Aktuelles zur IT-Sicherheitslage

Isabel Münch, Fachbereichsleiterin IT-Sicherheitslage

verinice.XP, Göttingen, 22. Februar 2023

Lage der IT-Sicherheit

Besondere Ereignisse

Aktuelle Teillagen

- Malware
- DDoS
- Botnetze
- Supply Chain Angriffe

Wie können Sie sich schützen?

Leitsatz

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

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

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•

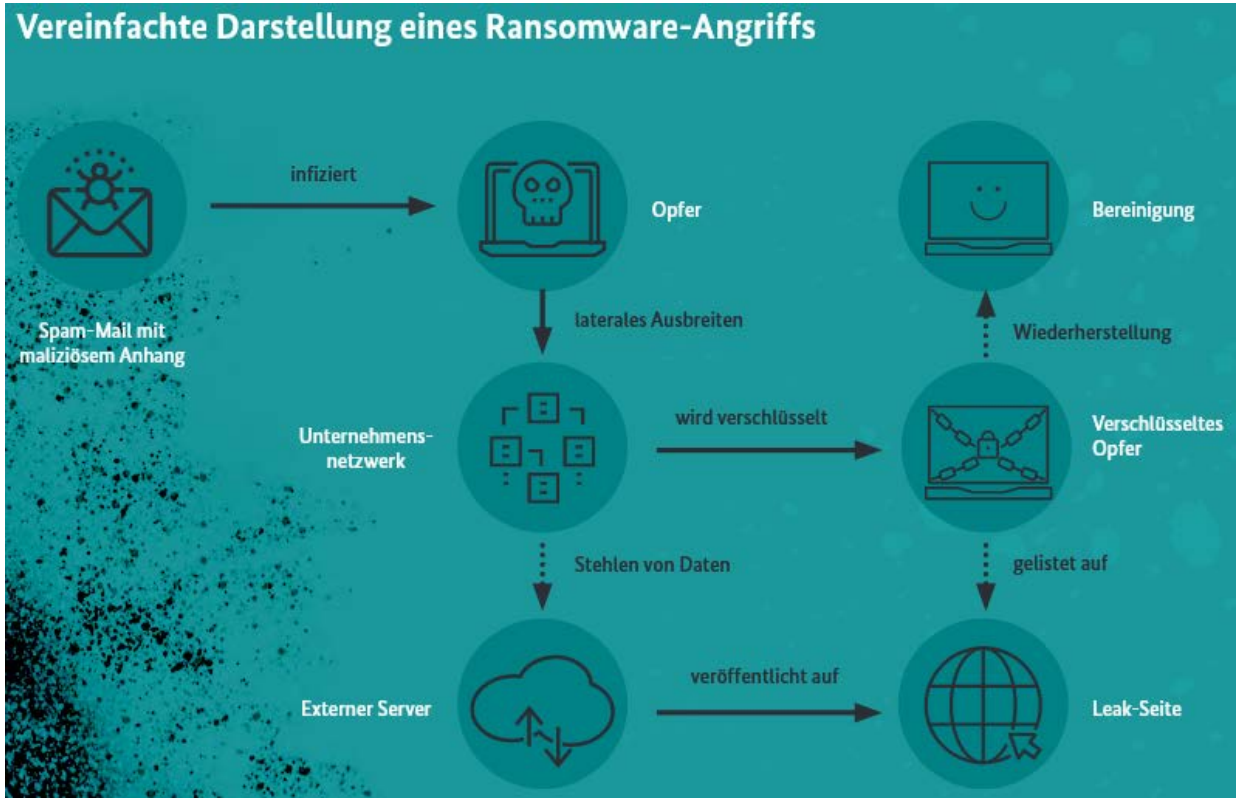
Bundesamt
für Sicherheit in der
Informationstechnik

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

Ransomware

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



BSI-Magazin 2022/02:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2022_02.html

