Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Ransomware, SolarWinds, Kaseya, Supply Chain Attacks, Zero Day Exploits - Erfahrungen aus der Vorfallsbearbeitung bei CERT-Bund

Gesellschaft für Informatik Regionalgruppe Rhein-Main

Robert Formanek
CERT-Bund Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

Bundesamt
für Sicherheit in der
Informationstechnik

Wie bedroht ist Deutschlands Cyber-Raum?

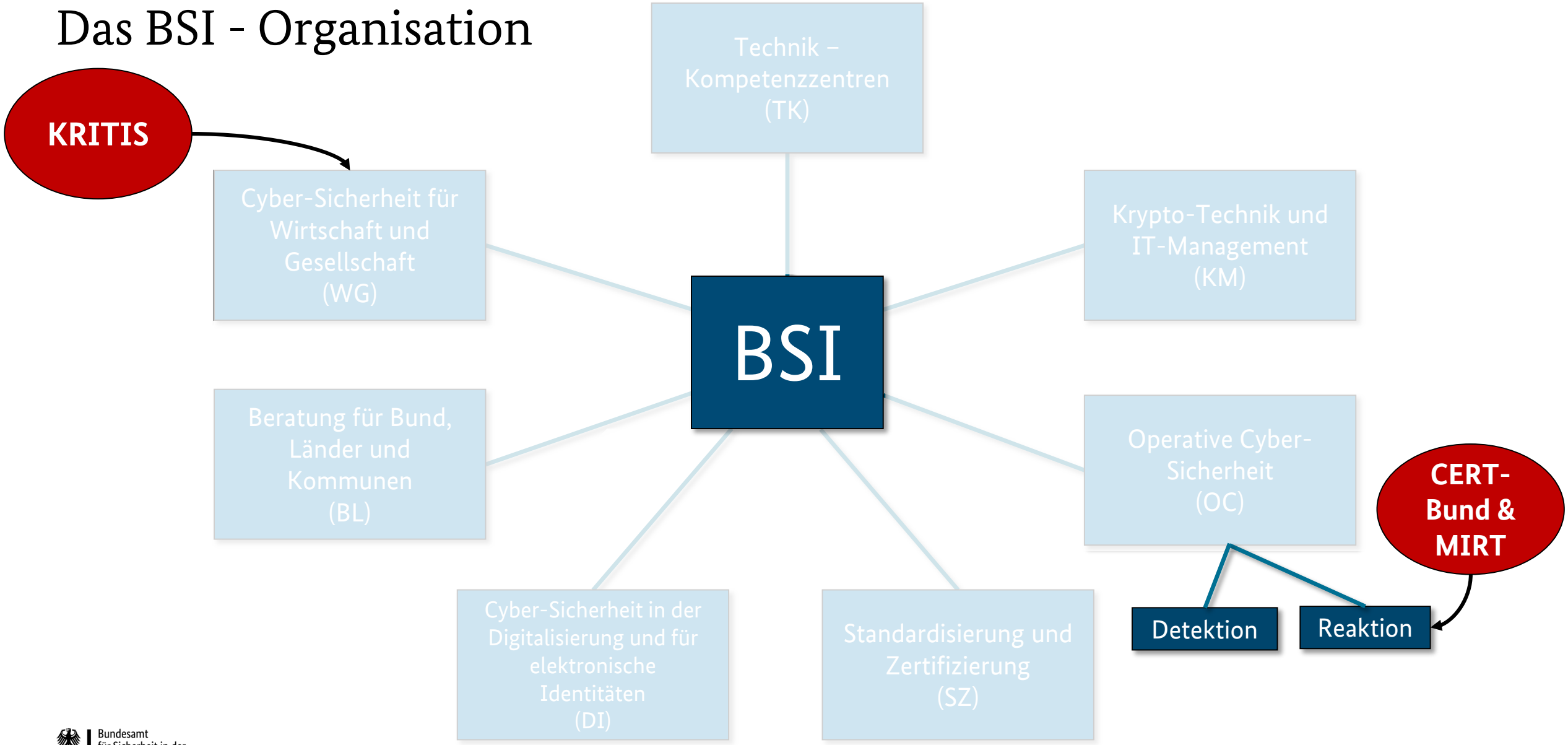
- Angreifer nutzen **Schadprogramme für cyber-kriminelle Massenangriffe** aber auch für **gezielte Angriffe** auf ausgewählte Opfer.
- In einer neuen Schadprogramm-Welle im **dominiert(e) Emotet die Lage**.
- Rund **117,4 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet. Das sind durchschnittlich **322.000 pro Tag, in Spitzenwerten 470.000**.
- Knapp **7 Millionen Meldungen zu Schadprogramm-Infektionen** hat das BSI an deutsche Netzbetreiber übermittelt.
- Bei Angriffen auf die Bundesverwaltung wurden rund **35.000 E-Mails mit Schadsoftware pro Monat** abgefangen.
- **24,3 Millionen Patientendatensätze** waren Schätzungen zufolge international frei im Internet zugänglich.
- Cyber-Kriminelle nutzen **COVID-19-Pandemie** für Social-Engineering-Angriffe aus.

