Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Wie KMU sicht gut gegen Cyber-Angriffe wappnen können

Manuel Bach, Leiter des Referats WG 23 - „Cyber-Sicherheit für KMU“
Bundesamt Bundesamt für Sicherheit in der Informationstechnik

Cybersecurity Konferenz 2023, Nürnberg, 16. Oktober 2023

Leitsatz

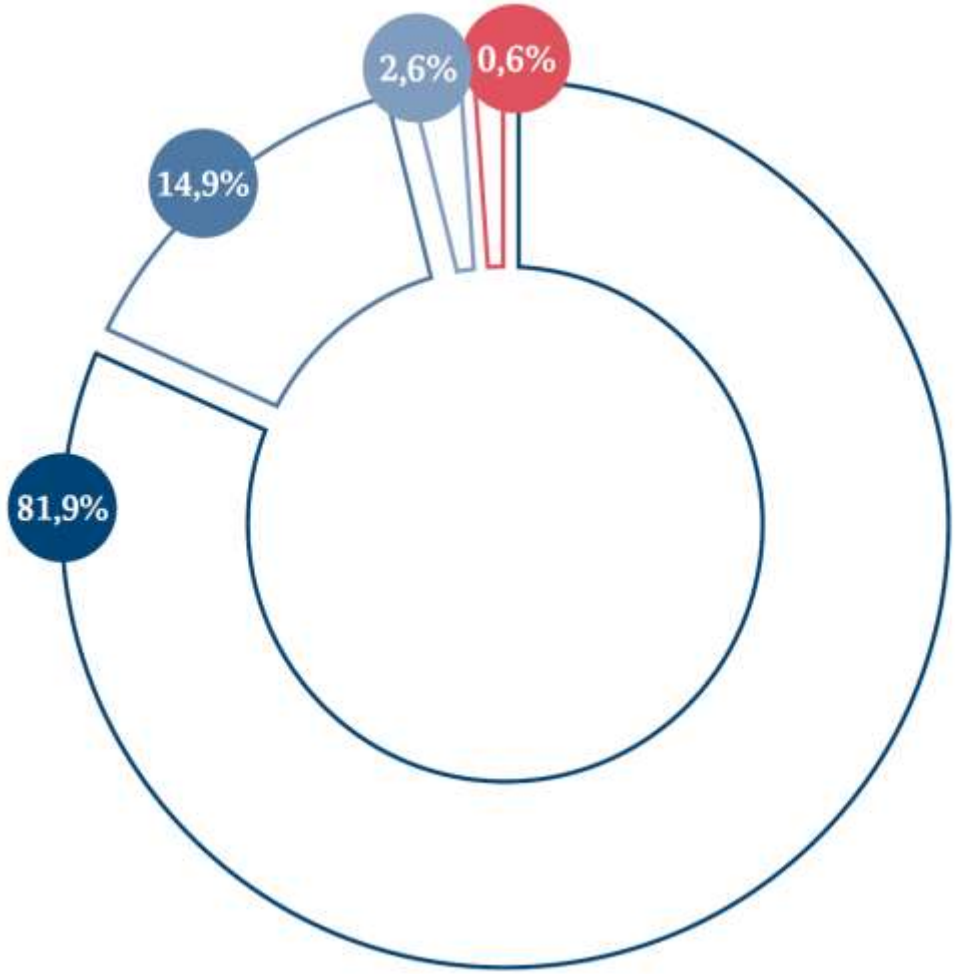
Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

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

Kurzprofil des BSI

Gründung
01. Januar 1991

217 Mio. Euro
Budget Haushalt 2022

Stellen 2021
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.

Wie bedroht ist Deutschlands Cyber-Raum?

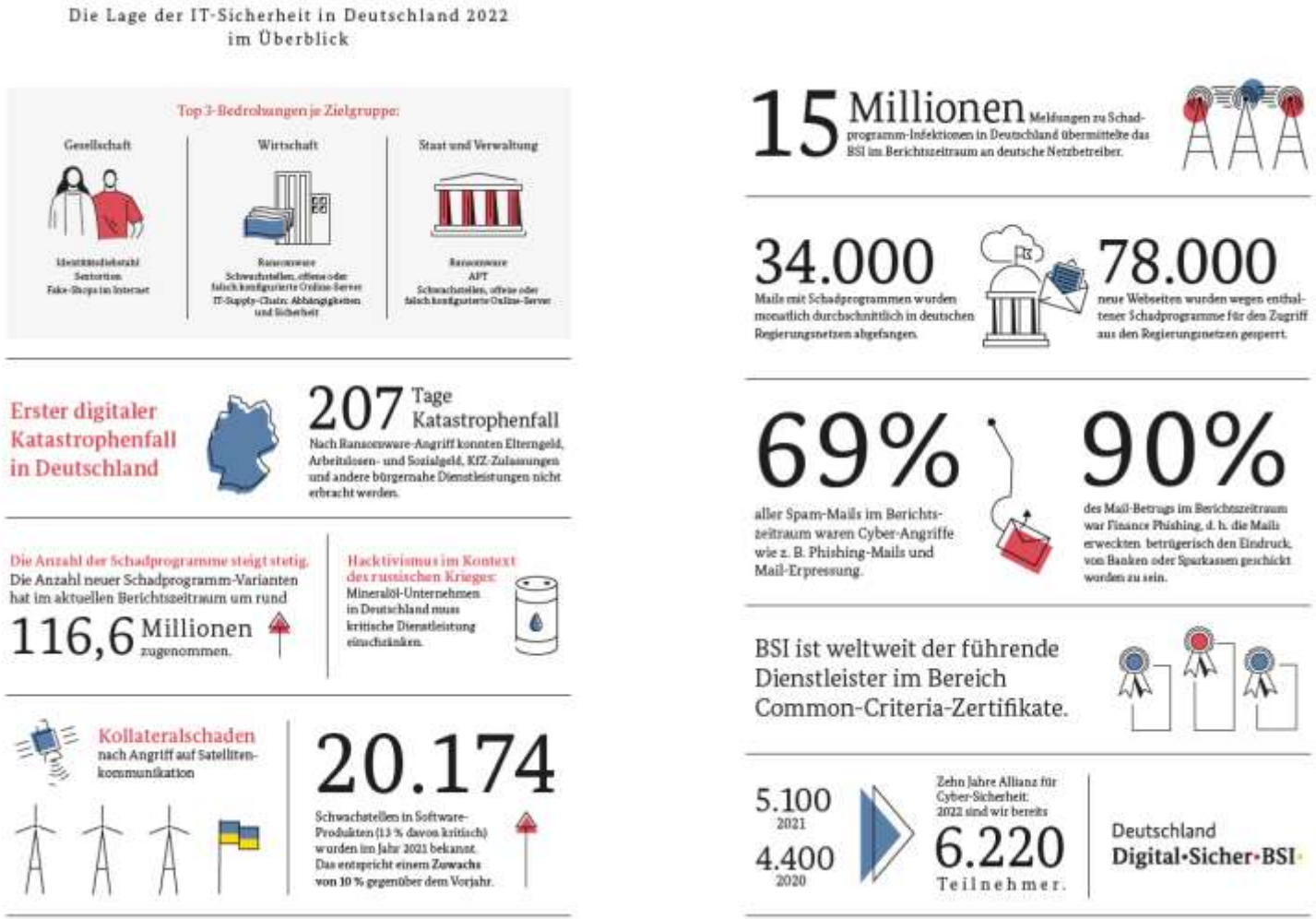
- Die Bedrohung im Cyber-Raum ist **so hoch wie nie zuvor.**
- Zur konstant hohen **Bedrohung durch Cybercrime** kommt Bedrohung durch Cyber-Angriffe in Folge des **russischen Angriffskriegs gegen die Ukraine**.
- **Ransomware ist weiterhin die größte Gefährdung** für die Informationssicherheit von Unternehmen, Organisationen und Behörden.
- Mehr als **116 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet. Das sind durchschnittlich **319.000 pro Tag, in Spitzenwerten 436.000.**