Weltweiter Ransomware-Angriff 01/2023

- Laut Medienberichten **tausende ESXi-Server verschlüsselt**
- ESXi-Server u. a. zur Virtualisierung von IT-Fachverfahren genutzt
- **Schwerpunkt der Angriffe** lag dabei auf Frankreich, den USA, Deutschland und Kanada
- Eine **bereits im Februar 2021 gepatchte Schwachstelle** als Angriffsvektor ausgenutzt
- Das BSI hatte zu dieser Zeit vor der Ausnutzung von Schwachstellen im entsprechenden Produkt gewarnt
- Das BSI hat eine aktuelle Cyber-Sicherheitswarnung mit **Schutzmaßnahmen veröffentlicht**

DDoS-Kampagne gegen ausgewählte Ziele in DE 01/2023

- **Angriffe insbesondere auf Websites** von Flughäfen und einzelne Ziele im Finanzsektor
- Websites der angegriffenen Unternehmen **zeitweise nicht erreichbar**
- Angriffe waren von der russischen Hackergruppierung **Killnet** angekündigt worden
- **Angriffe auf Websites der Bundes- und Landesverwaltung** konnten größtenteils **abgewehrt** werden und sind **ohne gravierende Auswirkungen** geblieben
- Bei **Ergreifen üblicher DDoS-Schutzmaßnahmen** sind keine direkte Auswirkungen auf die jeweilige Dienstleistung zu erwarten

Stadt Potsdam: Hinweise auf Cyber-Angriff 12/2022

- Warnung der Sicherheitsbehörden des Landes Brandenburg vor einem unmittelbar bevorstehenden Cyber-Angriff
- IT-Systeme am 29.12.2022 präventiv vom Internet getrennt
- **Brute-Force-Angriff** auf IT-Systeme detektiert
- Fachverfahren und **Dienstleistungen für Bürger eingeschränkt**
- **Schrittweise Wiederaufnahme** des Betrieb
- Die Stadt Potsdam war bereits Anfang des Jahres 2020 Ziel eines Cyber-Angriffs

Ransomware-Angriff auf Klinikverbund Lippe 11/2022

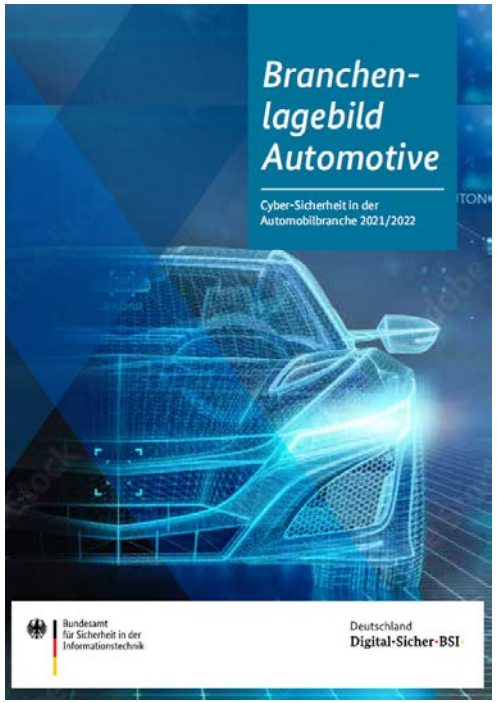
- IT-Systeme im Klinikverbund heruntergefahren
- **Mehrere Standorte betroffen**
- Deutliche **Einschränkungen im Krankenhaus-Betrieb**
- Planbare Operationen und Behandlungen zunächst ausgesetzt
- **Notfallversorgung gewährleistet**
- Unterstützung durch externen Dienstleister
- verschlüsselte **Daten aus vorhandener Datensicherung wiederhergestellt**

Ransomware-Angriff auf Babynahrungshersteller Hipp 10/2022

- **Produktionsausfälle** an den Standorten Pfaffenhofen und Herford
- Kommunikationskanäle für **Kunden betroffen**
- Hinweise auf **LockBit 3.0**
- Hipp will mit den Tätern nicht verhandeln und **kein Lösegeld** bezahlen
- Bereits 2016 Sicherheitsvorfall mit Diebstahl von Kundendaten

