Richtig reagieren auf die aktuelle Gefahrenlage

Rupp Julian, Referat W 25 - „Cybersicherheit bei KMU“
Bundesamt Bundesamt für Sicherheit in der Informationstechnik

Südwestfalen Protected,
23.09.2025

Bundesamt
für Sicherheit in der
Informationstechnik

Leitsatz

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung

durch **Prävention**, Detektion und Reaktion

für Staat, **Wirtschaft** und Gesellschaft.

Nationales IT-Lagezentrum BSI

CERT Bund

30 Jahre IT-Grundschutz

CyberRisiko Check

UP KRITIS

Allianz für Cyber-Sicherheit

Das BSI unterstützt Unternehmen mit Informationen und Best Practices, Warnmeldungen und Lageinformationen, Zertifizierungen und Standards, fördert die Zusammenarbeit mit Vernetzungsangeboten und hilft bei herausragenden Vorfällen.

Vision

Wir bauen gemeinsam die Cybernation Deutschland.

Cybersicherheit
auf die Agenda heben

Digitalisierung
voranbringen

Resilienz
erhöhen

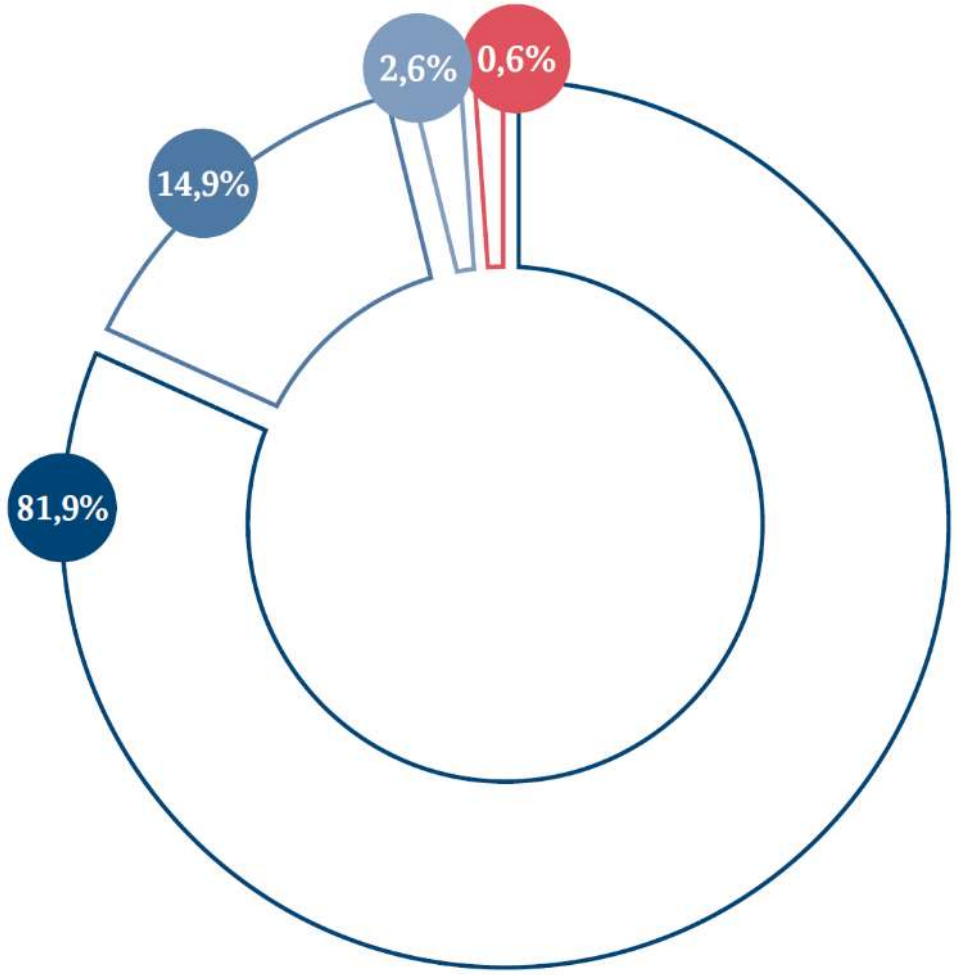
Cybersicherheit
gestalten

Technologie-kompetenz
nutzen

Cybermarkt Deutschland
aufbauen

Unternehmen in Deutschland nach Größe

Angaben in Prozent

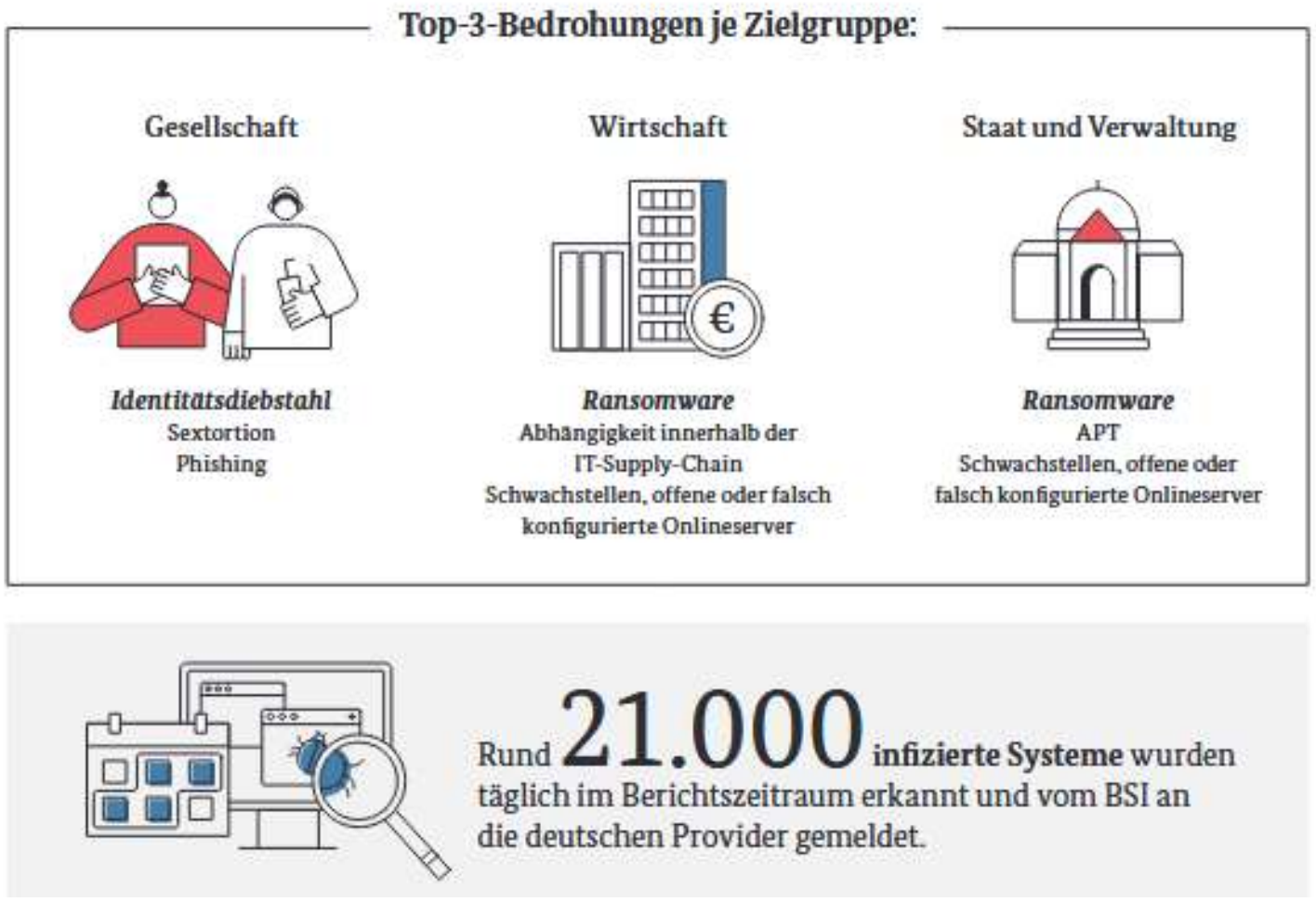


Quelle: Statistisches Bundesamt, Stand: Juli 2021

- Kleinstunternehmen
- Kleine Unternehmen
- Mittlere Unternehmen
- Großunternehmen

Wie bedroht ist Deutschlands Cyberraum?

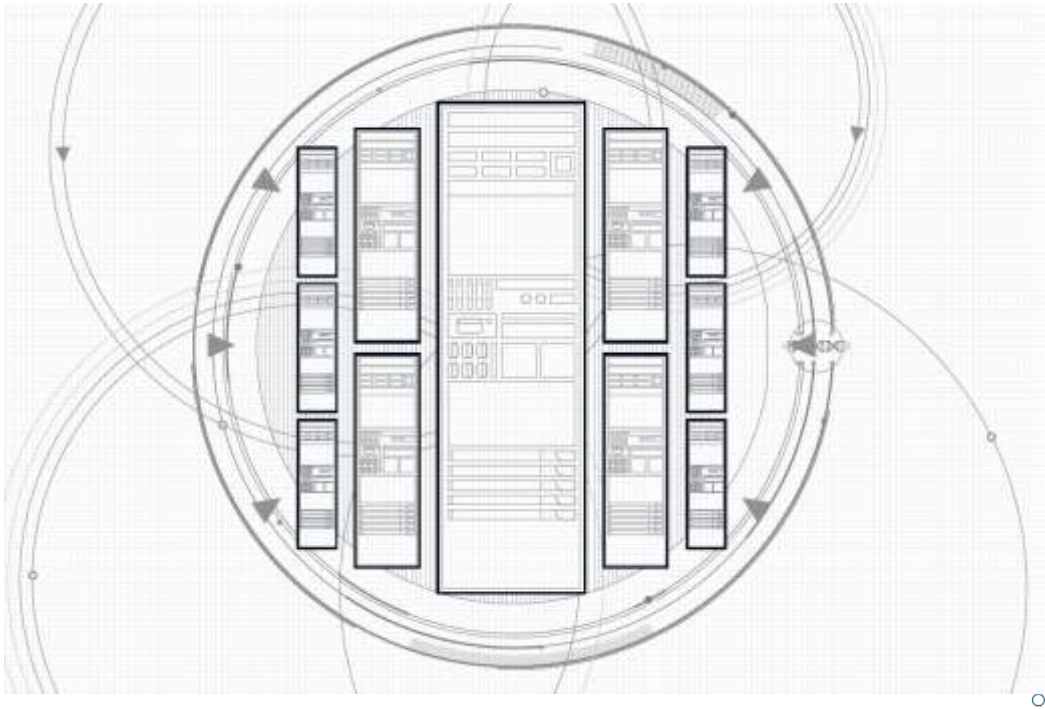
Die Lage der IT-Sicherheit in Deutschland 2023



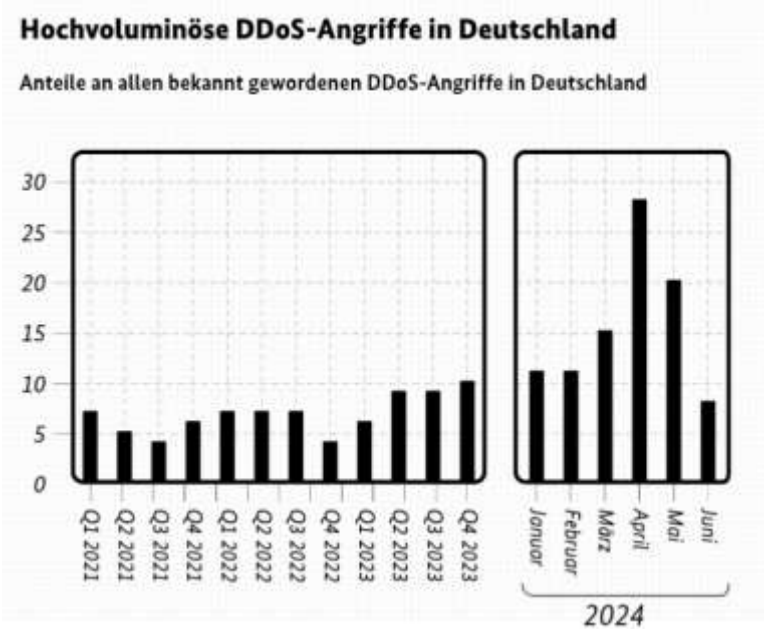
Wie bedroht ist Deutschlands Cyberraum? - Angriffsfläche

