Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Die größten Cyber-Fehler von KMU – und wie man sich dagegen wappnet

Manuel Bach, Leiter des Referats W 25 - „Cybersicherheit bei KMU“
Bundesamt Bundesamt für Sicherheit in der Informationstechnik

Industrie-Dialog am Nachmittag - „Hybride Bedrohungen im Fokus I: Prävention und Krisenbewältigung für KMU, MWVLW RLP, Mainz, 25. November 2024

Kurzprofil des BSI

Gründung
01. Januar 1991

237,9 Mio. Euro
Budget Haushalt 2024

Stellen 2024
1785

BSI vor Ort

- Standorte
- Stützpunkte
- Verbindungsstellen

Darüber hinaus engagiert sich das BSI seit langem intensiv im internationalen und nationalen Rahmen, unter anderem in enger Zusammenarbeit mit bilateralen Partnern sowie in multilateralen Handlungsfeldern rund um EU und NATO.

Leitsatz

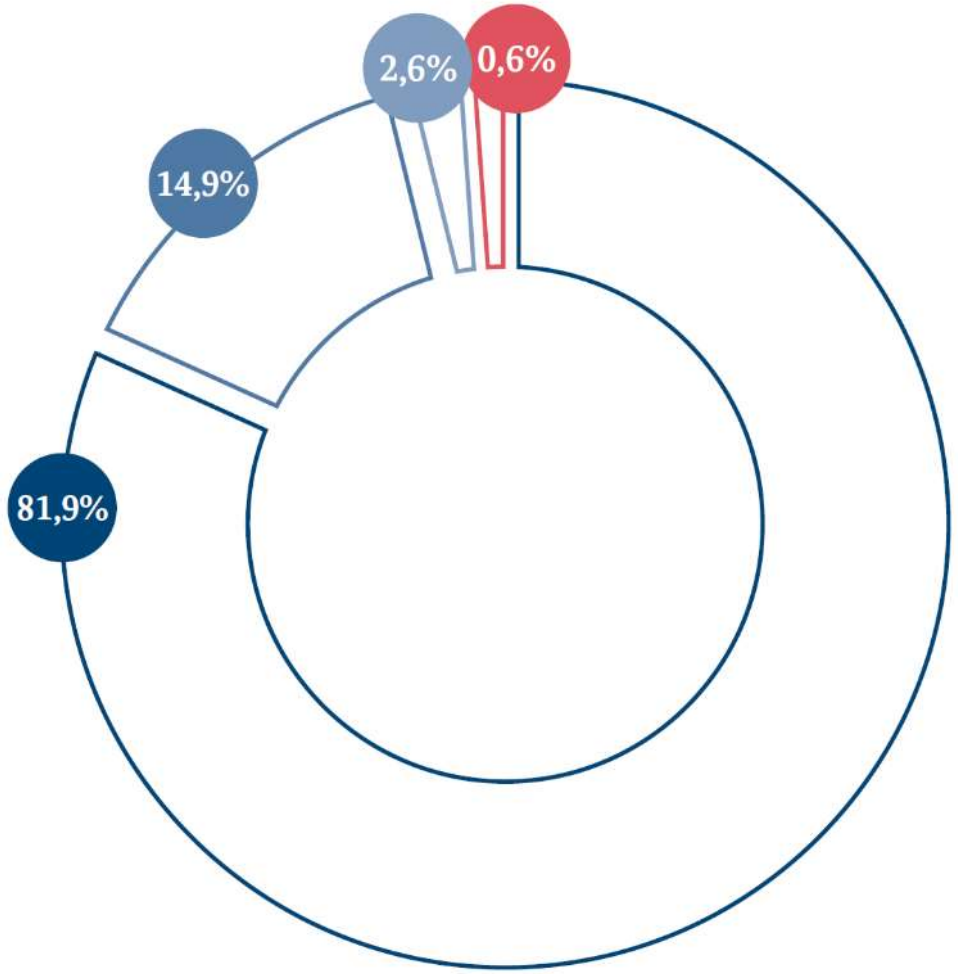
Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Leitsatz

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

Unternehmen in Deutschland nach Größe

Angaben in Prozent

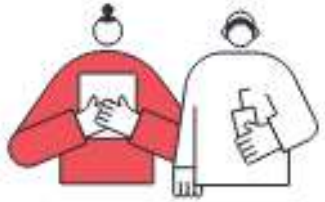


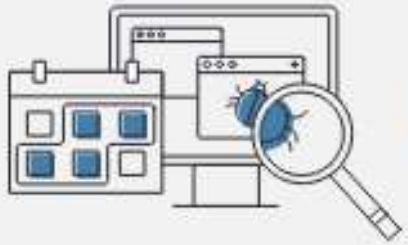
Quelle: Statistisches Bundesamt, Stand: Juli 2021

- Kleinstunternehmen
- Kleine Unternehmen
- Mittlere Unternehmen
- Großunternehmen

Wie bedroht ist Deutschlands Cyberraum?