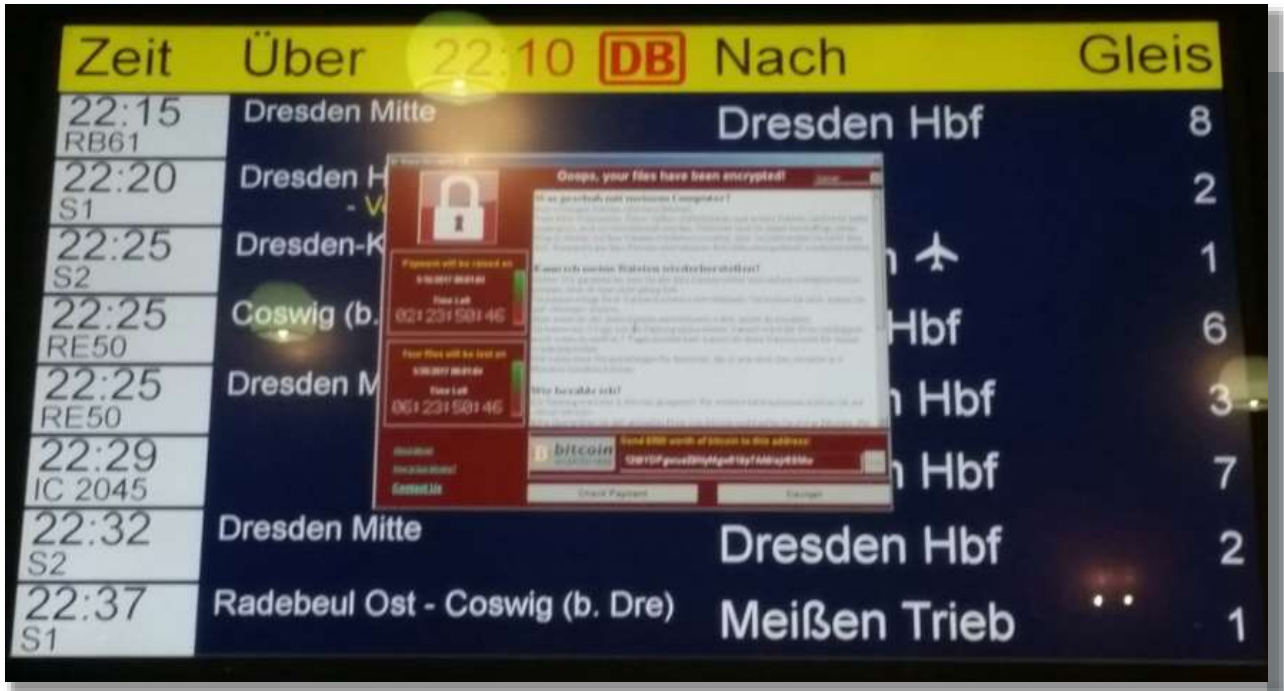
Wie bedroht ist Deutschlands Cyber-Raum?

- **Erster digitaler Katastrophenfall in Deutschland:** 207 Tage lang konnten Leistungen wie Elterngeld, Arbeitslosen- und Sozialgeld u. a. in einer Gemeinde in Sachsen-Anhalt nicht erbracht werden.
- Im Jahr 2021 wurden **20.174 Schwachstellen in Softwareprodukten** (13 % davon kritisch) festgestellt, 10 % mehr als im Jahr davor.
- **Russischer Angriffskrieg gegen die Ukraine**: Ansammlung kleinerer Vorfälle und Hacktivismus-Kampagnen, u. a. Kollateralschäden nach Angriff auf Satellitenkommunikation

Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

Hintergründe zur Digitalisierung





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 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!

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

Reagieren Sie schnell auf Warnungen!

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital·Sicher·BSI

Themen Das BSI Presse Publikationen IT-Sicherheitsvorfall Service

Presse

Aktive Ausnutzung der Citrix Schwachstelle

Ort Bonn
Datum 16.01.2020

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) liegen zahlreiche Meldungen vor, nach denen Citrix-Systeme erfolgreich angegriffen wurden. Das BSI ruft Anwender erneut dringend auf, die vom Hersteller Citrix bereitgestellten Workaround-Maßnahmen umgehend auszuführen und nicht auf die Sicherheitsupdates zu warten. Anwender, die die Workaround-Maßnahmen bislang nicht umgesetzt haben, sollten zudem ihre direkt mit dem Internet verbundenen Citrix-Systeme auf eine wahrscheinliche Kompromittierung prüfen. Angaben des Herstellers zufolge sollen Sicherheitsupdates je nach Verzweigung der betroffenen Produkte erst Ende Januar 2020 verfügbar sein. Diese sollten dann schnellstmöglich eingespielt werden.

Der US-Software-Hersteller Citrix hat am 17. Dezember 2019 über eine Schwachstelle (CVE-2019-19781) in den Produkten Citrix Gateway und Citrix Application Delivery Controller (ADC), am 16. Januar 2020 auch in der Citrix SD-WAN WANOP Appliance informiert. Die Produkte kommen für den Fernzugriff auf organisationseigene Anwendungen mit einem Web-Frontend bzw. zur Standortkopplung zum Einsatz. Die Schwachstelle ermöglicht es einem Angreifer, mittels von präparierten HTTP-/HTTPS-Anfragen aus dem öffentlich zugänglichen Verzeichnissen der Webanwendung auszubrechen und auf interne Verzeichnisse zuzugreifen. Dies kann in der Folge dazu führen, dass der Angreifer Konfigurationsdateien ausliest, Dateien ablegt oder manipuliert oder eigenen Code ausführt.

'In den vergangenen Tagen haben wir knapp 1.000 aus dem Internet erreichbare, verwundbare Citrix-Systeme an deutsche Netzbetreiber gemeldet. Derzeit sind davon immer noch rund 1.000 für Angreifer verwundbar. Leider reagieren die betroffenen Unternehmen oft nur langsam. Workarounds und Patches werden häufig nicht schnell genug umgesetzt. Wenn wir allein im WannaCry denken, so entstanden hier Schäden in Milliardenhöhe. Ich kann nur mit Nachdruck an die Wirtschaft appellieren, solche Warnungen nicht auf die lange Bank zu schieben. Wer Digitales nutzt, um Werte zu schaffen, muss seine Informationssicherheit hochhalten', erklärt BSI-Präsident Arne Schönbohm.