Die Lage der IT-Sicherheit in Deutschland 2024

- Pro Tag wurden 78 **neue Schwachstellen in Softwareprodukten** bekannt
- mind. 37 % der 45.000 **Exchange-Server in Deutschland** verwundbar
- 25 % der **Android-Geräte** in Deutschland erhalten **keine Sicherheits-Updates** mehr.
- **Schwachstellen nehmen seit Jahren kontinuierlich zu.**
- **Vielfältige Angriffstechniken treffen auf einen digitalisierten Alltag – alle können angegriffen werden.**



Angespannte Lage: Bedrohungen, Angriffsfläche und Angriffe

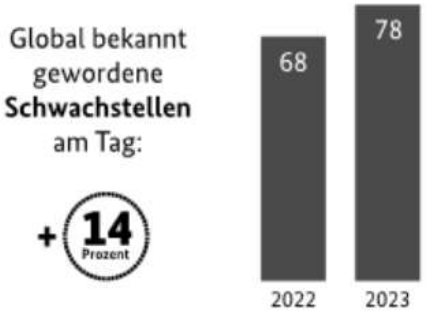


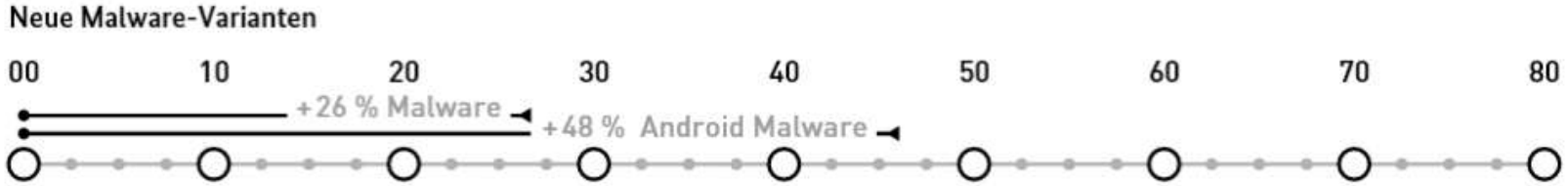
Schadprogramm-Varianten: Durchschnittlich 309 000 neue pro Tag

Schwachstellen in Softwareprodukten: Täglich 78 neue

DDoS-Angriffe: Über dem Mittel Verdopplung des Anteils der bandbreitenstarke Angriffe

Phishing-URLs und -IPs: Täglich 1000 neue





Wie bedroht ist Deutschlands Cyberraum?

Die Lage der IT-Sicherheit in Deutschland 2024

- Täglich wurde durchschnittlich rund 309.000 **neue Schadprogrammvarianten** entdeckt. Das ist ein **Zuwachs von 26%**
- In 2023 wurden mehr als **78 Schwachstellen in Softwareprodukten pro Tag** bekannt Das ist ein **Zuwachs von 14**%, im Vergleich zu 2022.
- **Russischer Angriffskrieg gegen die Ukraine**:
  Im Berichtszeitraum kam es zu einer Reihe pro-russischer Hacktivismus-Angriffe in Deutschland. Diese sind als Propaganda zu werten mit der Absicht, Verunsicherung zu stiften.

Wie bedroht ist Deutschlands Cyberraum?

Die Lage der IT-Sicherheit in Deutschland 2024

- **Ransomware** ist weiterhin die größte Bedrohung.
- Vermehrt wurden **kleine und mittlere Unternehmen (KMU) sowie Kommunalverwaltungen und kommunale Betriebe** angegriffen.
- **erfolgreiche Ransomware-Angriffe** auf IT-Dienstleister. 72 Kommunen, **1,7 Millionen Einwohner** und 20.000 Arbeitsplätze in Deutschland **betroffen**
- Außerdem hat das BSI den **Ausbau einer Schattenwirtschaft** cyberkrimineller Arbeitsteilung beobachtet.

Ransomware und seine Opfer

Die Lage der IT-Sicherheit in Deutschland 2024

Durchschnittliche Lösegeldzahlungen nach Quartal

In Dollar

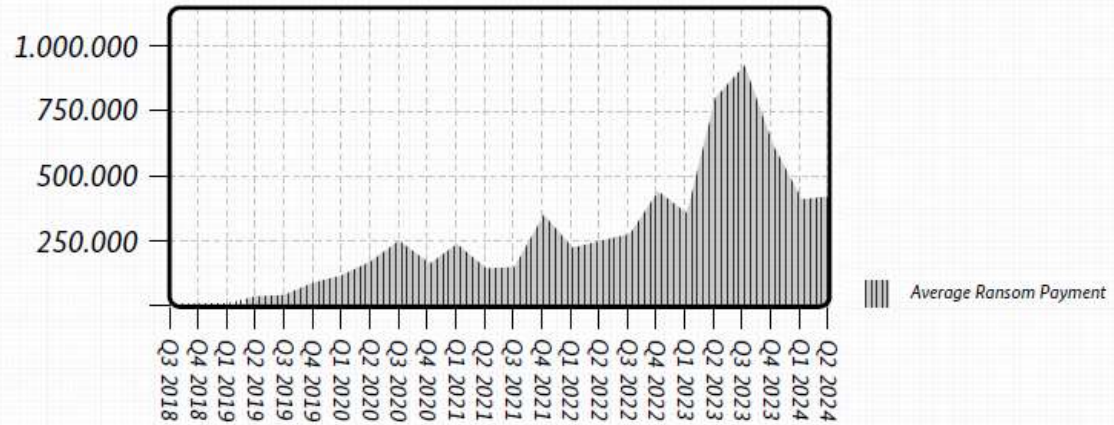


Abbildung 12: Durchschnittliche Lösegeldzahlungen nach Quartal (US-Dollar), (Quelle: Coveware)

Ransomware-Opfer, die Lösegeld zahlten

Anteil in Prozent an allen Ransomware-Opfern

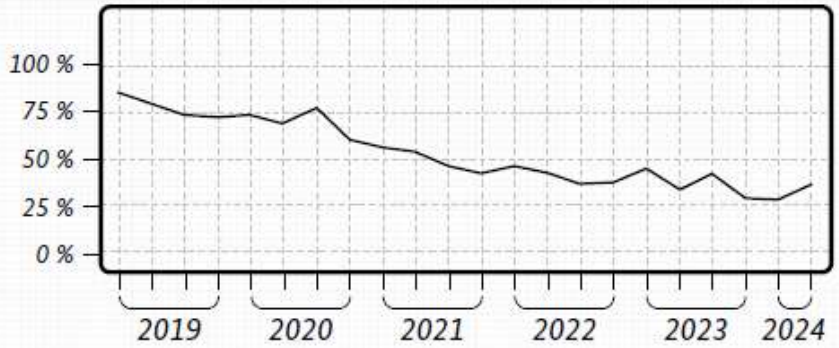


Abbildung 13: Ransomware-Opfer nach Zahlungsverhalten (Anteile) (Quelle: Coveware)