Top-3-Bedrohungen je Zielgruppe:

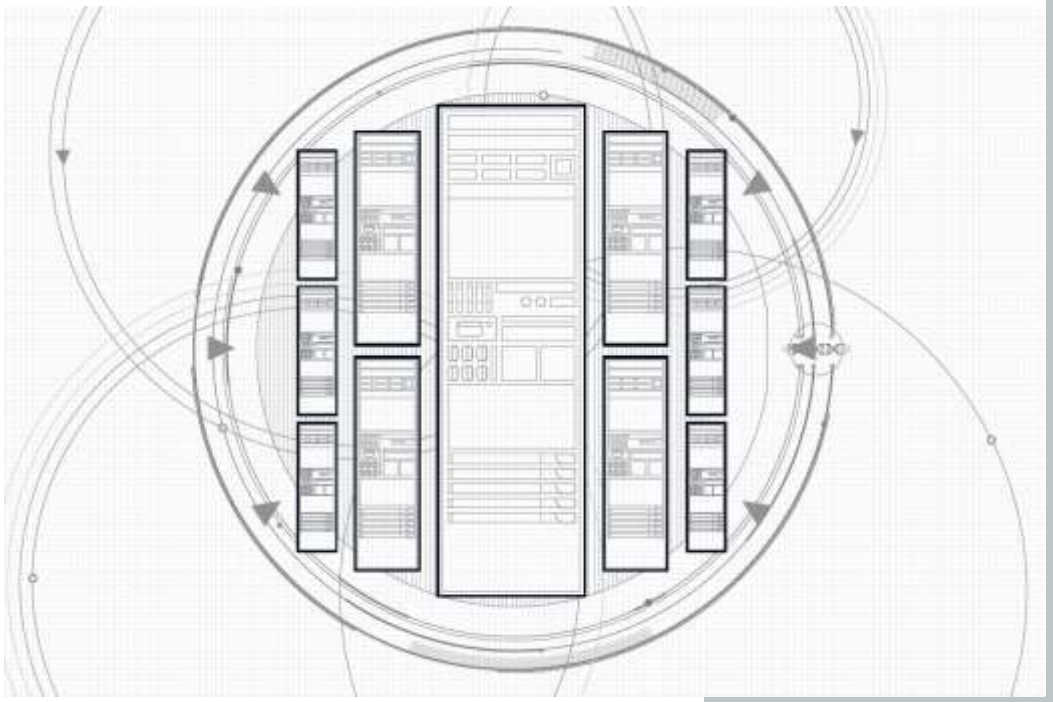
Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl	***Ransomware***	***Ransomware***
Sextortion	Abhängigkeit innerhalb der IT-Supply-Chain	APT
Phishing	Schwachstellen, offene oder falsch konfigurierte Onlineserver	Schwachstellen, offene oder falsch konfigurierte Onlineserver