Bereits seit 7. Januar 2020 informiert das BSI deutsche Netzbetreiber über verwundbare Citrix-Systeme. Auch die Bundesverwaltung, Betreiber Kritischer Infrastrukturen und andere IT-Nutzergruppen wurden vom BSI informiert, insbesondere nach dem seit 10. Januar 2020 verstärkt Exploit-Code zur Ausnutzung der Schwachstelle veröffentlicht wurde.

Inhaltsverzeichnis

- Presseinformationen
- Pressearchiv
- Kurzmeldungen
- Pressestelle
- Presseverteiler
- Mediathek
- Bildmaterial
- Kurzprofil des BSI

CERT Bund

Home
Über CERT-Bund
Links
Warn- und Informationsdienste
Meldungen Suchen
Übersicht Meldungen
Kurzinfos
Informationen
Hersteller Meldungen
Digitale Signatur
Fragen und Antworten

Kurzinfo CB-K19/1093 Update 6

Information zu Schwachstellen und Sicherheitslücken

Revisions Historie

- Version: 8
  Neue Updates aufgenommen
- Version: 7
  Weitere betroffene Produkte aufgenommen
- Version: 6
  Produktversionen ergänzt
- Version: 5
  Score angepasst
- Version: 4
  Exploit aufgenommen, Patch Ankündigung aufgenommen
- Version: 3
  workaround
- Version: 2
  Anpassung
- Version: 1
  Initiale Fassung

Beschreibung

1. Citrix Security Bulletin CTX267027 vom 2019-12-17
2. GitHub: Project Zero Initial Exploit vom 2020-01-12
3. Citrix Security Bulletin CTX267027 vom 2020-01-11
4. Citrix Security Bulletin CTX267027 vom 2020-01-10
5. Citrix Security Bulletin CTX267027

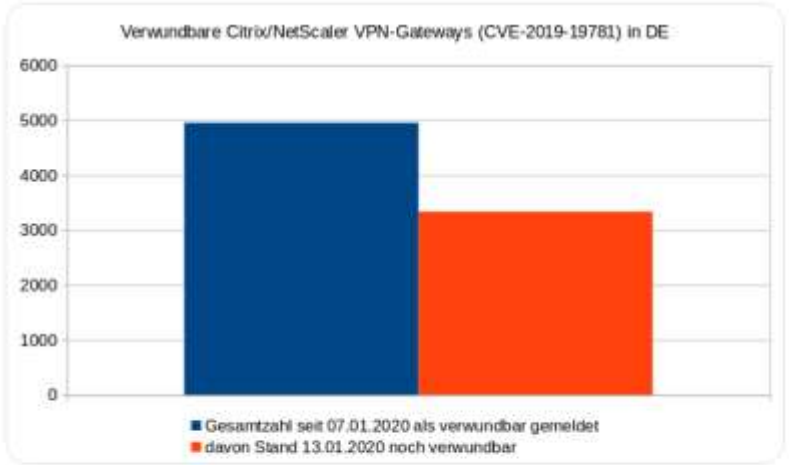
+ Authentifizierbare Ansicht dieser Meldung

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital·Sicher·BSI·

CERT-Bund
@certbund

In der letzten Woche hat CERT-Bund 4.957 verwundbare #Citrix/#NetScaler VPN-Gateways an deutsche Netzbetreiber gemeldet. Davon sind aktuell noch 3.338 verwundbar.

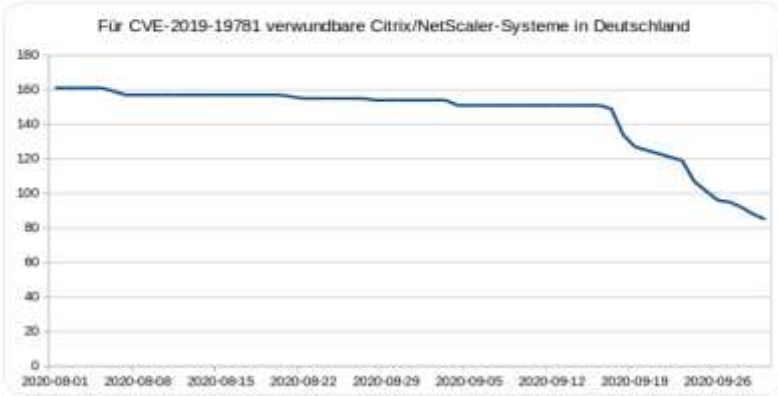


7:56 nachm. · 13. Jan. 2020 · Twitter Web App

42 Retweets **4** Zitierte Tweets **55** „Gefällt mir"-Angaben

CERT-Bund
@certbund

Parallel zur #Pressemitteilung vom 17.09.
bsi.bund.de/DE/Presse/Pres...
hat das @BSI_Bund die Geschäftsführungen aller deutschen #Unternehmen, die noch immer für #CVE-2019-19781 verwundbare #Citrix/#NetScaler #VPN-Gateways betrieben haben, per Briefpost angeschrieben.



9:27 vorm. · 2. Okt. 2020 · Twitter Web App

28 Retweets **20** Zitierte Tweets **57** „Gefällt mir"-Angaben

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

Zugriff auf das Firmennetz aus dem Homeoffice ausschließlich via VPN!

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 (MS20004, MS20008, MS20009).

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 SP3 Update Rollup (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

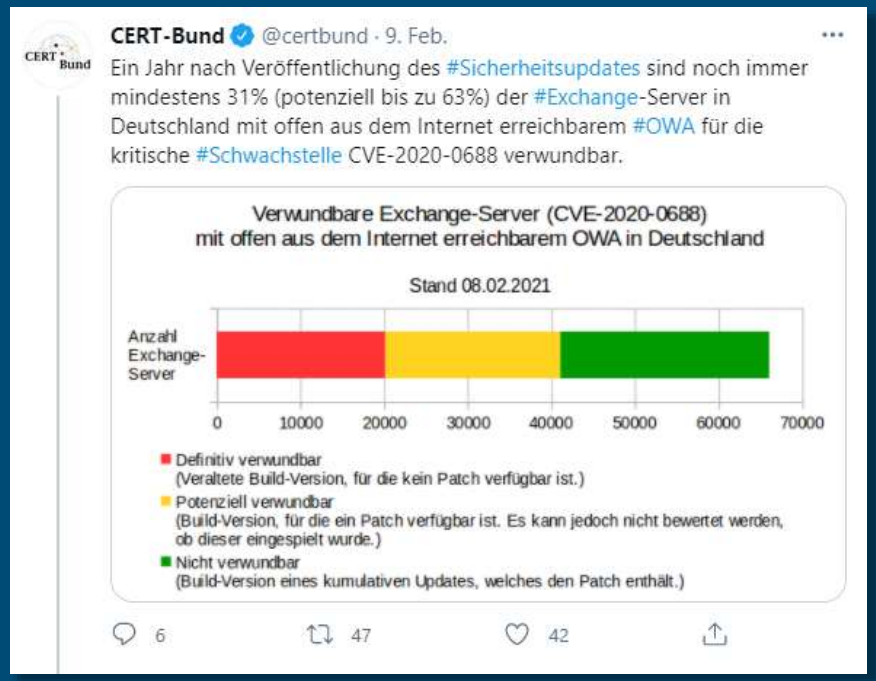
Ebenso betroffen sind ältere Produktversionen.

