

Der CyberRisikoCheck nach DIN SPEC 27076 als Antwort auf die katastrophale Informationssicherheitslage von KMU

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

Kurzprofil des BSI



Gründung
01. Januar 1991

217 Mio.
Euro Budget
Haushalt
2022

Stellen 2022

1733 ↗

183 Neue
Stellen
zum Vorjahr

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

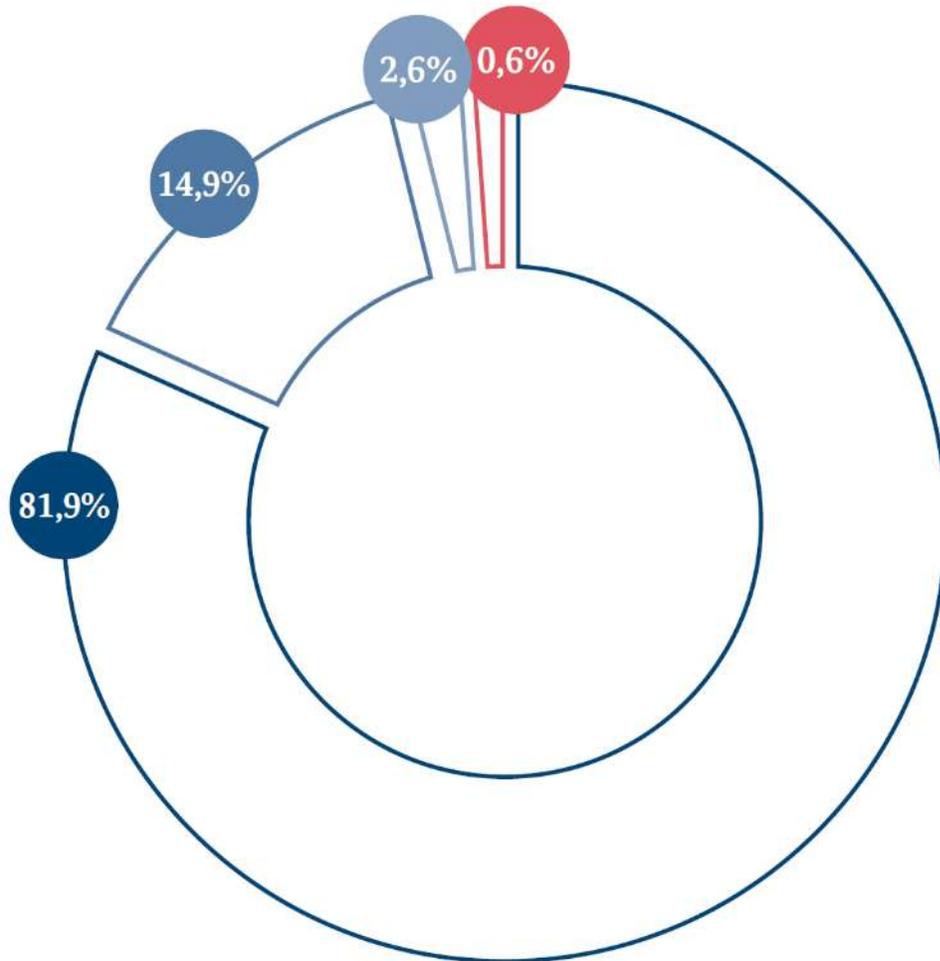
Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

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

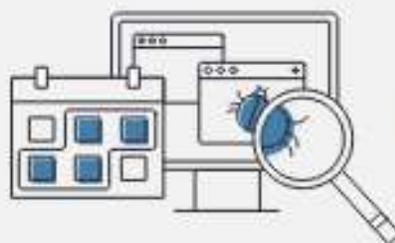


Quelle: Statistisches Bundesamt, Stand: Juli 2021

- Kleinstunternehmen
- Kleine Unternehmen
- Mittlere Unternehmen
- Großunternehmen

Wie bedroht ist Deutschlands Cyberraum?