Cyber-Sicherheit im Bereich „Automotive“ 09/2022

- Das BSI hat am 19.09.2022 die **zweite Auflage** des Branchenlagebild Automotive vorgestellt
- **Cyber-Sicherheit ist der Schlüssel für eine funktionierende Automobilindustrie!**
- **Erneut mehrere Ransomware-Vorfälle** bei Automobilzulieferern
- Neben den bestehenden Auswirkungen der **COVID-19**-Pandemie wird die Lage maßgeblich durch den **Krieg in der Ukraine** geprägt
- **Neuregelungen** für UBI und im EU-Typgenehmigungsrecht
- **Enge Zusammenarbeit** BSI – KBA und VDA



Cyber-Angriff gegen Montenegro 08/2022

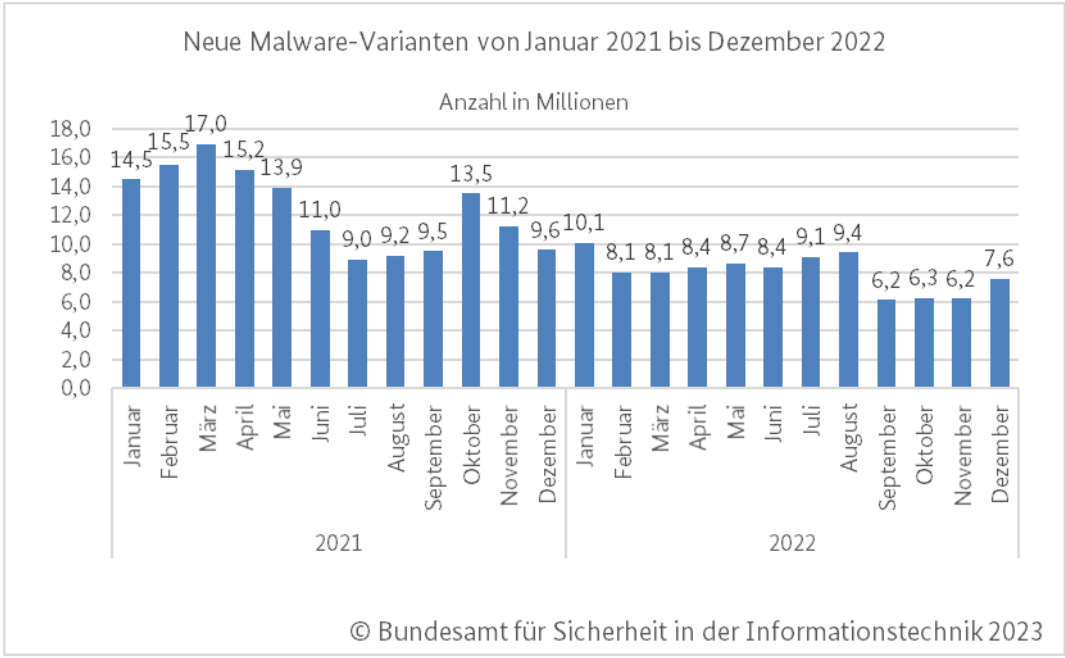
- **Montenegro** berichtet von **umfangreichen Cyber-Angriffen**
- Art der Angriffe: **Eher wahrscheinlich kriminell motiviert**
- Montenegrinischer Minister macht Ransomware-Gruppe verantwortlich
- Ausfall von **Regierungs- und Behörden-Webseiten**
- Die Agentur für nationale Sicherheit Montenegro (ANB) 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

