl. Trend Micro - Installation
  - Noch lange nicht abgeschlossen

Maßnahmen

<u>Rücksetzung der Passwörter</u>

- Generierung initialer neuer Passwörter im AD
- Druck von 18.000 Briefen mit temporären Passwort
  - Versand an Adressen aus HisInOne / Personalverwaltung
  - Amtshilfe durch Deutsche Rentenversicherung
  - Erweiterung des Selfservice Portals,
    Prüfung der neuen Passwörter

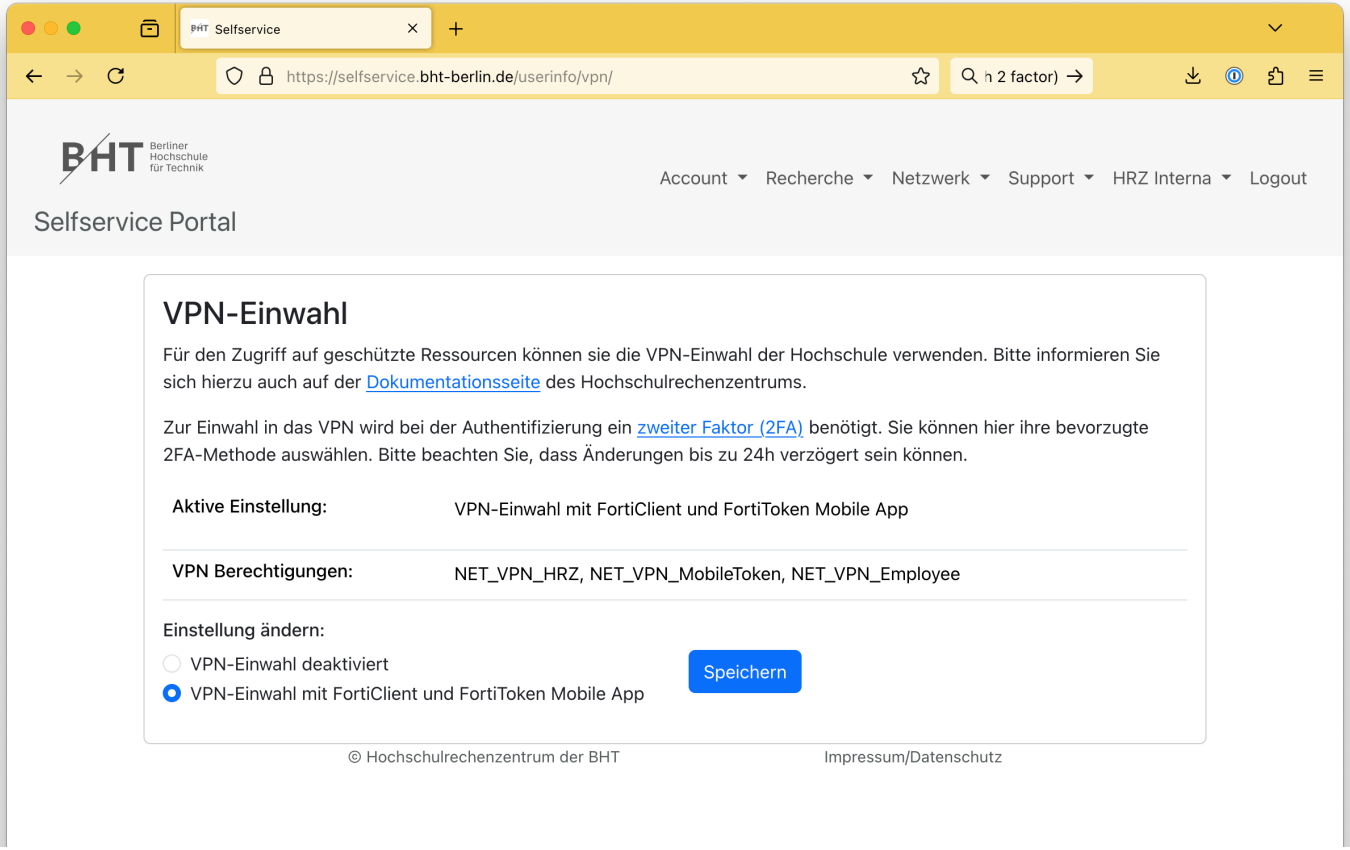




Maßnahmen

2FA für VPN-Einwahl

- Schwere Wahl zwischen schön (eduVPN, Wireguard, fudiscr) und schnell (Fortinet SSL VPN)
- Spannende nicht-technische Probleme
  - Zeiterfassung im Home Office
  - Mobile Token vs. Diensthandy
  - Bibliotheksangebote mit IP-Blockierung
  - Rollout von Software Token für große Nutzeranzahl



Fazit

6 Monate nach dem Angriff gefühlt wieder „Normalbetrieb“

Breiteres IDS und Virenabwehr zeigen „spannende“ Ecken des Netzwerks

Wiederherstellung der Labor-IT bei 30%

Organisationsstrukturen für IT-Steuerung werden massiv überarbeitet

Mühselige Abwägung zwischen Freiheit und Schutz der Hochschule

Härtung und Neustrukturierung geht unverändert weiter (danke Broadcom)

Fazit

Frequenz der Angriffe wächst kontinuierlich

Automatisierungsgrad der Abwehr müsste in gleicher Geschwindigkeit wachsen

Angreifer interessieren sich für das am meisten vernachlässigte System

Empfehlungen:

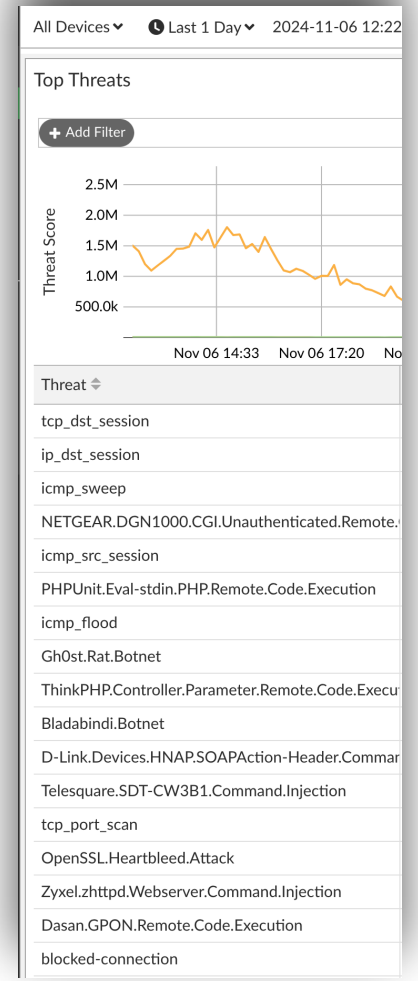
Klares Verständnis über kritische Kernsysteme, sauber getrenntes Backup

Klare Absprachen für Kommunikation im Notfall

„Fail fast“ - Mentalität

Sicherheit ist kein Zustand, sondern ein Prozess

Vielen Dank!


All Devices
Last 1 Day
2024-11-06 12:22
Top Threats
Add Filter
2.5M
2.0M
1.5M
1.0M
500.0k
Threat Score
Nov 06 14:33
Nov 06 17:20
Threat
tcp_dst_session
ip_dst_session
icmp_sweep
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.
icmp_src_session
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
icmp_flood
Gh0st.Rat.Botnet
ThinkPHP.Controller.Parameter.Remote.Code.Execu
Bladabindi.Botnet
D-Link.Devices.HNAP.SOAPAction-Header.Commar
Telesquare.SDT-CW3B1.Command.Injection
tcp_port_scan
OpenSSL.Heartbleed.Attack
Zyxel.zhttpd.Webserver.Command.Injection
Dasan.GPON.Remote.Code.Execution
blocked-connection


Irgendwas ist ja immer.