10 Jahre Allianz für Cyber-Sicherheit
Unternehmen sicher digitalisieren

Stefan Becker
Bundesamt für Sicherheit in der Informationstechnik
25.10.2022

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft

Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft

Ransomware
Schwachstellen, offene oder falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten und Sicherheit

Staat und Verwaltung

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.

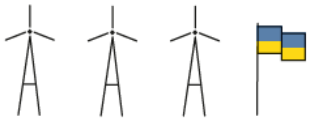
Die Anzahl der Schadprogramme steigt stetig.
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

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.

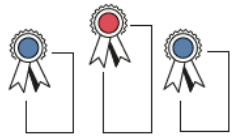
34.000
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

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 beträgerisch 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

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) festgestelt, 10 % mehr als im Jahr davor.
- **Russischer Angriffskrieg auf die Ukraine**: Ansammlung kleinerer Vorfälle und Hacktivismus-Kampagnen, u. a. Kollateralschäden nach Angriff auf Satellitenkommunikation

Besondere Lage durch den Krieg in der Ukraine

- Das BSI erkennt derzeit eine **erhöhte Bedrohungslage** für Deutschland.
- Allerdings ist **aktuell keine akute Gefährdung** der Informationssicherheit in Deutschland im Zusammenhang mit der Situation in der Ukraine ersichtlich.
- **Hacktivismus** als besonderes **Eskalationspotential**. Zum Beispiel:
  - Anonymous
  - Ransomware-Gruppe Conti
- **Spillover-Effekte.** Zum Beispiel: Viasat
- **Bedrohung für Kritische Infrastrukturen**. Zum Beispiel: Rosneft Deutschland

Gut vernetzt - Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Sie bietet eine Kooperationsbasis zwischen:

- Staat,
- Wirtschaft,
- Herstellern und
- Forschung

NETZWERKE SCHÜTZEN NETZWERKE

www.allianz-fuer-cybersicherheit.de

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Angebote der Allianz für Cyber-Sicherheit auf einen Blick