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

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55

Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55

Time Left
06:23:57:37

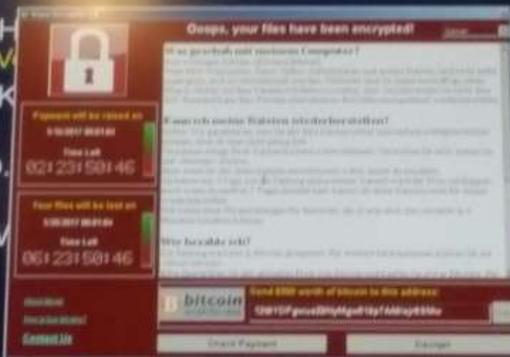
[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Bitcoin ACCEPTED HERE

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Zeit	Über	22:10 DB	Nach	Gleis
22:15 RB61	Dresden Mitte		Dresden Hbf	8
22:20 S1	Dresden Hbf		Dresden Hbf	2
22:25 S2	Dresden-K		Dresden Hbf	1
22:25 RE50	Coswig (b. Dre)		Dresden Hbf	6
22:25 RE50	Dresden M		Dresden Hbf	3
22:29 IC 2045	Dresden Mitte		Dresden Hbf	7
22:32 S2	Dresden Mitte		Dresden Hbf	2
22:37 S1	Radebeul Ost - Coswig (b. Dre)		Meißen Trieb	1



22:37 S1 Radebeul Ost - Coswig (b. Dre) Meißen Trieb

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“

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)



Uni Gießen nähert sich nach Hacker-Angriffe 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 Schirmacher

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!**

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:

0 8 0 0 - U L F



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!

SCHWACHSTELLE | GEFAHRUNG | 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 Cumulative Update 23
- Microsoft Exchange Server 2016 Cumulative Update 14 und 15
- Microsoft Exchange Server 2019 Cumulative 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-DipPolicy 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:

- **3 / Grün:** Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
- **2 / Gelb:** IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Senkung der Regelbetriebs.
- **1 / Orange:** Die IT-Bedrohungslage ist geschäftskritisch. Maximale Beeinträchtigung des Regelbetriebs.
- **0 / Rot:** Die IT-Bedrohungslage ist extrem kritisch. Zusätzlich: Szenario, das Regelbetriebs kann nicht aufrecht erhalten werden.

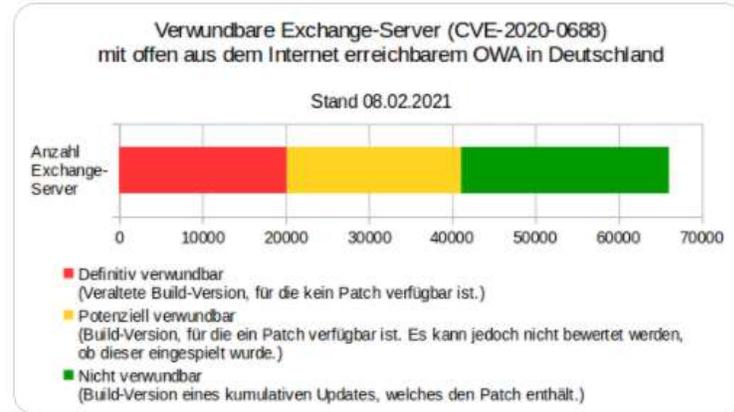
CSW # 2020-252437-1131 | Version 1.1 vom 13.10.2020

Seite 1 von 3



CERT-Bund @certbund · 9. Feb.