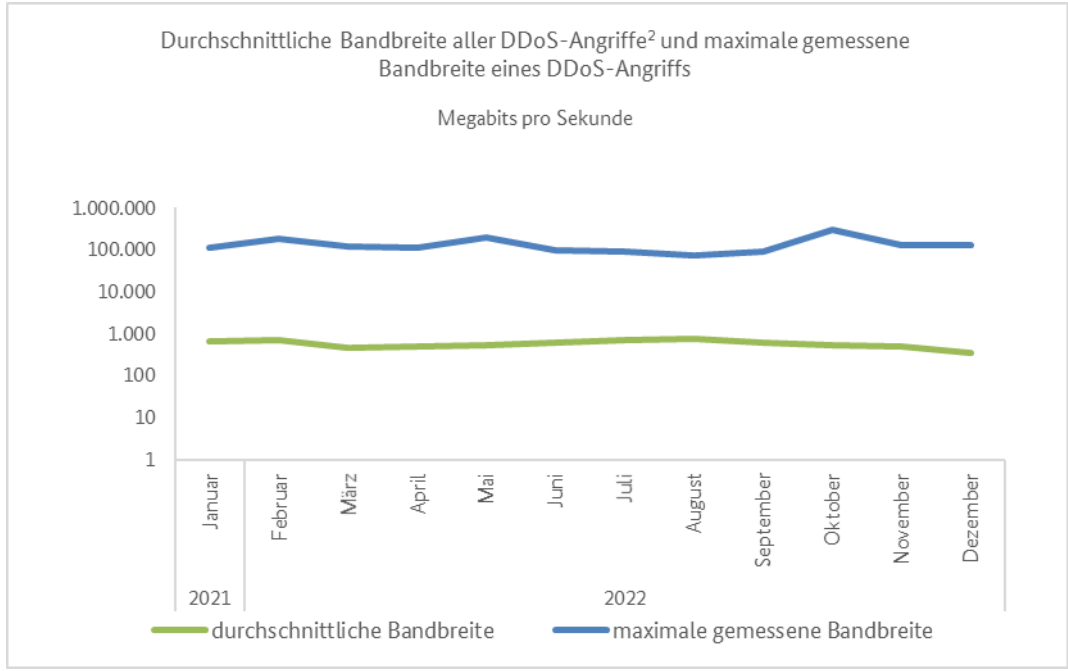
Malware

- Weiterhin **eine der größten Bedrohungen**
- Keine Erkennung mittels herkömmlicher signaturbasierter Detektion
- **Dezember 2022**:
  - 7,6 Millionen neue Varianten
  - Täglich durchschnittlich 246.000
  - 0,3 Millionen neue PUA-Varianten
  - Bedrohungslage durchschnittlich bedrohlich



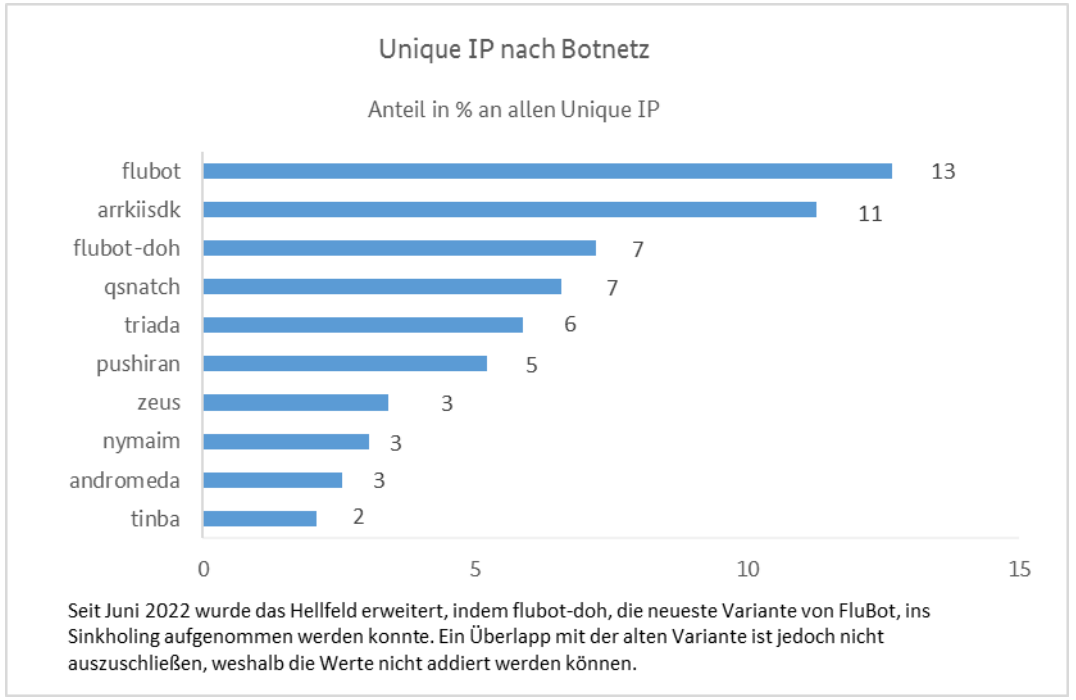
Distributed Denial of Service (DDoS)

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



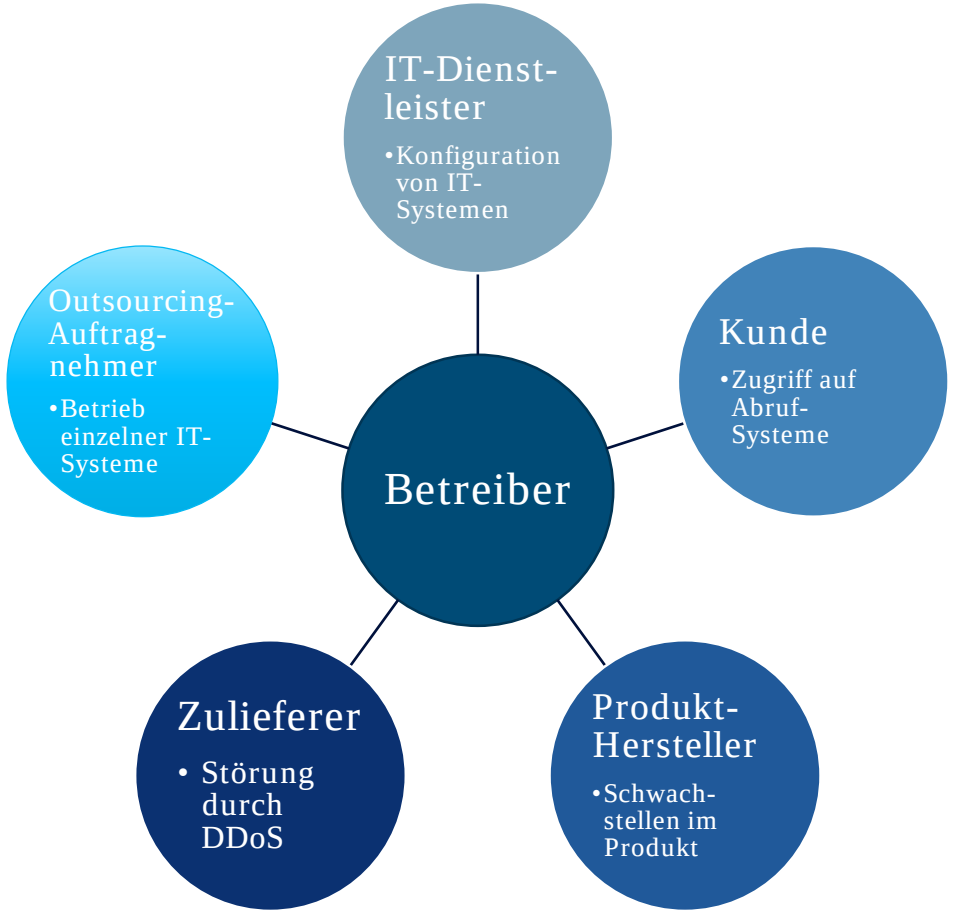
Botnetze

- Botnetz-Familien **besitzen mehrere Funktionalitäten** (z. B. DDoS, Ransomware)
- **Dunkelziffer hoch**
- **Dezember 2022**:
  - Unique-IP-Index bei 384 Punkten
  - *Flubot* mit 13% das größte Botnetz



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)



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!**

Onepager: „Management von Cyber-Risiken“

https://www.allianz-fuer-cybersicherheit.de/dok/cyberriskmanagement

IT-Grundschutz-Kompendium Edition 2023

Weiterentwicklung IT-Grundschutz-Kompendium -> Edition 2023

- Aktuell 111 IT-Grundschutz-Bausteine
- Überarbeitung Kreuzreferenztabellen zu elementaren Gefährdungen
- Anpassungen an ISO 27001:2022
- Zuordnungstabelle **ISO/IEC 27001 sowie ISO/IEC 27002 zum IT-Grundschutz** wird überarbeitet

Neue IT-Grundschutz-Bausteine

CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

OPS.1.1.1 Allgemeiner IT-Betrieb

OPS.2.3 Nutzung von Outsourcing (ersetzt OPS.2.1 Outsourcing für Kunden)

OPS.3.2 Anbieten von Outsourcing (ersetzt OPS.3.1 Outsourcing für Dienstleister)

APP.5.4 Unified Communications und Collaboration (UCC)

SYS.1.2.3 Windows Server

SYS.1.9 Terminalserver

SYS.2.5 Client-Virtualisierung und SYS.2.6 Virtual Desktop Infrastructure

NET.3.4 Network Access Control

Überarbeite IT-Grundschutz-Bausteine

ORP.1 Organisation

CON.1 Kryptokonzept

CON.2 Datenschutz

OPS.1.1.2 Ordnungsgemäße IT-Administration

OPS.1.1.3 Patch- und Änderungsmanagement

OPS.1.2.5 Fernwartung

APP.1.1 Office-Produkte

APP.1.2 Webbrowser

APP.2.1 Allgemeiner Verzeichnisdienst

APP.2.2 Active Directory (->Active Directory Domain Services)

APP.2.3 OpenLDAP

APP.5.3 Allgemeiner E-Mail-Client und –Server

SYS.1.1 Allgemeiner Server

SYS.2.2.3 Clients unter Windows 10 (->Clients unter Windows)

SYS.4.3 Eingebettete Systeme

SYS.4.4 Allgemeines IoT-Gerät

SYS.4.5 Wechseldatenträger

INF.1 Allgemeines Gebäude

INF.2 Rechenzentrum sowie Serverraum

INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum

Sonstige Änderungen

Entfallene Bausteine

- SYS.2.2.2 Clients unter Windows 8.1
- OPS.2.1 Outsourcing für Kunden und OPS.3.1 Outsourcing für Dienstleister

Geschlechtergerechtere Sprache

Umbenennung von 14 Rollen (Auswahl)

- Generell: Verwendung Plural (*beauftragte statt *beauftragter)
- Benutzer -> Benutzende
- Mitarbeiter -> Mitarbeitende
- …

IT-Grundschutz-Berater und IT-Grundschutz-Praktiker

- Aus der kontinuierlich hohen Bedrohungslage und der schnell voranschreitenden Digitalisierung erwächst mehr und mehr der Bedarf an Informationssicherheit.
- Für einen Informationssicherheitsprozess fehlt es in vielen Institutionen an der entsprechenden Expertise.
- Es besteht eine große Auswahl an Dienstleistern, doch wer hat die von mir benötigte Expertise?
- Das Schulungskonzept des BSI stellt ein einheitliches hohes Niveau an fachlicher Expertise sicher.
- Über 150 IT-Grundschutz-Berater
- ca. 40 Schulungsanbieter

- **Ausbildung von fast 3500 IT-Grundschutz-Praktikern seit 2019**

Wesentliche Neuerungen zum **zweiten CD** des **BSI-Standards 200-4**

Vereinfachung und **Öffnung** der Voranalyse für Alternativen

Struktur des Standards folgt nun **alleine** dem **BCM-Prozess**

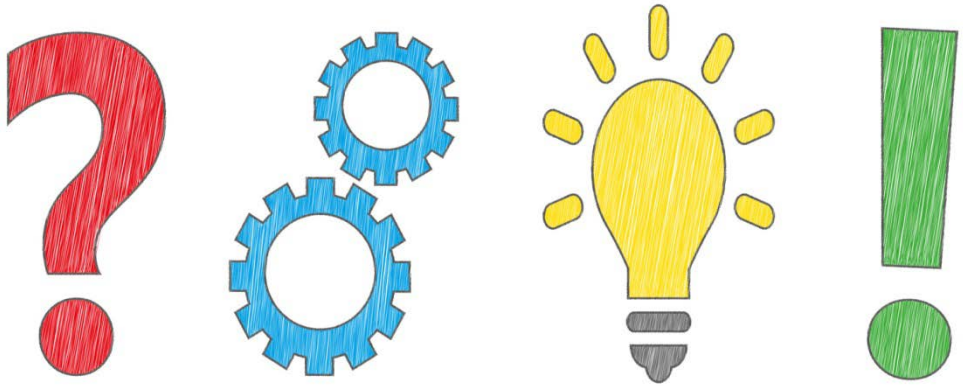
Schärfung des Wordings **(BCB etc.)**

Berücksichtigung des **Anwenderfeedbacks** – **viele** Detailverbesserungen

Annäherung der Stufen an Stellen, wo eine Differenzierung nicht zielführend ist.

Outsourcing und Lieferanten fortan als **herkömmliche** BC-Strategie Öffnung für **verschiedene** Ansätze

Gerne jetzt oder später



Geplante IT-Grundschutz-Tage 2023

- 1. IT-Grundschutz-Tag: 2. März 2023
- 2. IT-Grundschutz-Tag: 25. April 2023
- 3. IT-Grundschutz-Tag: 14. Juni 2023
- 4. IT-Grundschutz-Tag: 11. Oktober 2023

Bleiben Sie im Kontakt

- IT-Grundschutz-Hotline:
  grundschutz@bsi.bund.de
  (0)22899-9582-5369
- Twitter: @BSI_Bund, #ITGrundschutz

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

Vielen Dank für Ihre Aufmerksamkeit!

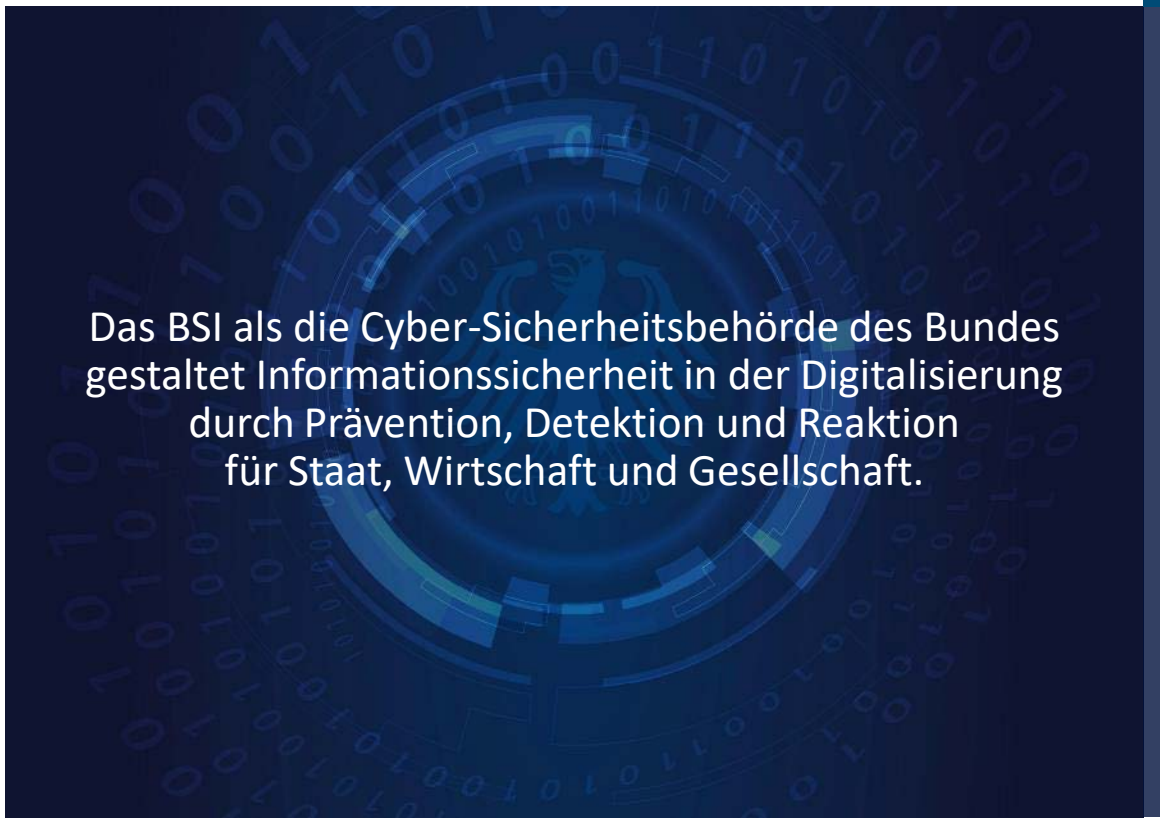
Deutschland
Digital•Sicher•BSI•

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