Aktuelles zur IT-Sicherheitslage

Isabel Münch, Fachbereichsleiterin IT-Sicherheitslage

it-sa, 27. Oktober 2022, Messe Nürnberg

Lage der IT-Sicherheit

Besondere Ereignisse

Aktuelle Teillagen

- Malware
- DDoS
- Botnetze
- Supply Chain Angriffe

Leitsatz

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

Hintergründe zur Digitalisierung

Die Lage der IT-Sicherheit in Deutschland 2022
im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen, offene oder falsch konfigurierte Online-Server IT-Supply-Chain: Abhängigkeiten und Sicherheit	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

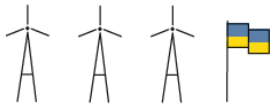
Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:
Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden
nach Angriff auf Satellitenkommunikation



20.174

Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

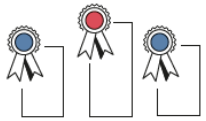
34.000
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%
aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.

90%
des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikate.



5.100 2021
4.400 2020

Zehn Jahre Allianz für Cyber-Sicherheit: 2022 sind wir bereits

6.220 Teilnehmer.

Deutschland
Digital•Sicher•BSI•

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 auf die Ukraine**: Ansammlung kleinerer Vorfälle und Hacktivismus-Kampagnen, u. a. Kollateralschäden nach Angriff auf Satellitenkommunikation

Ransomware

- **Größte operative Bedrohung**
- Qualität steigt stetig
- Ransomware als Dienstleistung (RaaS)
- **Gezielte Kampagnen** mit Double Extortion
- Neu: Copy&Wipe
- Angriffe mit hoher Agilität
- **BSI rät von Zahlungen ab!**

Cyber-Sicherheitslage im Kontext Ukraine-Krieg

- Seit Beginn des Krieges sind eine **Reihe von Aktivitäten** im Cyber-Raum zu beobachten.
- Bisher vor allem **unzusammenhängende Einzelereignisse**
  Keine zentral gesteuerte Kampagne wie in einem Hybriden Krieg erwartet erkennbar
- Das vermutete **Potenzial von Cyber-Kampagnen** wird nach derzeitigem Kenntnisstand von keiner Seite **ausgeschöpft**
- **Hacktivismus** von diversen Seiten in verschiedenen Ausprägungen
- Für Deutschland und Europa besteht eine **erhöhte Gefährdungslage**
- Erstmals **Cyber-Kollateralschäden** beobachtet

Cyber-Angriff auf deutschen Automobilzulieferer 08/2022

- **BSI und andere Behörden unterstützen** gemeinsam mit Dienstleister
- Das BSI geht derzeit von Cyber-Crime mittels **Ransomware** aus
- **Bereinigung** inzwischen **abgeschlossen**
- **BSI verteilt IoCs** in der Automobilbranche

Cyber-Angriff auf IHK 08/2022

- **Webseiten und E-Maildienste nicht verfügbar**
- Kompromittierung wahrscheinlich vor über einem Monat
- **Frühzeitig entdeckt**: Keine Verschlüsselung erfolgt, kein Datenabfluss festgestellt
- **Unterstützung durch BSI** qualifizierten APT-Dienstleister
- IT-Systeme vorsorglich heruntergefahren
- Aktuell gibt es **keine Hinweise auf einen Zusammenhang zum Krieg in der UKR**