Quelle: BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Was ist die Aufgabe des CERT Bund?

Das BSI - Organisation



Zielgruppe für (direkte) Vorfallsunterstützung

Definierte Zielgruppen (u.a. §5 b BSIG)

- Institutionen der **Bundesverwaltung**
- Betreiber von **Kritischen Infrastrukturen** (gem. Rechtsverordnung KRITIS)
- IT-Sicherheitsgesetz 2.0
  - Unternehmen im besonderen öffentlichen Interesse

In **begründeten Einzelfällen** kann das BSI auch bei anderen Institutionen unterstützen

- Angriff von **besonderer technischer Qualität**
- zügige **Wiederherstellung** der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems **von besonderem öffentlichem Interesse**
- Betroffenheit einer **Stelle eines Landes** idR. ein begründeter Einzelfall

Unterstützung im Rahmen der Amtshilfe

CERT-Bund Vorfallsbearbeitung

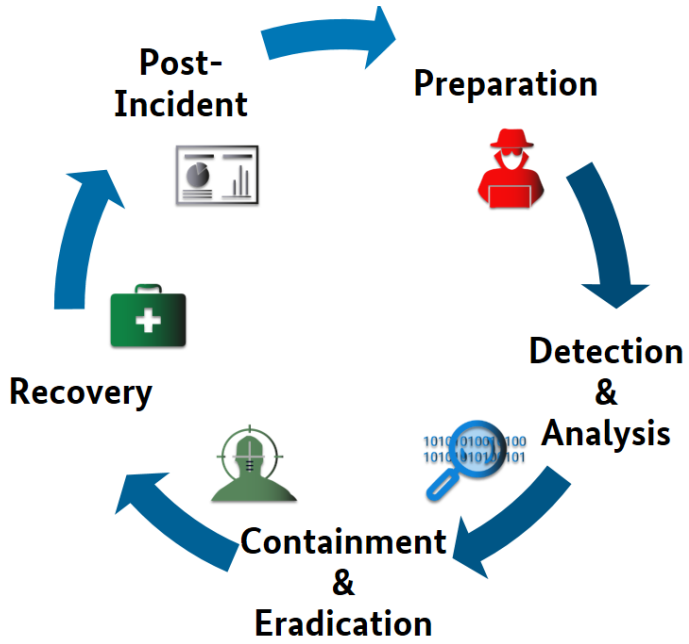
Vorfallsbearbeitung / Incident Handling
- Breites Unterstützungsangebot

1. Papiere
2. Beratung
3. Incident Response / Incident Management
4. Fallbezogene Cybersicherheitswarnungen
5. Koordination der MIRT-Einsätze

Abuse / Takedown

CERT-Bund Reports (320 Mio Events, 3 Mio Reports (2020))

Operative Zusammenarbeit / Unterstützung durch Gremien:
- National (VCV VerwaltungsCERT-Verbund, G4C, BundesCERTs, CERT Verbund, DCSO, CSSA und
- international (EGC Group, EU CSIRT-Network, IWWN, TI, FIRST, NATO, CERT-EU)



