Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Herzlich Willkommen!

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mittelstandsforum 2020

Ausblick auf 2021 - Warum die Corona-Pandemie und der Brexit nicht die größten Gefahren für Ihr Unternehmen sind

Manuel Bach, Referatsleiter „Cyber-Sicherheit für Kleine und Mittlere Unternehmen (KMU)“

Wie bedroht ist Deutschlands Cyber-Raum?

- Angreifer nutzen **Schadprogramme für cyber-kriminelle Massenangriffe** aber auch für **gezielte Angriffe** auf ausgewählte Opfer.
- In einer neuen Schadprogramm-Welle im **dominiert Emotet die Lage**.
- Rund **117,4 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet. Das sind durchschnittlich **322.000 pro Tag, in Spitzenwerten 470.000**.
- Knapp **7 Millionen Meldungen zu Schadprogramm-Infektionen** hat das BSI an deutsche Netzbetreiber übermittelt.
- Bei Angriffen auf die Bundesverwaltung wurden rund **35.000 E-Mails mit Schadsoftware pro Monat** abgefangen.
- **24,3 Millionen Patientendatensätze** waren Schätzungen zufolge international frei im Internet zugänglich.
- Cyber-Kriminelle nutzen **COVID-19-Pandemie** für Social-Engineering-Angriffe aus.

Quelle: BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Artikel 3:

„Et hätt noch emmer joot jejange.“*

Bundesamt
für Sicherheit in der
Informationstechnik

Artikel 3:

„Et hätt noch emmer joot jejange.“*

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

Cyber-Sicherheit in der Digitalisierung

Vernetzung

Komplexität

Allgegen-
wärtigkeit

Digitalisierung bedeutet…

…mehr Möglichkeiten,

auf die Deutschland nicht verzichten kann und soll

…mehr Gefahren,

auf die Deutschland vorbereitet sein muss

Cyber-Sicherheit **…unverzichtbare Voraussetzung für das Gelingen der Digitalisierung**

Entwicklung der Digitalisierung

…mehr Datenübertragung

2016	2021
108.000 TB pro Std[1]	*400.000 TB 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 Geräte p.K. in D[1]	*neun webfähige Geräte p.K. in D*[1]