Bei CVE-2020-16875 handelt es sich um eine durch die fehlerhafte Argument-Validierung der 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:

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

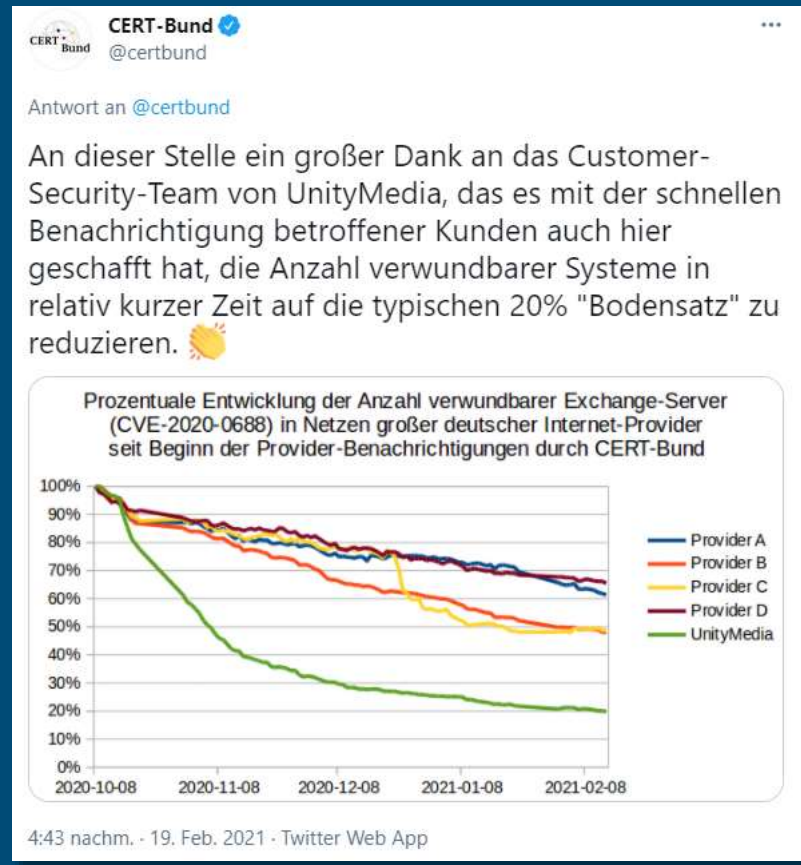
BSI-Cyber-Sicherheitswarnung



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

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 (MS20200a, MS20200b, MS16020c).

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 SP3 Update RU16 (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-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 nennenswerte Auffälligkeiten auf aufrechtem hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit erweiterter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs
3 / Orange: Die IT-Bedrohungslage ist gravierend hoch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht mehrere Behörden 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. Hierzu 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 unsichere deserialisation 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 abgefangene Administrator-Zugangsdaten erfolgen.

Nach Angaben des Herstellers richteten sich die Angriffe gegen amerikanische Forschungseinrichtungen mit Pandemie-Fokus, Hochschulen, Anwaltsfirmen, Organisationen aus den 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 (MS20211a).

Die Attacken erforderen 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 nennenswerte Auffälligkeiten auf aufrechtem hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit erweiterter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs
3 / Orange: Die IT-Bedrohungslage ist gravierend hoch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht mehrere Behörden werden.

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

BSI-IT-Sicherheitswarnung

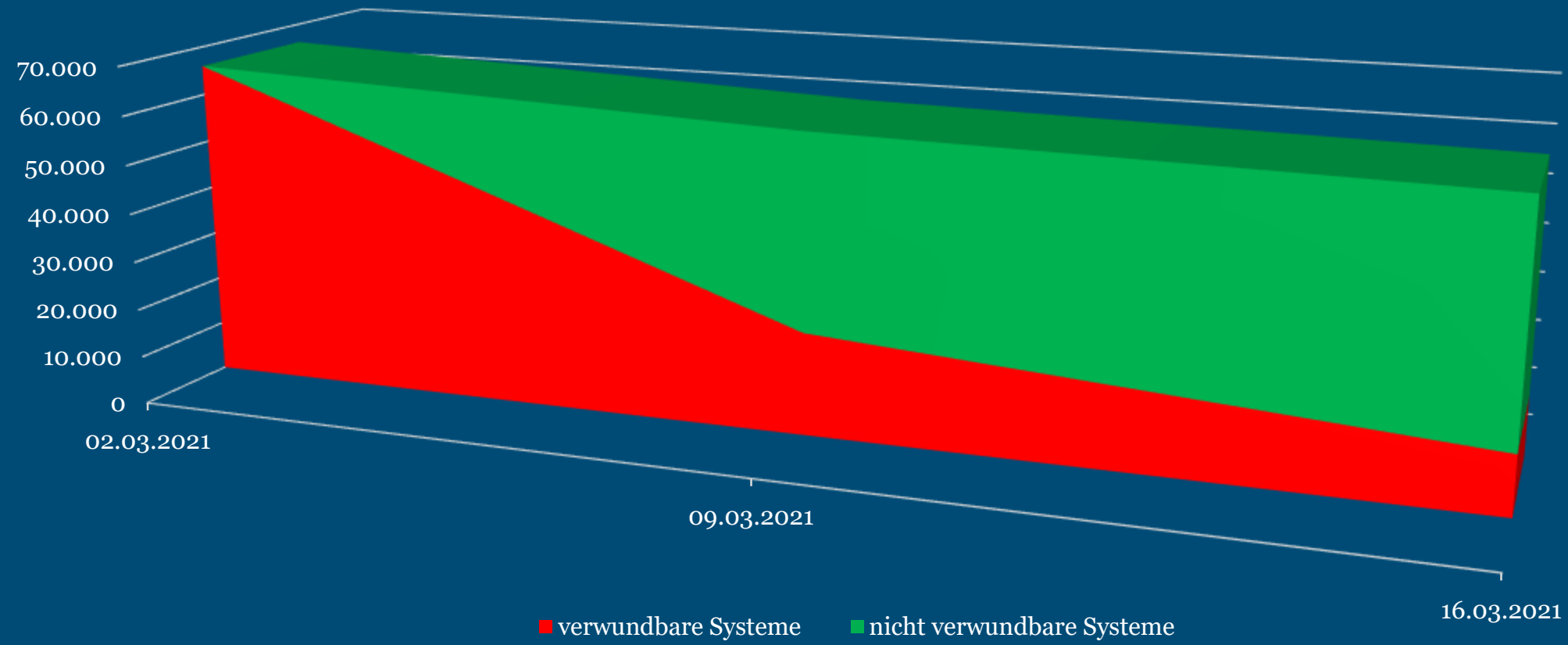
Nach Exchange-Hackerangriff

EU-Bankenaufsichtsbehörde muss gesamtes Mailsystem abschalten

Hacker nutzten eine Sicherheitslücke in Microsofts Programm Exchange, um Zugriff auf Systeme der europäischen Bankenaufsicht EBA zu bekommen. Weltweit könnten Zehntausende Unternehmen von der Attacke betroffen sein.

