



Cyberangriffe und Schutzmaßnahmen

Ein Überblick aus Sicht des BSI

MesseAcademy, 08.04.2022

Warum ist Cybersicherheit relevant?



Ransomware – Schlagzeilen aus Deutschland 2021

Software AG Opfer von Clop-Ransomware Attacke

NACH CYBERANGRIFF AUF ANHALT-BITTERFELD

Spekulationen um Name der Hackergruppe - „Pay or Grief“ soll hinter Lösegeldforderung stecken

Autozulieferer aus Esslingen

Eberspächer meldet Cyberangriff

Ransomware-Attacke auf Medatixx:
Großalarm im Gesundheitswesen

Cyber attack on the KISTERS Group: Expiry of the ultimatum and publication of captured data

After ransomware attack, global logistics firm Hellmann warns of scam calls and mail

Digital healthcare: ransomware attack on Compugroup Medical

KASEYA

Was über Ransomware-Betroffene in Deutschland bekannt ist

Ein großer Ransomware-Angriff hat Hunderte Unternehmen weltweit getroffen. Auch deutsche Firmen sind darunter, manche hatten aber offenbar Glück.

Cyberangriff: Stadtverwaltung Witten online nicht erreichbar

Ransomware legt Verwaltung von Schwerin und benachbartem Landkreis lahm

Verschlüsselungstrojaner

MediaMarkt und Saturn offenbar von Ransomware betroffen

Trends der Technik und Vorgehensweise

Cybercrime-as-a-Service

- Jeder Bestandteil eines Cyber-Angriffs lässt sich als Service beziehen.
- Es wird teilweise umfassender Support geboten.

Proliferation

- Beobachtung von IT-Sicherheitsdienstleister- und Behördenberichten
- Gegenseitige Beobachtung unter Ransomware-Angreifer führt zu Ransomware Best Practices.

Living off the Land

- Missbrauch von legitimen Administrationswerkzeugen
- Ausnutzung von Penetrationstestwerkzeugen für Cyber-Angriffe

Automatisierung

- Einbetten von Datendiebstahl-Funktionen in Ransomware und Anbindung an Leak-Seite
- Möglichkeit zur Einbettung von verschiedenen Zugangsdaten in Ransomware



Rechtliche Rahmenbedingungen

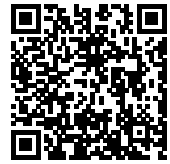
Pflichten für Kritische Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse (BSIG und IT-Sicherheitsgesetz)

Pflichten zum Arbeitsschutz

Vorgaben zum Schutz von Mitarbeitern und Umwelt (Störfall-VO -> KAS-51)

Vorsorge, aber wie?





Vorgehensweise zur Absicherung von Unternehmen
-> BSI-Standards

Umfangreiche Dokumentation von Gefährdungen und Anforderungen
-> IT-Grundschutz-Kompendium



Schulungsmaterial für den Einstieg



Allianz für Cybersicherheit

Allianz für
Cyber-Sicherheit



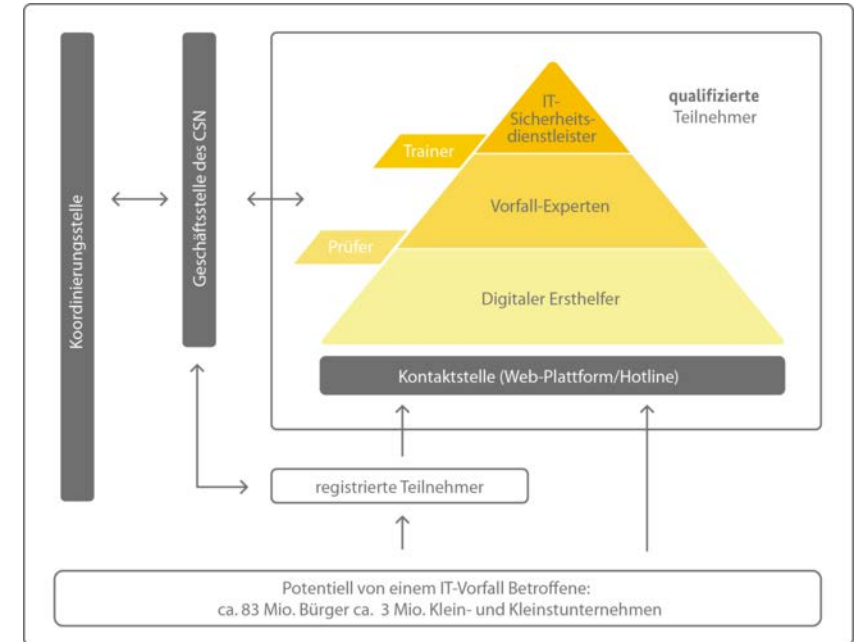
- bietet Wissens- und Erfahrungsaustausch zum Umgang mit Cyber-Risiken,
- stellt aktuelle Informationen bereit
- ermöglicht den stetige Ausbau von Sicherheitskompetenzen durch Workshops und Veranstaltungen

<https://www.allianz-fuer-cybersicherheit.de>

Cyber-Sicherheitsnetzwerk

- ein freiwilliger Zusammenschluss von qualifizierten Experten für eine Vorfallobarbeitung
- Unternehmen stellen individuelle Expertise und Knowhow zur Behebung von IT-Sicherheitsvorfällen zur Verfügung
- Ziel ist die IT-Sicherheitslage in Deutschland zu verbessern, Schadensausmaß zu begrenzen sowie weitere Schäden abzuwenden

Cyber-
Sicherheitsnetzwerk



Fazit



Zusammenfassung

- Bedrohung durch Cyberangriffe ist real und es kann jeden treffen.
- Gesetzliche Anforderungen steigen
- Schutzmaßnahmen sind umsetzbar.
- Jeder kann etwas tun.
- Austausch mit „Gleichgesinnten“ hilft.

Hausaufgabe

- Nehmen Sie sich 10 Minuten um
 - die vorhandenen Vorgaben im Unternehmen zu sichten oder
 - einen Blick in die Sicherheitskonzepte für ihren Bereich zu werfen oder
 - einmal der Böse zu sein und zu überlegen, was Sie als Krimineller im Unternehmen tun würden und was dagegen helfen würde.

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Jens Cordt

jens.cordt@bsi.bund.de

Tel. +49 (0) 228 99 9582 5936

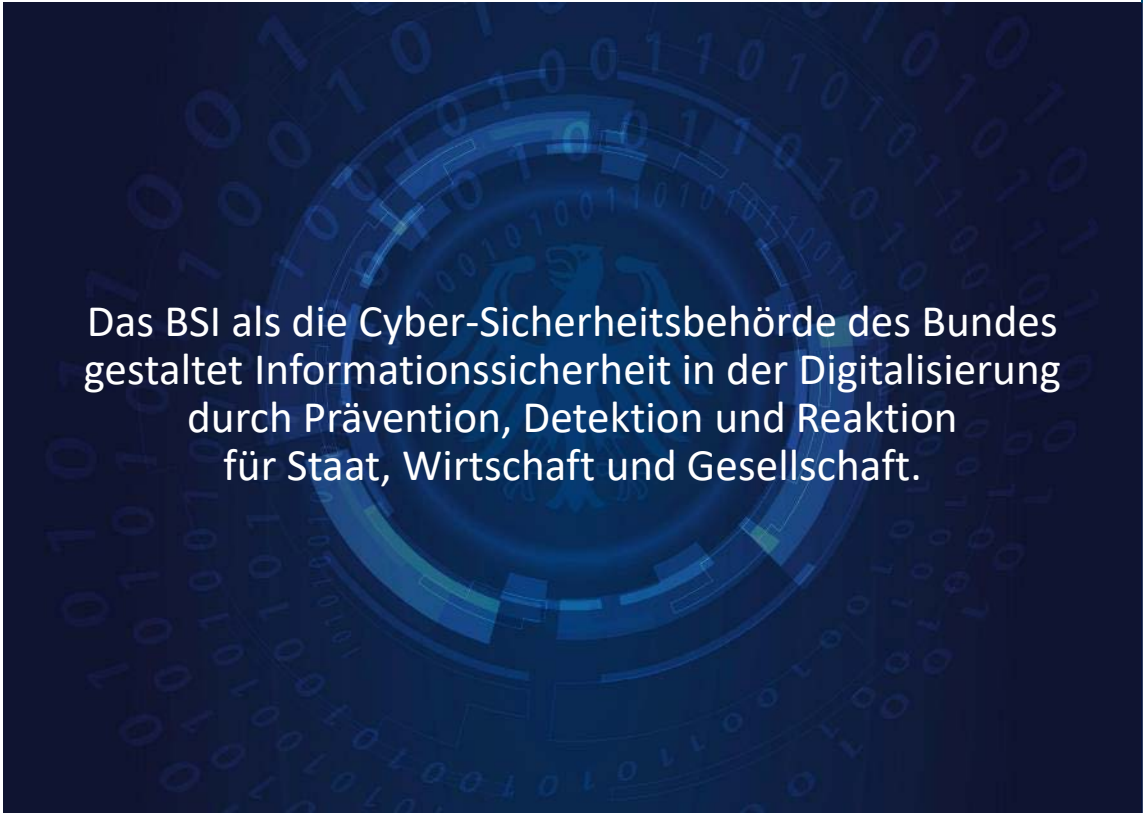
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185-189

53175 Bonn

www.bsi.bund.de

Deutschland
Digital•Sicher•BSI



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