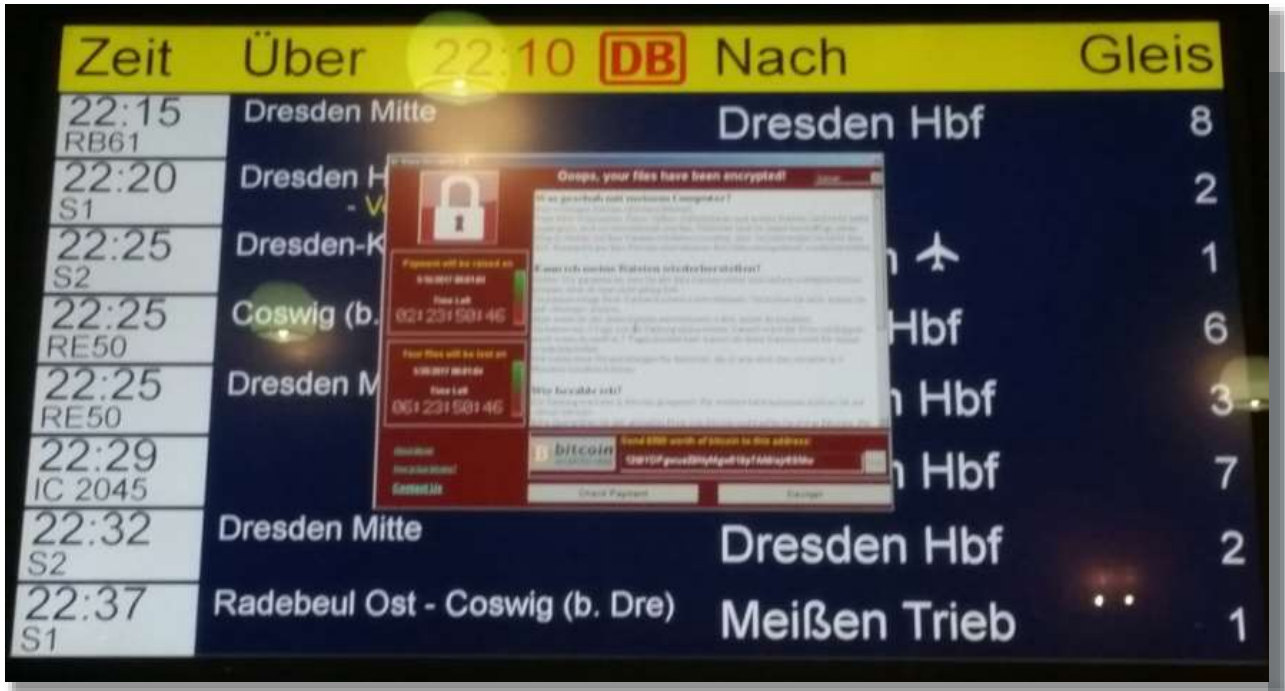


Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Wie bedroht ist Deutschlands Cyberraum? - Angriffsfläche

- 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.**





Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite“

„Garmin mit Komplettausfall“

„Angreifer legten Alu-Konzern mit Erpressersoftware lahm“

„Hackerangriff auf Uniklinik: Ermittlungen wegen fahrlässiger Tötung eingeleitet“

Deutschlandfunk

Startseite › Dlf-Magazin › Cyberangriff auf das Berliner Kammergericht › 06.02.2020

Datenschutz

Cyberangriff auf das Berliner Kammergericht

Nach einem Cyberangriff auf das Berliner Kammergericht ist bislang unklar, ob Daten abgeflossen sind. Die Hacker konnten womöglich auf alle Daten des Gerichts zugreifen, so der Präsident des Gerichts. Hackerangriffe werden für Behörden zunehmend zur Gefahr.

Von Johannes Kuhn

Hören Sie unsere Beiträge in der Dlf Audiothek

„Das Kammergericht ist eigentlich überall", so die Berliner IT-Staatssekretärin Sabine Smentek (imago / Christian Ditsch)

heise online heise+

heise online › News › 01/2020 › Uni Gießen nähert sich nach Hacker-Attacke wieder dem Normalbetrieb

Uni Gießen nähert sich nach Hacker-Attacke wieder dem Normalbetrieb

Aufgrund eines IT-Sicherheitsvorfalls war die Universität Gießen um Weihnachten 2019 zeitweise komplett offline. Nun gehen erste Dienste wieder online.

Lesezeit: 1 Min. In Pocket speichern 55

(Bild: dpa, Oliver Berg)

06.01.2020 14:19 Uhr

Von Dennis Schirrmacher

Mögliche Cyberattacke: Stadt Potsdam nimmt Server der Verwaltung vom Netz

Nach Malware-Infektion: Katastrophenfall im Landkreis Anhalt-Bitterfeld

KEINE E-MAILS, FRANKFURT.DE OFFLINE

„Emotet“ legt Stadt-Computer lahm

Stadtwerke Wismar: Ermittlungen nach Cyberattacke laufen

Hackerangriff auf Verwaltungen in Wesel und Witten

Brandenburg fährt die Server runter

CYBERANGRIFF

Hackerangriff in Mecklenburg-Vorpommern legt Kommunalverwaltungen seit Tagen lahm

SCHWERIN UND LUDWIGSLUST-PARCHIM

Probleme nach Cyberangriff dauern an – Sicherheitslücke bisher nicht gefunden

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 Chefsache!

Sorgen Sie für klare Zuständigkeiten!


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

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.

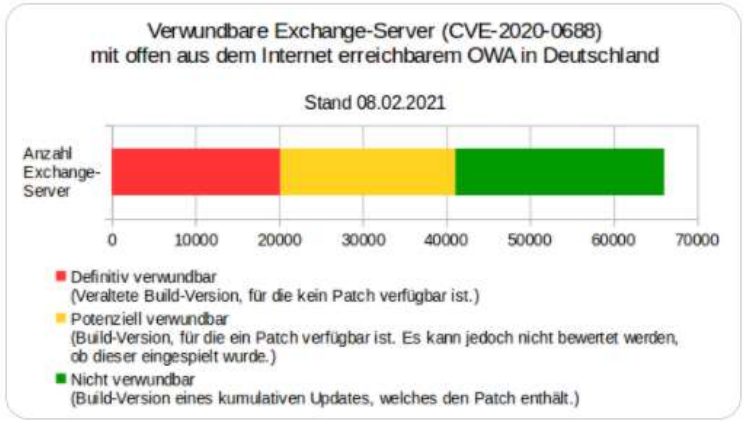
Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

* 1 / 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

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.

