Netzwerk Digital: Cyber Security Risiken und Prävention

Manuel Bach, Referatsleiter „Cybersicherheit für KMU“,
Bundesamt für Sicherheit in der Informationstechnik

Netzwerk Digital / Deutsch—Ungarische Industrie- und Handelskammer, 3. März 2022

Leitsatz

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

Kurzprofil des BSI

Gründung
01. Januar 1991

197 Mio. Euro
Budget Haushalt 2021

Stellen 2021
1550 ↗

116 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.

Produkte und Dienstleistungen

Übernahme technischer Schutzmaßnahmen
Sichere mobile Lösungen, Schadsoftware-Prävention, Analysen, DDoS-Mitigation, IT-Notfallmanagement für Regierungsnetze, Angriffserkennung, Nationales IT-Lagezentrum, Technische Richtlinien (TR)

Kooperation
Nationales Verbindungswesen, Cyber-Sicherheitstage, IT-Grundschutztage, Jahrestagung der Informationssicherheitsbeauftragten (ISB), Beirat Digitaler Verbraucherschutz, Cyber-Abwehrzentrum, Allianz für Cybersicherheit, UP KRITIS

Technische Unterstützung und Dienstleistungen
CERT-Bund, Kryptosysteme, Abstrahl-/Lauschabwehrprüfungen, IS-Penetrationstests, Mobile Incident Response Teams (MIRTs), technische Evaluierung, Malware Information Sharing Platform (MISP), Warnungen

Begleitung in der Aus- und Fortbildung
ISB-Ausbildung, Sensibilisierungsvorträge (u. a. Live Hacking), Übungszentrum Netzverteidigung

Beratung
Managementsystem für Informationssicherheit (ISMS), Abhörsicherheit, nach Vorfallsmeldungen, Unterstützung Digitalisierungsprojekte, Digitaler Persönlichkeits- und Verbraucherschutz, Gesellschaftlicher Dialog, Service-Center

Information
IT-Grundschutz, Mindeststandards, Technische Richtlinien (TR), CS-Empfehlungen, Liste zertifizierter und zugelassener Produkte, Lageberichte, Zertifizierungen, IT-Sicherheitskennzeichen (IT-SiK)

Organisation des BSI

Stand: 15.12.2021

Leitungsstab

Präsident

Vizepräsident

Abteilung Z Zentrale Aufgaben	**Abteilung TK** Technik-Kompetenzzentren	**Abteilung KM** Krypto-Technik und IT-Management	**Abteilung OC** Operative Cyber-Sicherheit	**Abteilung SZ** Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen	**Abteilung DI** Cyber-Sicherheit in der Digitalisierung und für elektronische Identitäten	**Abteilung BL** Beratung für Bund, Länder und Kommunen	**Abteilung WG** Cyber-Sicherheit für Wirtschaft und Gesellschaft
Fachbereich Z 1 Zentrale Aufgaben 1	**Fachbereich TK 1** IT-Systeme	**Fachbereich KM 1** Zulassung und Bereitstellung von VS- und IT-Sicherheitssystemen	**Fachbereich OC 1** Detektion	**Fachbereich SZ 1** Standardisierung, Grundsätze der Zertifizierung, Aufsicht	**Fachbereich DI 1** Cyber-Sicherheit für elektronische Identitäten (eID)	**Fachbereich BL 1** Informationssicherheits-beratung und Geheimschutz	**Fachbereich WG 1** Cyber-Sicherheit für Kritische Infrastrukturen
Fachbereich Z 2 Zentrale Aufgaben 2	**Fachbereich TK 2** IT-Infrastrukturen	**Fachbereich KM 2** Vorgaben, Entwicklung und Prüfung von Krypto-, VS- und IT-Sicherheitssystemen	**Fachbereich OC 2** CERT-Bund	**Fachbereich SZ 2** Zertifizierungsverfahren	**Fachbereich DI 2** Cyber-Sicherheit in der Digitalisierung	**Fachbereich BL 2** Kundenmanagement und Recht	**Fachbereich WG 2** Cyber-Sicherheit für die Wirtschaft
		Fachbereich KM 3 IT-Management	**Fachbereich OC 3** IT-Sicherheitslage	**Fachbereich SZ 3** Cyber-Sicherheit in mobilen Infrastrukturen und Chiptechnologie		**Fachbereich BL 3** Informationssicherheit der konsolidierten Bundes-Rechenzentren und -Netze	**Fachbereich WG 3** Digitaler Verbraucherschutz, Cyber-Sicherheit für Gesellschaft und Bürger

Wie bedroht ist Deutschlands Cyber-Raum?

- **Ausweitung** bekannter cyber-krimineller Erpressungsmethoden
- Neben **Lösegelderpressungen** traten **Schweigegelderpressung** unter Androhung der Enthüllung vertraulicher Informationen (Double Extortion) und **Schutzgelderpressungen** unter Androhung von DDoS auf.
- Rund **144 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet. Das sind durchschnittlich **394.000 pro Tag, in Spitzenwerten 533.000 (höchster je gemessener Wert).**

Wie bedroht ist Deutschlands Cyber-Raum?

- Unmittelbar nach Bekanntwerden der kritischen **Schwachstellen in Microsoft Exchange-Servern**, waren **rund 98 %** aller geprüften Systeme verwundbar.
- Bei Angriffen auf die Bundesverwaltung wurden rund **44.000 E-Mails mit Schadsoftware pro Monat** abgefangen.
- **COVID-19-Pandemie**: Neue Gefährdungslage durch Cyber-Angriffe **im Gesundheitsbereich auf Firmen, Behörden und Verbraucher**

Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

Neuer Trend

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung

Lösegeld-Erpressung

Schutzgeld-Erpressung

13 Tage lang konnte ein Universitätsklinikum nach einem *Ransomware*-Angriff keine Notfall-Patienten aufnehmen.

144 MIO. neue Schadprogramm-Varianten

+22 % gegenüber 2020: 117,4 MIO.

DURCHSCHNITTLICH **394.000** neue Schadprogramm-Varianten pro Tag (2020: 322.000)

IM HÖCHSTWERT **553.000** (2020: 470.000)

DOPPELT SO VIELE BOT-INFEKTIONEN DEUTSCHER SYSTEME pro Tag im Tagesspitzenwert

20.000 > 40.000

98 % aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

14,8 MIO.

Meldungen zu Schadprogramm-Infektionen übermittelte das BSI an deutsche Netzbetreiber, mehr als **DOPPELT SO VIEL** wie im Jahr zuvor.

44.000 Mails mit Schadprogrammen wurden im Durchschnitt pro Monat in deutschen Regierungsnetzen abgefangen.

2020 ..... 35.000

74.000 Webseiten wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt.

2020 ..... 52.000

BSI unter **TOP 3 NATIONEN** weltweit bei Common-Criteria-Zertifikaten.

5.100 MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT

- 2020: 4.400
- 2019: 3.700
- 2018: 2.700

< 10 % waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in **MS Exchange** verwundbar.

Deutschland Digital•Sicher•BSI•

Artikel 3:

„Et hätt noch emmer joot jejange.“*

* … in einer anderen Zeit und unter völlig anderen Rahmenbedingungen!

Entwicklung der Digitalisierung

…mehr Datenübertragung

2016	2021
108.000 TB	***400.000 TB***
pro Std[1]	*pro Std[1]*

…mehr Geschwindigkeit

2016	2021
***27 Mbps** (fix)*	***53 Mbps** (fix)*
***7 Mbps** (mobil)[1]*	***20 Mbps** (mobil)[1]*

…mehr Geräte

2016	2021
***fünf** webfähige*	***neun** webfähige*
Geräte p.K. in D[1]	*Geräte p.K. in D[1]*

…mehr Vernetzung

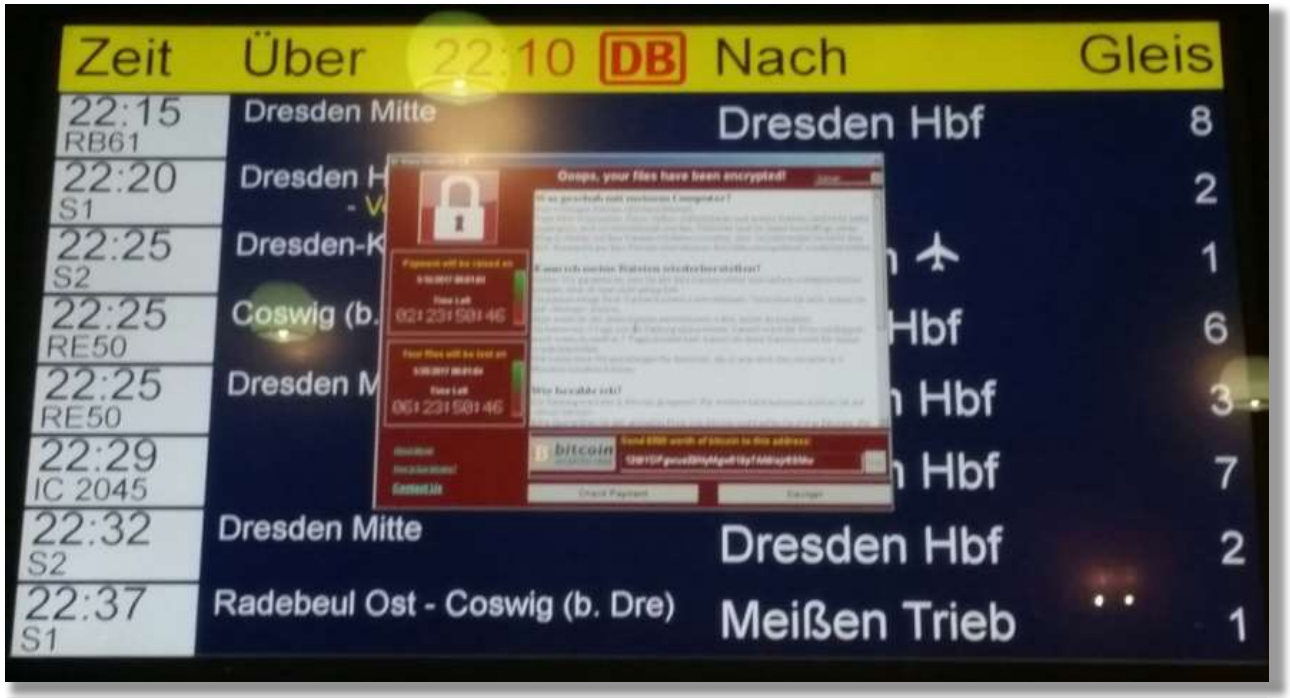
2016	2021
***6 Mrd.** M2M*	***14 Mrd.** M2M*
fähige Geräte[1]	*fähige Geräte[1]*

…mehr Angriffe

2016	2021
***1,3 Mio.** DDoS*	***3,1 Mio** DDoS*
Angriffe >1 Gbps	*Angriffe >1 Gbps*


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
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
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


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
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
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


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

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


Allianz
Top 10 Geschäftsrisiken weltweit in den vergangenen 10 Jahren
Allianz Risk Barometer 2013 - 2022
Diese Grafik zeigt, wie sich die Sichtweise ausgewählter Top-Risiken in den letzten 10 Jahren verändert hat (% der Antworten). Nicht alle Risiken, die in der jährlichen Umfrage genannt wurden, erscheinen in dieser Grafik, da sich Risiken und Kategorisierungen im Laufe der Zeit verändert haben. Um die Top-Risiken für jedes Jahr nach Rangfolge zu sehen, klicken Sie auf: Allianz Risk Barometer.
2013 2014 2015 2016 2017 2018 2019 2020 2021 2022
Cybervorfälle 44%
Betriebsunterbrechung 42%
Naturkatastrophen 25%
Ausbruch einer Pandemie 22%
Rechtliche Veränderungen 19%
Klimawandel 17%
Feuer, Explosion 17%
Marktveränderungen 15%
Fachkräftemangel 13%
Makroökonomische Entwicklungen 11%
Reputationsverlust 10%
Neue Technologien 9%
Politische Risiken 9%
Produktrückruf, Qualitätsmanagement, Serienfehler 6%
Diebstahl, Betrug und Korruption 5%
AGCS News & Insights
Quelle: Allianz Global Corporate & Specialty

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

Regel Nr. 3:

Prävention ist wesentlich preiswerter als Reaktion!

Regel Nr. 3:

Prävention ist wesentlich preiswerter als Reaktion!

→ 20 Prozent Ihres IT-Budgets für IT-Sicherheit

Regel Nr. 4:

Teure Reaktion ist immer noch preiswerter als Kapitulation!

Regel Nr. 4:

Teure Reaktion ist immer noch preiswerter als Kapitulation!

→ **Professionelle externe Hilfe kann kostspielig sein, ist aber oftmals nötig**

Grundsätzliches

„Ich glaube, um sowas kümmert sich der Ulf …“

IT-Sicherheit ist Chefsache!

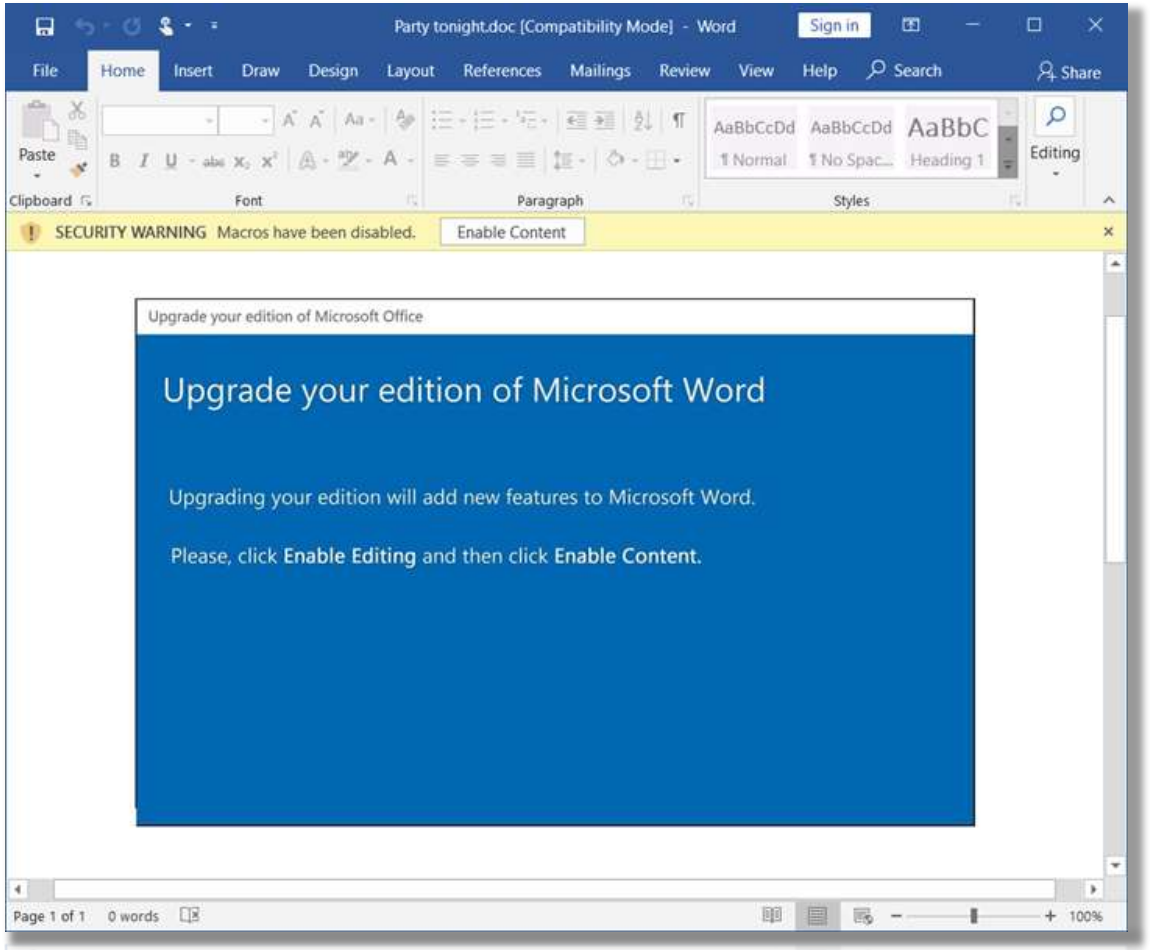
Sorgen Sie für klare Zuständigkeiten!


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

Typischer Angriff über Makros

Kostenlose Gegenmaßnahme

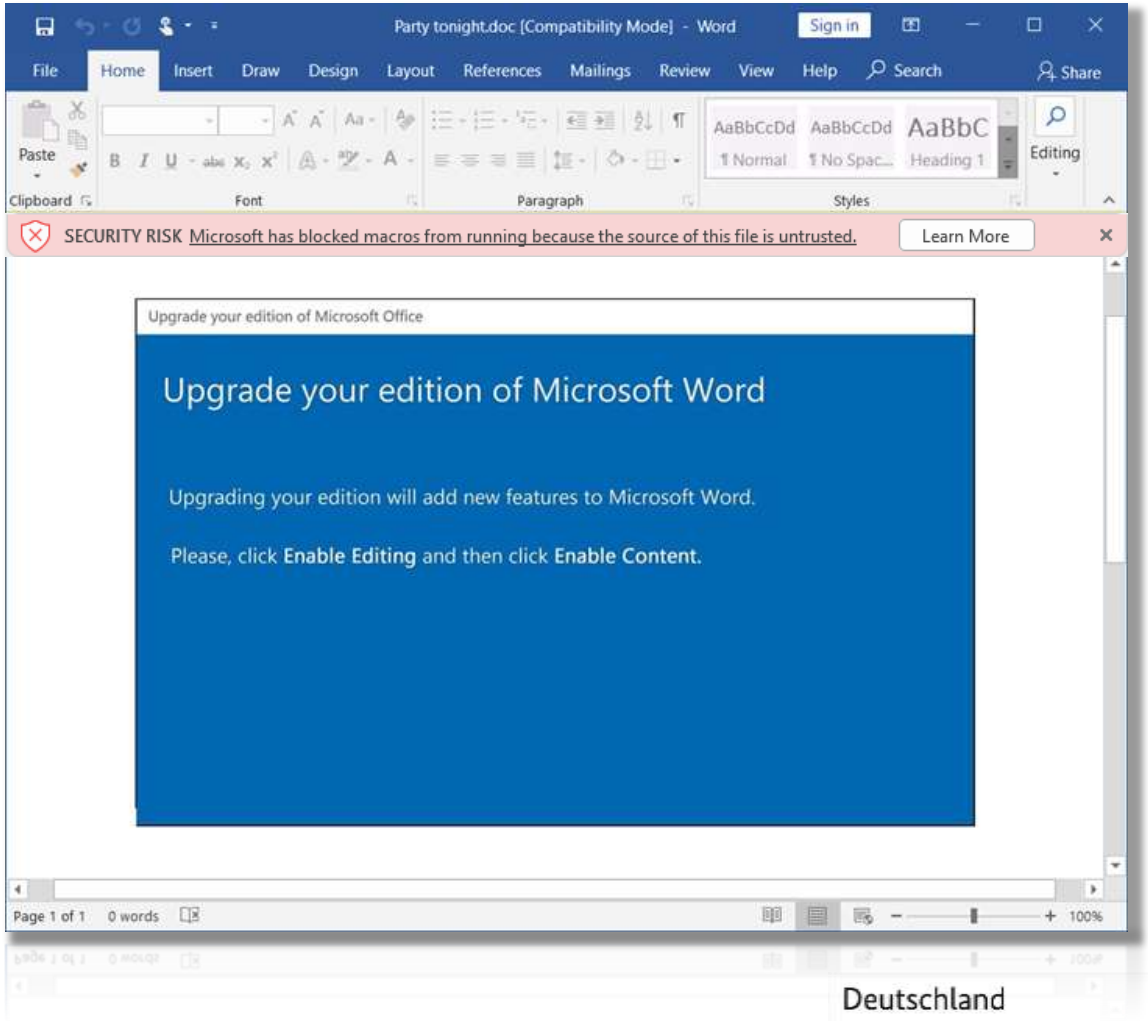
- Deaktivieren Sie in den Windows-Gruppenrichtlinien die Ausführung von Makros.
- Falls Makros unbedingt benötigt werden, lassen Sie nur signierte Makros zu.



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.



Typischer Phishing-Angriff

Gegenmaßnahme

- Komplexe Passwörter
- Passwort-Manager
- Zwei-Faktor-Authentisierung

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

Reagieren Sie schnell auf Warnungen!

Typischer Angriff über Makros

- Ausgenutzte Schwachstelle:
  CVE-2017-0144: Windows SMB Remote Code Execution Vulnerability („EternalBlue“)
- Durch Microsoft geschlossen am 14.03.2017
- Ausgenutzt durch WannaCry ab dem 12.05.2017

Kostenlose Gegenmaßnahme

- Zeitnahes Einspielen von Updates
- Ggf. Umsetzen von Work-Arounds

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 mögliche Kompromittierung prüfen. Angaben des Herstellers zufolge seien Sicherheitsupdates je nach Versionszweig 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 10. Januar 2020 auch in der Citrix SD-WAN WANOP Appliance informiert. Die Produkte kommen für den Fernzugriff auf organisationsinterne Anwendungen mit einem Web-Frontend bzw. zur Standortkopplung zum Einsatz. Die Schwachstelle ermöglicht es einem Angreifer, mittels von präparierten HTTP-/HTTPS-Anfragen aus den öffentlich zugänglichen Verzeichnissen der Weboberfläche auszubrechen und auf interne Verzeichnisse zuzugreifen. Dies kann in der Folge dazu führen, dass der Angreifer Konfigurationsdateien auslesen, Dateien ablegen oder manipuliert oder eigenen Code ausführen.

"In den vergangenen Tagen haben wir knapp 2.000 aus dem Internet erreichbare, verwundbare Citrix-Systeme an deutsche Netzbetreiber gemeldet. Derzeit sind davon immer noch rund 1.100 für Angreifer verwundbar. Leider reagieren die betroffenen Unternehmen oft nur langsam. Workarounds sind Pflicht, werden häufig nicht schnell genug umgesetzt. Wenn wir allein an WannaCry denken, es 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 Wert 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 vorliegt Exploit-Code zur Ausnutzung der Schwachstelle veröffentlicht wurde.

Inhaltsverzeichnis

- Pressemitteilungen
- Pressereden
- Kurzmeldungen
- Pressefotos
- Pressevertreter
- Mediathek
- Bildmaterial
- Kurzprofil des BSI

CERT Bund

Home
Über CERT-Bund
Warn- und Informationsdienste

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
  Kurze eingefügt
- Version: 4
  Exploit aufgenommen, Patch-Verfügbarkeit aufgenommen
- Version: 3
  workaround
- Version: 2
  Aktualisierung
- Version: 1
  Initiale Meldung

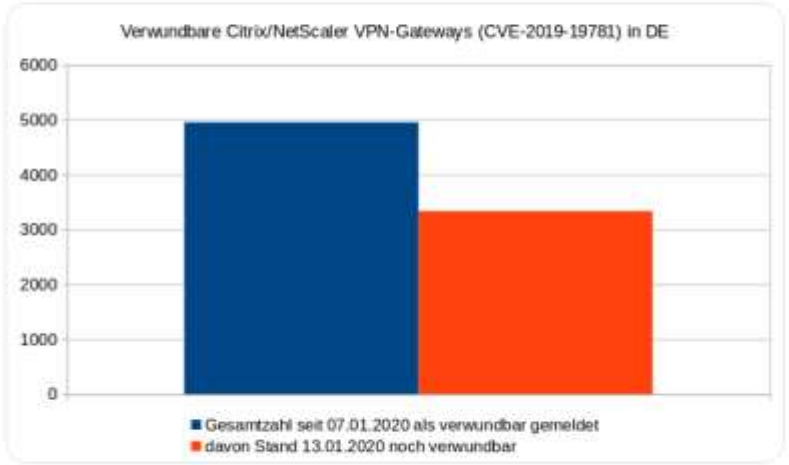
Beschreibung

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.

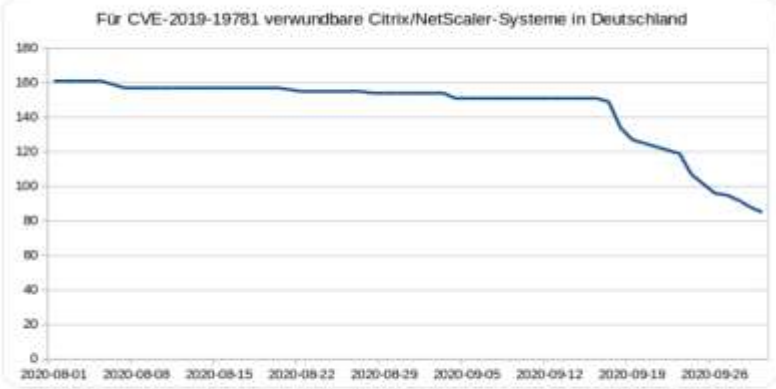


7:56 nachm. · 13. Jan. 2020 · Twitter Web App

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

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

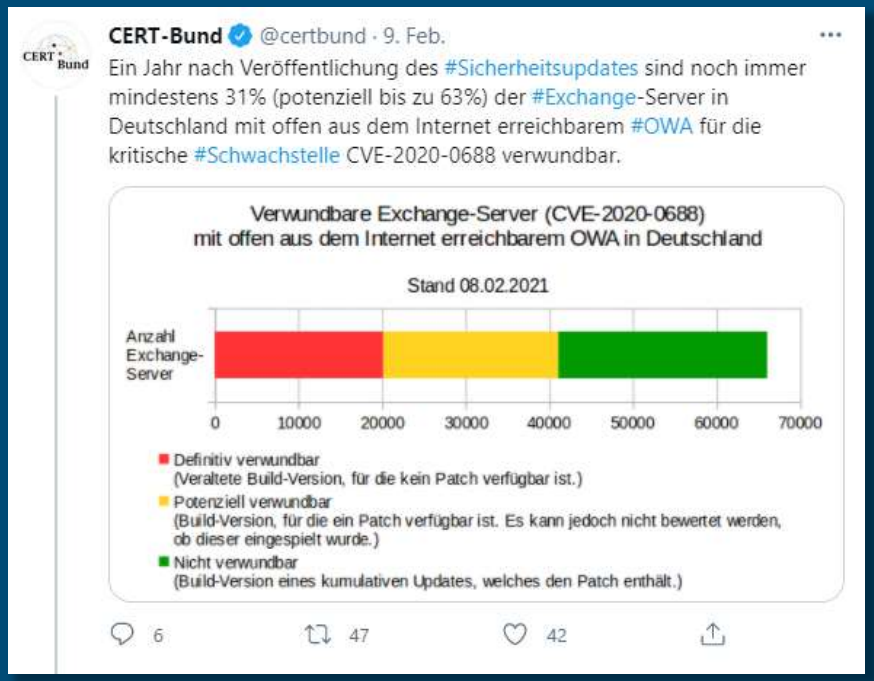
Ebenso betroffen sind ältere Produktversionen.

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:

BSI-Cyber-Sicherheitswarnung

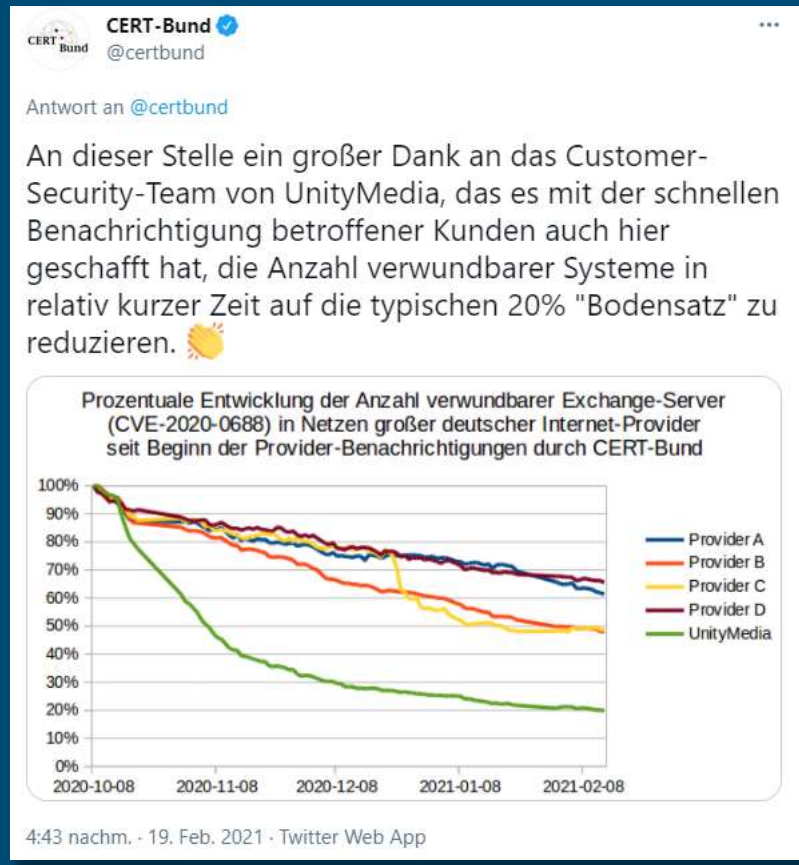
CSW # 2020-252437-1131 | Version 1.1 vom 13.10.2020 Seite 1 von 3



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



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 [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-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 schadsoftwarebedingte Vorfälle.
2 / Gelb: IT-Bedrohungslage mit verstärkter 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 weiterhin 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 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 [MS2021a].

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 nennenswerte Auffälligkeiten auf schadsoftwarebedingte Vorfälle.
2 / Gelb: IT-Bedrohungslage mit verstärkter 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 weiterhin erhalten werden.

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

BSI-IT-Sicherheitswarnung

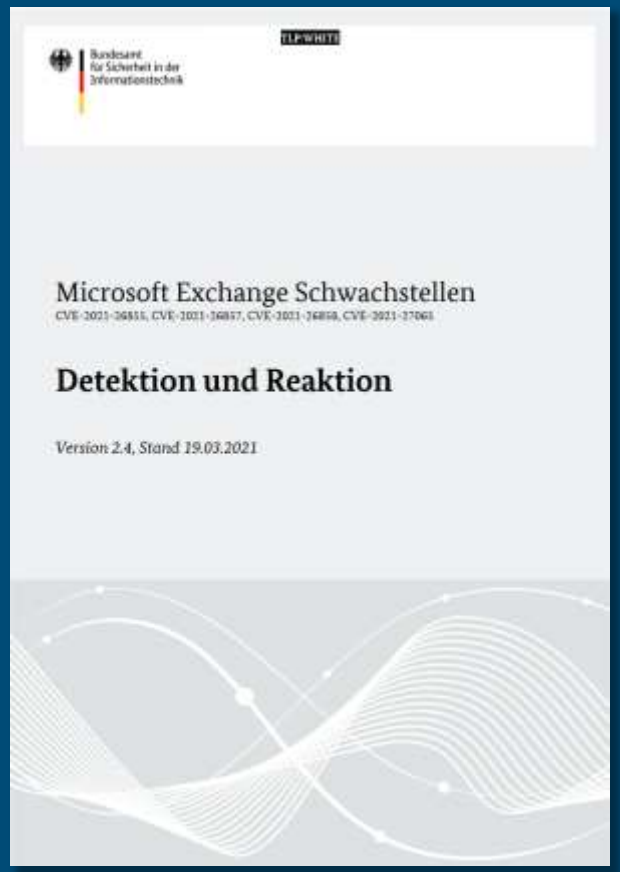
Nach Exchange-Hackerangriff

EU-Bankenaufsichtsbehörde muss gesamtes Mailsystem abschalten

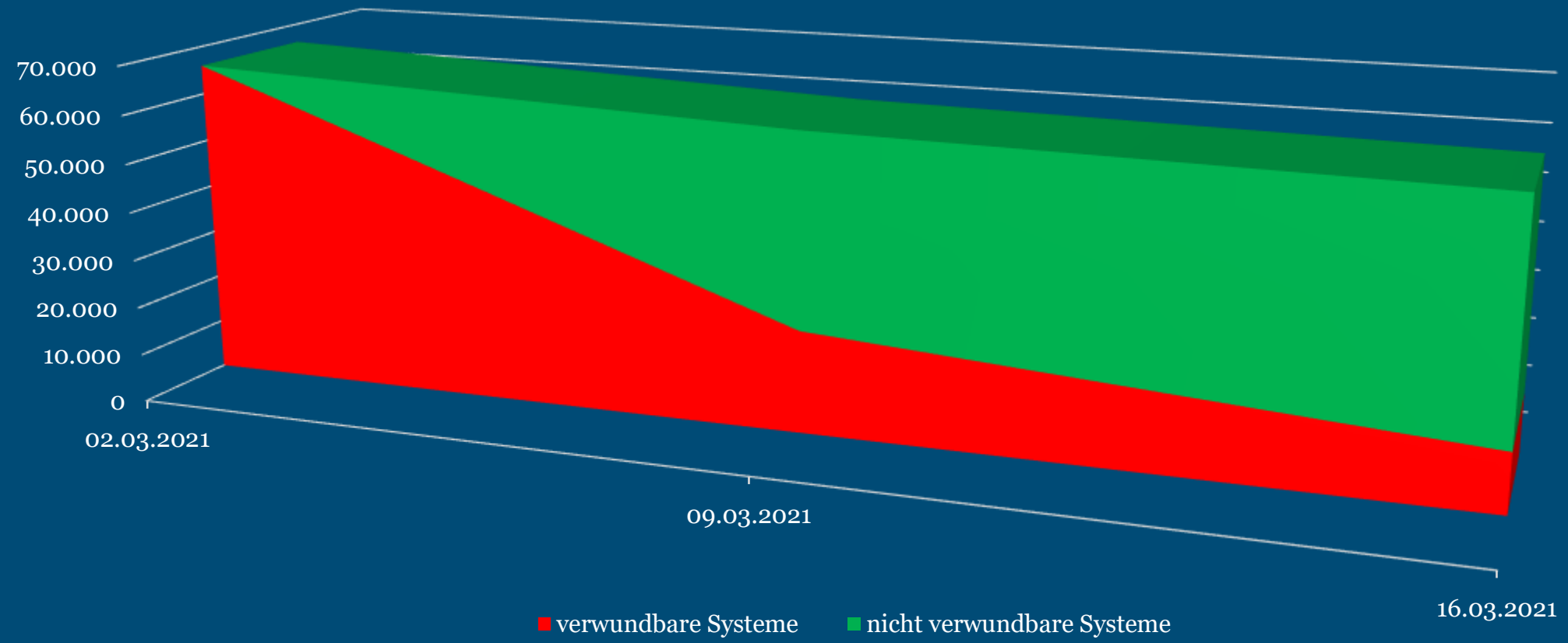
Hacker nutzten eine Sicherheitslücke in Microsofts Programm Exchange, um Zugriff auf Systeme der europäischen Bankenaufsicht EBA zu bekommen. Weltweit könnten Zehntausende Unternehmen von der Attacke betroffen sein.

08.03.2021, 14.08 Uhr


Livestream „BSI-Update MS Exchange Schwachstellen - Infos und Hilfestellungen“
11.03.2021, 15.30-16.30 Uhr
Fragen per Kommentar oder
Mail an livestream@bsi.bund.de
BSI
LIVE
Bundesamt für Sicherheit in der Informationstechnik
Update: MS Exchange Schwachstellen - Infos und Hilfestellungen | BSI
22.681 Aufrufe • Live übertragen am 11.03.2021
571
4
TEILEN
SPEICHERN

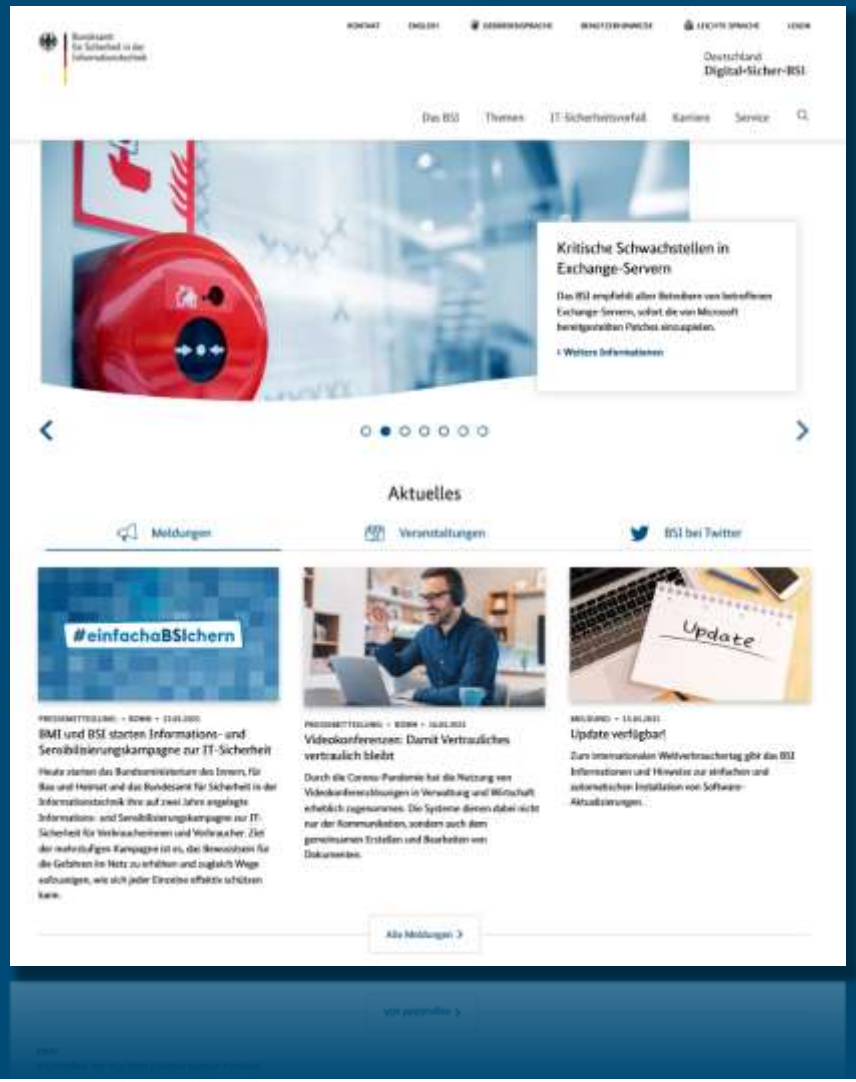

TLP:WHITE
Bundesamt für Sicherheit in der Informationstechnik
Microsoft Exchange Schwachstellen
CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065
Detektion und Reaktion
Version 2.4, Stand 19.03.2021

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



Üben Sie den Ernstfall !

Nutzen Sie das BSI !



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

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:

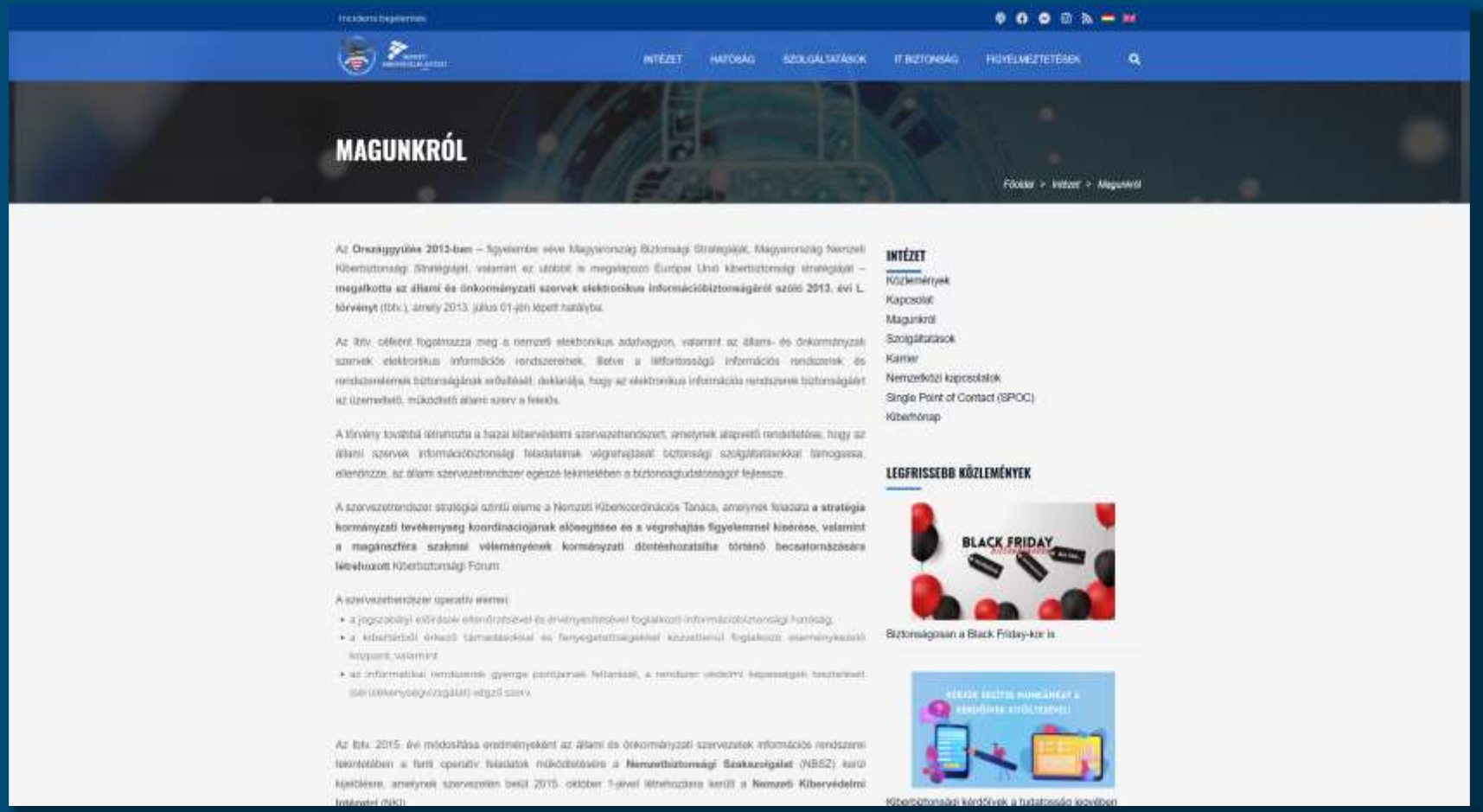
- Staat,
- Wirtschaft,
- Herstellern und
- Forschung

www.allianz-fuer-cybersicherheit.de

Angebote für Unternehmen und Institutionen

Informationen erhalten	Erfahrungen austauschen	Kompetenzen erwerben
Online-Informationspool: • BSI-Warnungen • Aktuelle Lagebilder • Lösungshinweise und Anleitungen • Hintergrund-wissen • Veranstaltungs-dokumentation	Cyber-Sicherheits-Tage	Übungszentrum Netzverteidigung
	Umfrage	**Angebote der Partner:** • Schulungen und Workshops • Analysen und Erstberatung • Pen-Tests • Tools
	ERFA-Kreise	
	Experten-Kreise	

https://nki.gov.hu



Vielen Dank für Ihre Aufmerksamkeit!

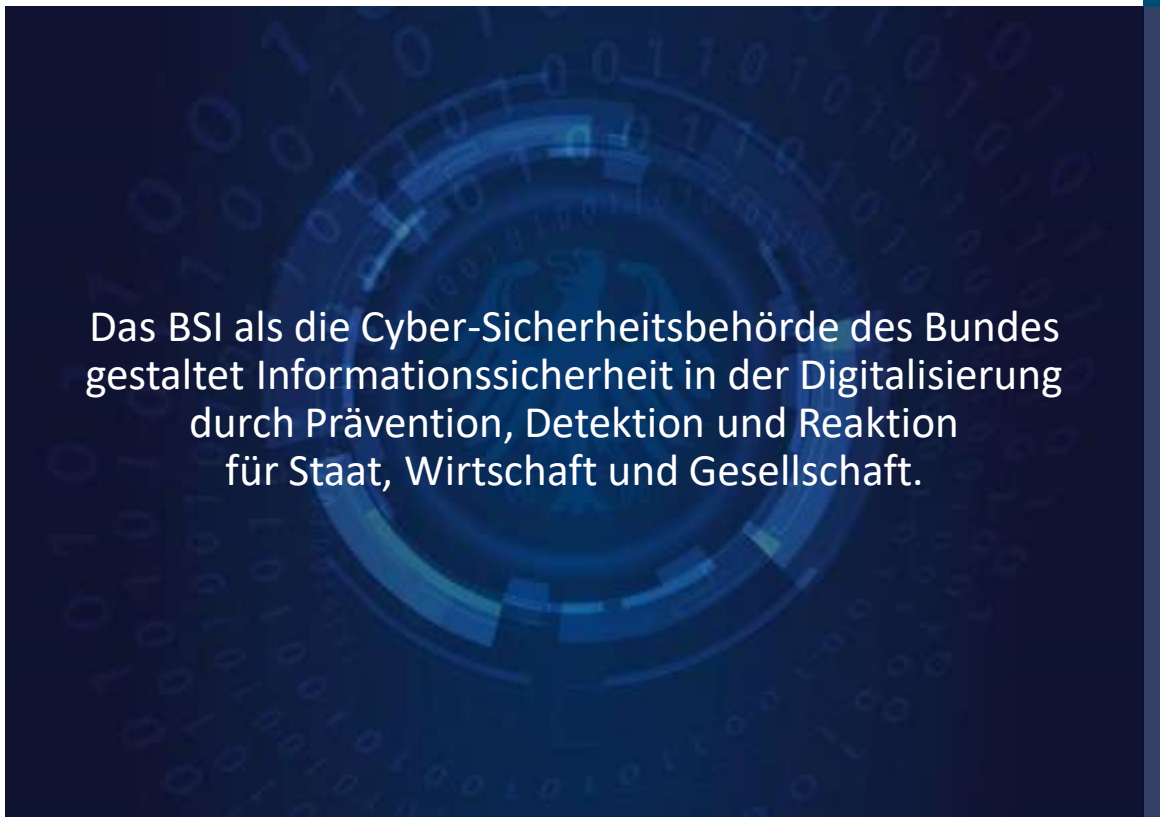
Deutschland
Digital•Sicher•BSI•

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