Unterstützung

Mobile Incident Response Team (1/2)

Mobile Incident Response Team

Vor Ort Unterstützung

- In der Regel am nächsten Tag vor Ort
- Incident Response & Forensik Experten
- Umfangreiche Hardwareaustattung für Data Aquisition, Analyse und Auswertung

Im Backoffice eigenes Team & Hardware für weitergehende technische Analysen

Unterstützung

Mobile Incident Response Team (2/2)

Mobile Incident Response Team

- Data Aquisition
  - Forensische Sicherungen
  - Mitschnitt des Netzverkehrs
- Durchführung von forensischen Analysen vor Ort
- Hostbasierte Suchen / Hunting
- Live-Analyse großer Datenmengen vor Ort

Bundesamt
für Sicherheit in der
Informationstechnik

Hafnium - Angriffe auf Exchange-Server in Deutschland

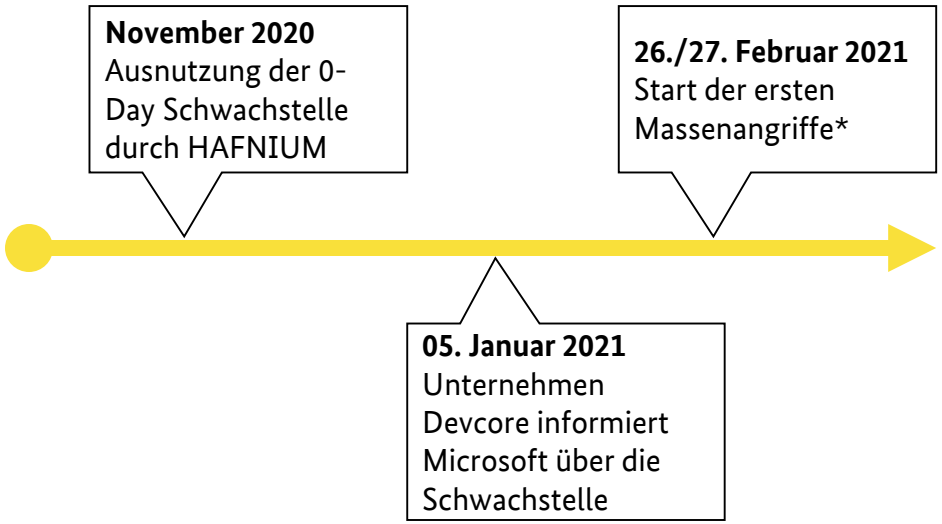
Die vier Schwachstellen & die Anbahnung der Lage

CVE-2021-26855 (ProxyLogon)
- Server-side request forgery (SSRF) – Erlaubt es Angreifer HTTP-Requests zu senden und sich am Exchange-Server zu authentisieren.

CVE-2021-26857
- Insecure deserialization im UMS. Hierüber kann beliebigen Programmcode als SYSTEM auf Exchange-Server ausgeführt werden.

CVE-2021-26858 und CVE-2021-27065
- Dadurch konnten beliebige Dateien auf dem Exchange-Server erstellt werden.

Ein Angreifer kann eine nicht-vertrauenswürdige Verbindung zu Port 443* dazu nutzen, um „aus der Ferne“ Code auf dem Server auszuführen.
(Remote Code Execution)



** geändertes Täterverhalten*

Patches und Timeline bis 3. März

- Microsoft veröffentlichte in der Nacht auf Mittwoch den 3. März Out-of-Band Updates
  Exchange Server **2010** (SP 3 RU), Exchange Server **2013** (CU 23), Exchange Server **2016** (CU 19, CU 18), Exchange Server **2019** (CU 8, CU 7)
- 0-Day Schwachstellen wurden in Kombination für gezielte Angriffe genutzt
  - APT-Kampagne der Gruppe HAFNIUM (Quelle: Microsoft)
  - Zugang zu den E-Mail-Accounts erlangt, sowie weitere Malware zur Langzeit-Persistenz installiert