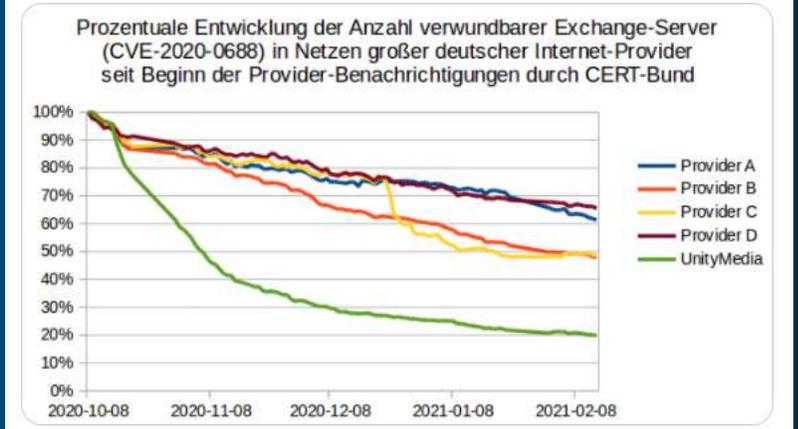
Ein Jahr nach Veröffentlichung des #Sicherheitsupdates sind noch immer mindestens 31% (potenziell bis zu 63%) der #Exchange-Server in Deutschland mit offen aus dem Internet erreichbarem #OWA für die kritische #Schwachstelle CVE-2020-0688 verwundbar.



6 47 42

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

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 Cumulative Update 23
- Microsoft Exchange Server 2016 Cumulative Update 14 und 15
- Microsoft Exchange Server 2019 Cumulative 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-DipPolicy 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 einer wesentlichen Aufklärbarkeit und enthält keinen Hinweis.
- **2 / Gelb:** IT-Bedrohungslage mit verstärkter Beobachtung von Aufklärbarkeit unter temporärer Beeinträchtigung des Regelbetriebs.
- **3 / Orange:** Die IT-Bedrohungslage ist geschätzlich. Massive Beeinträchtigung des Regelbetriebs.
- **4 / Rot:** Die IT-Bedrohungslage ist extrem kritisch. Anhaltender Hinweis, 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

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, dem 3. März 2021, hat Microsoft Out-of-Band Updates für Exchange Server veröffentlicht. Hiermit werden vier Schwachstellen geschlossen, die in Kombination bereits für diegerichtetste Angriffe verwendet werden und Taten die Möglichkeit bieten, Daten abzurufen 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-Anfragen zu senden und sich am Exchange-Server zu authentifizieren.
- CVE-2021-26857 ist eine insecure deserialization Schwachstelle im Unified Messaging Service. Bei insecure deserialization werden Nutzer-identifizierende Daten von einem Programm deserialisiert. Hierüber ist es möglich, beliebigen Programmcode als SYSTEM auf dem Exchange-Server auszuführen. Dies erlaubt Administrator-Rechte über die Auswertung einer eingegangenen weiteren Schwachstelle.
- CVE-2021-26870 und CVE-2021-27065 sind Schwachstellen, mit denen – nach Authentifizierung – beliebige Dateien auf dem Exchange-Server geschaltet werden können. Die Authentifizierung kann z. B. über CVE-2021-26855 oder abgefangene Administrator-Zugangsdaten erfolgen.

Nach Angaben des Herstellers richteten sich die Angriffe gegen amerikanische Forschungsorganisationen mit Pandemic, Polaris, Hochschule, American firmen, Organisationen aus dem Rüstungssektor, Think Tanks und NGOs. Microsoft verweist hierbei den Vorfallern eine staatliche Hackengruppe aus China, die HAFNIUM genannt wird.

Namen der ursprünglichen Opfer sind im BSI nicht bekannt. Bei den betroffenen Angreifern wurde hierbei Zugang zu den E-Mail-Accounts erlangt, sowie weitere Malware zur Logginsid-Permanenz installiert [MCC2021a].

