



IT-Sicherheitsbeauftragter

Abteilung 10.3 (Sicherheit und Datenschutz)

Sebastian Gall

10.3 IT-Sicherheitsbeauftragter

Inhalt

- Zur Person
- Notwendigkeit eines IT-Sicherheitsbeauftragten
- Gefahren im digitalen Umfeld
- Herausforderungen für die Universitäts- und Hansestadt Greifswald
- Arbeitsschwerpunkte



10.3 IT-Sicherheitsbeauftragter

Zur Person

- Name: Sebastian Gall
- Geboren: 1983, Greifswald
- 2 Kinder (17 Jahre)

Zum Ehrenamt

- Vorsitzender Schulelternrat EMA-UHGW
- 1, Stellvertreter Vors. Kreiselternrat VG
- Landeselternrat
 - Vorstandsmitglied
 - Vors. Ausschuss Berufliche Schulen
 - Stellv. Vors. AG Digitalisierung
 - BOB

Zur Laufbahn

- Softwareentwicklung
- Marketing
- Infrastruktur
- Freier Dozent
- Ausbilder
- Selbstständig
- Standortleitung
- Abteilungsleitung

Notwendigkeit

eines IT-Sicherheitsbeauftragten

- IT-SiBe wurde seit 2018 durch eGo-MV bereitgestellt
- gestiegene Anforderungen bei (Online-) Fachverfahren/ OZG
- vertragliche Leistungen mit eGo-MV haben nicht mehr ausgereicht
- Stellenausschreibung eines eigenen IT-Sicherheitsbeauftragten
- seit 01/2024 besetzt



Notwendigkeit

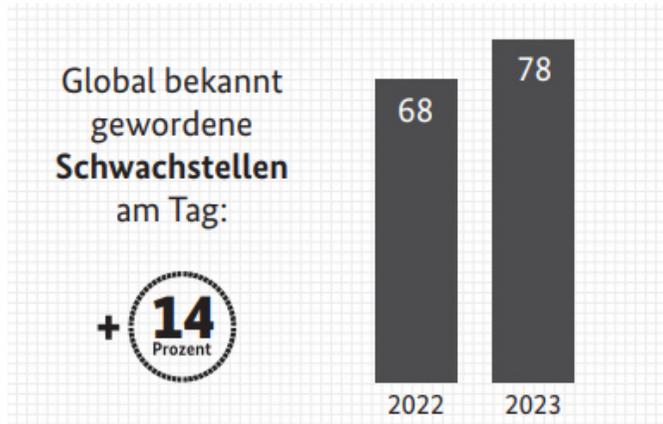
eines IT-Sicherheitsbeauftragten

- stetige Auditierung durch Verfahrensanbieter und Regierung
- steigende Anzahl von Online-Diensten
- Komplexität der IT-Landschaft wächst
- ständige Zunahme von Cyber-Angriffen durch ausländische Aggressoren



Welche

Gefahren existieren

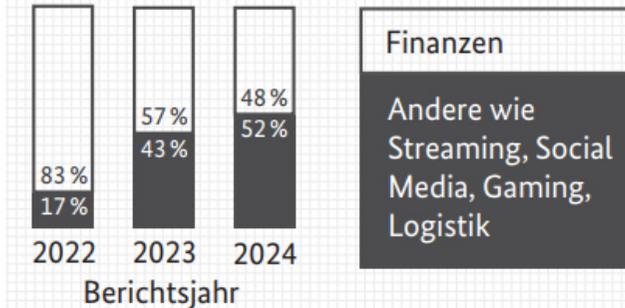


Global bekannt gewordene Schwachstellen 2023 nach möglicher Angriffsart (Mehrfachnennungen möglich)

Ausführen von Schadcode	45 %
Umgehung von Schutzmechanismen	44 %
Auslesen von Anwendungsdaten	44 %
Abschalten von Diensten	29 %
Manipulation von Anwendungsdaten	21 %

Phishing durchwächst alle Marktsegmente

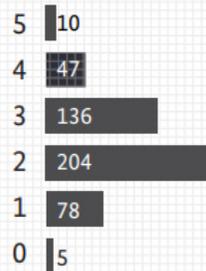
Von Verbraucherinnen und Verbrauchern gemeldete Phishing-Mails nach Art der ausgenutzten Marktsegmente (Anteilswerte in %)



Welche

Gefahren existieren

Fokus KRITIS: Reifegrade Systeme zur Angriffserkennung Ersterfassung 2023



Umsetzungsgrad: Maßnahmen

- 5 – MUSS, SOLLTE, KANN erfüllt
- 4 – MUSS und SOLLTE erfüllt
- 3 – MUSS erfüllt
- 2 – Umsetzung begonnen
- 1 – in Planung
- 0 – nicht vorhanden

Welche

Gefahren existieren

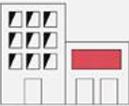
Ransomware

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 Software-Produkten (15 % davon kritisch) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein Zuwachs von 24 %.

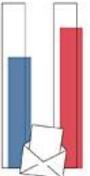


Eine Viertelmillion neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



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.

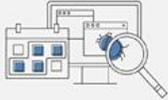


Top 3-Bedrohungen je Zielgruppe:

Zielgruppe	Bedrohung
Gesellschaft	Identitätsdiebstahl, Sextortion, Phishing
Wirtschaft	Ransomware, Abhängigkeit innerhalb der IT-Supply-Chain, Schwachstellen, offene oder falsch konfigurierte Online-Server
Staat und Verwaltung	Ransomware, APT, Schwachstellen, offene oder falsch konfigurierte Online-Server



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

7.120 Teilnehmer hatte die Allianz für Cybersicherheit im Jahr 2023.

5.100 2021



Deutschland Digital • Sicher • BSI

Gefahren

Im digitalen Umfeld

- 95 % der Vorfälle basieren auf **menschliches Versagen** (Quelle: IBM)
- KI-gestützte Angriffe
- deutlich gestiegene Angriffe seit Ukraine-Krieg



Herausforderungen

für die Universitäts- und Hansestadt Greifswald

Intern

- Resilienz der Stadtverwaltung schaffen
- Vereinfachung der Einführung neuer Systeme/ Fachverfahren
- Privacy/ Security by Design
- Vertrauen der Mitarbeiter in die Digitalisierung schaffen
- bestehende Prozesse neu denken
- Um- und Ausbau der bestehenden IT-Landschaft
- Informationssicherheitsgesetz MV (ISichG MV) ab 01.01.2026

Extern

- Vertrauen der Bevölkerung in die Digitalisierung schaffen
- digitale Kompetenzen entwickeln
- Politischer und wirtschaftlicher Wandel

Arbeitsschwerpunkte

aktuell und zukünftig

- Etablierung des BSI-Grundschatz-Kompandiums (10 Bausteine, 111 Maßnahmen)
- Prüfen, Erweitern und Aktualisieren der bestehenden Dokumentation
- Erstellen von Konzepten/ Verfahren für die Sicherheit und Daten und Informationen
- Sensibilisieren der Mitarbeiter
- Umsetzung BSI-Grundschatz bzw. ISO/IEC 27001

**Vielen Dank für Ihre
Aufmerksamkeit !**