Timeline	
Datum	**Ereignis**
Ab November 2020	Nutzung der Schwachstellen im Rahmen gezielter Angriffe (Quelle: Volexity)
05.01.2021	Unternehmen Devcore informiert Microsoft über die Schwachstelle
26-27.02.2021	Start von ersten Massenangriffen *https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/*
02.03.2021	**Meldung vom Microsoft Security Team, Information zu Angriffen und Out-of-Band Updates** *https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/*
03.03.2021	**BSI versendet Warnung Nr. 2021-197772-xxxx v 1.0 - Mehrere Schwachstellen in MS Exchange**
03.03.2021	Volexity veröffentlicht, dass von 2200 überprüften Kundenservern 176 kompromittiert sind *https://www.reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers/*

Bedrohungspotential und Timeline ab 4. März

- Bislang: Ausnutzung durch mehrere Tätergruppen, die in der Vergangenheit mit Spionage in Verbindung gebracht wurden.
- Jetzt: PoC Code zur Ausnutzung der Schwachstellen öffentlich verfügbar
- Exploits massenhaft gegen Tausende von Zielen eingesetzt - offenbar weltweit. (Bedrohungsszenario: Ransomware)
- Unklar: Wann ist man „betroffen“?

Timeline	
Datum	**Ereignis**
Do 04.03.2021	**Erste Meldungen von kompromittierten Systemen aus den Kernzielgruppen, BSI aktualisiert Warnung -> v1.1.**
Fr 05.03.2021	**BSI stuft Warnung von 3/Orange auf 4/Rot hoch -> v1.2.**
Sa 06.03.2021	**Unterstützung von betroffenen Behörden - Update der Warnmeldung (v1.3/v1.4).**
Mo 08.03.2021	**Mittlere zweistellige Anzahl an Betroffenen (Bundesverwaltung, Landesverwaltungen, KRITIS, Allianz für Cybersicherheit, KMUs).**
Mo 08.03.2021	**BSI ruft die „begrenzte IT-KRISE“ aus. Update der Warnmeldung (v1.5).**
Mi 10.03.2021	**ESET spricht von mindestens zehn Angreiffergruppen, welche die Schwachstellen missbrauchen.**
Mi 17.03.2021	**Kryptomining-Schadsoftware (DLTMiner) wird auf betroffenen Systemen installiert.**
Fr 26.03.2021	**Die ersten Vorfälle mit Ransomware werden bekannt.**
Di 13.04.2021	**5104 ungepatcht und frei im Internet angreifbar.**