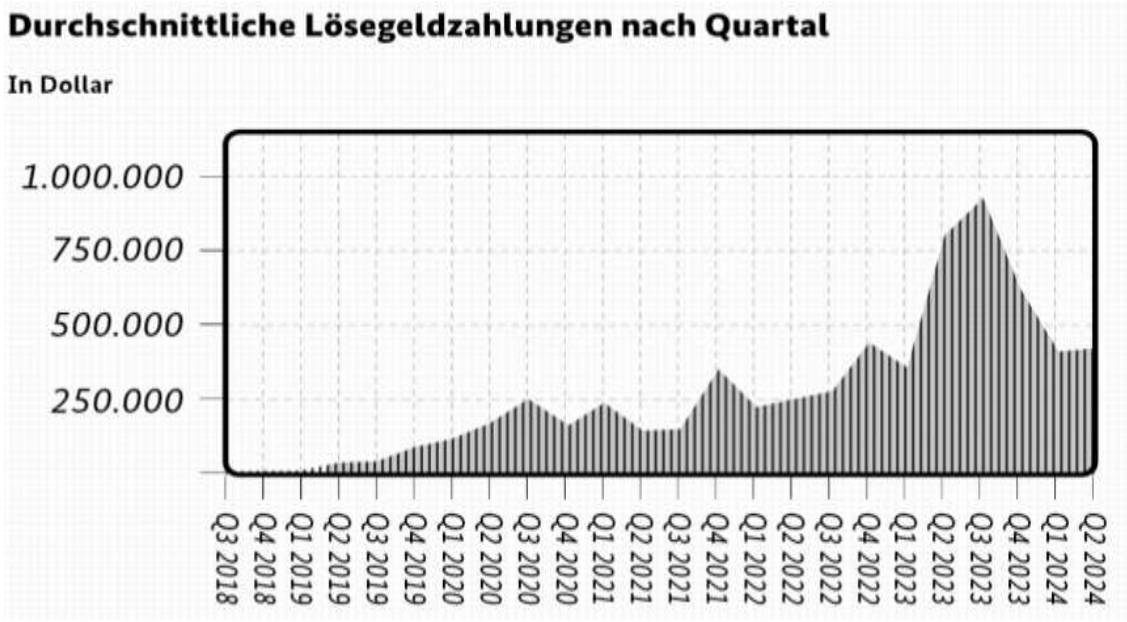
Angespannte Lage: Schadwirkung

Bundesamt für Sicherheit in der Informationstechnik

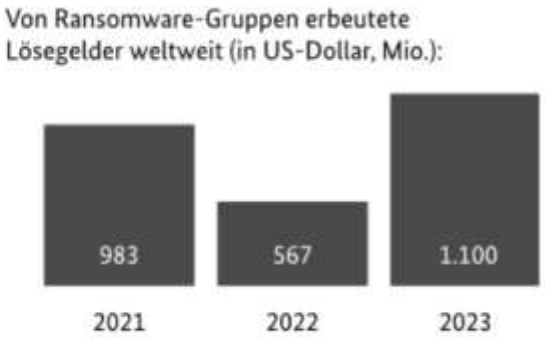
Bitkom-Studie: 179 Milliarden Euro Schaden durch Cyberangriffe im Jahr 2024 bei deutschen Unternehmen

Meldungen an das BSI: 726 Meldungen aufgrund von Cybervorfällen. Anstieg um 33%.

CrowdStrike-Vorfall: 5 Milliarden Schaden durch fehlerhaftes Update



Ransomware



Regel Nr. 1:

Jeder wird angegriffen, es gibt keine Ausnahmen!

Regel Nr. 1:

Jeder wird angegriffen, es gibt keine Ausnahmen!

- Identifizieren Sie Risikoprofil u. Kronjuwelen
- Sensibilisieren Sie Ihre Mitarbeiter
- Sichern Sie Ihre Systeme möglichst gut ab

Regel Nr. 2:

Früher oder später werden Ihre Schutzmaßnahmen versagen!

Regel Nr. 2:

Früher oder später werden Ihre Schutzmaßnahmen versagen!

- Erarbeiten Sie ein Notfallkonzept
- Befolgen Sie Ihre Backup-Strategie !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
- Bereiten Sie die Einholung externer Hilfe vor

  Schließen Sie ggf. eine Cyber-Versicherung ab

IT-Sicherheit ist Chefinnen- und Chefsache!

Sorgen Sie für klare Zuständigkeiten!

Reagieren Sie schnell auf Warnungen!

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zehntausende deutscher Microsoft Exchange Server haben kritische Sicherheitslücken

CSW-Nr. 2020-252437-1131, Version 1.1, 13.10.2020

IT-Bedrohungslage*: 3 / Orange

Sachverhalt

Seit mehreren Monaten stehen von Microsoft für die unter CVE-2020-0688, CVE-2020-0692 und CVE-2020-16875 gelisteten Sicherheitslücken des Groupware- und E-Mail-Servers Exchange Sicherheitsupdates bereit [MS2020a, MS2020b, MS2020c].

Bei CVE-2020-0688 handelt es sich um eine Static Key Schwachstelle im Microsoft Exchange Control Panel (ECP) die unter Verwendung eines gestohlenen E-Mail-Kontos die volle Systemkompromittierung ermöglicht. CVE-2020-0692 erlaubt die Eskalation von Privilegien.

Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

- Microsoft Exchange Server 2010 SP 3 Update RU30 (CVE-2020-0688)
- Microsoft Exchange Server 2013 Cummulative Update 23
- Microsoft Exchange Server 2016 Cummulative Update 14 und 15
- Microsoft Exchange Server 2019 Cummulative Update 3 und 4

Ebenso betroffen sind ältere Produktversionen.