Cyber-Angriff gegen Montenegro 08/2022

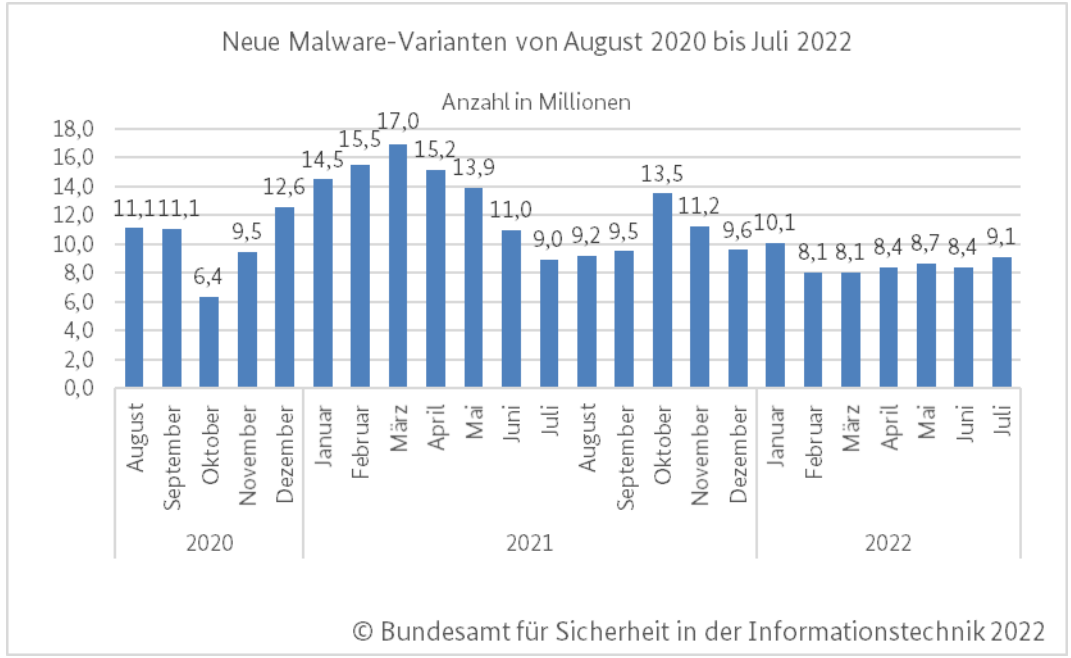
- **Montenegro** berichtet von **umfangreichen Cyber-Angriffen**
- Art der Angriffe: **Eher wahrscheinlich kriminell motiviert**
- Montenegrinischer Minister macht Ransomware-Gruppe verantwortlich
- Ausfall von **Regierungs- und Behörden-Webseiten**
- Die Agentur für nationale Sicherheit Montenegro (ANB) vermutet zunächst **RUS Akteure**
- BSI steht **im Austausch mit internationalen Partnerbehörden** die dort unterstützen.

BSI Produktwarnung Elektr. Türschloss 08/2022

- Schwachstelle im Produktset **Funk-Türschlossantrieb** HomeTec Pro CFA3000 und Wireless remote control CFF3000 (**Funkfernbedienung** für das Produkt CFA3000) des deutschen Herstellers ABUS
- **Coordinated Vulnerability Disclosure** Prozess im BSI
- **Keine Möglichkeit zum Patch** der Schwachstelle
- Laut Unternehmen: **Auslaufmodell**
- **BSI Produktwarnung** nach §7 BSIG am 10. August 2022

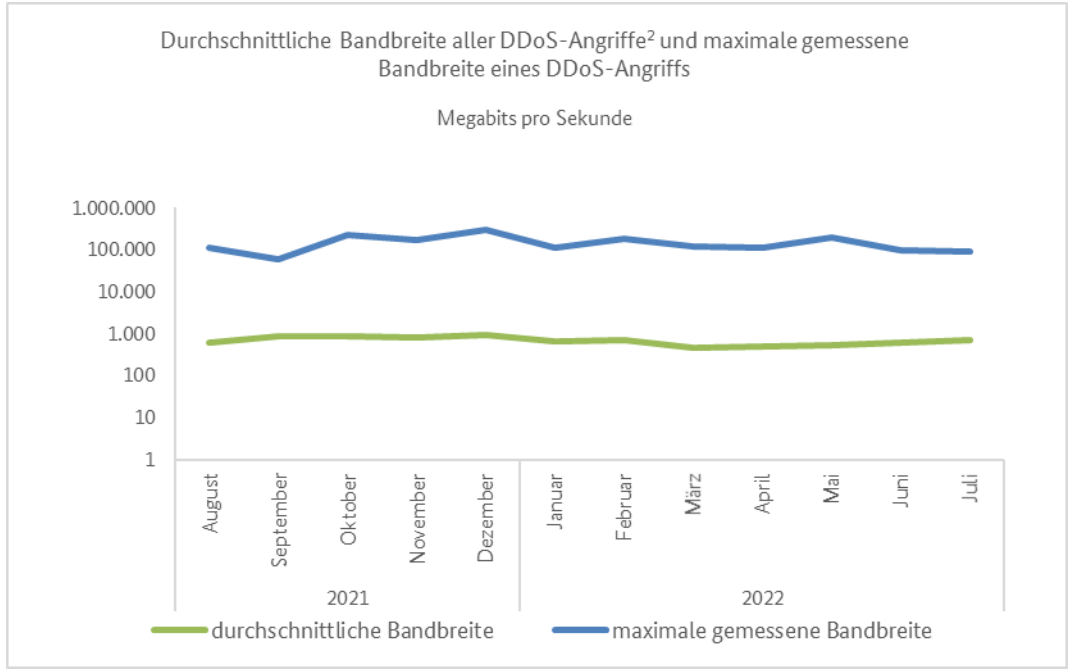
Malware

- Weiterhin **eine der größten Bedrohungen**
- Keine Erkennung mittels herkömmlicher signaturbasierter Detektion
- **Juli 2022**:
  - 9,1 Millionen neue Varianten
  - Täglich durchschnittlich 304.000
  - 0,2 Millionen neue PUA-Varianten
  - Bedrohungslage durchschnittlich bedrohlich



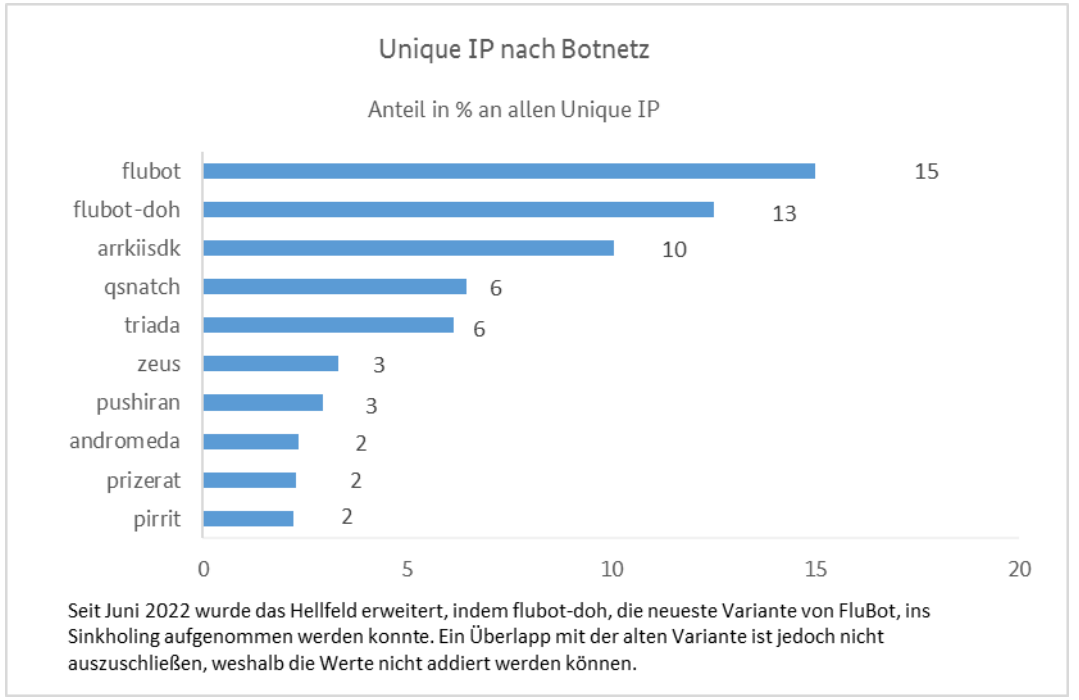
Distributed Denial of Service (DDoS)

- **Zunahme der Angriffs-Qualität**
- Immer wieder Werte von über 150 Gbit/s
- **Neue Strategien**: Carpet Bombing
- **Juli 2022**:
  - Die nationale Bedrohungslage im Bereich DDoS war durchschnittlich bedrohlich



Botnetze

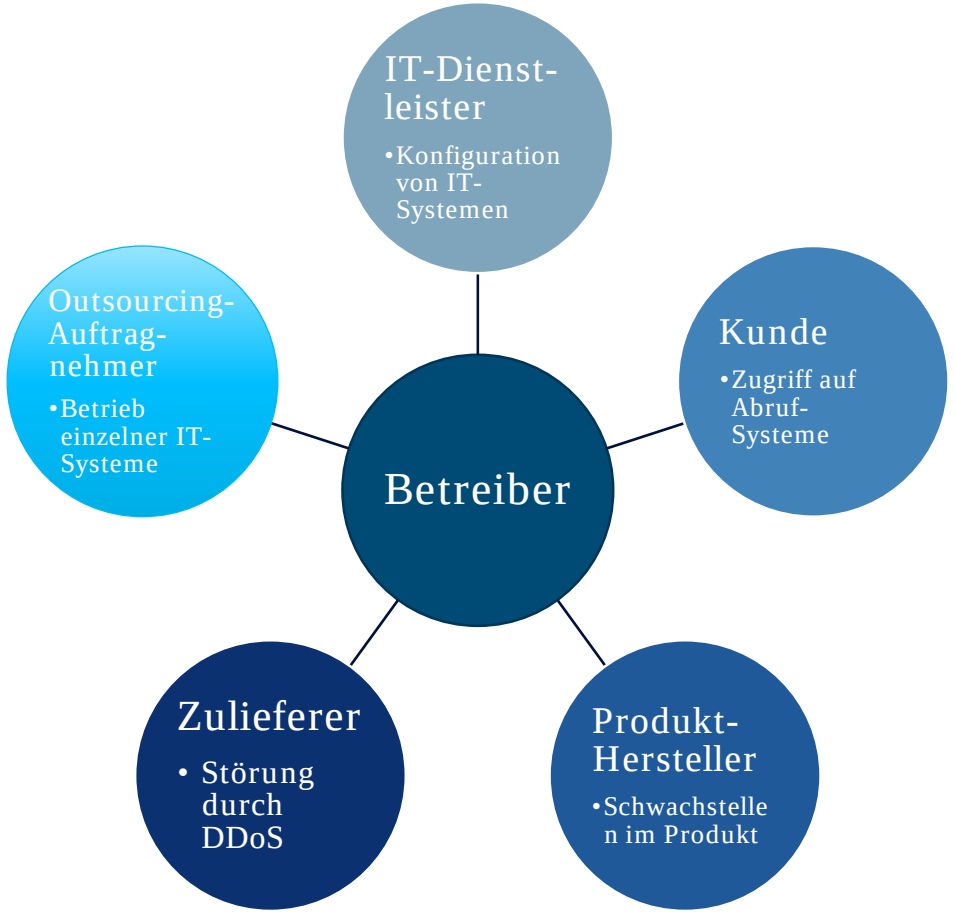
- Botnetz-Familien **besitzen mehrere Funktionalitäten** (z. B. DDoS, Ransomware)
- **Dunkelziffer hoch**
- **Juli 2022**:
  - Unique-IP-Index bei 483 Punkten
  - *Flubot* mit 15% das größte Botnetze



Seit Juni 2022 wurde das Hellfeld erweitert, indem flubot-doh, die neueste Variante von FluBot, ins Sinkholing aufgenommen werden konnte. Ein Überlapp mit der alten Variante ist jedoch nicht auszuschließen, weshalb die Werte nicht addiert werden können.

Supply Chain Angriffe

- Steigende Abhängigkeit und Vernetzung der IT-Infrastrukturen
- Ausfall oder Beeinträchtigung von IT-Netzen oder zentralen Komponenten haben schnell fatale und finanzielle Folgen
- Cyber-Angriffe qualitativ immer ausgereifter und zielgerichteter
- Office-IT-Netze und Fernzugriffe als Einfallstor (Dienstleister, Home Office)
- Auch Software-Lieferketten betroffen (vgl. Log4j, Kaseya, NotPetya)



Weiterführende Informationen des BSI

- Die Lage der IT-Sicherheit in Deutschland: https://www.bsi.bund.de/lageberichte
- Ransomware / Fortschrittliche Angriffe: https://www.bsi.bund.de/ransomware
- Allianz für Cyber-Sicherheit: https://www.allianz-fuer-cybersicherheit.de
- Kritische Infrastrukturen: https://www.bsi.bund.de/kritis
- IT-Grundschutz: https://www.bsi.bund.de/grundschutz

Lageübersicht

- Durch den russischen Angriffskrieg gegen die Ukraine hat sich die **Bedrohungslage in Deutschland insgesamt weiter erhöht**.
- Die Vorfälle im Kontext des Krieges in der UKR treffen auf **eine ohnehin angespannte Bedrohungslage** (insbesondere durch Ransomware).
- Cybercrime eine stetig zunehmende Bedrohung
- **Zunehmende Vernetzung und Abhängigkeiten** der Lieferketten erhöhen die Angriffsfläche
- **Ransomware derzeit eine der größten Bedrohungen** für die IT von Unternehmen / Organisationen
- **Big Game Hunting**: Trend zu gezielten Angriffen auf Unternehmen

Was können Sie tun?

- **Cyber-Sicherheit muss Chefinnen- und Chefsache sein!**
  - Zum Teil des Risiko-Managements machen
  - SBOM bei Zulieferern einfordern
  - Budget für IT-Sicherheit erhöhen
- **Umsetzung IT-Grundschutz**
- **IT-Sicherheitsvorfälle melden!**
- **Werden Sie Teilnehmer der Allianz für Cyber-Sicherheit!**

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/NACD/handbuch.html

Vielen Dank für Ihre Aufmerksamkeit!

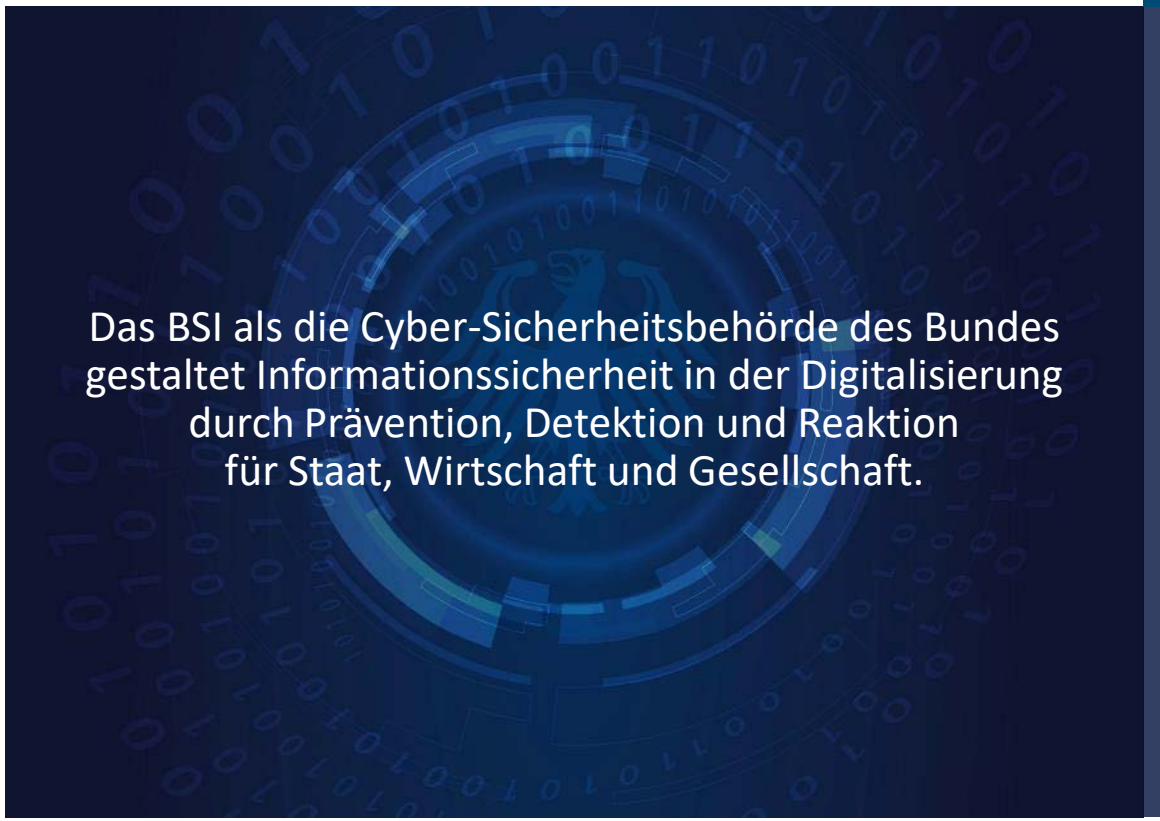
Deutschland
Digital•Sicher•BSI•

Kontakt

Isabel Münch

Fachbereichsleiterin IT-Sicherheitslage

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



Bundesamt
für Sicherheit in der
Informationstechnik