Die Angriffe erfordern die Möglichkeit, eine nicht vertrauenswürdige Verbindung zu BSI aus dem Internet auf Port 443 am Exchange-Server zu etablieren. Daten sind Server geschützt, welche nicht vertrauenswürdig Verbindungen beschreiben oder nur per VPN erreichbar sind. Diese Leistung schließt

- **1 / Grün:** Die IT-Bedrohungslage ist einer wesentlichen Aufklärbarkeit und enthält keinen Hinweis.
- **2 / Gelb:** IT-Bedrohungslage mit verstärkter Beobachtung von Aufklärbarkeit unter temporärer Beeinträchtigung des Regelbetriebs.
- **3 / Orange:** Die IT-Bedrohungslage ist geschätzlich. Massive Beeinträchtigung des Regelbetriebs.
- **4 / Rot:** Die IT-Bedrohungslage ist extrem kritisch. Anhaltender Hinweis, der Regelbetrieb kann nicht aufrecht erhalten werden.

2021-197772-1500 | Version 1.5 vom 08.03.2021

Seite 1 von 6

BSI-IT-Sicherheitswarnung

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**

Wichtig: Für die Schwachstelle sind unmittelbare Webpages dieser Informationen sind um diese Informationen informiert zu geben gemäß dem Trade-Off-Prinzip (T.O.P.) die Lage eines Dienstes zu bewerten.

UNTERSCHIED: Unbegrenzte Weitergabe

Angabe von unbeschränktem Anspruch, da die T.O.P. nicht absehbar. Daher Informationen um dem T.O.P. (T.O.P.) eine Beschränkung für weitergegeben werden.

Der Dokument ist durch die Befugnisse entsprechend der veröffentlichten Aufklärungsmaßnahmen von anderen Informationen abweichend mit T.O.P. zu verwenden, zu verbreiten, zu befragen und zu verwenden. Wenn Informationen vom T.O.P. abhören für ein Team dieser Informationen.

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 schnell einzupflegen.

Aktuell werden in Deutschland rund 45.000 Microsoft-Exchange-Server mit allen aus dem Internet erreichbaren Outlook Web Access (OWA) betriebs. 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 einer wesentlichen Aufklärbarkeit und enthält keinen Hinweis.
- **2 / Gelb:** IT-Bedrohungslage mit verstärkter Beobachtung von Aufklärbarkeit unter temporärer Beeinträchtigung des Regelbetriebs.
- **3 / Orange:** Die IT-Bedrohungslage ist geschätzlich. Massive Beeinträchtigung des Regelbetriebs.
- **4 / Rot:** Die IT-Bedrohungslage ist extrem kritisch. Anhaltender Hinweis, der Regelbetrieb kann nicht aufrecht erhalten werden.

CSW # 2024-223466-1032 | Version 1.0 vom 26.03.2024

Seite 1 von 6

BSI IT-Sicherheitsinformation

General statistics World map

Filters

Map type: Standard ?

Day: 2024-09-15 < >

Sources: exchange X ?

Severity: Select one or more options...

Tags: eol X

Countries: Europe

Population: Min - Max
in millions

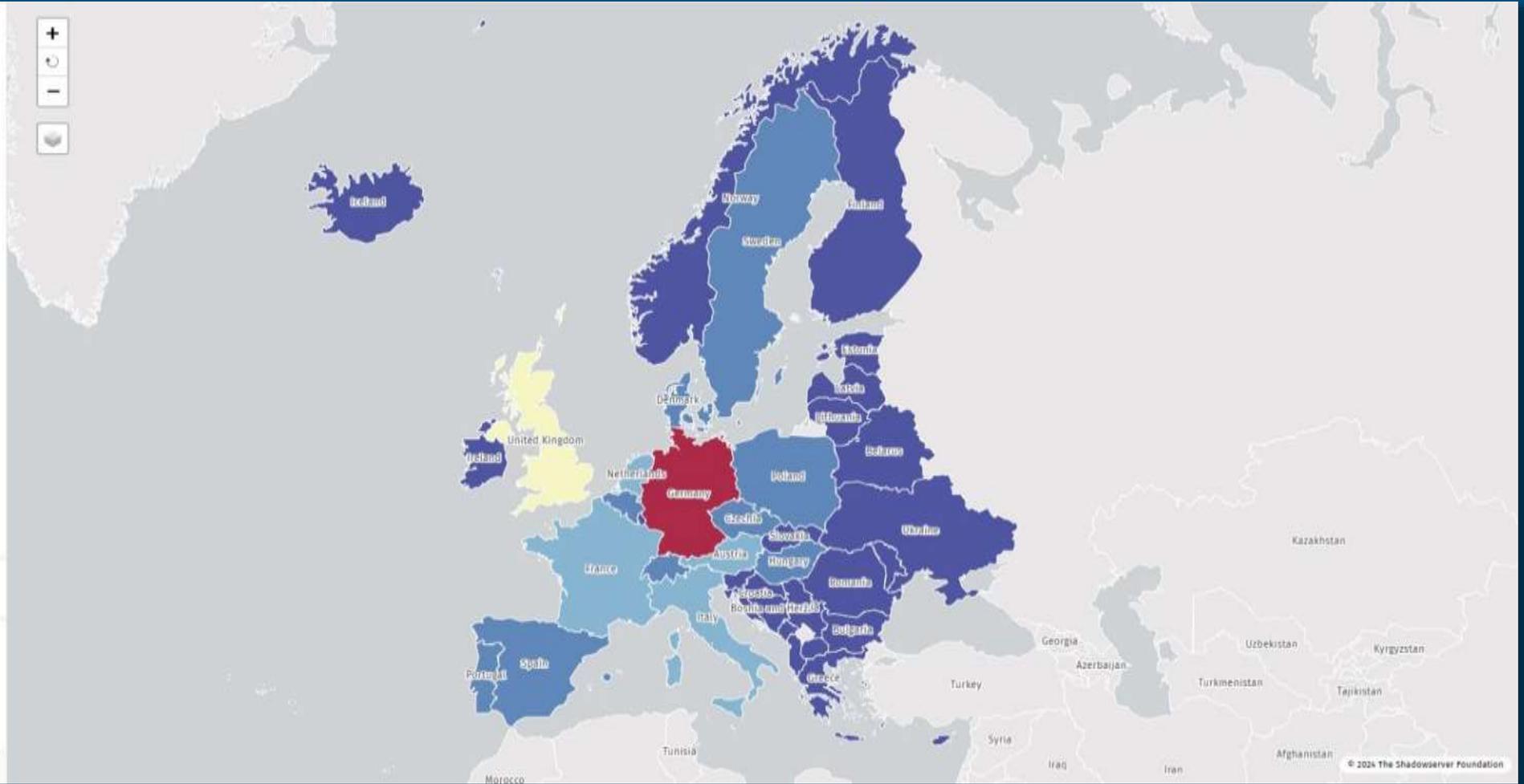
GDP: Min - Max
in billions of USD

Data set: Count

Data scale: Linear

Download as PNG

Legend



General statistics
World map

Filters

Map type: Standard

Day: 2024-09-15

Sources: exchange-X

Severity: Select one or more options...

Tags: eol-X

Countries: All

Population: Min - Max
in millions

GDP: Min - Max
in billions of USD

Data set: Count

Data scale: Linear

Download as PNG

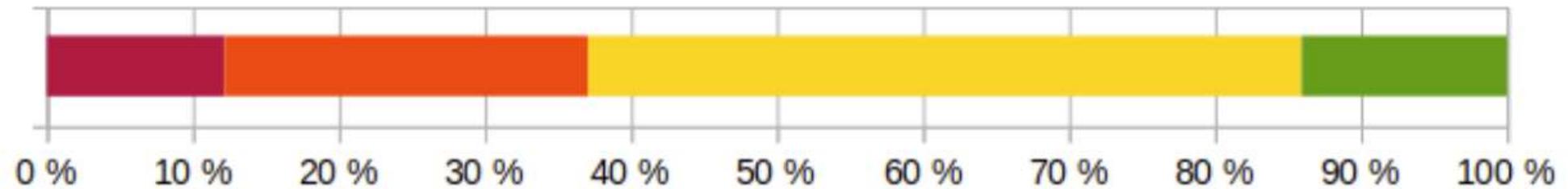
Legend



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



- End-of-Life (Exchange 2010/2013)
- Für CVE-2023-36439 und ggf. weitere ältere kritische Schwachstellen verwundbar
- Potenziell für CVE-2024-21410 verwundbar
- Wahrscheinlich nicht für CVE-2024-21410 verwundbar

Üben Sie den Ernstfall !

Schließen Sie eine Cyber-Versicherung ab!



**Führen Sie einen
CyberRisikoCheck durch!!!**

www.cyberrisikocheck.de

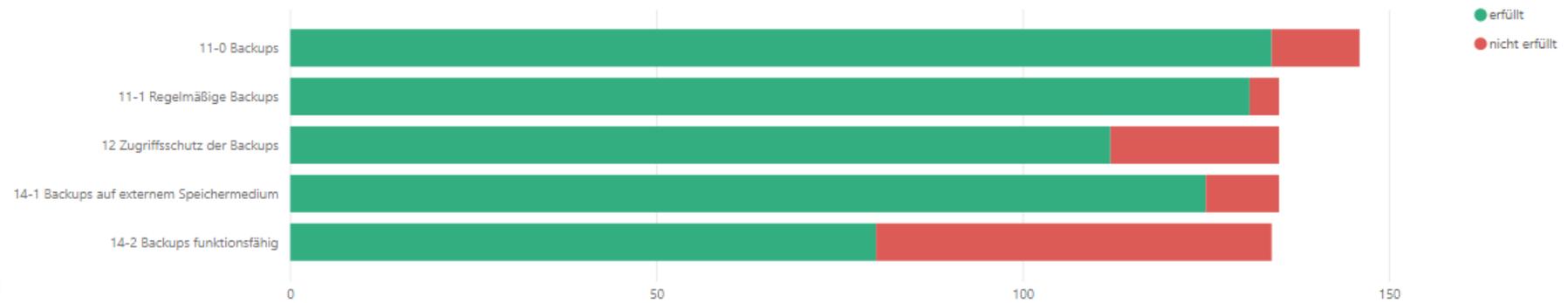
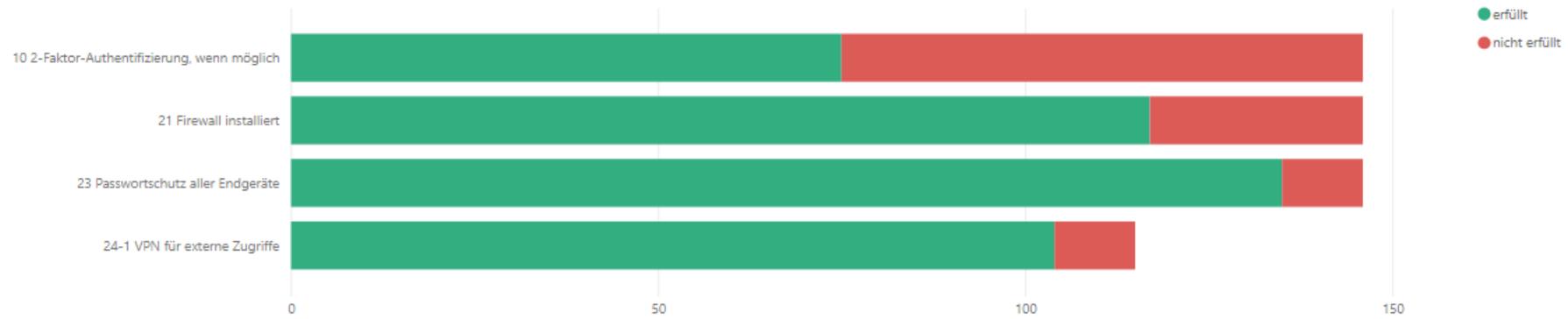
CyberRisikoCheck