NETZWERKE SCHÜTZEN NETZWERKE

www.allianz-fuer-cybersicherheit.de

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

2022

10 Jahre Allianz für Cyber-Sicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

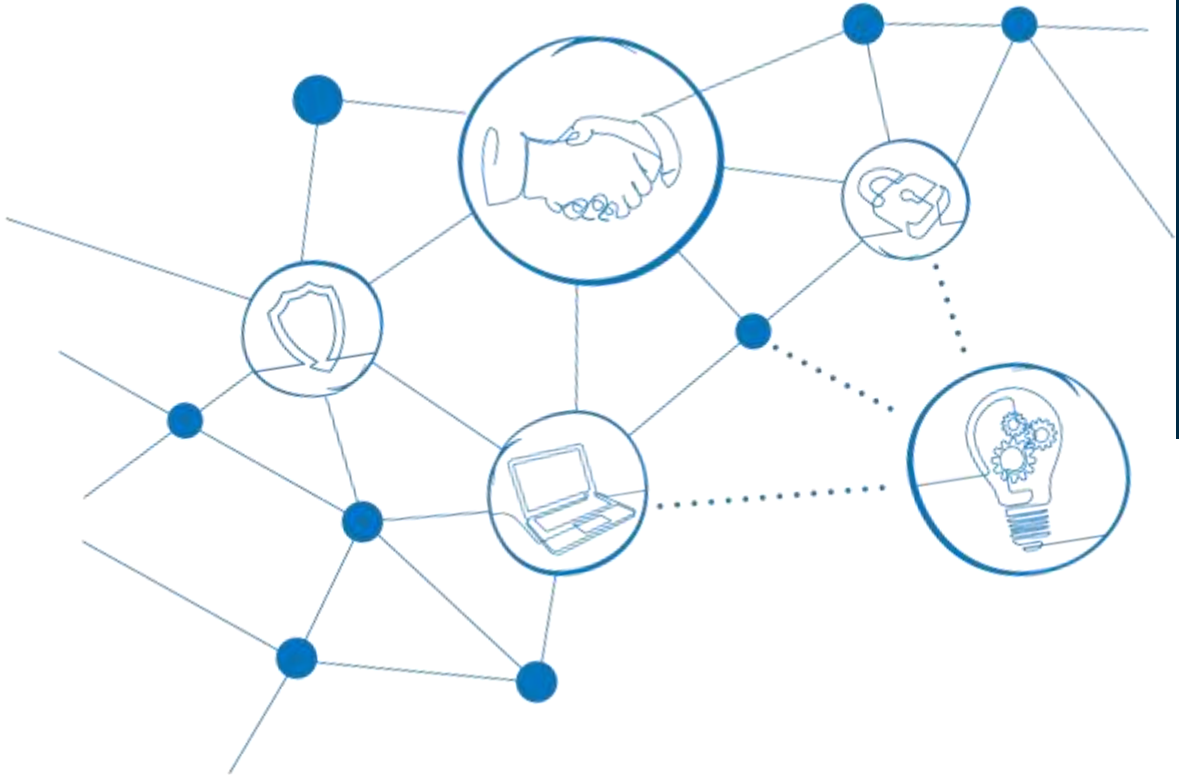
Erfahrungen austauschen

Erfahrungsaustausch- und Expertenkreise

- Erfahrungsaustausch-Kreise:
  „miteinander voneinander lernen“
- Expertenkreise:
  „Cyber-Sicherheit gemeinsam gestalten“

- Beispiele:

→ ERFA-Kreis Praxisorientierte Awareness
→ Expertenkreis Cyber-Sicherheit
→ Expertenkreis CyberMed



Dialog der Cyber-Sicherheits-Initiativen in Deutschland

Kompetenzen erwerben

Partner-Angebote

Die Partner der Allianz für Cyber-Sicherheit (ACS) aus Wirtschaft und Forschung bringen ihre Expertise zu unterschiedlichen Aspekten der Informationssicherheit regelmäßig in Form von Partner-Angeboten in das Netzwerk ein.

Beispiele:

→ Publikationen (Fachartikel, Whitepaper)
→ Schulungen, Seminare oder Workshops
→ Tools, Nutzungslizenzen oder Dienstleistungen

Erfahrungen austauschen

Cyber-Sicherheits-Tage

- Forum für bis zu 250 Teilnehmende an wechselnden Standorten im gesamten Bundesgebiet
- Fachvorträge, Workshops, Diskussionsrunden und Networking zu aktuellen Themen der Cyber-Sicherheit

Cyber-Sicherheits-Web-Talk

- Online-Seminar der ACS

Podcast der ACS - CYBERSNACS

- Cyber-Sicherheit „to go“

Service-Paket für mehr Cyber-Resilienz

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet? Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System? (Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT

- Fokus IT-Notfälle -

Um eine ganzheitliche Cyber-Sicherheits-Strategie verfolgen zu können, sollten Sie ein Informations-Sicherheits-Management-System (ISMS) nach anerkannten Standards etablieren. Ein ISMS wird unterstützt von einem Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- einen Notfallhandbuch.

Ein vollständiges Notfallmanagement/BCM beschränkt sich nicht nur auf den Ausfall der Ressource Informationstechnik, sondern betrachtet auch den Ausfall der Ressourcen Personal, Infrastruktur (z. B. Gebäude und Anlagen) und Dienstleister. Der Maßnahmenkatalog beschränkt sich auf IT-Notfälle und richtet sich in erster Linie an Geschäftsführer und IT-Verantwortliche in kleinen und mittelständischen Unternehmen, die

- ihren Einstieg in diese Thematik gestalten möchten,
- sich den vielfältigen Bedrohungen aus der voranschreitenden Digitalisierung stellen wollen und
- durch ein IT-Notfallmanagement die Cyber-Resilienz ihres Unternehmens erhöhen wollen.

VORBEREITUNG

- Bestimmen Sie Beauftragte für die Belange der Informationssicherheit und des Notfallmanagements in Ihrem Unternehmen, nach Möglichkeit nicht in Personalunion. Beide arbeiten bei IT-Notfällen eng zusammen.
- Stellen Sie in dem Zusammenhang sicher, dass Ihnen Ihre individuellen und fallbezogenen Erstmaßnahmen im IT-Notfall vorliegen (u. a. Alarmierungs- und Meldewege).
- Identifizieren Sie notfallkritische Geschäftsprozesse und Assets (Kronjuwelen) im Rahmen einer strukturierten Prozess (Empfehlung: Business Impact Analyse (BIA)) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, für welche IT-Notfälle Unterstützung geleistet werden kann (Distributed-Denial-of-Service (DDoS), Ransomware, Online-Betrug, Hacking der Webpräsenz, u. a.).
- Identifizieren Sie Dienstleister, die Sie bei IT-Notfällen geeignet unterstützen können und nehmen Sie im Vorfeld Kontakt zu diesen auf.
- Fertigen Sie eine Liste mit allen Ansprechpartnern und treffen Sie Vorabsprachen mit diesen (u. a. Erreichbarkeit, Verfügbarkeit, ggf. Service-Level-Agreement).
- Legen Sie Regeln zur Kommunikation nach innen und außen fest. Eine erfolgreiche Presse- und Öffentlichkeitsarbeit während einem IT-Notfalls kann einen evtl. Imageschaden erheblich begrenzen. Auf diesem Gebiet gibt es Unterstützungsangebote von Dienstleistern. Prüfen Sie vorab, ob Sie solche Angebote in Anspruch nehmen möchten und nehmen Sie frühzeitig Kontakt auf.

TOP 12 MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

- Wurden erste Bewertungen des Vorfalls durchgeführt, um feststellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen dokumentiert, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders schützenswerten und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder Geschäfts-/Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (privilegierte und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgesetzt?

Management von Cyber-Risiken:

Handbuch für Unternehmensvorstände und Aufsichtsräte

6 grundlegende Prinzipien für das Management:

Prinzip 1: Cyber-Sicherheit als Thema des unternehmensweiten **Risiko-Managements** verstehen

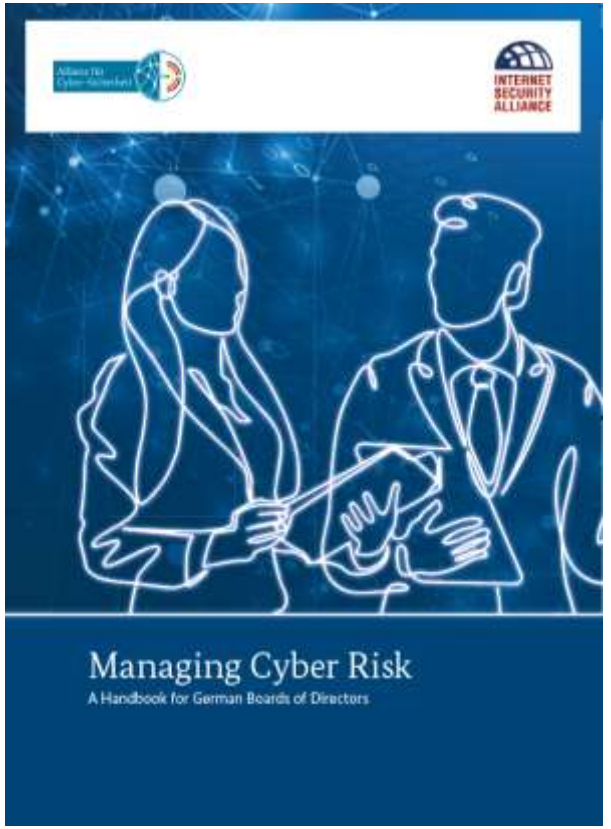
Prinzip 2: **Rechtliche Auswirkungen** von Cyber-Risiken verstehen

Prinzip 3: Grundlegende **Cyber-Sicherheits-Expertise** erwerben

Prinzip 4: Umsetzung geeigneter **Rahmenbedingungen und Ressourcen** für das Cyber-Risiko-Management sicherstellen

Prinzip 5: **Risikobereitschaft** in Abhängigkeit von Geschäftszielen und -strategien definieren

https://www.allianz-fuer-cybersicherheit.de/NACD-Handbuch



Allianz für Cyber-Sicherheit

Sie möchten die Cyber-Sicherheit in Ihrem Unternehmen erhöhen?

Werden Sie Teil eines starken Netzwerks!

10 Jahre Netzwerke schützen Netzwerke

www.allianz-fuer-cybersicherheit.de

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Informationen:

Cyber-Sicherheit für die Wirtschaft und Allianz für Cyber-Sicherheit

- Geschäftsstelle der Allianz für Cyber-Sicherheit
- c/o Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 – 189
53175 Bonn

info@cyber-allianz.de
www.allianz-fuer-cybersicherheit.de
Tel. +49 (0) 228 99 9582 5977
Fax +49 (0) 228 99 109582 6050

Sie finden uns auch in Sozialen Netzwerken.

Twitter

www.twitter.com/CyberAllianz

Xing

www.xing.com/net/allianz-fuer-cybersicherheit

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•