Tag 1 nach den Patches

TOTAL RESULTS

266,629

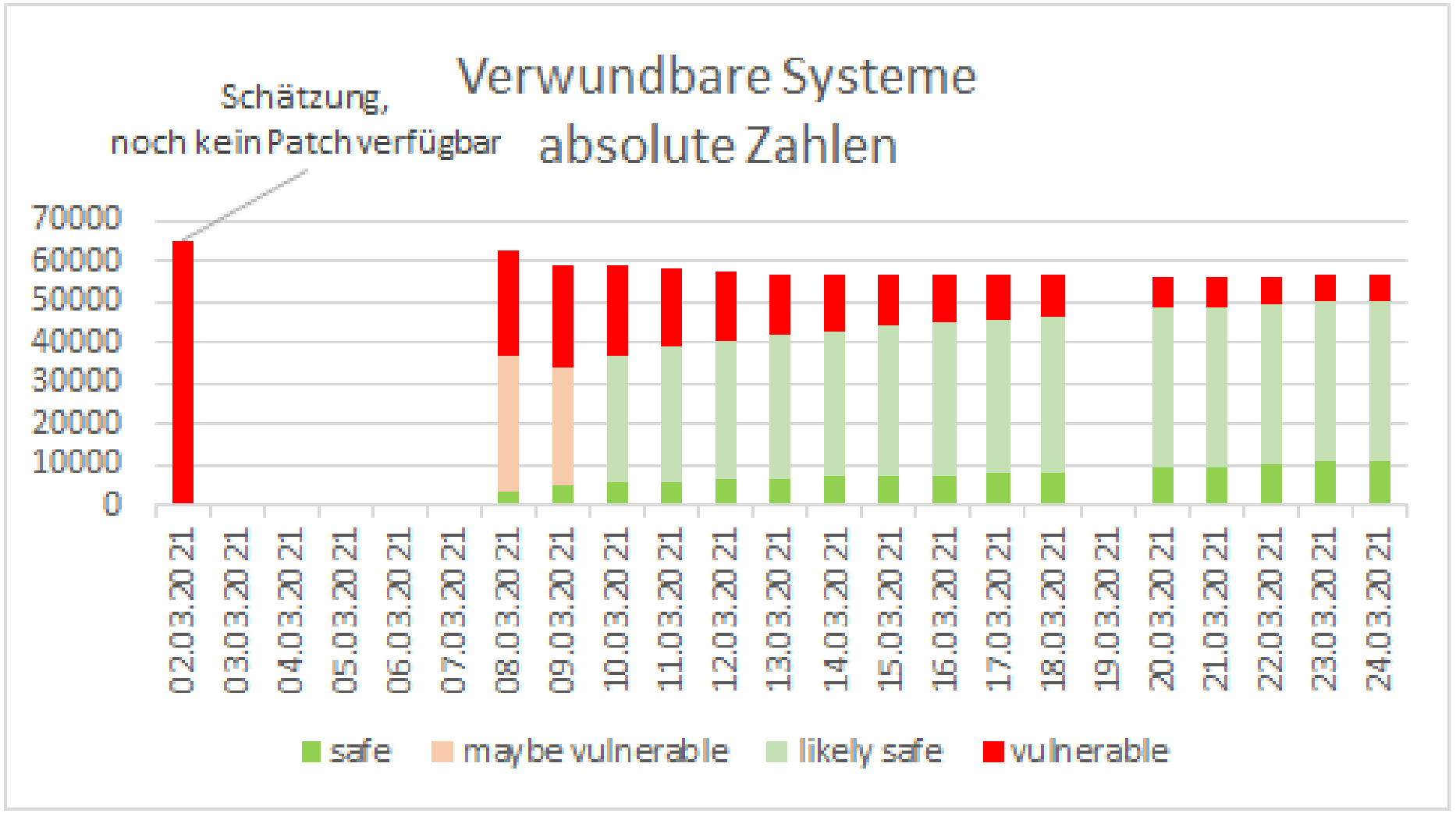
TOP COUNTRIES

United States	66,522
Germany	57,702
United Kingdom	15,712
Netherlands	10,986
France	10,660