08.03.2021, 14.08 Uhr

Verwundbarkeit deutscher Exchange-Server für ProxyLogon
(CVE-2021-26855 et al.)



Phishing-Angriffe

tagesschau.de

Startseite | Videos & Audios | Inland | Ausland | Investigativ | Wirtschaft | Wahlen | Wetter | Ihre Meinung | Mehr

Startseite • Ausland • Bitcoin-Masche: Hackerangriff auf Twitter-Konten von Promis

Bitcoin-Masche

Hackerangriff auf Twitter-Konten von Promis

Stand: 16.07.2020 07:11 Uhr

Unbekannten ist es gelungen, Werbung für Kryptowährungs-Deals über Twitter-Accounts von US-Prominenten wie Obama, Biden und Bezos zu verbreiten. Noch nie wurden so viele Accounts auf einmal missbraucht.

Unbekannte Hacker haben sich Zugriff auf Twitter-Konten von amerikanischen Prominenten wie Ex-Präsident Barack Obama, Präsidentschaftskandidat Joe Biden und Amazon-Chef Jeff Bezos verschafft, um dubiose Bitcoin-Deals anzubieten.

Über die Accounts der Betroffenen wurden gefälschte Tweets abgesetzt, die 2000 Dollar für 1000 Dollar versprachen, die an eine bestimmte Bitcoin-Adresse geschickt würden. Neben Obama, Biden und Unternehmer Michael Bloomberg waren eine Reihe von Milliardären wie Microsoft-Mitgründer Bill Gates und Tesla-Chef Elon Musk betroffen. Auch Stars wie Kanye West und seine Frau Kim Kardashian West wurden gehackt.

VIDEO

Hacker verschaffen sich Zugriff auf Twitter-Konten prominenter Personen. Tagesschau 20:00 Uhr, 16.07.2020. Stefan Niemann, ARD Washington | video

AUDIO

Hackerangriff auf Twitter. Marcus Schuler, ARD-Hörfunkstudio Los Angeles, 16.07.20 07:58 Uhr | audio

MEHR AUSLAND

Fünf Szenarien: Was macht Trump nach einer Niederlage?

Iran-USA: Ziemlich beste Feinde

Süddeutsche Zeitung

SZ.de Zeitung Magazin

20. September 2016, 17:06 Uhr Bundesregierung ist alarmiert

Hackerangriff auf deutsche Parteien

Private Tablets und Smartphones sind im Bundestag tabu. Aber auch auf scheinbar dienstlichem Weg können Hackerangriffe erfolgen. (Foto: Maurizio Gambarini/dpa)

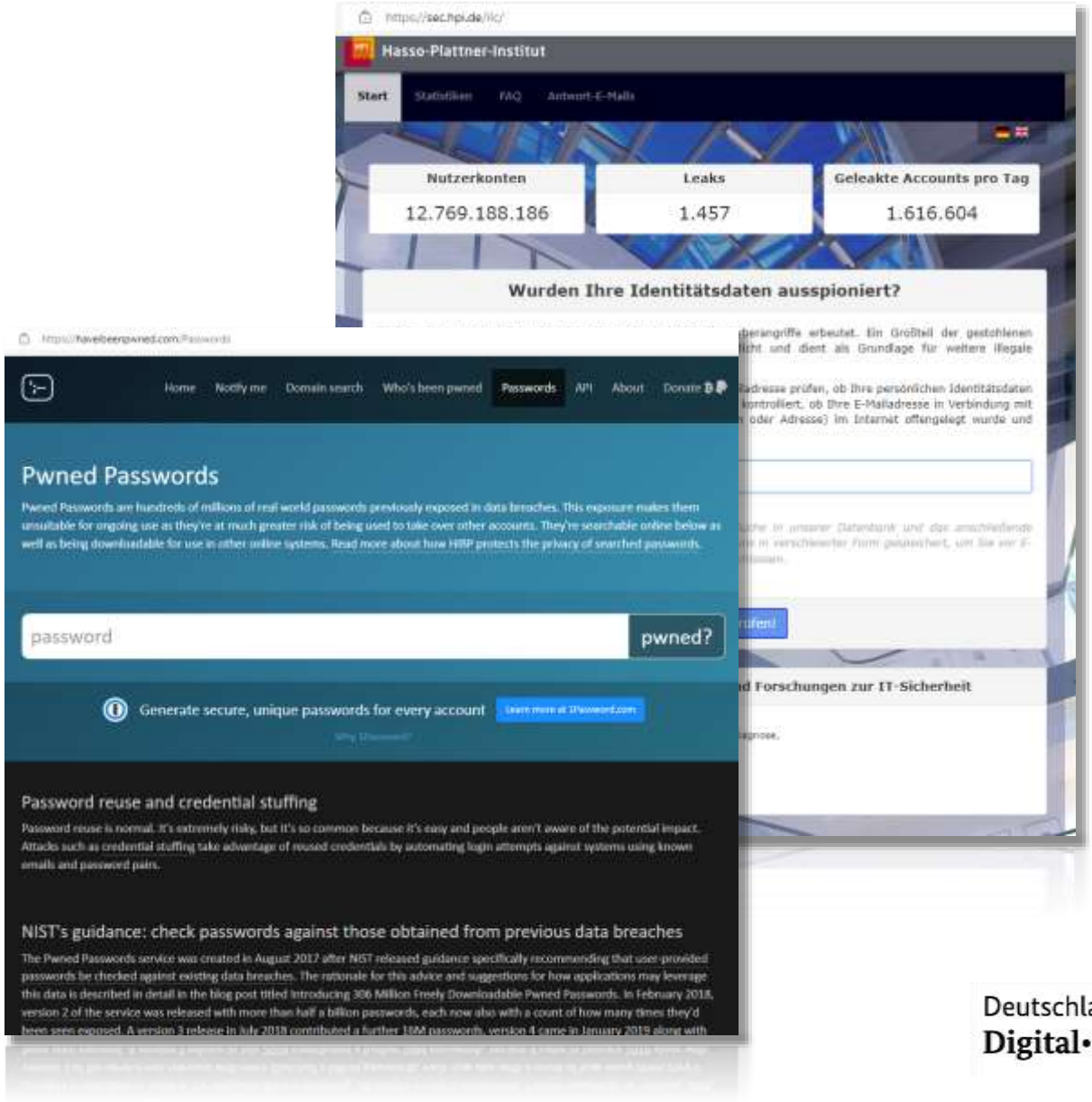
Hochrangige Politiker haben mehrmals E-Mails mit einer Spähsoftware erhalten. Die Regierung befürchtet, dass Abgeordnete vor der Bundestagswahl ausgespäht werden.