nach DIN SPEC 27076 IT-Sicherheitsberatung für KKK

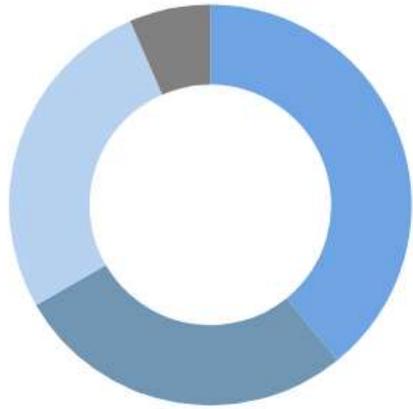
Analyse des Informationssicherheitsniveaus eines KMU:

- (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



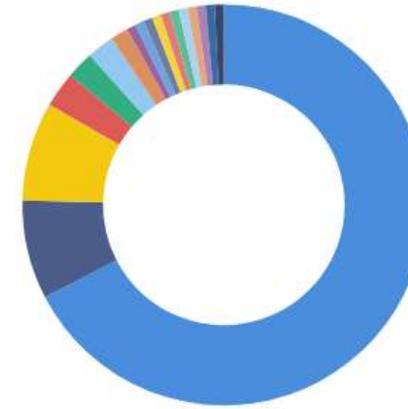






- KMU
- kleines Unternehmen
 - mittleres Unternehmen
 - Kleinstunternehmen
 - Großunternehmen

138
durchgeführte CRCs



- Rechtsform
- GmbH
 - Einzelunternehmen
 - GmbH & Co. KG
 - GbR
 - AG
 - e.V.
 - Beratungsgesellschaft mbH
 - AöR
 - e.K.
 - eingetragener Verein
 - Einzelperson
 - gGmbH
 - mbB



WZ-Code	Anzahl von WZ-	WZ 2008 - Bezeichnung
WZ-Code	Anzahl von WZ- Code	WZ 2008 - Bezeichnung
62		
62	10	Erbringung von Beratungsleistungen auf dem Gebiet der Informationstechnologie
70	6	Sonstige Softwareentwicklung
52	5	Unternehmensberatung
62	3	Lagerei sowie Erbringung von sonstigen Dienstleistungen für den Verkehr
73	3	Programmierungstätigkeiten
78	3	Werbeagenturen
86	3	Vermittlung von Arbeitskräften
86	3	Gesundheitswesen a. n. g.
10	3	Sonstige selbstständige Tätigkeiten im Gesundheitswesen
25	2	Herstellung von Backwaren (ohne Dauerbackwaren)
25	2	Herstellung von Metallkonstruktionen
28	2	Herstellung von Metallwaren a. n. g.
32	2	Herstellung von Maschinen für sonstige bestimmte Wirtschaftszweige a. n. g.
38	2	Herstellung von medizintechnischen Apparaten und Materialien a. n. g.
43	2	Sammlung nicht gefährlicher Abfälle
45	2	Elektroinstallation
52	2	Instandhaltung und Reparatur von Kraftwagen mit einem Gesamtgewicht von 3,5 t oder weniger (ohne Lackierung und Autowäsche)
62	2	
68	2	Erbringung von Dienstleistungen der Informationstechnologie
69	2	Vermietung, Verpachtung von eigenen oder geleasteten Grundstücken, Gebäuden und Wohnungen
78	2	Rechtsanwaltskanzleien ohne Notariat
96	2	Sonstige Überlassung von Arbeitskräften
0	2	Erbringung von sonstigen Dienstleistungen a. n. g.
10	1	
10	1	Kartoffelverarbeitung
14	1	Herstellung von Dauerbackwaren
14	1	Herstellung von Bekleidung
16	1	Herstellung von sonstiger Bekleidung und Bekleidungszubehör a. n. g.
16	1	Herstellung von sonstigen Konstruktionsteilen, Fertigbauteilen, Ausbauelementen und Fertigteilbauten aus Holz
20	1	Herstellung von Verpackungsmitteln, Lagerbehältern und Ladungsträgern aus Holz
20	1	
21	1	Herstellung von Schädlingsbekämpfungsmitteln, Pflanzenschutz- und Desinfektionsmitteln
23	1	Herstellung von pharmazeutischen Grundstoffen
25	1	Veredlung und Bearbeitung von Flachglas
25	1	Stahl- und Leichtmetallbau
25	1	Herstellung von Metallkonstruktionen
	1	25.61.1