…mehr Vernetzung

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

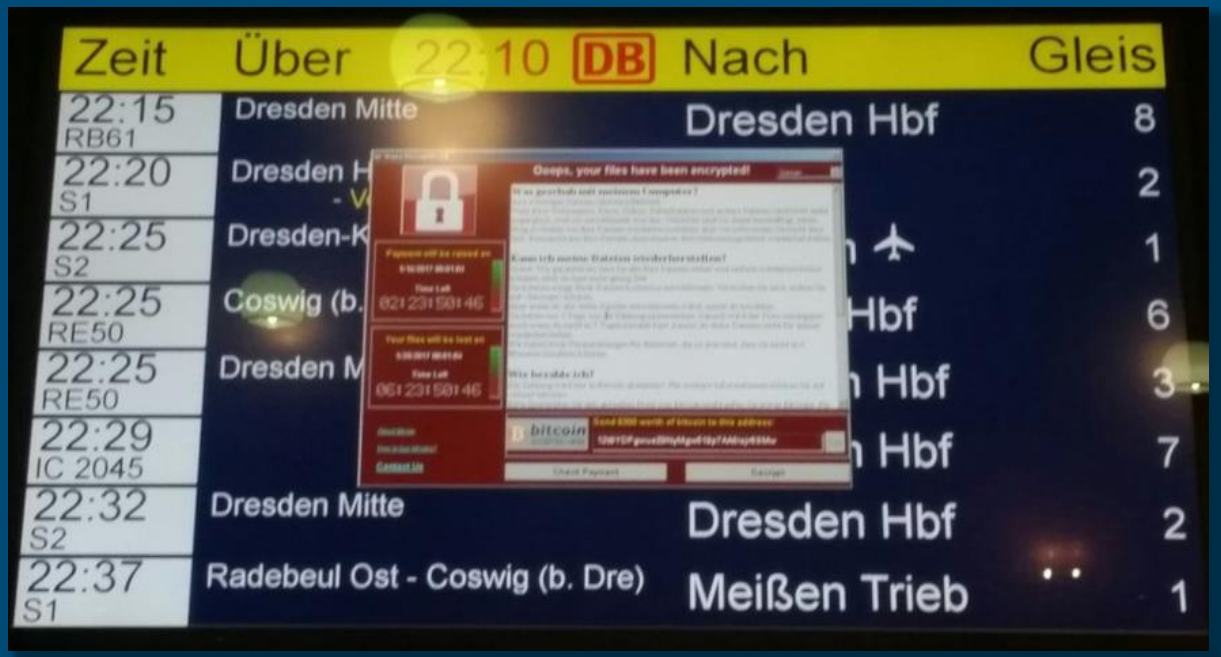
…mehr Angriffe

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

1 Quelle: CISCO VNI, 2017

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik



Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik

„Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite“

Bundesamt
für Sicherheit in der
Informationstechnik

„Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite“

„Angreifer legten Alu-Konzern mit Erpressersoftware lahm“

Bundesamt
für Sicherheit in der
Informationstechnik

„Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite“

„Garmin mit Komplettausfall“

„Angreifer legten Alu-Konzern mit Erpressersoftware lahm“

Bundesamt
für Sicherheit in der
Informationstechnik

„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“

Bundesamt
für Sicherheit in der
Informationstechnik

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

Bundesamt
für Sicherheit in der
Informationstechnik

Regel Nr. 1:

Jeder wird angegriffen - Es gibt keine Ausnahmen!

Bundesamt
für Sicherheit in der
Informationstechnik

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

Bundesamt
für Sicherheit in der
Informationstechnik

Regel Nr. 2:

Früher oder später werden Ihre Schutzmaßnahmen versagen!

Bundesamt
für Sicherheit in der
Informationstechnik

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

Bundesamt
für Sicherheit in der
Informationstechnik

Regel Nr. 3:

Prävention ist wesentlich preiswerter als Reaktion!

Bundesamt
für Sicherheit in der
Informationstechnik

Regel Nr. 3:

Prävention ist wesentlich preiswerter als Reaktion!

→ 15 Prozent Ihres IT-Budgets für IT-Sicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

Regel Nr. 4:

Teure Reaktion ist immer noch preiswerter als Kapitulation!

Bundesamt
für Sicherheit in der
Informationstechnik

Regel Nr. 4:

Teure Reaktion ist immer noch preiswerter als Kapitulation!