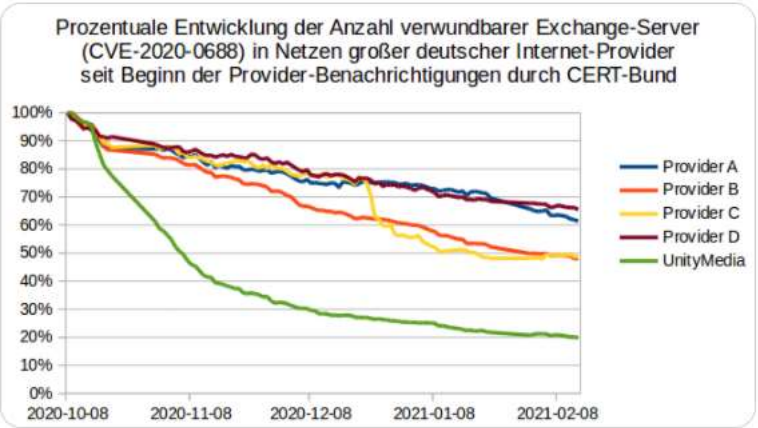


6 47 42

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 felderhafte 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.

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

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 auszugreifen 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 in 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 abgefangene 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 [MSC2021a].

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

2021-197772-1500 | Version 1.5 vom 08.03.2021 Seite 1 von 6

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

TLP:CLEAR: Unbegrenzte Weitergabe

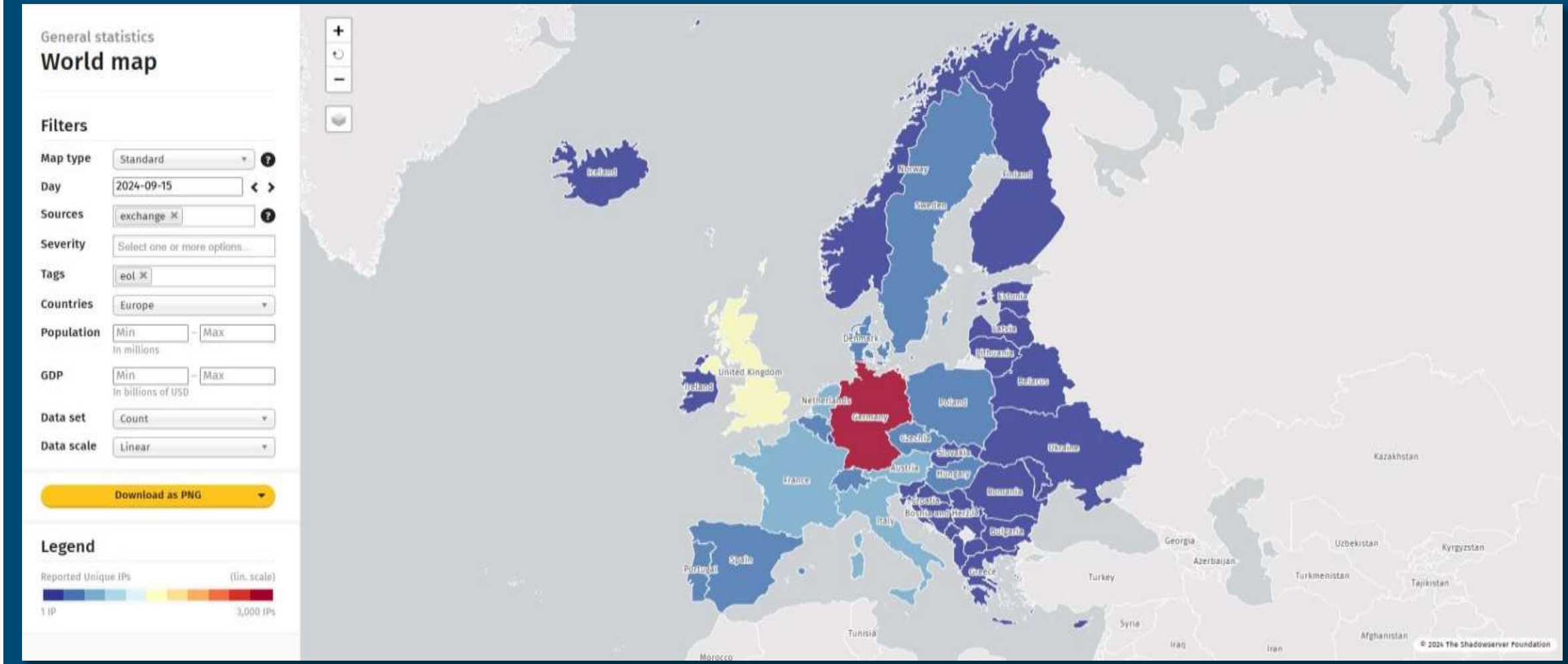
Sachverhalt

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 Informationen des BSI hatten 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.

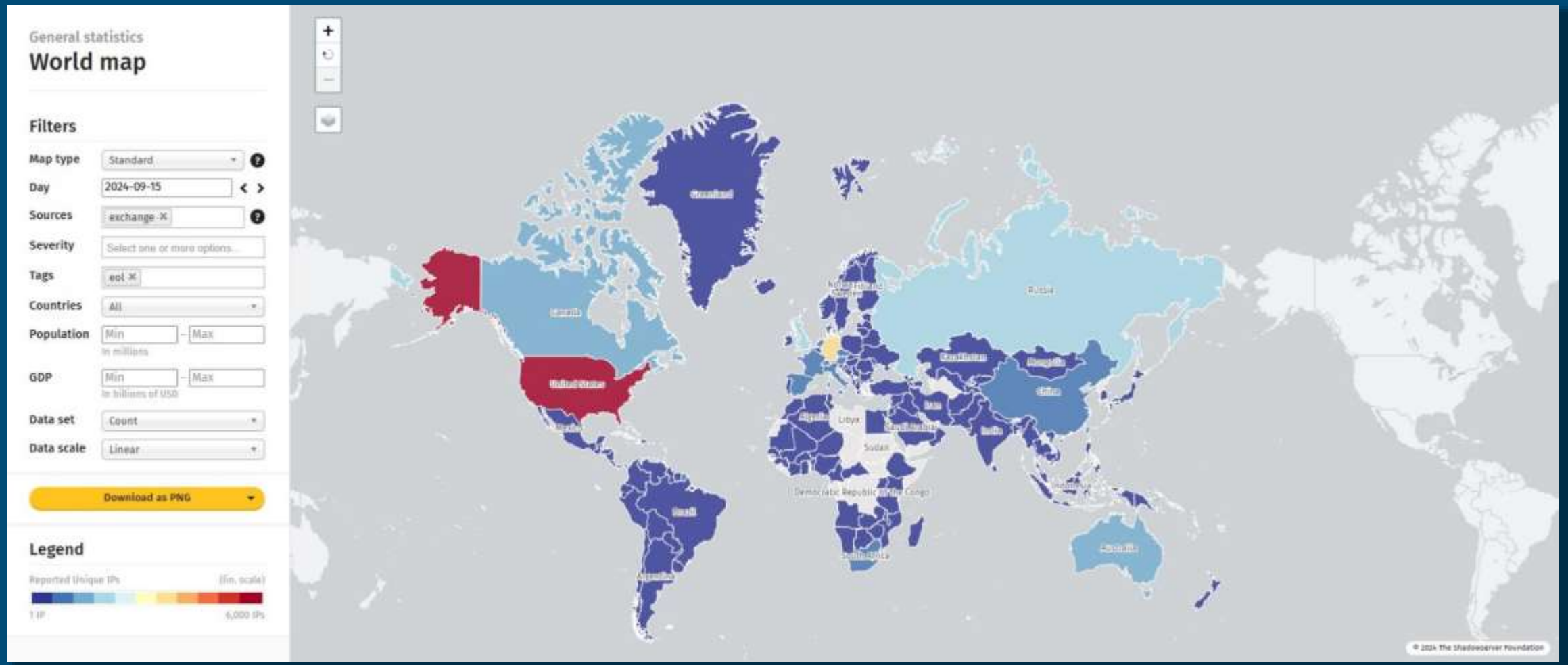
CSW # 2024-223466-1032 | Version 1.0 vom 26.03.2024 Seite 1 von 6

BSI IT-Sicherheitsinformation



Bundesamt
für Sicherheit in der
Informationstechnik

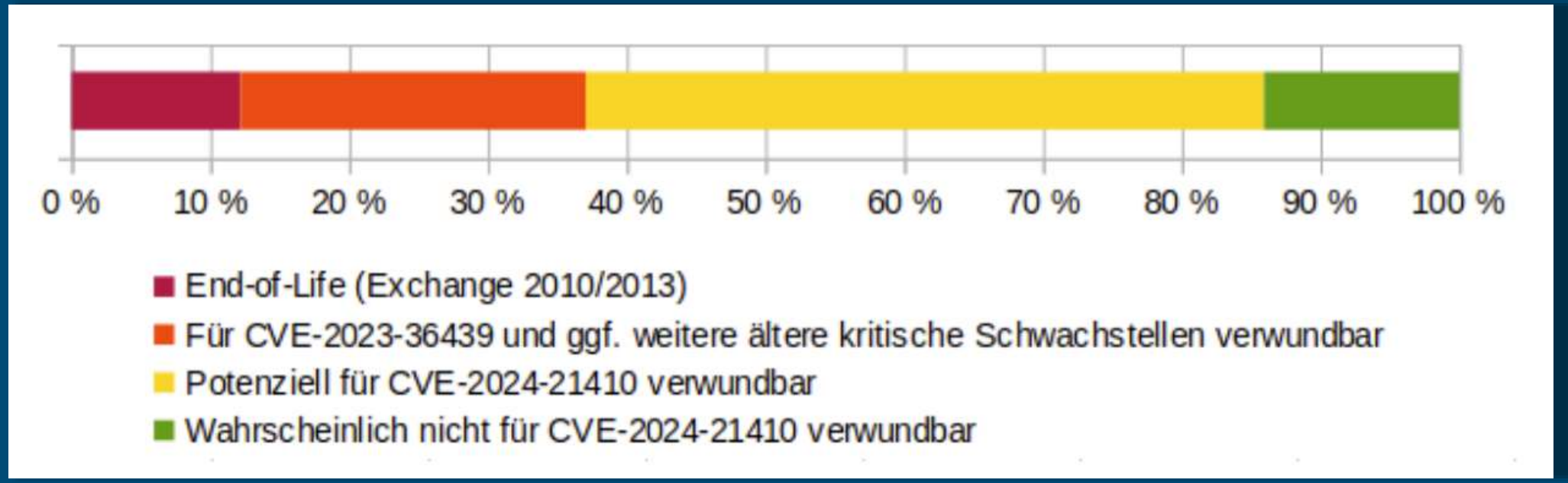
Deutschland
Digital•Sicher•BSI•



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

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



Üben Sie den Ernstfall !

Schließen Sie eine Cyber-Versicherung ab!

Führen Sie einen CyberRisikoCheck durch!!!

www.cyberrisikocheck.de

CyberRisikoCheck

nach DIN SPEC 27076 IT-Sicherheitsberatung für KKU

Analyse des Informationssicherheitsniveaus eines KMU:

- **(Online-) Befragung durch einen IT-Dienstleister**
- **Bewertung anhand eines standardisierten Scoring-Modells**

- **Erstellung eines Berichtes, 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**

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages

Aktueller Stand

Deutschland Digital•Sicher•BSI•

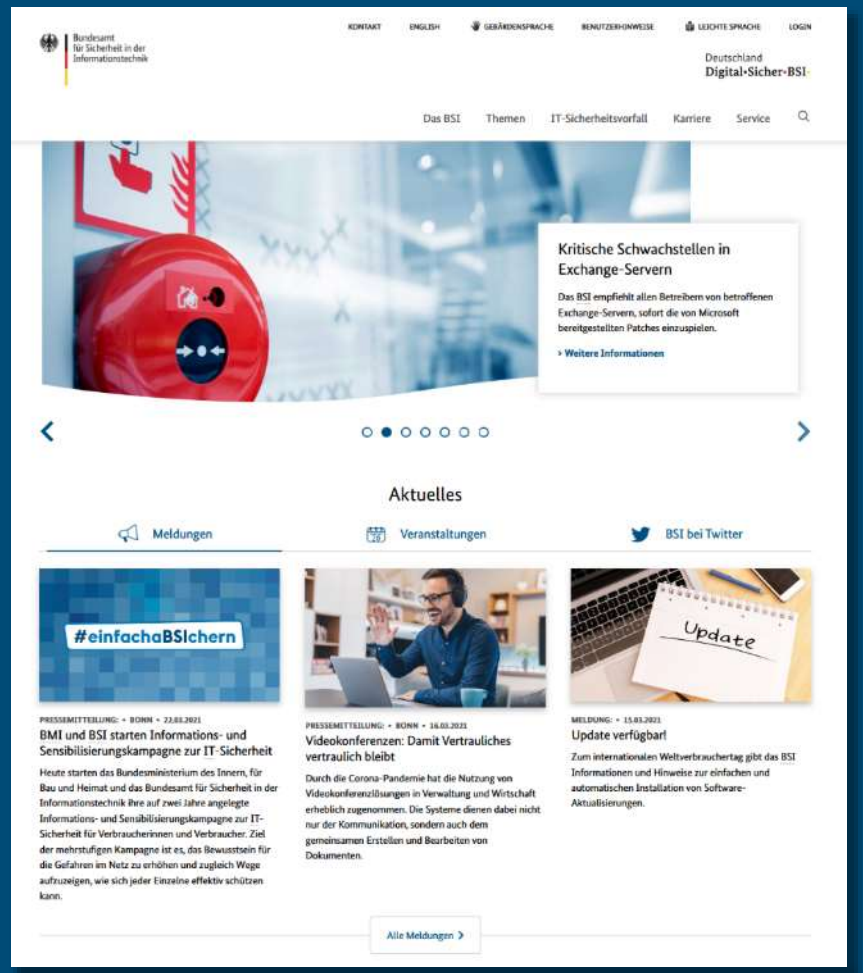
Bisher durchgeführte Schulungen für IT-Dienstleister:
in Präsenz: 3
als Webinar: 5

Weitere bereits geplante Schulungen in 2024:
in Präsenz: 2
als Webinar: 0

Geschulte IT-Dienstleister: 459
Geschulte Mitarbeiter: 691

Bundesamt für Sicherheit in der Informationstechnik

Nutzen Sie das BSI !



Direktlink zum Angebot für KMU:

www.bsi.bund.de/kmu

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

Cyber-Sicherheit umgangssprachlich auf einfachem Niveau erklärt.

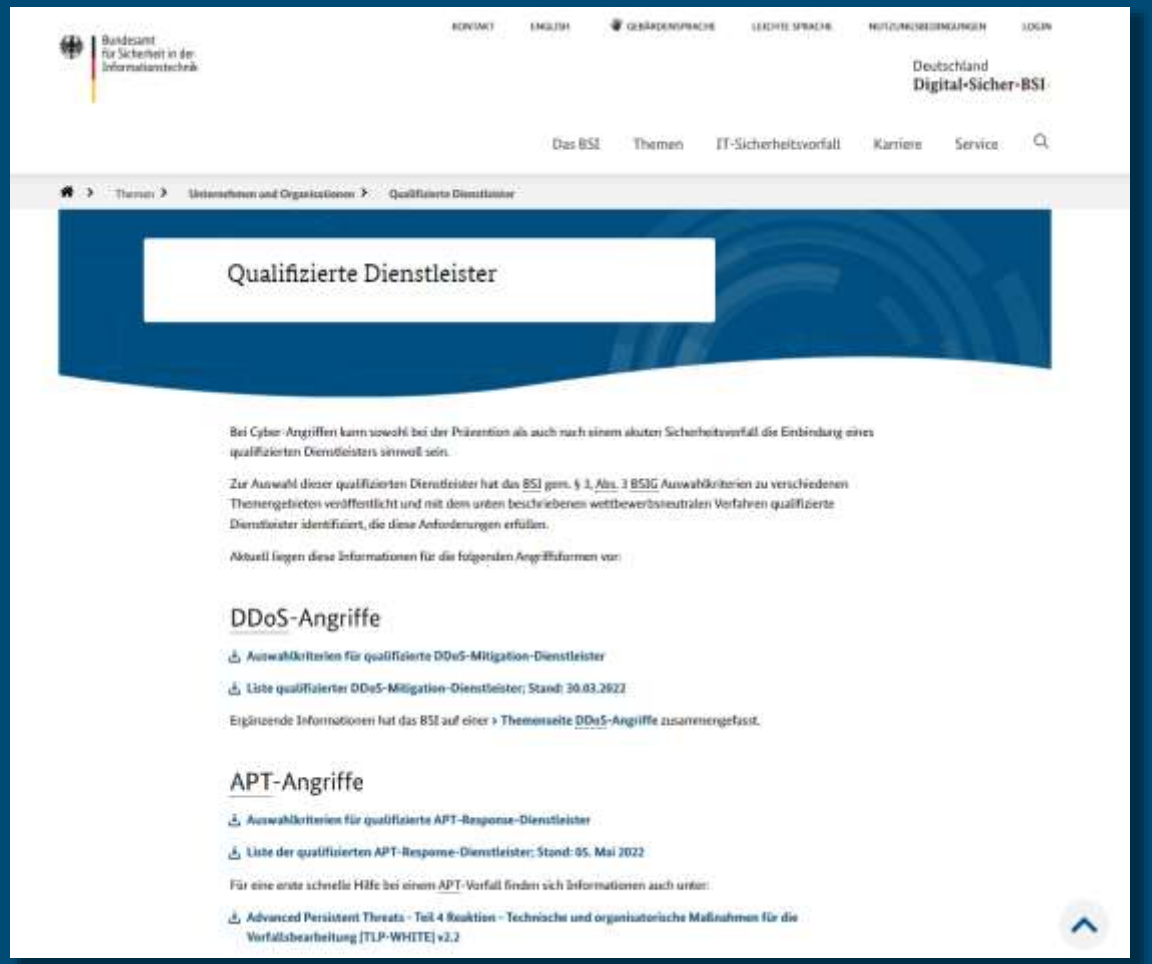
Gut vernetzt – Allianz für-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Sie bietet eine Kooperationsbasis zwischen:

- Staat,
- Wirtschaft,
- Herstellern und
- Forschung

www.allianz-fuer-cybersicherheit.de


Bundesamt für Sicherheit in der Informationstechnik
Deutschland Digital•Sicher•BSI
Das BSI
Themen
IT-Sicherheitsvorfall
Karriere
Service
Qualifizierte Dienstleister
Bei Cyber-Angriffen kann sowohl bei der Prävention als auch nach einem akuten Sicherheitsvorfall die Einbindung eines qualifizierten Dienstleisters sinnvoll sein.
Zur Auswahl dieser qualifizierten Dienstleister hat das BSI gem. § 3, Abs. 3 BSIG Auswahlkriterien zu verschiedenen Themengebieten veröffentlicht und mit dem unten beschriebenen wettbewerbsneutralen Verfahren qualifizierte Dienstleister identifiziert, die diese Anforderungen erfüllen.
Aktuell liegen diese Informationen für die folgenden Angriffsformen vor:
DDoS-Angriffe
Auswahlkriterien für qualifizierte DDoS-Mitigation-Dienstleister
Liste qualifizierter DDoS-Mitigation-Dienstleister; Stand: 30.03.2022
Ergänzende Informationen hat das BSI auf einer › Themenseite DDoS-Angriffe zusammengefasst.
APT-Angriffe
Auswahlkriterien für qualifizierte APT-Response-Dienstleister
Liste der qualifizierten APT-Response-Dienstleister; Stand: 05. Mai 2022
Für eine erste schnelle Hilfe bei einem APT-Vorfall finden sich Informationen auch unter:
Advanced Persistent Threats - Teil 4 Reaktion - Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung [TLP-WHITE] v2.2

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

NIS-2-Richtlinie – Was ist neu?

- 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 durch **Änderung des BSI-Gesetzes** im NIS2UmsuCG.
- BSI wird 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 **abgestuften Registrierungs-, Nachweis- und Meldepflichten** für bwE und wE

Sektoren, Umsatz und Mitarbeitendenzahl

Betroffenheit – Welche Unternehmen fallen in die Regulierung?

KRITIS

- Unternehmen gehört zu einem der **KRITIS-Sektoren**
- Betreibt eine **kritische Anlage** im Sinne der BSI-KritisV
- Über dem **Schwellenwert** (> 500.000 versorgte Personen, Ausdifferenzierung nach Anlagenkategorie)

bwE

- Unternehmen gehört **zu NIS-2-Sektor (Anhang I)**
- Überschreitet **Schwellenwerte** bei Umsatz, Bilanz oder Mitarbeitendenzahl: **Mittleres Unternehmen**
- **Sonderfälle im Sektor IT und Telekommunikation** (qTSP, TLD, DNS, TK-Anbieter)

wE

- Unternehmen gehört zu **NIS-2-Sektor (Anhang I oder II)**
- Überschreitet **Schwellenwerte** bei Umsatz, Bilanz oder Mitarbeitendenzahl: Kleinst-/Kleinunternehmen
- Vertrauensdienste

Anhänge I und II der NIS-2-Richtlinie

Betroffenheit – Welche Sektoren gehören zur NIS-2?

Anhang I (Sektoren bwE)		Anhang II (Sektoren wE)	
1. Energie	2. Verkehr	1. Post- und Kurierdienste	2. Abfallbewirtschaftung
3. Bankwesen	4. Finanzmarktinfrastruktur	3. Produktion, Herstellung und Handel mit chemischen Stoffen	4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln
5. Gesundheitswesen	6. Trinkwasser	5. Verarbeitendes Gewerbe / Herstellung von Waren	6. Anbieter digitaler Dienste
7. Abwasser	8. Digitale Infrastruktur	7. Forschung	
9. Verwaltung von IKT-Diensten	10. *Öffentliche Verwaltung*		
11. Weltraum			

*neuer KRITIS-Sektor

Size Cap – Mitarbeitendenzahl, Umsatz und Bilanz

Betroffenheit – Größe der Unternehmen/Size Cap

bwE **Anhang I (Sektoren bwE)**		**wE** **Anhang I (Sektoren bwE)/Anhang II (Sektoren wE)**	
≥ 250 Mitarbeitende **oder**	> 50 Mio. € Jahresumsatz **und** > 43 Mio. € Jahresbilanzsumme	≥ 50 Mitarbeitende **oder**	> 10 Mio. € Jahresumsatz **und** > 10 Mio. € Jahresbilanzsumme
qualifizierte Vertrauensdiensteanbieter (qTSP) TLD Name Registry DNS-Diensteanbieter		nichtqualifizierte Vertrauensdiensteanbieter	
Anbieter TK-Dienste/TK-Netze **und**	≥ 50 Mitarbeitende **oder** > 10 Mio. € Jahresumsatz **und** > 10 Mio. € Jahresbilanzsumme	Anbieter TK-Dienste/TK-Netze (Kleinst-/Kleinunternehmen)	

Size Cap ggf. anders im finalen NIS2UmsuCG

NIS-2-Umsetzung – Was beinhaltet die Regulierung?

Unterstützung von Unternehmen – Wie hilft das BSI?

Betroffenheitsprüfung

- Überprüfung, ob das Unternehmen von **NIS-2 betroffen** ist
- Basierend auf **Eigenauskünften**
- Ergebnis **rechtlich nicht verbindlich**
- Derzeit basierend auf der **Richtlinie**, Anpassung an das Gesetz nach Verabschiedung

NIS-2-FAQ

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

NIS-2-Was tun?

- Was können Unternehmen jetzt schon tun, um sich auf NIS-2 **vorzubereiten**
- Personen **benennen**
- **Verantwortung** übernehmen, **Bestandsaufnahme** der IT-Sicherheit, Informations-sicherheit **verbessern**, **Meldepflicht** und Empfang von Warnungen und Lage-informationen **vorbereiten**

NIS-2-Betroffenheitsprüfung – Ist mein Unternehmen reguliert?

- **Orientierung**, ob Unternehmen von NIS-2 betroffen ist
- Kurze und präzise Ja/Nein-Fragen
- Grundlage **Eigenangaben**, Ergebnis **nicht rechtlich bindend**
- Basiert aktuell auf der **Richtlinie**, wird an das **Gesetz angepasst**, sobald es verabschiedet wurde

https://betroffenheitspruefung-nis-2.bsi.de/

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt

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

manuel.bach@bsi.bund.de
Tel. +49 (0) 228 9582 5941
Fax +49 (0) 228 10 9582 5941

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

Bundesamt
für Sicherheit in der
Informationstechnik