Aktueller Stand

Bisher durchgeführte Schulungen für IT-Dienstleister:

in Präsenz: 3
als Webinar: 5

Weitere bereits geplante Schulungen in 2024:

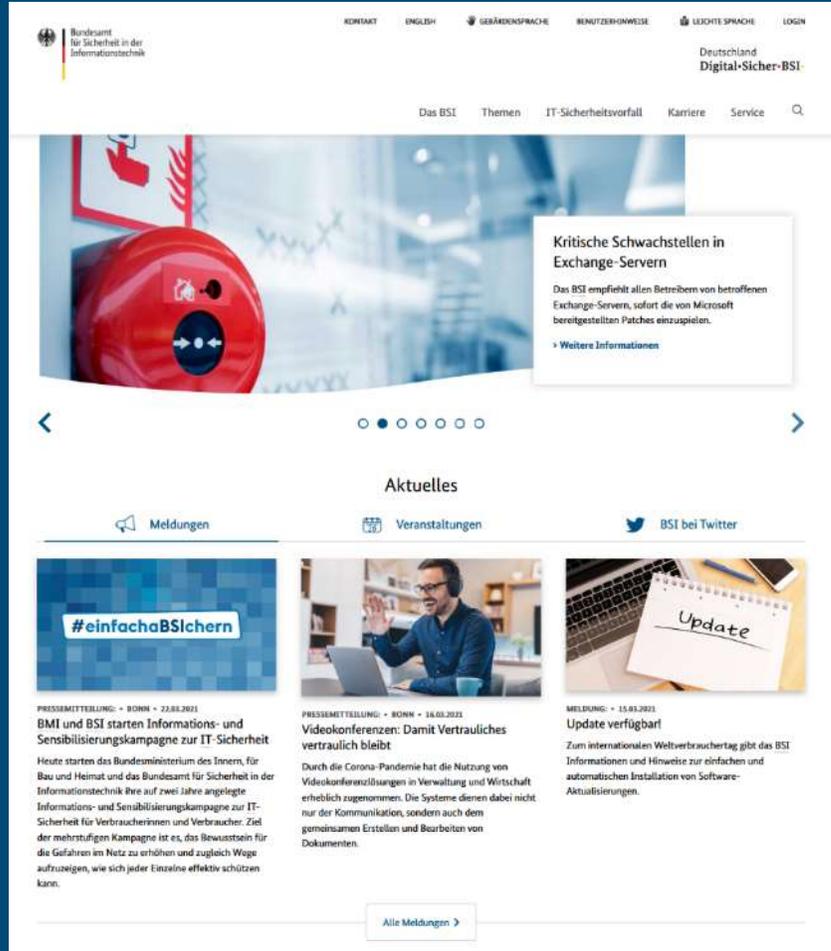
in Präsenz: 2
als Webinar: 0

Geschulte IT-Dienstleister: 459

Geschulte Mitarbeiter: 691



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



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 BSI-G 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: 30.01.2023](#)

Ergänzende Informationen hat das BSI auf einer [Themensseite 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 Vorfallbearbeitung \[TLP-WHITE\] 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



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



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. Finanzmarktinфраstruktur	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. <i>Öffentliche Verwaltung</i>		
11. Weltraum			

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

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI

Kontakt

Manuel Bach
Leiter Referat „Cybersicherheit bei kleinen und mittleren 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



https://www.soscisurvey.de/bsikmu/?q=vortrag_20241113