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

Grundsätzliches

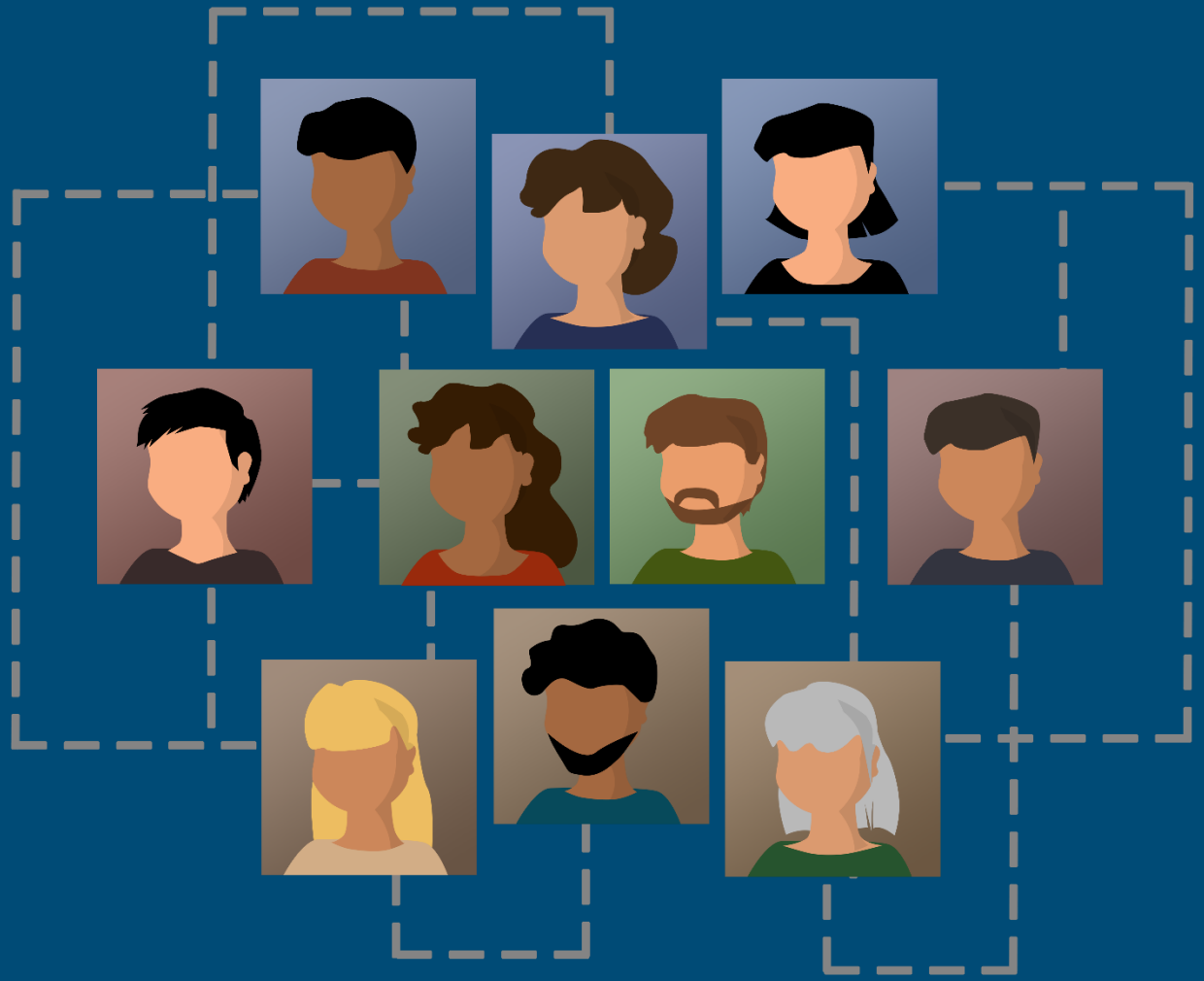
Bundesamt
für Sicherheit in der
Informationstechnik

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

Bundesamt
für Sicherheit in der
Informationstechnik

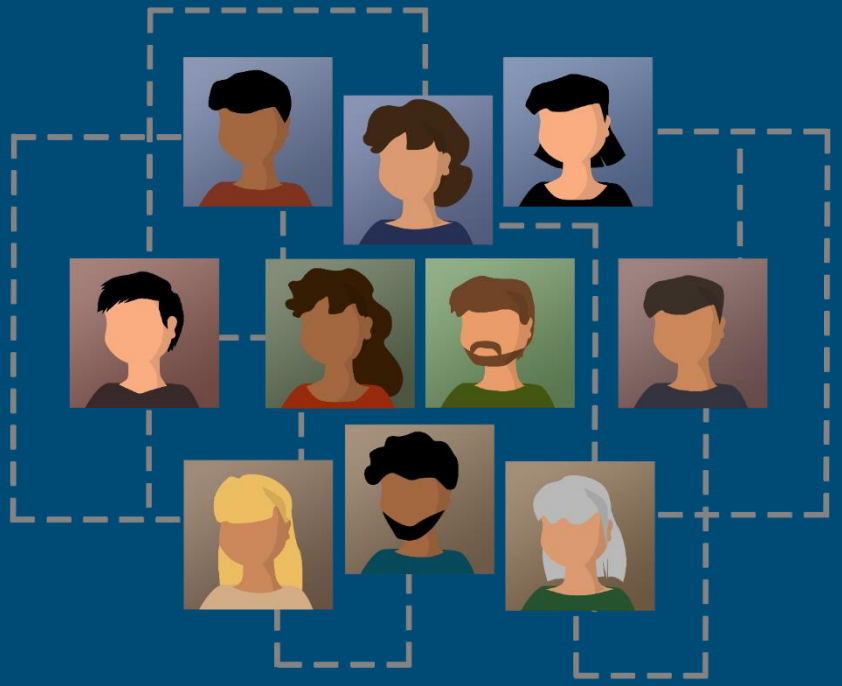
IT-Sicherheit ist Chefsache!