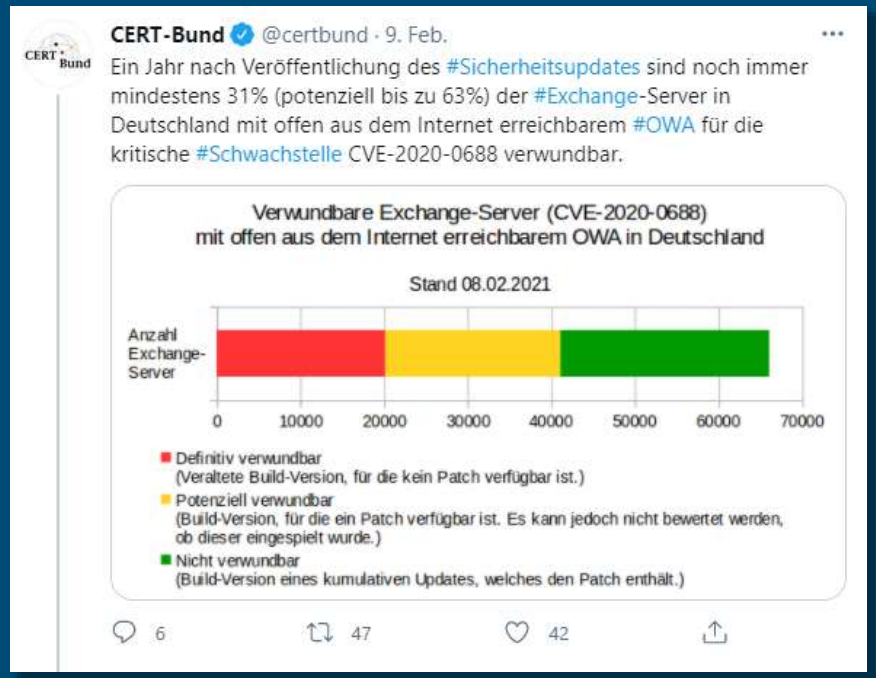
Bei CVE-2020-16875 handelt es sich um eine durch die fehlerhafte Argument-Validierung des New-DlpPolicy cmdlet bedingte Sicherheitslücke, die nach vorheriger Authentifizierung ebenfalls Remote Code Execution erlaubt.

Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

* 1 / Grün: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf erhöhtem Niveau.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

CSW # 2020-252437-1131 | Version 1.1 vom 13.10.2020 Seite 1 von 3

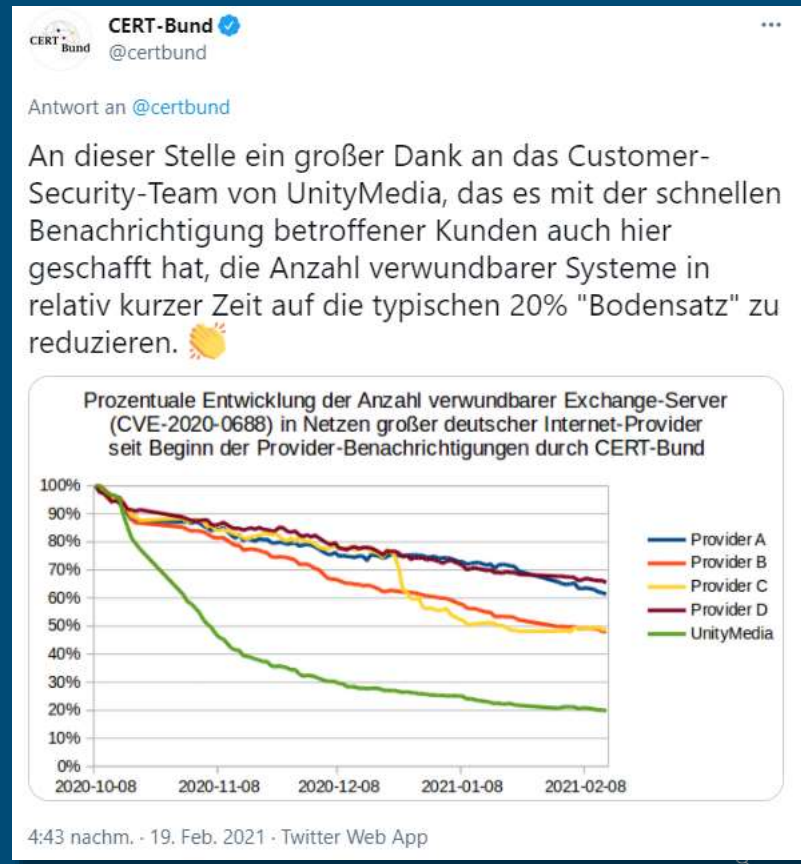
BSI-Cyber-Sicherheitswarnung



CERT-Bund @certbund · 9. Feb.

Ein Jahr nach Veröffentlichung des #Sicherheitsupdates sind noch immer mindestens 31% (potenziell bis zu 63%) der #Exchange-Server in Deutschland mit offen aus dem Internet erreichbarem #OWA für die kritische #Schwachstelle CVE-2020-0688 verwundbar.

6 47 42

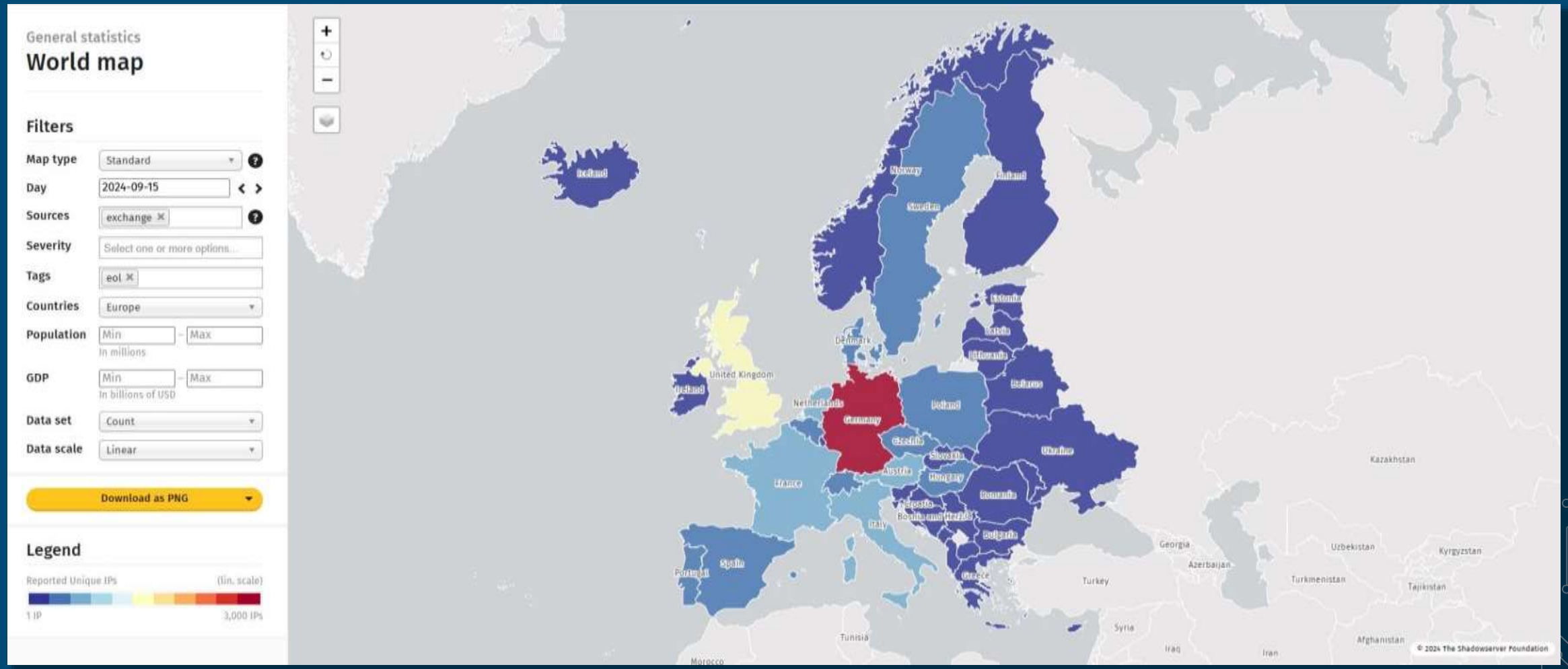


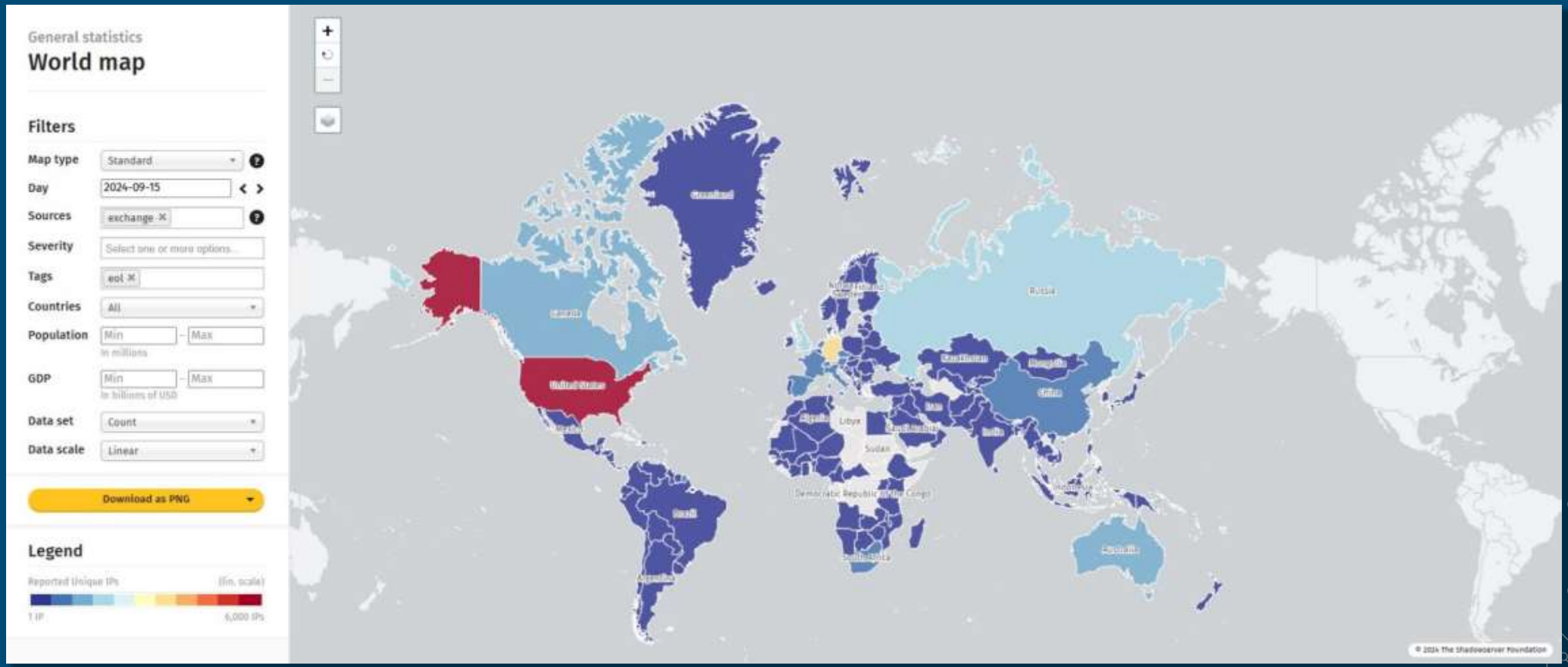
CERT-Bund @certbund

Antwort an @certbund

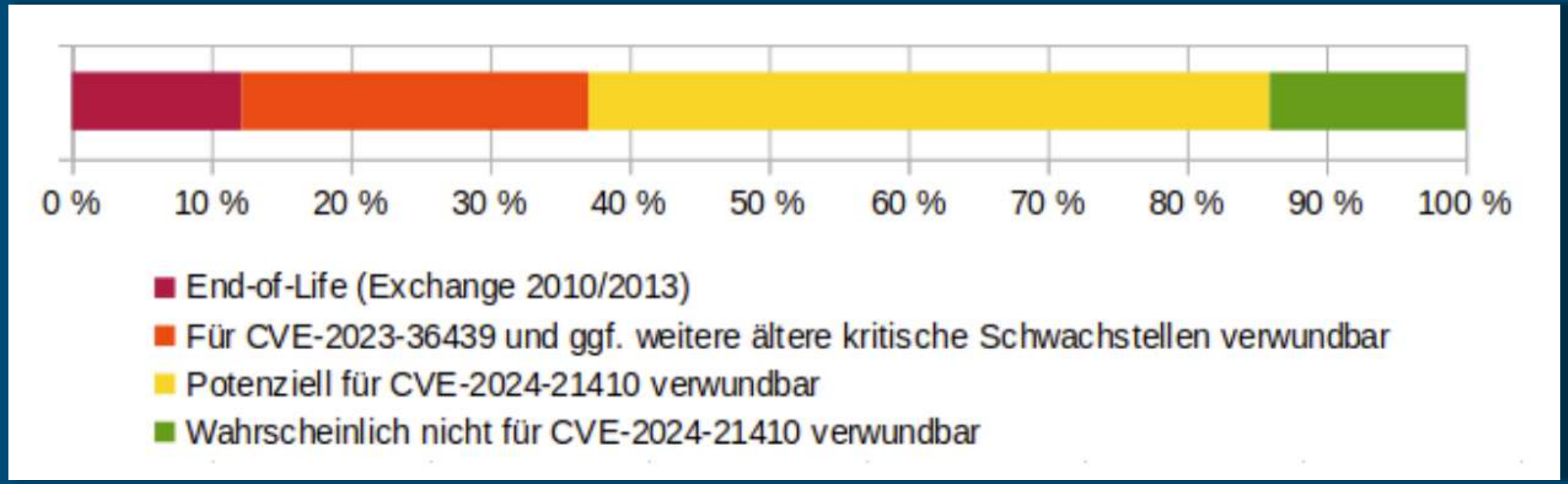
An dieser Stelle ein großer Dank an das Customer-Security-Team von UnityMedia, das es mit der schnellen Benachrichtigung betroffener Kunden auch hier geschafft hat, die Anzahl verwundbarer Systeme in relativ kurzer Zeit auf die typischen 20% "Bodensatz" zu reduzieren. 👏

4:43 nachm. · 19. Feb. 2021 · Twitter Web App


General statistics
World map
Filters
Map type
Standard
Day
2024-09-15
Sources
exchange
Severity
Select one or more options...
Tags
eol
Countries
Europe
Population
Min
Max
In millions
GDP
Min
Max
In billions of USD
Data set
Count
Data scale
Linear
Download as PNG
Legend
Reported Unique IPs
(lin. scale)
1 IP
3,000 IPs
Iceland
Norway
Sweden
Finland
Denmark
United Kingdom
Ireland
Netherlands
Germany
Poland
Belarus
Ukraine
France
Austria
Slovakia
Hungary
Romania
Italy
Bulgaria
Greece
Spain
Portugal
Turkey
Georgia
Azerbaijan
Kazakhstan
Uzbekistan
Kyrgyzstan
Turkmenistan
Tajikistan
Syria
Iraq
Iran
Afghanistan
Tunisia
Morocco
© 2024 The Shadowserver Foundation


General statistics
World map
Filters
Map type
Standard
Day
2024-09-15
Sources
exchange
Severity
Select one or more options...
Tags
eol
Countries
All
Population
Min
Max
In millions
GDP
Min
Max
In billions of USD
Data set
Count
Data scale
Linear
Download as PNG
Legend
Reported Unique IPs
(lin. scale)
1 IP
6,000 IPs
Russia
Libya
Sudan
© 2024 The Shadowserver Foundation

Ca. 45.000 Microsoft-Exchange-Server mit offen aus dem Internet erreichbaren Outlook Web Access / Outlook on the web



Üben Sie den Ernstfall !


VERHALTEN BEI IT-NOTFÄLLEN
Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!
IT-Notfallrufnummer:
0800-ULF
Wer meldet?
Welches IT-System ist betroffen?
Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?
Wann ist das Ereignis eingetreten?
Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)
Verhaltenshinweise
Weitere Arbeit am IT-System einstellen
Beobachtungen dokumentieren
Maßnahmen nur nach Anweisung einleiten
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Schließen Sie eine Cyber-Versicherung ab!

Führen Sie einen CyberRisikoCheck durch!!

nach DIN SPEC 27076

Warum noch ein Standard in der IT-Landschaft?

Das Problem:

- Selbstchecks funktionieren nur bedingt
- Anforderungen bestehender Standards für KMU oft zu hoch

Die Lösung:

- Bundesweiter standardisierter Beratungsprozess für KKU zur Feststellung des aktuellen **Cyberrisikostatus -** getragen von den relevanten Beteiligten der Cybersicherheitslandschaft
- Niederschwelliges Präventionsangebot – „Einstieg" in die Cybersicherheit und Sensibilisierung
- Interview: IT-Berater -> Unternehmensleitung
  - 6 Handlungsfelder
  - 27 Anforderungen – Fragen – Handlungsempfehlungen
  - -> Definierter Bericht

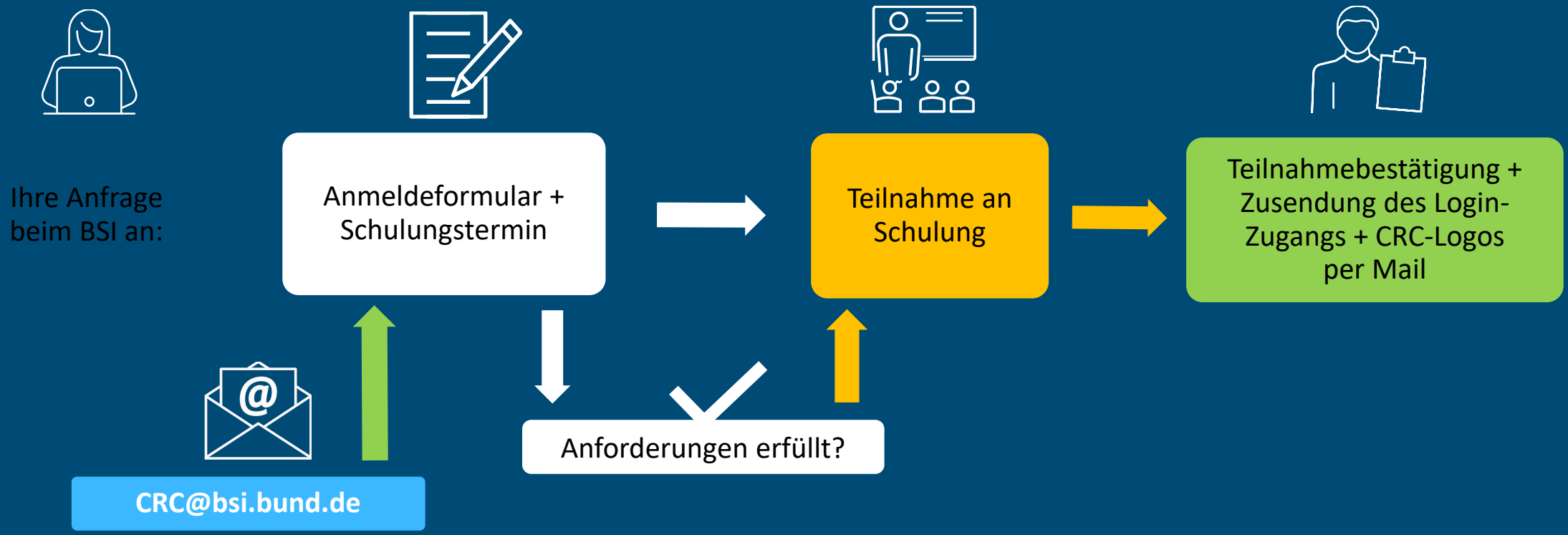
Warum stellt das BSI eine Software bereit?

- Abbau von Hürden für den Einstieg in die Cybersicherheitsberatung nach DIN SPEC 27076 für die IT-Dienstleister
  - → Keine Investition in Eigenentwicklung einer Software nötig
  - → Keine Lizenzverhandlungen mit dem DIN nötig
- Leichtere Standardisierung der Beratung über verschiedene Dienstleister hinweg
- Änderungen basierend auf Rückmeldungen aus der Beratung kommen direkt allen anderen zugute

Voraussetzungen für die Nutzung

- Sowohl akademisches als auch praxisbezogenes Wissen gewünscht
- Mindestens ein Jahr Erfahrung in der Durchführung von IT-Sicherheitsberatungen/Audits;
- Mindestens drei Referenzprojekte der Durchführung von IT-Sicherheitsberatungen/Audits mit Klein- oder Kleinstunternehmen;
- Nachweis des für die Beratung notwendigen methodischen Wissens zur Gesprächsmethode des semistrukturierten Leitfadeninterviews
  (→ wird durch die Teilnahme an der BSI-Schulung erbracht)
- Andere Qualifikationen können anerkannt werden

Wo bitte geht‘s zum Login?



Das BSI qualifiziert IT-Dienstleistungsunternehmen

2024 & 2025 insgesamt mehr als **15 Schulungen** für IT-Dienstleistungsunternehmen **zur Anwendung des CyberRisikoChecks**

- **über 1.000 geschulte Personen**
- **Über 550 Unternehmen**

Schulungstermine für 2025:

- **ausgebucht**

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/CyberRisikoCheck/Karte/karte_node.html

Cyber-Sicherheit umgangssprachlich auf einfachem Niveau erklärt.

Direktlink zum Angebot für KMU:

www.bsi.bund.de/kmu

- Informationen zum CyberRisikoCheck
- Tipps und Tricks für die Zielgruppe KMU
- Kontaktmöglichkeit bei Sicherheitsvorfällen
- Abomöglichkeit KMU-Newsletter

#nis2know

#nis2know
Wissen, wie es weitergeht

Wie es für Unternehmen nach der Bundestagswahl mit NIS-2 weitergeht

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (2022/2555)

NIS-2-Richtlinie – Worum geht es?

- rechtliche Maßnahmen zur **Steigerung des Gesamtniveaus der Cybersicherheit** in der EU
- **Einheitliches Sicherheitsniveau** in den Mitgliedstaaten der EU **schaffen und verbessern**
- **Umsetzung** der NIS-2-RL in nationales Recht wahrscheinlich durch **Änderung des BSI-Gesetzes**
- BSI wird wahrscheinlich für ca. **29.000** neue besonders wichtige (bwE) und "wichtige" Einrichtungen (wE) zur **Aufsichtsbehörde**; die bisherigen regulierten KRITIS werden eine Teilmenge der bwE
- Einführung von **Registrierungs- und Meldepflichten** für bwE und wE
- Unternehmen müssen **angemessene, wirksame und geeignete Risikomanagementmaßnahmen** umsetzen, dokumentieren und regelmäßig überprüfen lassen

Intensität Regulierung

Keine Angst vor Artikel 21

Risikomanagementmaßnahmen

Angemessen, wirksam und verhältnismäßig umsetzen, dokumentieren und ggf. überprüfen lassen:

Risikoanalyse und Sicherheit für Informationssysteme	Bewältigung von Sicherheitsvorfällen	BCM und Krisenmanagement	Sichere Lieferkette	NIS-Sicherheits-maßnahmen und Schwachstellen-management
Wirksamkeit von Risikomanagementmaßnahmen	Cyberhygiene und Schulungen	Kryptografie/ Verschlüsselung	Sicherheit des Personals/ Zugriffskontrolle	MFA/ Authentifizierung, und sichere Kommunikation

Wenn Unternehmen IT-Sicherheit ernst nehmen, werden diese Maßnahmen höchstwahrscheinlich schon übererfüllt

#nis2know Infopakete sind in Arbeit

Unterstützung von Unternehmen – Wie hilft das BSI?

Betroffenheitsprüfung

- Überprüfung, ob das Unternehmen von **NIS-2 betroffen** ist
- Basierend auf **Eigenauskünften**
- Ergebnis **rechtlich nicht verbindlich**

NIS-2-FAQ

- Sammlung von **Antworten** auf die am häufigsten gestellten **Fragen zur NIS-2-Richtlinie**
- Stand der **Gesetzgebung**
- Erste Details zu **gesetzlichen Pflichten**
- **Sektorspezifische Informationen**

NIS-2-Was tun?

- Was können Unternehmen jetzt schon tun, um sich auf NIS-2 **vorzubereiten**
- **Praktische Hinweise, Hilfestellungen**
- Wird stetig **ergänzt und aktualisiert**

Nutzen Sie das BSI !

Fazit

Der **CyberRisikoCheck** ist der erster Schritt für **KMU** zur sicheren digitalen **Wertschöpfung** & zur Stärkung der **Cybernation**!

-

Besuchen Sie unsere Webseite!

Investieren Sie jetzt in Präventionsmaßnahmen.

Es lohnt sich!

Cybersicherheit ist Chefinnen- und Chefsache!

Bauen wir gemeinsam die Cybernation Deutschland!

» https://www.bsi.bund.de/kmu

Vielen Dank für Ihre Aufmerksamkeit!

Julian Rupp

Referat „Cyber-Sicherheit für Kleine und Mittlere Unternehmen (KMU)“

Julian.Rupp@bsi.bund.de

crc@bsi.bund.de

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

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: