Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

(Er)kenne Deinen Feind.

Ein Jahr Systeme zur Angriffserkennung

Christine Hofer, Cybersicherheit für Kritische Infrastrukturen

Gliederung

Aussicht: Cybernation Deutschland

Einblicke in die Bedrohungslage

Durchblick und Empfehlungen

Ausblick

Einsicht

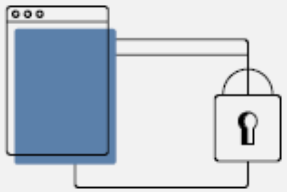
Vision

Die Lage der IT-Sicherheit in Deutschland 2023 im Überblick

Ransomware

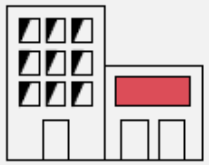
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 davon richteten sich gegen **IT-Dienstleister**.



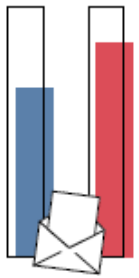
Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion

neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

66%

aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34 % Erpressungsmails,
32 % Betrugsmails



84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

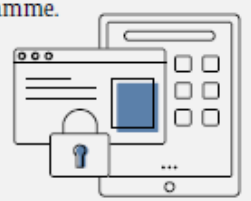
Top-3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Phishing	***Ransomware*** Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Onlineserver	***Ransomware*** APT Schwachstellen, offene oder falsch konfigurierte Onlineserver

Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.



6.220 2022
5.100 2021

7.120 Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik

Angriffserkennung

„Erkennen“

- so deutlich sehen, dass jemand weiß, wen oder was er vor sich hat
- aufgrund bestimmter Merkmale ausmachen, identifizieren

Vorgehensweisen der Gruppierung VoltTyphoon

- Living Off the Land
- Schwachstellenausnutzung
- Erbeutung legitimer Zugangsdaten
- Lateral Movement
- Reconnaissance
- Prepositioning
- Datenexfiltration

Vorgehensweisen bauen teilweise aufeinander auf oder werden in Kombination genutzt, um weitere Aktivitäten auf den Systemen des Opfers ausüben zu können.

Durchblick - Empfehlungen Detektion

- Erhebung und Auswertung von Logs
  Event Logs, System Logs, etc.
- Analyse des Netzwerkverkehrs
- Überwachung und Plausibilisierung von Logins
  Zeitpunkt, Frequenz, Dauer, Lokation, etc.
- Auswertung der Ausführungs- und Ablagepfade von Software bzw. Dateien
- Anomalieerkennung

Durchblick - Orientierungshilfe Systeme zur Angriffserkennung (OH SzA)

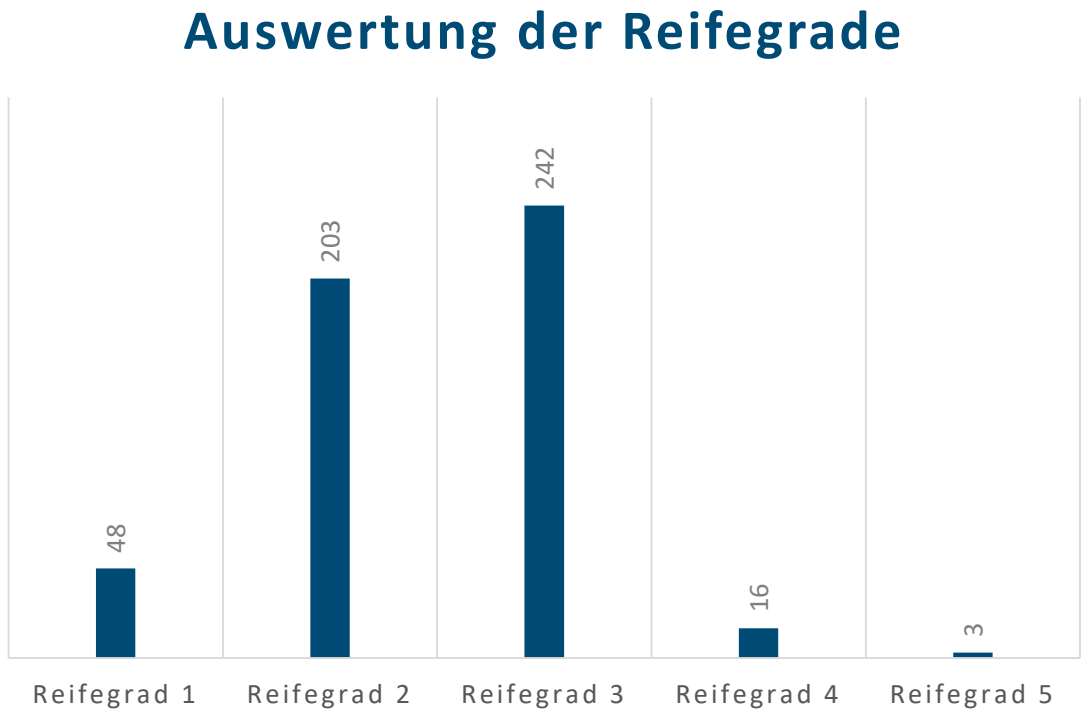
- OH gibt Betreibern und Prüfer:innen Anhaltspunkte zur Implementierung von SzA
- Beschreibt Vorstellungen des BSI welche Anforderungen ein SzA erfüllen muss
- Ist an BSI Grundschutz angelehnt
- Bereiche SzA: Protokollierung, Detektion und Reaktion
- MUSS-Anforderungen für Reifegrad 3

Hier geht's zur OH

Ausblick auf die kommenden Monate

Zum Stichtag 31.12.23 (EnWG):

- 512 vollständige Nachweise
- Insgesamt 2801 Mängel
- **BSIG SzA werden in 2024 erwartet**



Einsicht

„Systeme zur Angriffserkennung“

- sind Ihre Augen und Ohren im Netz
- sorgen für besseren Ein- und Durchblick

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Christine Hofer
Fachbereichsleitung WG1

fachbereich-wg1@bsi.bund.de

Tel. +49 (0) 228 9582 5776
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de