Von Georg Heil, Georg Mascolo, Reiko Pinkert und Nicolas Richter, Berlin

Phishing-Angriffe

Die 10 häufigsten Passwörter in Leak-Listen

1. 12345	6. quertz
2. passwort	7. schatz
3. 12345	8. basteln
4. hallo	9. berlin
5. 123456789	10. 12345678



Phishing-Angriffe

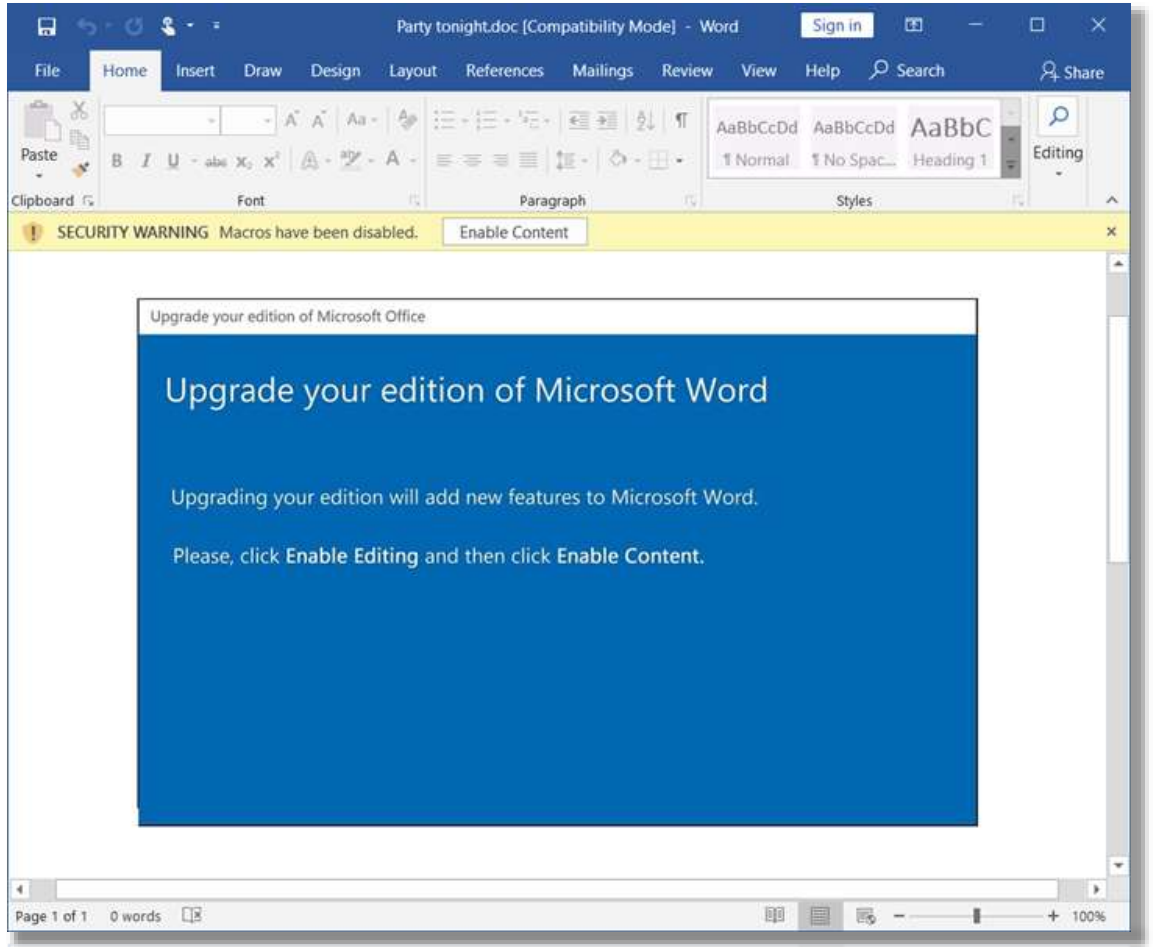
Gegenmaßnahme

- Lange, komplexe, neue Passwörter
- Passwort-Manager
- Zwei-Faktor-Authentisierung
- Personalausweis
- Passkey

Typischer Angriff über Makros

Kostenlose Gegenmaßnahme

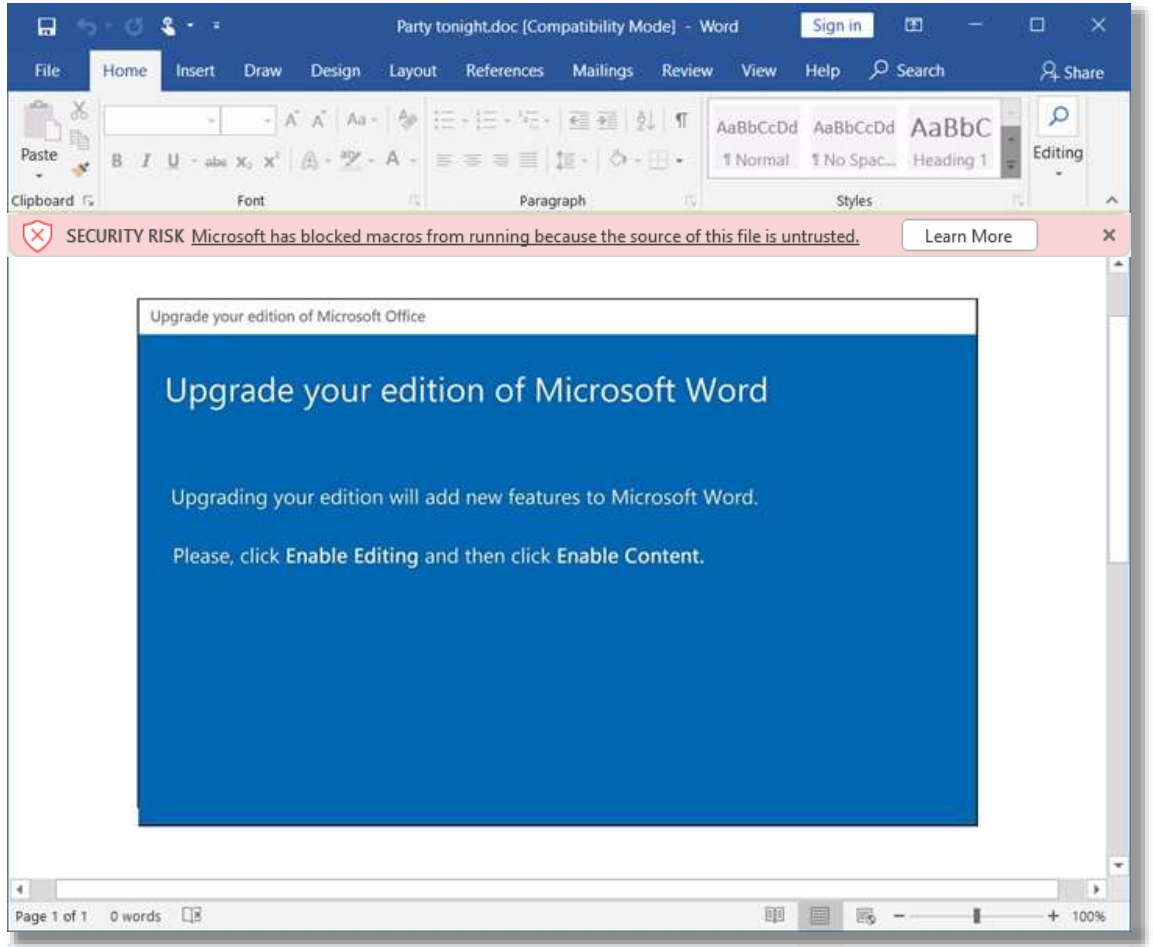
- Deaktivieren Sie in den Windows-Gruppenrichtlinien die Ausführung von Makros.
- Falls Makros unbedingt benötigt werden, lassen Sie nur signierte Makros zu.



Typischer Angriff über Makros

Kostenlose Gegenmaßnahme

- Deaktivieren Sie in den Windows-Gruppenrichtlinien die Ausführung von Makros.
- Falls Makros unbedingt benötigt werden, lassen Sie nur signierte Makros zu.



Üben Sie den Ernstfall !

Schließen Sie eine Cyber-Versicherung ab!

CyberRisikoCheck

nach DIN SPEC 27076 IT-Sicherheitsberatung für KMU

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**

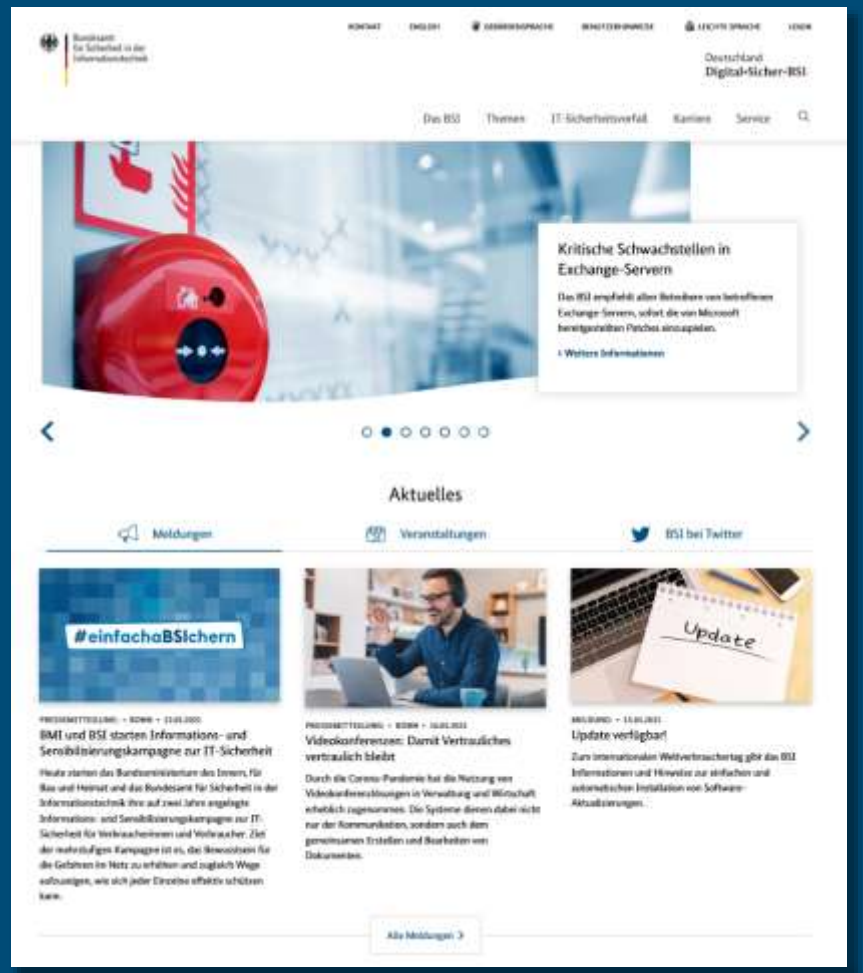
DIN SPEC 27076:2023-02 – „IT-Sicherheitsberatung für kleine und Kleinstunternehmen“

Für Unternehmen, die den CyberRisikoCheck durchführen lassen möchten:
Ausweitung der Förderprogramme (Zuschüsse bei Bund, Ländern und Kommunen)

Für IT-Dienstleister:
Kostenlose Bereitstellung einer webbasierten Software zur Durchführung des CyberRisikoChecks und Erstellung der Beratungsberichte

Weitere Informationen unter:
www.bsi.bund.de/dok/crc

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.

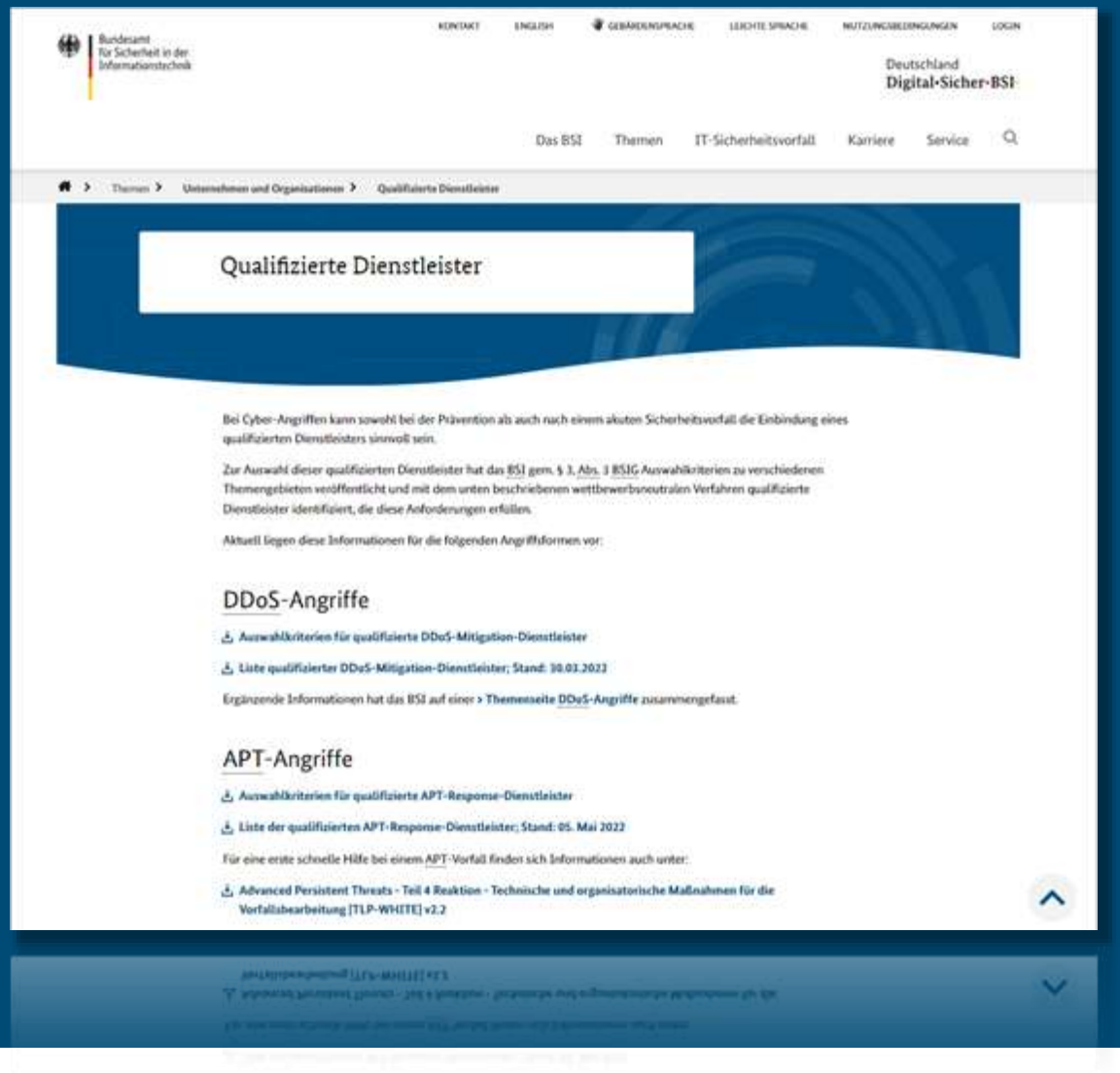
Gut vernetzt – Allianz für-Sicherheit

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

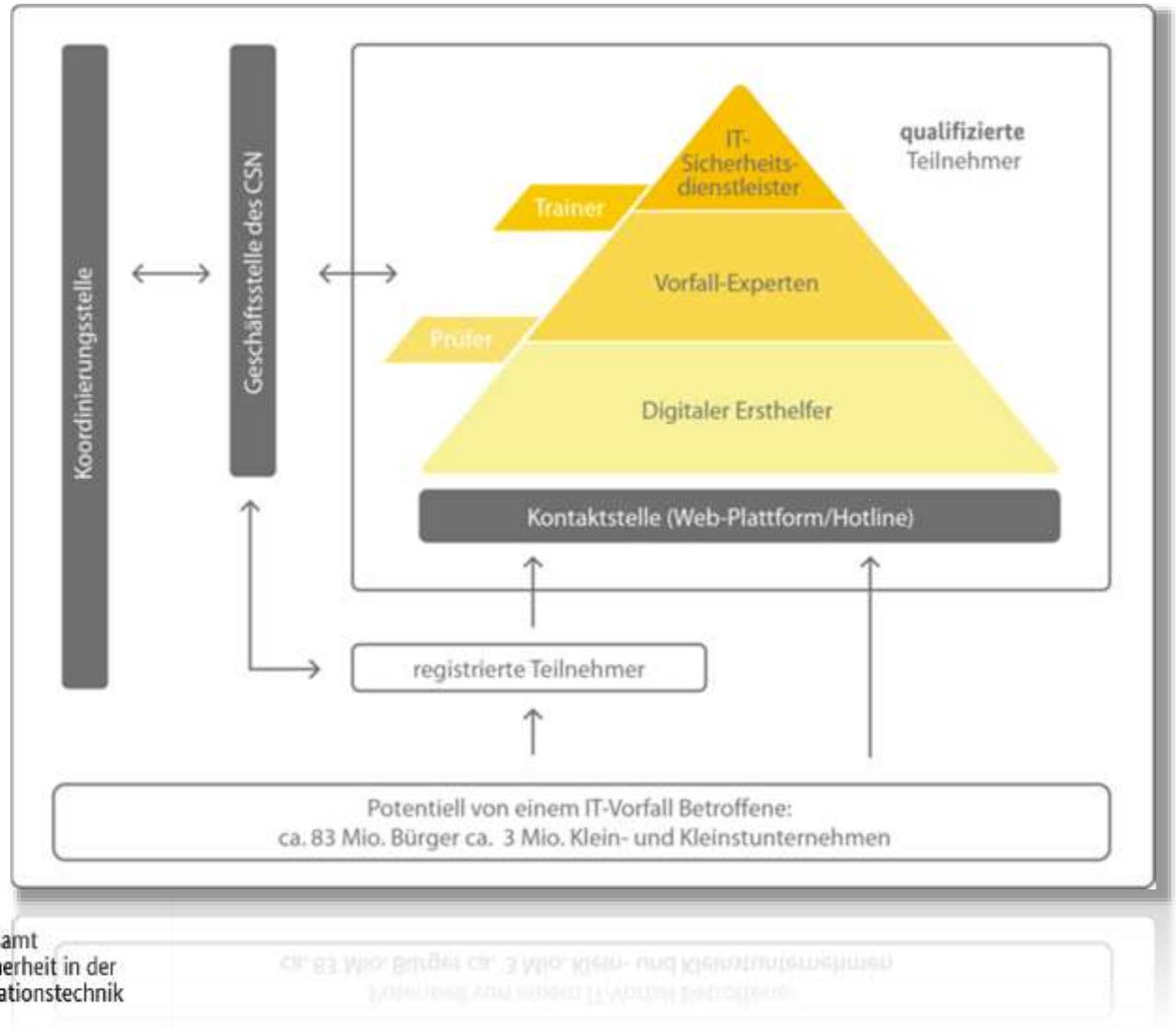
Sie bietet eine Kooperationsbasis zwischen:

- Staat,
- Wirtschaft,
- Herstellern und
- Forschung

www.allianz-fuer-cybersicherheit.de


KONTAKT
ENGLISH
GEBÄRDENSPRACHE
LEICHTE SPRACHE
NUTZUNGSBEDINGUNGEN
LOGIN
Bundesamt für Sicherheit in der Informationstechnik
Deutschland Digital•Sicher•BSI
Das BSI
Themen
IT-Sicherheitsvorfall
Karriere
Service
Themen > Unternehmen und Organisationen > Qualifizierte Dienstleister
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. 1 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: 30.03.2023
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

Cybersicherheits-Netzwerk (Pilotphase)



- Betroffene erhalten nach einem IT-Sicherheitsvorfall durch qualifizierte Teilnehmer des Cyber-Sicherheitsnetzwerks Unterstützung
- Trainer und Prüfer unterstützen das Qualifizierungskonzept und sichern die Qualität des unterstützenden Dienstleistungsangebotes durch Schulung bzw. die Abnahme einer Prüfung.
- Das Cyber-Sicherheitsnetzwerk ist eng mit der Allianz für Cyber-Sicherheit verzahnt und ergänzt dessen Angebot durch seine reaktive Dienstleistung.

https://www.bsi.bund.de/Cyber-Sicherheitsnetzwerk

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