Bundesamt
für Sicherheit in der
Informationstechnik



Stärken Sie Ihrem IT-Sicherheits-Verantwortlichen den Rücken!

Bundesamt
für Sicherheit in der
Informationstechnik



“S.F. official locked out of computer network
Engineer jailed after allegedly refusing to hand over password”

Bundesamt
für Sicherheit in der
Informationstechnik

Sorgen Sie für klare Zuständigkeiten!

Bundesamt
für Sicherheit in der
Informationstechnik

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

Bundesamt
für Sicherheit in der
Informationstechnik

Reagieren Sie schnell auf Warnungen!

Bundesamt
für Sicherheit in der
Informationstechnik

- 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

LEICHTE SPRACHE GEBÄRDENSPRACHE ENGLISH KONTAKT LOGIN Suchbegriff

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 werden. 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 Versionszweig der betroffenen Produkte erst Ende Januar 2020 verfügbar sein. Diese sollten dann schnellstmöglich eingespielt werden.

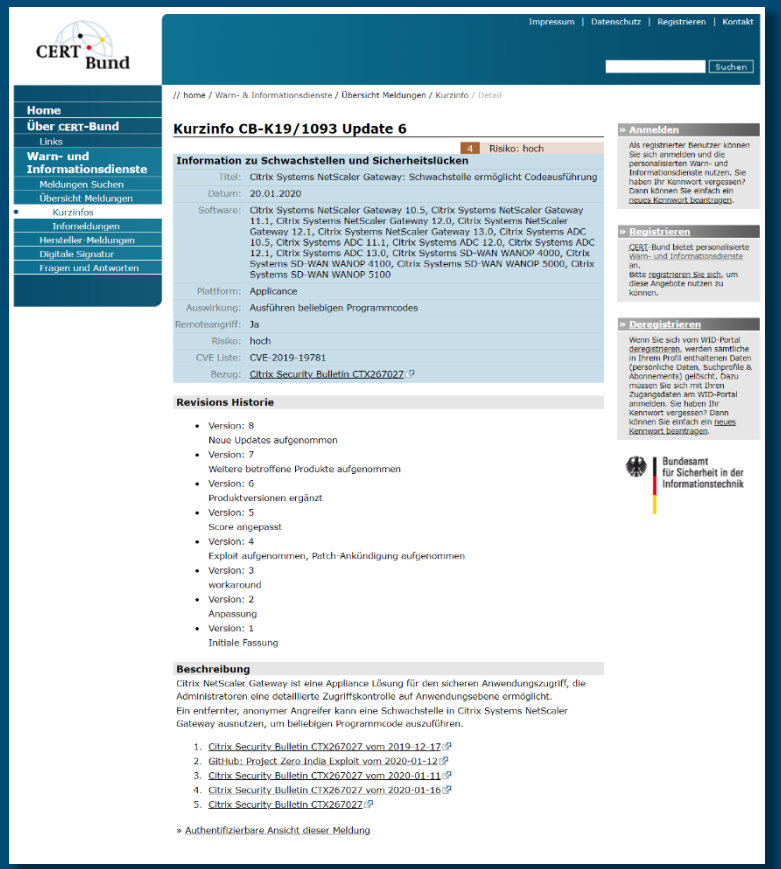
Der US-Software-Hersteller Citrix hat am 17. Dezember 2019 über eine Schwachstelle (CVE-2019-19781) in den Produkten Citrix Gateway und Citrix Application Delivery Controller (ADC), am 16. Januar 2020 auch in der Citrix SD-WAN WANOP Appliance informiert. Die Produkte kommen für den Fernzugriff auf organisationsinterne Anwendungen mit einem Web-Frontend bzw. zur Standortkopplung zum Einsatz. Die Schwachstelle ermöglicht es einem Angreifer, mithilfe von präparierten HTTP-/HTTPS-Anfragen aus den 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 5.000 aus dem Internet erreichbare, verwundbare Citrix-Systeme an deutsche Netzbetreiber gemeldet. Derzeit sind davon immer noch rund 1.500 für Angreifer verwundbar. Leider reagieren die betroffenen Unternehmen oft nur langsam, Workarounds und Patches werden häufig nicht schnell genug umgesetzt. Wenn wir allein an 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 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 verstärkt Exploit-Code zur Ausnutzung der Schwachstelle veröffentlicht wurde.

Inhaltsverzeichnis

- *Pressemitteilungen*
- Pressearchiv
- Kurzmeldungen
- Pressestelle
- Presseverteiler
- Mediathek
- Bildmaterial
- Kurzprofil des BSI



CERT Bund

Impressum | Datenschutz | Registrieren | Kontakt

Suchen

// home / Warn- & Informationsdienste / Übersicht Meldungen / Kurzinfo / Detail

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

Kurzinfo CB-K19/1093 Update 6

4 Risiko: hoch

Information zu Schwachstellen und Sicherheitslücken

Titel:	Citrix Systems NetScaler Gateway: Schwachstelle ermöglicht Codeausführung
Datum:	20.01.2020
Software:	Citrix Systems NetScaler Gateway 10.5, Citrix Systems NetScaler Gateway 11.1, Citrix Systems NetScaler Gateway 12.0, Citrix Systems NetScaler Gateway 12.1, Citrix Systems NetScaler Gateway 13.0, Citrix Systems ADC 10.5, Citrix Systems ADC 11.1, Citrix Systems ADC 12.0, Citrix Systems ADC 12.1, Citrix Systems ADC 13.0, Citrix Systems SD-WAN WANOP 4000, Citrix Systems SD-WAN WANOP 4100, Citrix Systems SD-WAN WANOP 5000, Citrix Systems SD-WAN WANOP 5100
Plattform:	Applicance
Auswirkung:	Ausführen beliebigen Programmcodes
Remoteangriff:	Ja
Risiko:	hoch
CVE Liste:	CVE-2019-19781
Bezug:	Citrix Security Bulletin CTX267027

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

Citrix NetScaler Gateway ist eine Appliance Lösung für den sicheren Anwendungszugriff, die Administratoren eine detaillierte Zugriffskontrolle auf Anwendungsebene ermöglicht.
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Citrix Systems NetScaler Gateway ausnutzen, um beliebigen Programmcode auszuführen.

1. Citrix Security Bulletin CTX267027 vom 2019-12-17
2. GitHub: Project Zero India Exploit vom 2020-01-12
3. Citrix Security Bulletin CTX267027 vom 2020-01-11
4. Citrix Security Bulletin CTX267027 vom 2020-01-16
5. Citrix Security Bulletin CTX267027

» Authentifizierbare Ansicht dieser Meldung

» Anmelden
Als registrierter Benutzer können Sie sich anmelden und die personalisierten Warn- und Informationsdienste nutzen. Sie haben Ihr Kennwort vergessen? Dann können Sie einfach ein neues Kennwort beantragen.

» Registrieren
CERT Bund bietet personalisierte Warn- und Informationsdienste an.
Bitte registrieren Sie sich, um diese Angebote nutzen zu können.

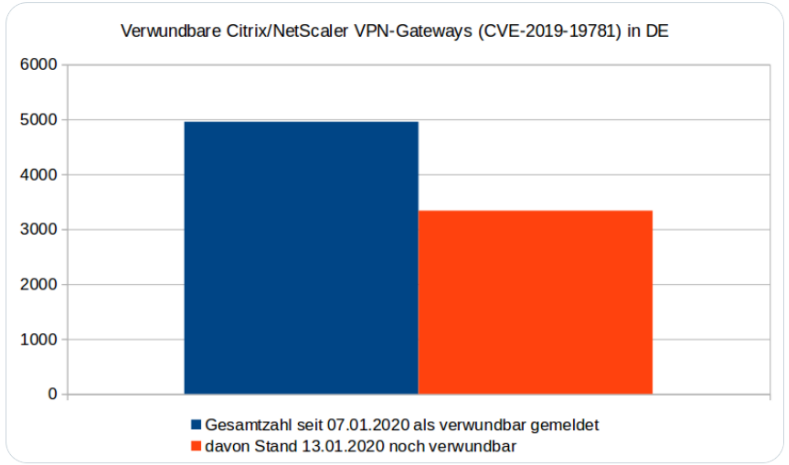
» Deregistrieren
Wenn Sie sich vom WID-Portal deregistrieren, werden samtliche in Ihrem Profil enthaltenen Daten (persönliche Daten, Suchprofile & Abonnements) gelöscht. Dazu müssen Sie sich mit Ihren Zugangsdaten am WID-Portal anmelden. Sie haben Ihr Kennwort vergessen? Dann können Sie einfach ein neues Kennwort beantragen.

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik

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.

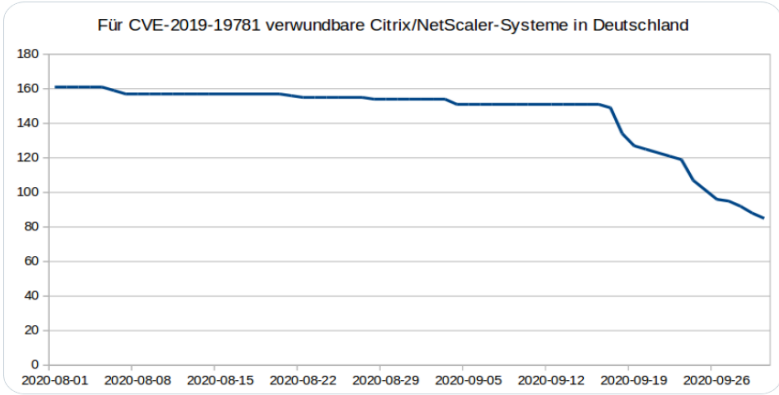


7:56 nachm. · 13. Jan. 2020 · Twitter Web App

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

CERT-Bund
@certbund

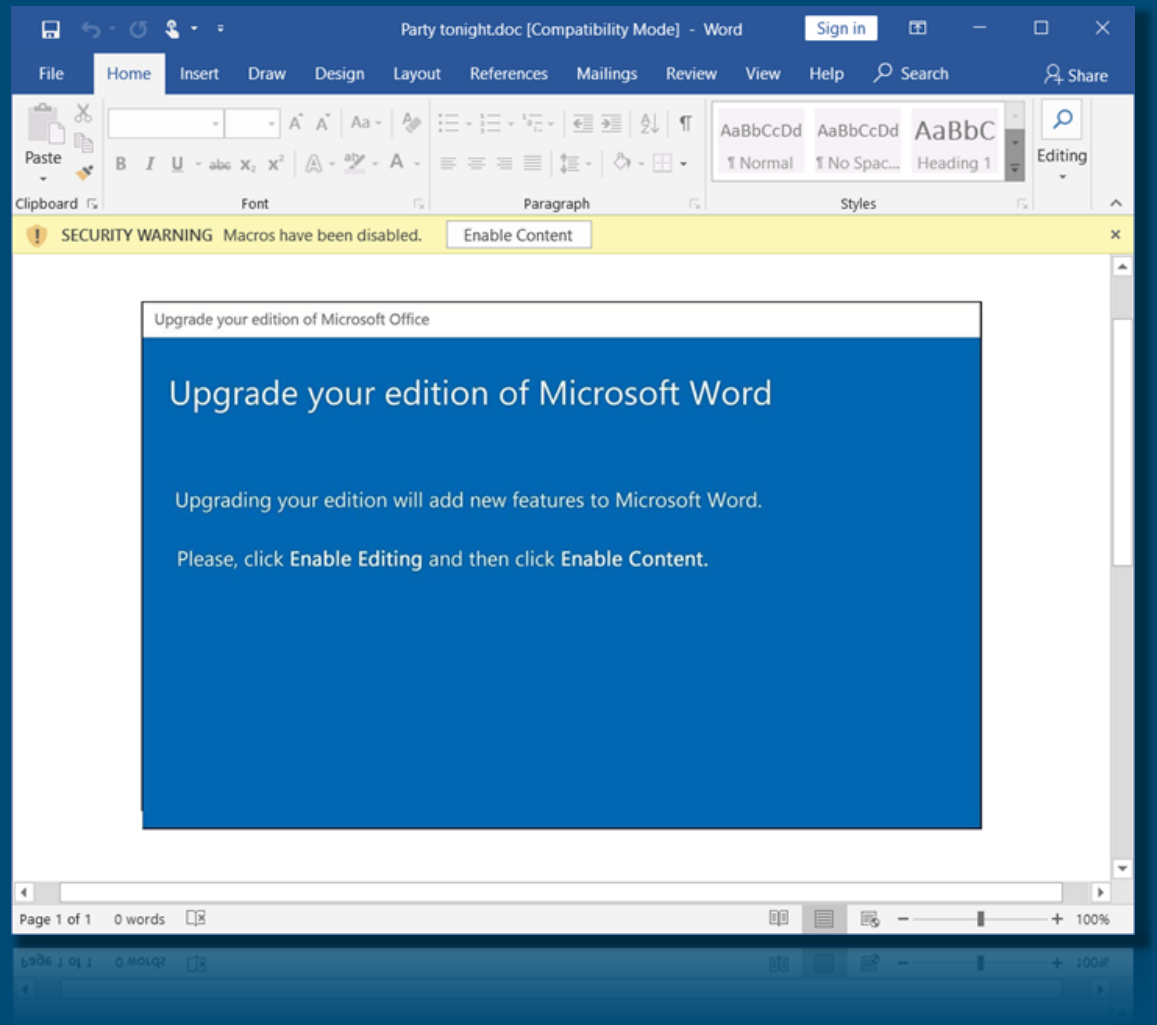
Parallel zur #Pressemitteilung vom 17.09.
bsi.bund.de/DE/Presse/Pres...
hat das @BSI_Bund die Geschäftsführungen aller deutschen #Unternehmen, die noch immer für #CVE-2019-19781 verwundbare #Citrix/#NetScaler #VPN-Gateways betrieben haben, per Briefpost angeschrieben.



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

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

Bundesamt
für Sicherheit in der
Informationstechnik



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.

Bundesamt
für Sicherheit in der
Informationstechnik

Typischer Phishing-Angriff

Gegenmaßnahmen

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

1. 123456
2. 123456789
3. 12345678
4. 1234567
5. Password
6. 111111
7. 1234567890
8. 123123
9. 000000
10. abc123

Bundesamt
für Sicherheit in der
Informationstechnik

Üben Sie den Ernstfall!

Bundesamt
für Sicherheit in der
Informationstechnik

Nutzen Sie das BSI!

Bundesamt
für Sicherheit in der
Informationstechnik

Gut vernetzt - Allianz für Cyber-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

Angebote für Unternehmen und Institutionen

NETZWERKE SCHÜTZEN NETZWERKE

www.allianz-fuer-cybersicherheit.de

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	

Bundesamt für Sicherheit in der Informationstechnik

Vielen Dank
für Ihre Aufmerksamkeit!

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
www.bsi-fuer-buerger.de