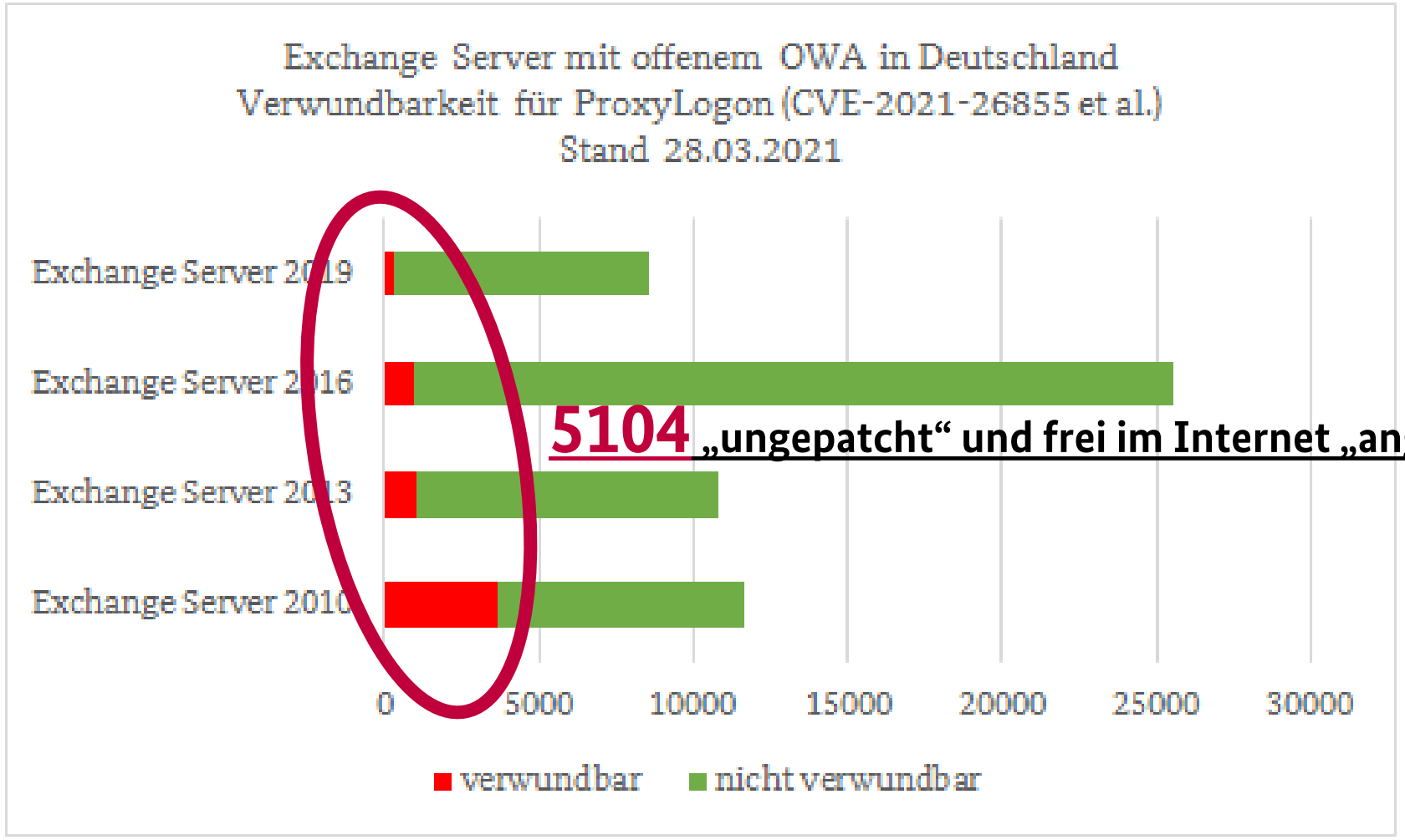
More...

Quelle: https://twitter.com/shodanhq/status/1367525621065261062

Timeline verwundbare Systeme



Situation in Deutschland 13. April 2021

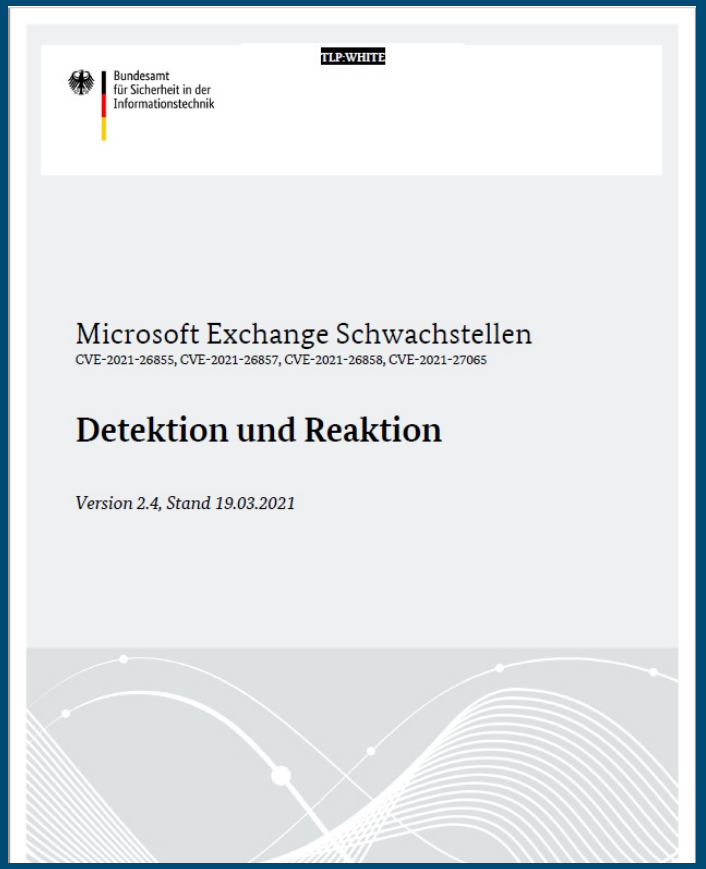


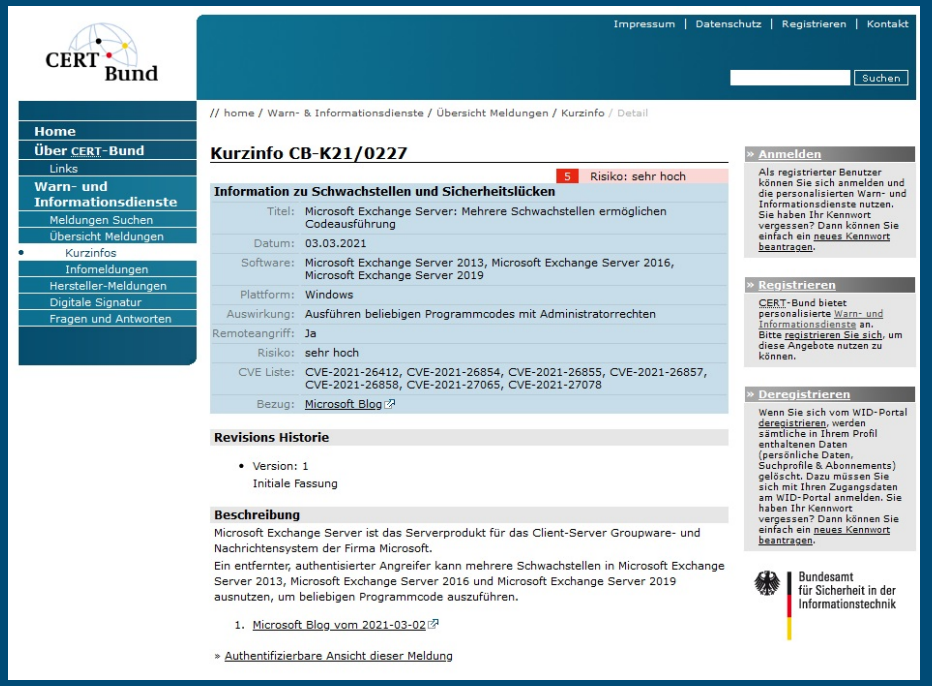
5104 „ungepatcht“ und frei im Internet „angreifbar“.

https://www.twitter.com/certbund

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik





Aufwand bei Hafnium

→ Erstmalig „Begrenzte IT-Krise“ gem. IT-KM der BV aus 03/2011 (zum 3. Mal Warnung ROT (nach IE 2010 und Heartbleed 2014).

→ Ca. 400 Meldungen an das BSI-Lagezentrum.

→ 170 FTE (~ 8 Personen-Monate); bis zu ca. 24 FTE/Tag, incl. WE.

Derzeitige Beobachtungen

Nach initialer Kompromittierung werden Rollover/Plead und Gh0st eingesetzt. Die Payloads werden dabei von Github nachgeladen.

CobaltStrike - Ziele vor allem Nordamerika.

ChinaChopper-Webshell (mittels Powershell typische Reconnaissance-Befehle).

Seit August 2021 (Orange Tsai, DEVCORE):

- Zugriffe auf /autodiscover/autodiscover.json
  https://blog.orange.tw/2021/08/proxyoracle-a-new-attack-surface-on-ms-exchange-part-2.html
- ProxyLogon is Just the Tip of the Iceberg
  https://www.youtube.com/watch?v=5mqid-7zp8k

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Robert Formanek
CERT-Bund, Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum

cerbtbund@bsi.bund.de
Tel. +49 (0) 228 9582 5110

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik