Workshop „Der CyberRisikoCheck für kleine Unternehmen“

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

Cybersecurity Day, IHK München
29.01.2025

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

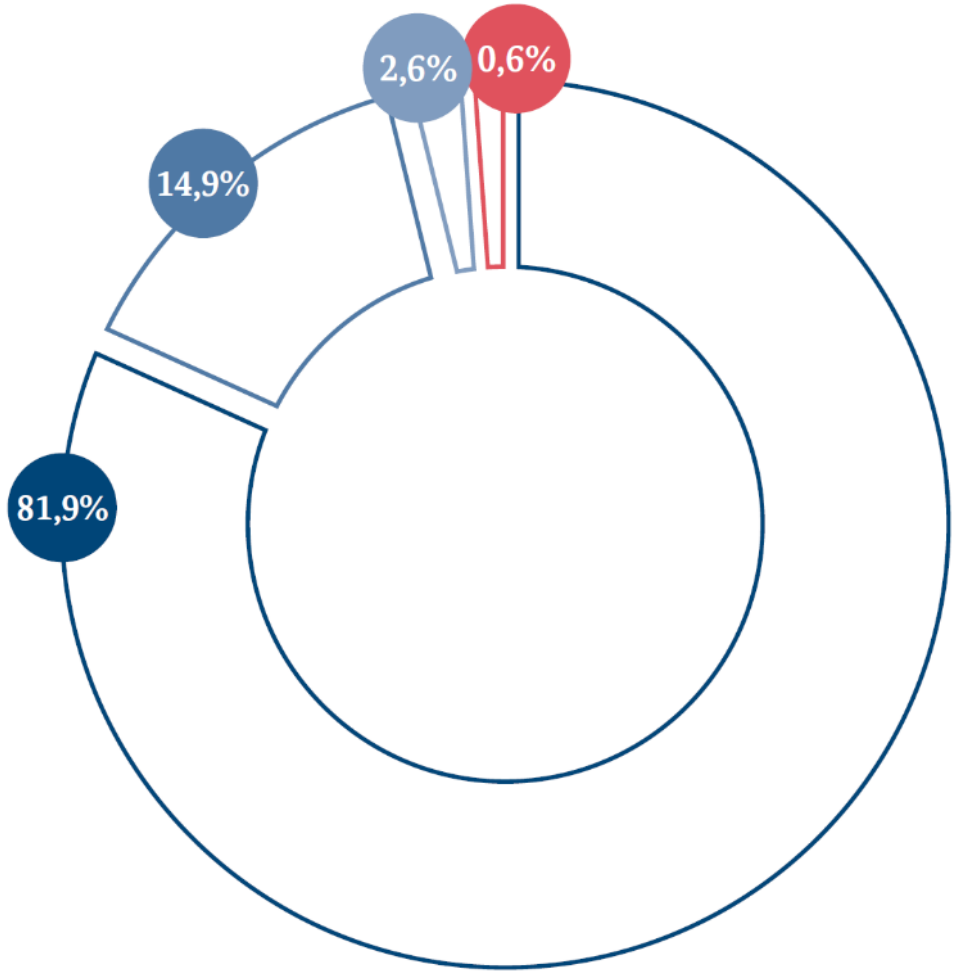
Cybersicherheit
gestalten

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

Bundesamt für Sicherheit in der Informationstechnik

Top-3-Bedrohungen je Zielgruppe:

Gesellschaft

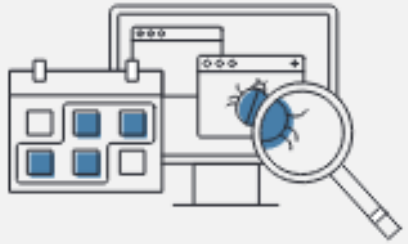
Identitätsdiebstahl
Sextortion
Phishing

Wirtschaft

Ransomware
Abhängigkeit innerhalb der IT-Supply-Chain
Schwachstellen, offene oder falsch konfigurierte Onlineserver

Staat und Verwaltung

Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Onlineserver

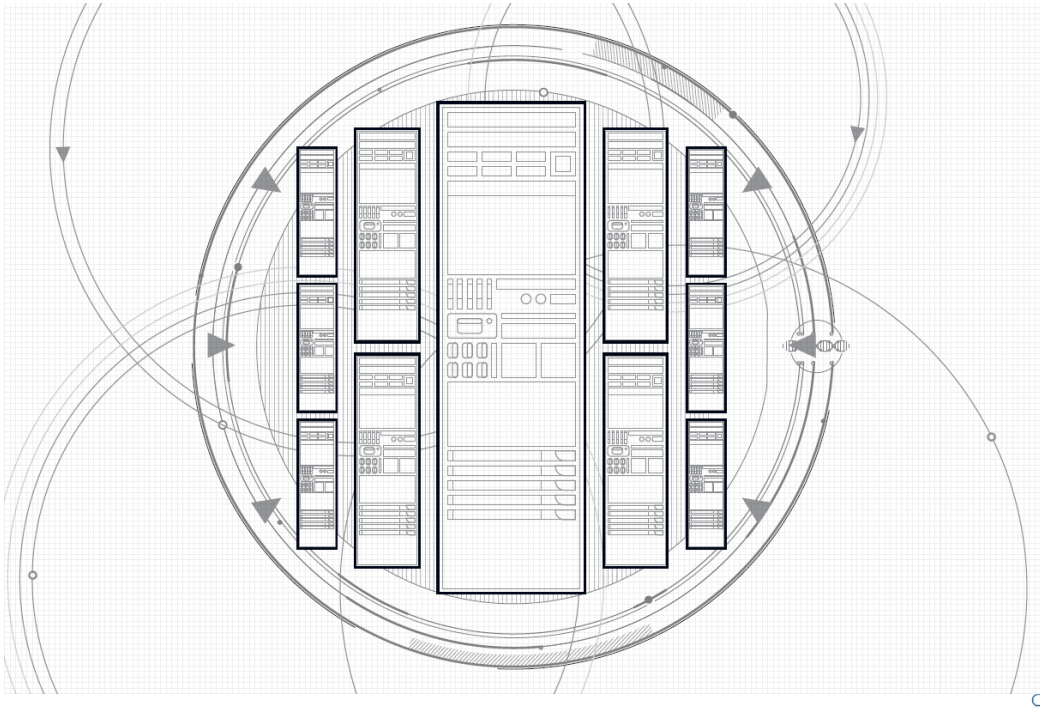


Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

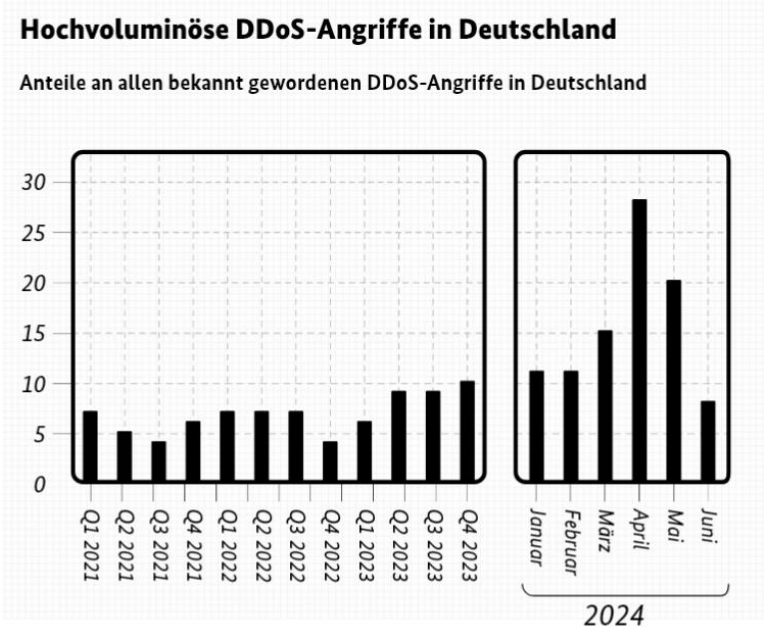
Wie bedroht ist Deutschlands Cyberraum? - Angriffsfläche

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

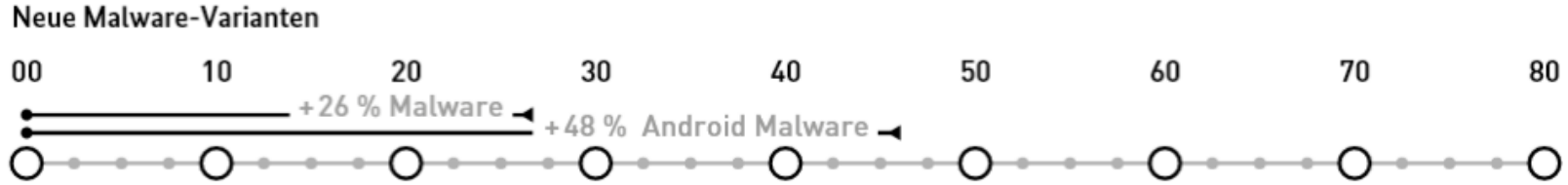


Schadprogramm-Varianten: Durchschnittlich 309 000 neue pro Tag

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

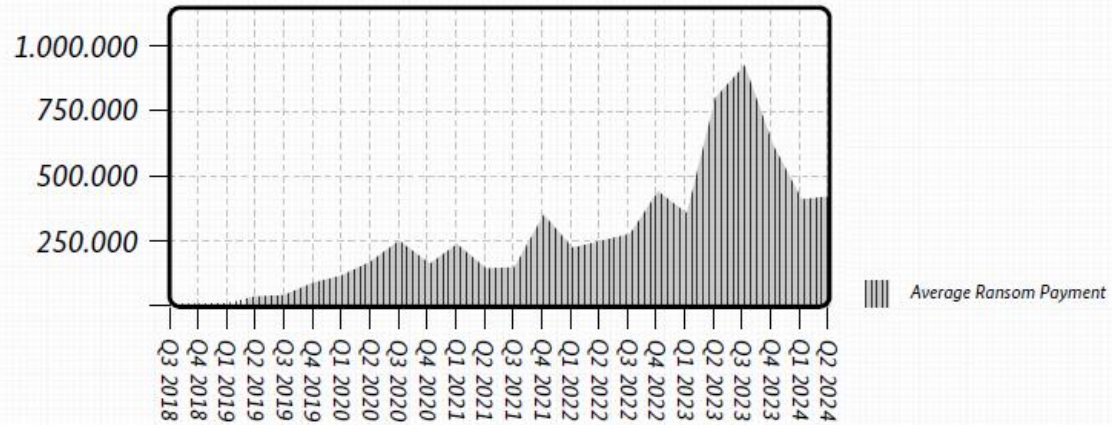


Abbildung 12: Durchschnittliche Lösegeldzahlungen nach Quartal (US-Dollar), (Quelle: Coveware)

Ransomware-Opfer, die Lösegeld zahlten

Anteil in Prozent an allen Ransomware-Opfern

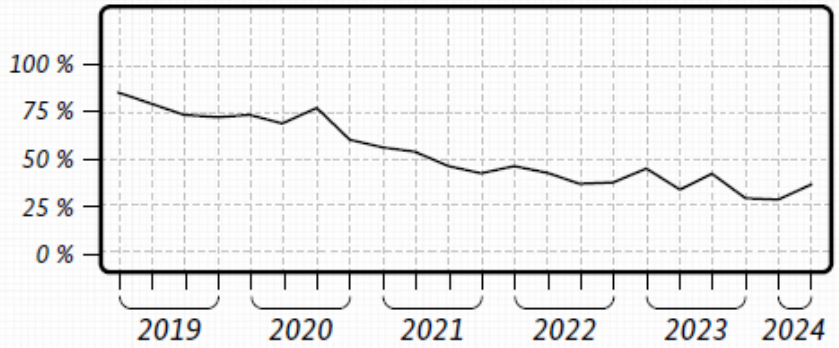


Abbildung 13: Ransomware-Opfer nach Zahlungsverhalten (Anteile) (Quelle: Coveware)

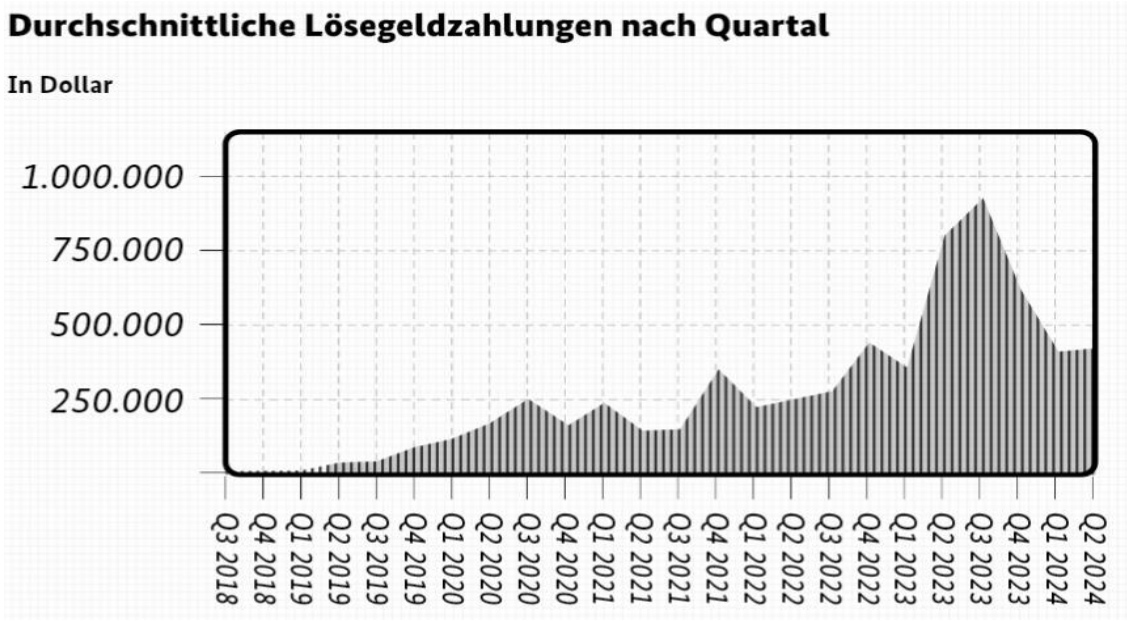
Angespannte Lage: Schadwirkung

Bundesamt für Sicherheit in der Informationstechnik

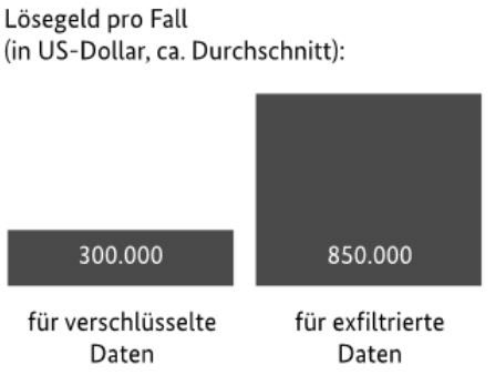
Bitkom-Studie: 179 Milliarden Euro Schaden durch Cyberangriffe im Jahr 2024 bei deutschen Unternehmen

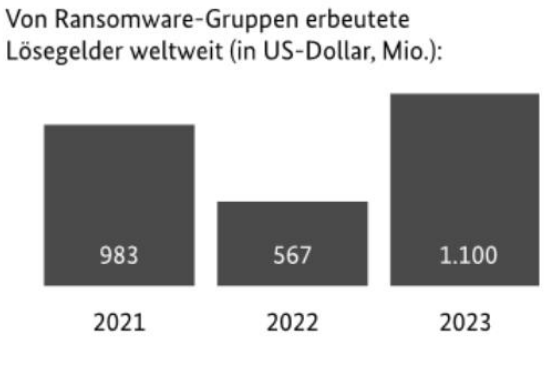
Meldungen an das BSI: 726 Meldungen aufgrund von Cybervorfällen. Anstieg um 33%.

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 geführten 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 Authentisierung ebenfalls Remote Code Execution erlaubt.

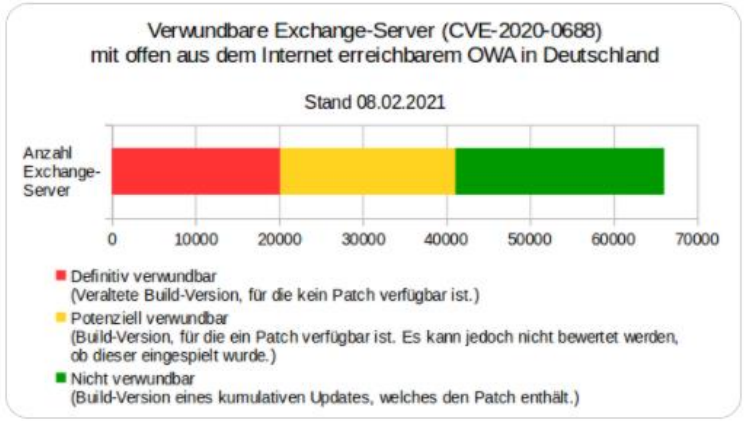
Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem 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.

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.

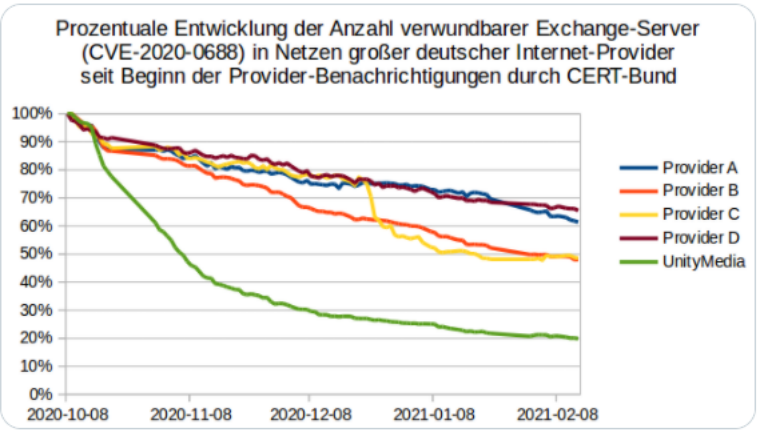


6 47 42

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

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 geführten 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

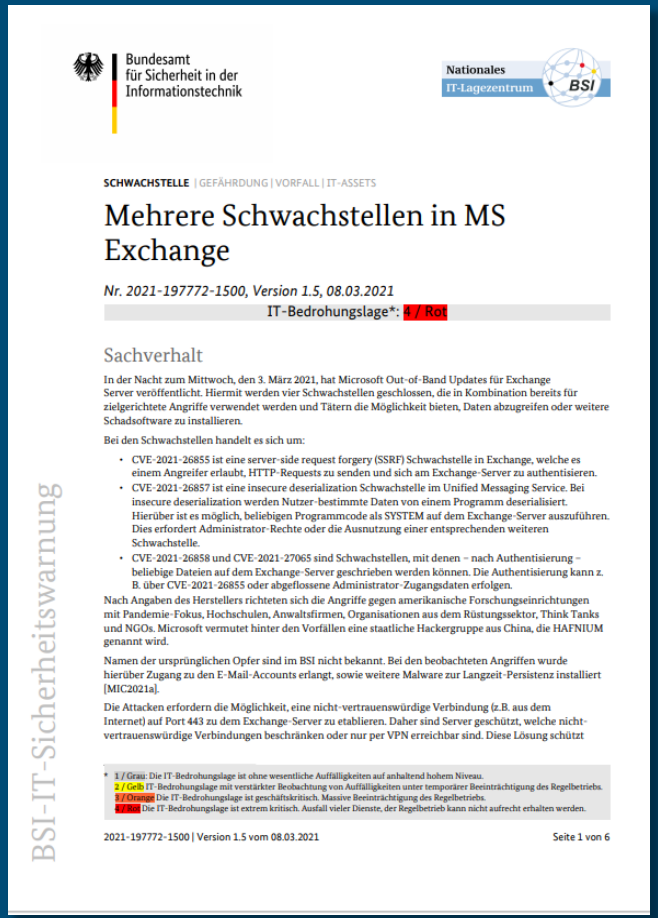
Ebenso betroffen sind ältere Produktversionen.

Bei CVE-2020-16875 handelt es sich um eine durch die fehlerhafte Argument-Validierung des New-DlpPolicy cmdlet bedingte Sicherheitslücke, die nach vorheriger Authentisierung 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 anhaltend hohem 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.

BSI-Cyber-Sicherheitswarnung



Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Mehrere Schwachstellen in MS Exchange

Nr. 2021-197772-1500, Version 1.5, 08.03.2021

IT-Bedrohungslage*: 4 / Rot

Sachverhalt

In der Nacht zum Mittwoch, den 3. März 2021, hat Microsoft Out-of-Band Updates für Exchange Server veröffentlicht. Hiermit werden vier Schwachstellen geschlossen, die in Kombination bereits für zielgerichtete Angriffe verwendet werden und Tätern die Möglichkeit bieten, Daten abzugreifen oder weitere Schadsoftware zu installieren.

Bei den Schwachstellen handelt es sich um:

- CVE-2021-26855 ist eine server-side request forgery (SSRF) Schwachstelle in Exchange, welche es einem Angreifer erlaubt, HTTP-Requests zu senden und sich am Exchange-Server zu authentisieren.
- CVE-2021-26857 ist eine insecure deserialization Schwachstelle im Unified Messaging Service. Bei insecure deserialization werden Nutzer-bestimmte Daten von einem Programm deserialisiert. Hierüber ist es möglich, beliebigen Programmcode als SYSTEM auf dem Exchange-Server auszuführen. Dies erfordert Administrator-Rechte oder die Ausnutzung einer entsprechenden weiteren Schwachstelle.
- CVE-2021-26858 und CVE-2021-27065 sind Schwachstellen, mit denen – nach Authentisierung – beliebige Dateien auf dem Exchange-Server geschrieben werden können. Die Authentisierung kann z. B. über CVE-2021-26855 oder abgeflossene Administrator-Zugangsdaten erfolgen.

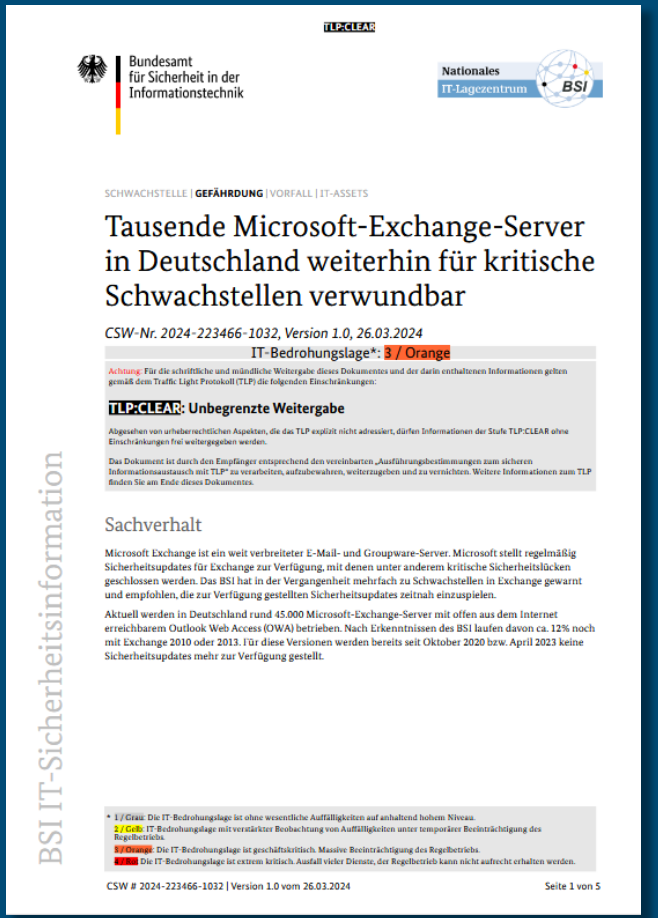
Nach Angaben des Herstellers richteten sich die Angriffe gegen amerikanische Forschungseinrichtungen mit Pandemie-Fokus, Hochschulen, Anwaltsfirmen, Organisationen aus dem Rüstungssektor, Think Tanks und NGOs. Microsoft vermutet hinter den Vorfällen eine staatliche Hackergruppe aus China, die HAFNIUM genannt wird.

Namen der ursprünglichen Opfer sind im BSI nicht bekannt. Bei den beobachteten Angriffen wurde hierüber Zugang zu den E-Mail-Accounts erlangt, sowie weitere Malware zur Langzeit-Persistenz installiert [MIC2021a].

Die Attacken erfordern die Möglichkeit, eine nicht-vertrauenswürdige Verbindung (z.B. aus dem Internet) auf Port 443 zu dem Exchange-Server zu etablieren. Daher sind Server geschützt, welche nicht-vertrauenswürdige Verbindungen beschränken oder nur per VPN erreichbar sind. Diese Lösung schützt

* 1 / Grün: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem 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.

BSI-IT-Sicherheitswarnung



TLP:CLEAR

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | **GEFÄHRDUNG** | VORFALL | IT-ASSETS

Tausende Microsoft-Exchange-Server in Deutschland weiterhin für kritische Schwachstellen verwundbar

CSW-Nr. 2024-223466-1032, Version 1.0, 26.03.2024

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP" zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Microsoft Exchange ist ein weit verbreiteter E-Mail- und Groupware-Server. Microsoft stellt regelmäßig Sicherheitsupdates für Exchange zur Verfügung, mit denen unter anderem kritische Sicherheitslücken geschlossen werden. Das BSI hat in der Vergangenheit mehrfach zu Schwachstellen in Exchange gewarnt und empfohlen, die zur Verfügung gestellten Sicherheitsupdates zeitnah einzuspielen.

Aktuell werden in Deutschland rund 45.000 Microsoft-Exchange-Server mit offen aus dem Internet erreichbarem Outlook Web Access (OWA) betrieben. Nach Erkenntnissen des BSI laufen davon ca. 12% noch mit Exchange 2010 oder 2013. Für diese Versionen werden bereits seit Oktober 2020 bzw. April 2023 keine Sicherheitsupdates mehr zur Verfügung gestellt.

* 1 / Grün: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem 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.

BSI IT-Sicherheitsinformation

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

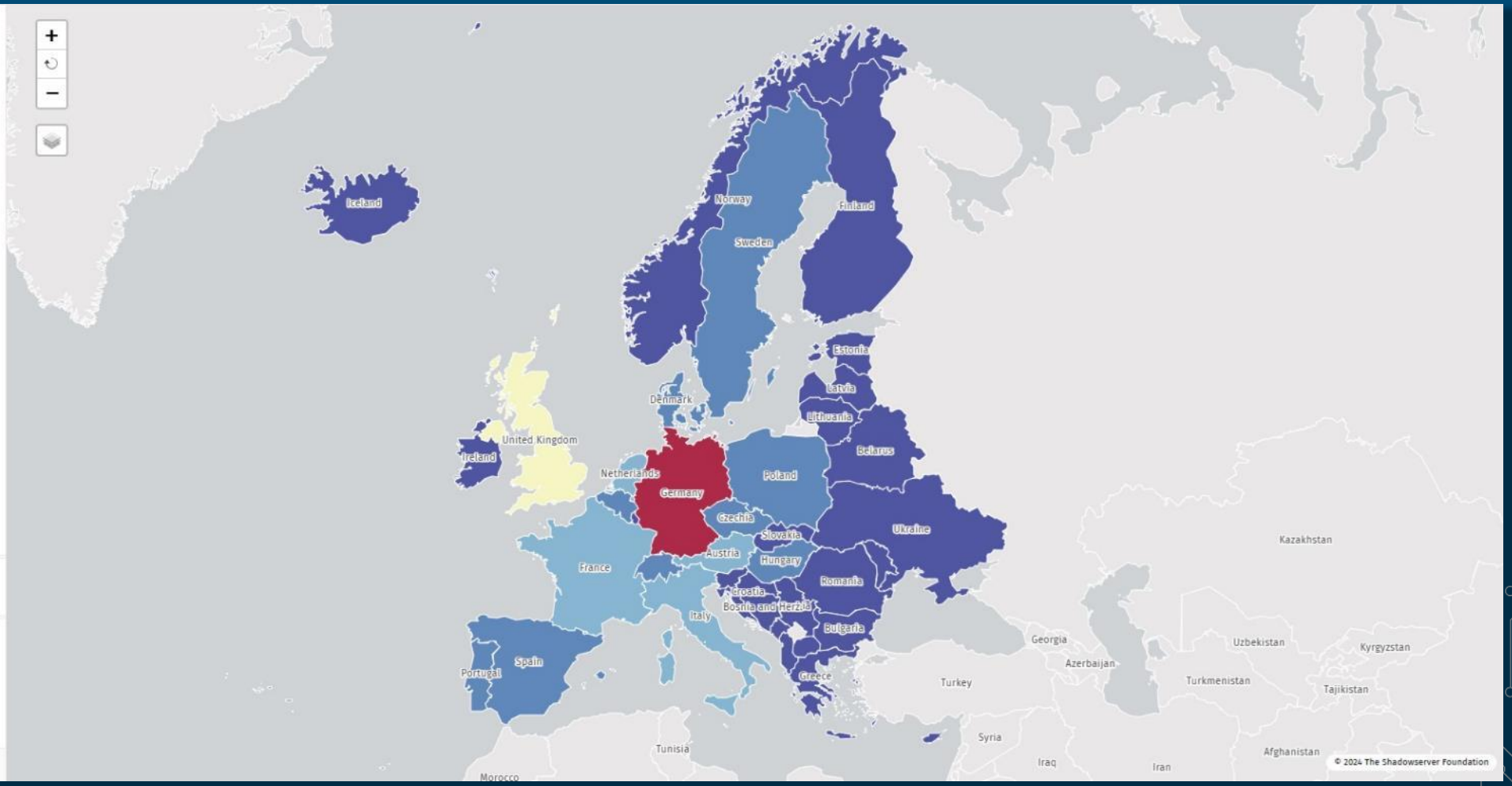
Data scale: Linear

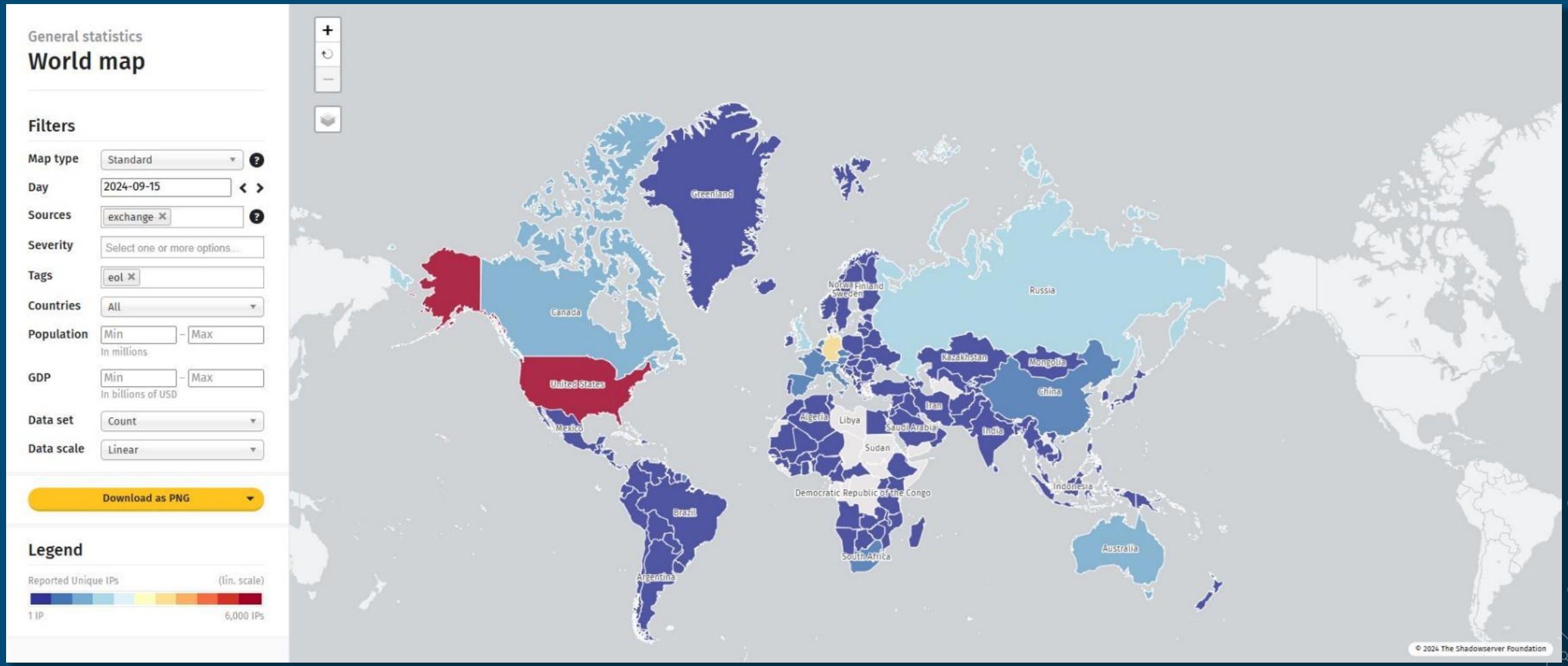
Download as PNG

Legend

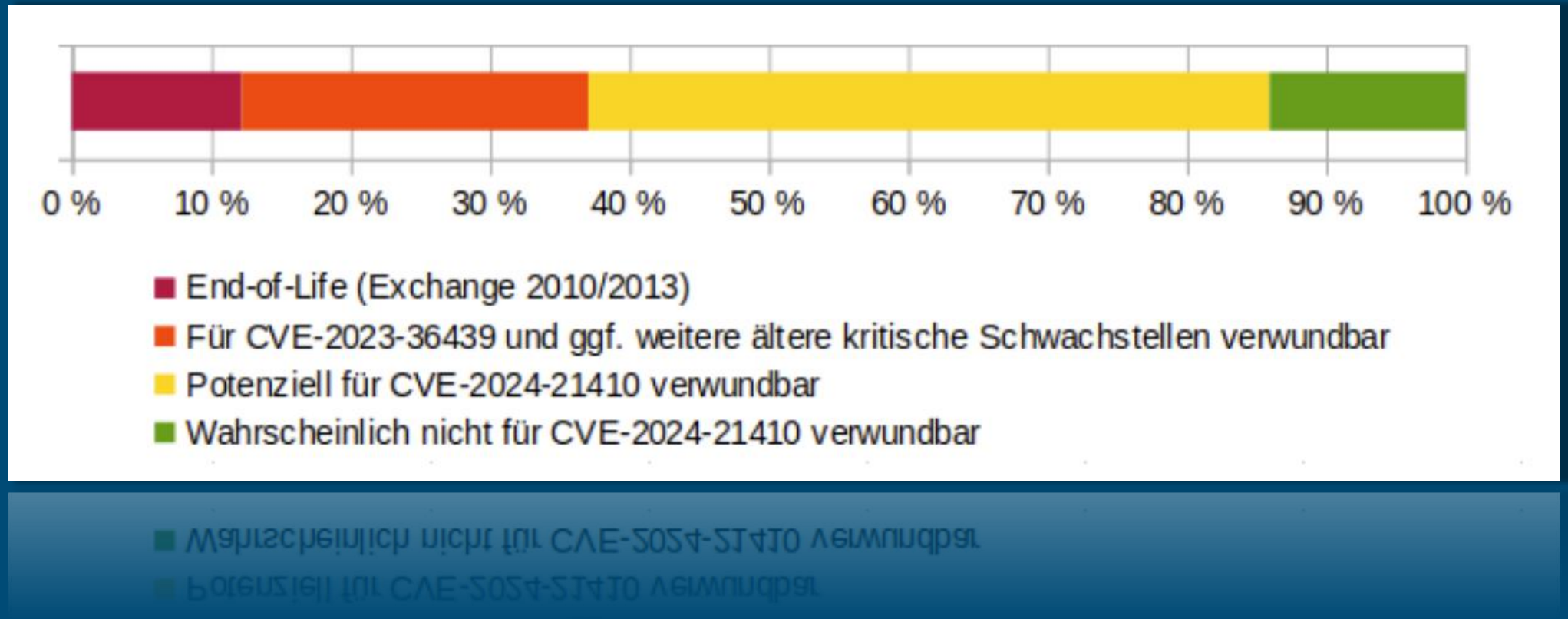
Reported Unique IPs (lin. scale)

1 IP — 3,000 IPs




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
Greenland
Canada
United States
Mexico
Brazil
Argentina
Norway
Finland
Sweden
Russia
Kazakhstan
Mongolia
China
Iran
Algeria
Libya
Saudi Arabia
India
Sudan
Democratic Republic of the Congo
South Africa
Indonesia
Australia
© 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

Der Ablauf

1 Das Erstgespräch

- Wer soll an dem Termin teilnehmen?
- Wie lange dauert die Befragung?
- Welche passenden Fördermittel gibt es?
- Was erwartet das Unternehmen?

2 Analyse des Informationssicherheitsniveaus eines KMU:

- (Online-) Befragung durch einen IT-Dienstleister
- Soll – Ist – Vergleich mit Hilfe des Anforderungs- & Fragenkatalogs
- Bewertung anhand eines standardisierten Scoring-Modells

3 Erstellung eines Ergebnisberichtes, dieser enthält:

- IST-Stand des Informationssicherheitsniveaus inkl. der ermittelten Score-Werte
- Priorisierte Handlungsempfehlungen zur weiteren Verbesserung der Informationssicherheit und als Grundlage für die Beauftragung eines IT-Dienstleisters

4

Präsentation des Ergebnisberichts & ggfs. Umsetzung der Handlungsempfehlungen

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

Vorteile der Nutzung der BSI-Software

Für Dienstleister:

- Nennung als Dienstleister für den CyberRisikoCheck auf der BSI-Seite
- Verwendung des offiziellen CyberRisikoCheck-Logos des BSI
- Sicherstellung der standardkonformen Beratung
- Unbegrenzte Anzahl an Checks möglich
- Übernahme der fälligen Lizenzgebühren des DIN durch das BSI!
- Mitgestaltung: Ihr Feedback ist uns wichtig!

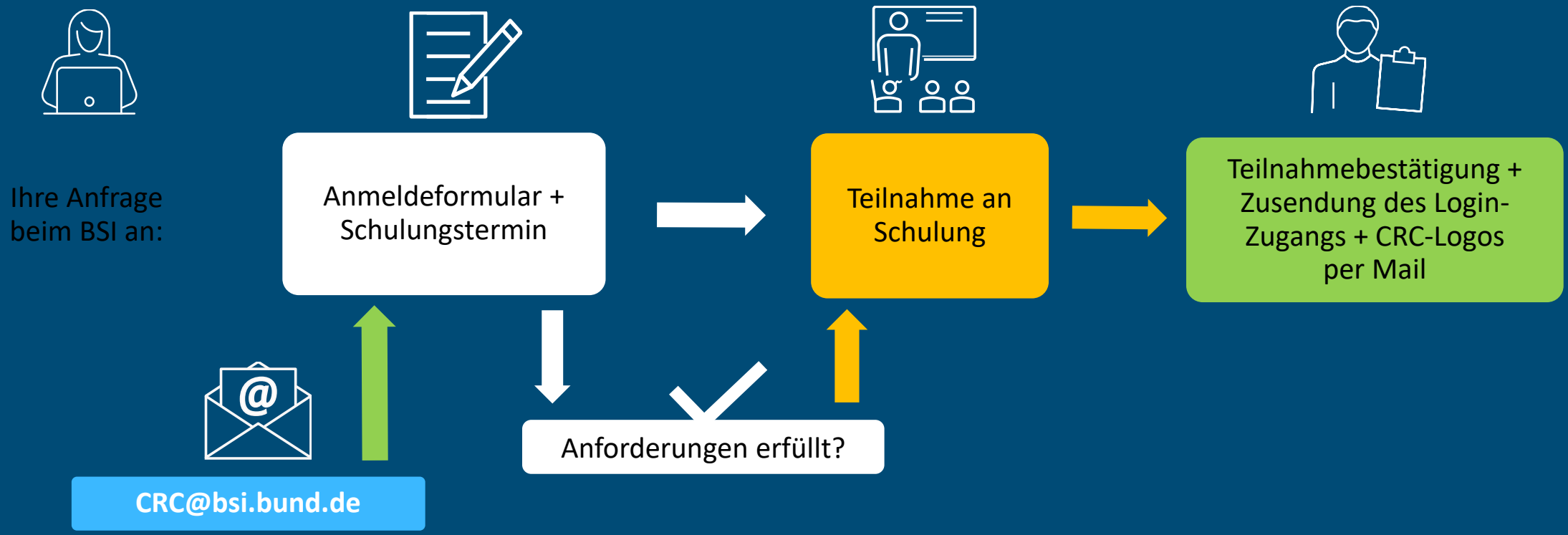
Für das BSI:

- BSI nutzt die **anonymen** Daten zur Erstellung des nationalen KMU-Lagebildes
- Zielgerichtete Prävention auf der Grundlage der Daten möglich

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?



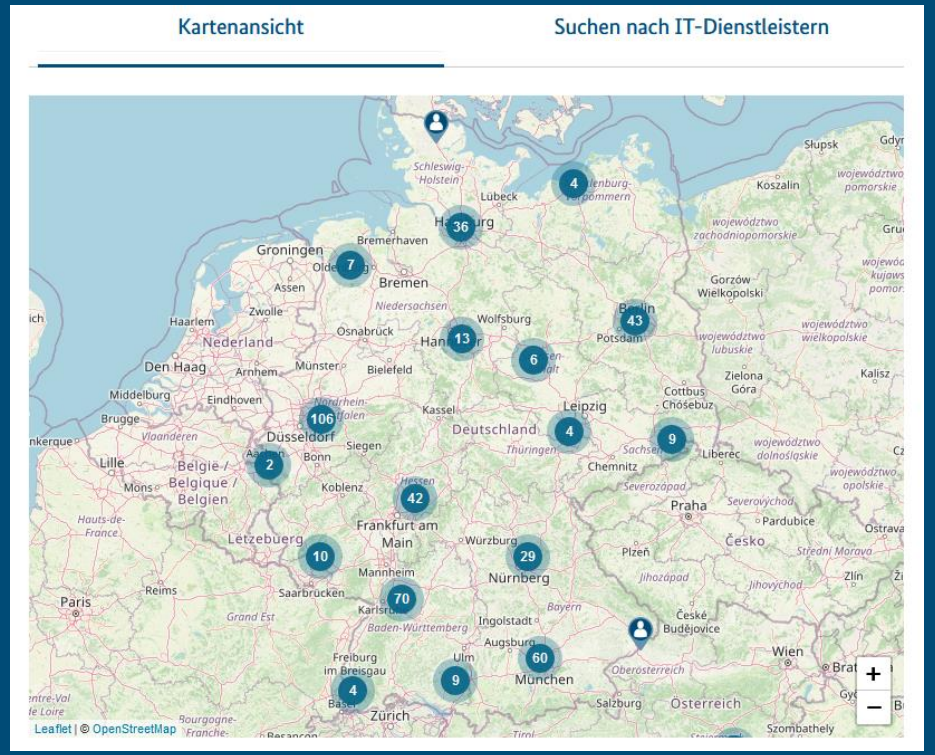
Das BSI qualifiziert IT-Dienstleistungsunternehmen

2024 insgesamt **10 Schulungen** für IT-Dienstleistungsunternehmen **zur Anwendung des CyberRisikoChecks**

- **über 750 geschulte Personen aus**
- **Über 460 Unternehmen**

Schulungstermine für 2025:

- **20.02.2025 (ausgebucht)**
- **01.04.2025 (online)**



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

Weitere Infomaterialien

Vor dem CyberRisiko-Check: Optimal vorbereitet

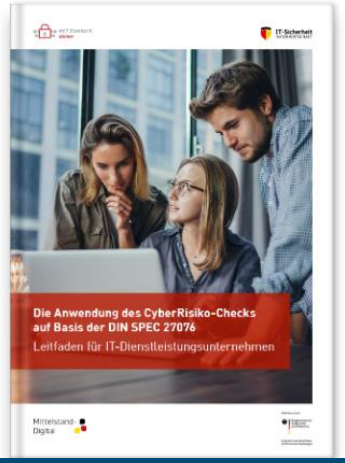
Das müssen kleine Unternehmen vor dem CyberRisiko-Check beachten

Nach dem CyberRisiko-Check: Ein erfolgreicher Abschluss

Damit fahren kleine Unternehmen zielgerichtet fort

Leitfaden für IT-Dienstleistungsunternehmen

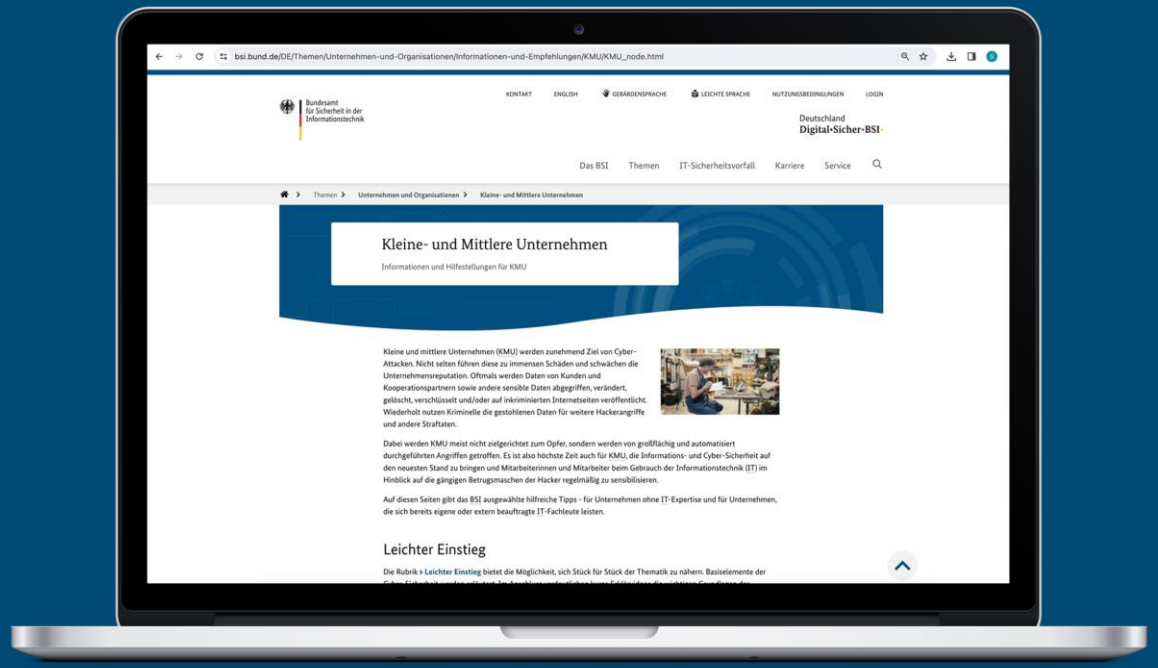
Leitfaden für die Anwendung des CyberRisiko-Checks



https://mit-standard-sicher.de/informationsmaterialien/

Nutzen Sie das BSI !

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

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

wwww.soscisurvey.de/bsikmu/?q=qnr10

Follow us: