Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Aktuelle Cybersicherheitslage – Von Risiken zu Lösungen

- Stefan Becker
- Bundesamt für Sicherheit in der Informationstechnik

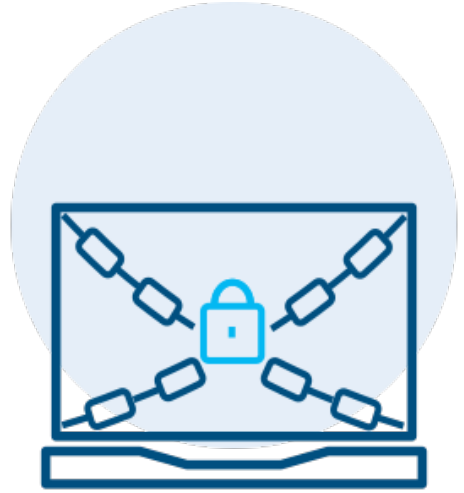
- 22. August 2024 | Südwestfalen Protected

Regel Nr. 1:
Jede und Jeder wird angegriffen -
Es gibt keine Ausnahmen!

Regel Nr. 2:
Die Frage ist nicht ob, sondern wann ein Angriff erfolgreich sein wird!

Ransomware

- Aktuell die **größte operative Bedrohung** der Cyber-Sicherheit
- **Qualität steigt** stetig
- Angriffe mit **hoher Agilität**
- Wirtschaftsmodell mit Arbeitsteilung: **Cybercrime-as-a-Service**
- **Big Game Hunting**: Trend zu gezielten Angriffen auf Unternehmen
- **Maximierung des Erpressungsdrucks** mit zum Beispiel:
  - -> Verschlüsselung
    -> Daten-Leaks
    -> DDoS
    -> Kontaktaufnahme zu Kunden & Partnern
- **BSI rät grundsätzlich von Zahlungen ab**



Wie verändert KI die Cybersicherheitslandschaft?

Chancen	Risiken
• KI gestützte Spam-Erkennung • (Halb-) Automatisiertes Pentesting • Unterstützung bei Auswahl optimaler Verteidigungsstrategien • Intrusion-Detection Systeme	• Phishing • Generierung von Malware • Automatisierte Angriffe • Deepfakes, Fake News • Unterstützung von Kriminellen ohne besondere IT-Kenntnisse

Beide Seiten nutzen KI-Vorteile (z.B. bei KI-unterstützter Entwicklung)
Vorteile für Angreifer bei Desinformation und Social Engineering. Bei KI-gestützten Angriffen und Schwachstellensuche erwartbar
Schnelllebiges Feld - Aufmerksames Beobachten notwendig

IT-Angriffe auf Kommunen

- BSI und kommunale Spitzenverbände starteten im Mai 2023 das **Pilotprojekt für bessere IT-Absicherung in Kommunen: „Weg in die Basis-Absicherung“ (WiBA)**
- **Mehrere deutsche Kommunen** wurden bereits **Opfer von IT-Angriffen**, u.a:
  - Januar 2024: Minden - Bad Oeynhausen (Nordrhein-Westfalen), Vaterstetten (Bayern), Kelheim (Bayern)
  - Februar 2024: Petersberg (Hessen)
- **In der Regel** wurde bei den Vorfällen **Ransomware** vermutet oder später bestätigt
- **Derzeit gibt es keine bundesweit einheitlichen Vorgaben bezüglich IT-Sicherheit oder Meldepflichten zu IT-Sicherheitsvorfällen auf Kommunalebene**
- BSI empfiehlt die Umsetzung des IT-Grundschutz-Profils für Kommunen und veröffentlicht im Oktober 2023 **Checklisten für Kommunen**

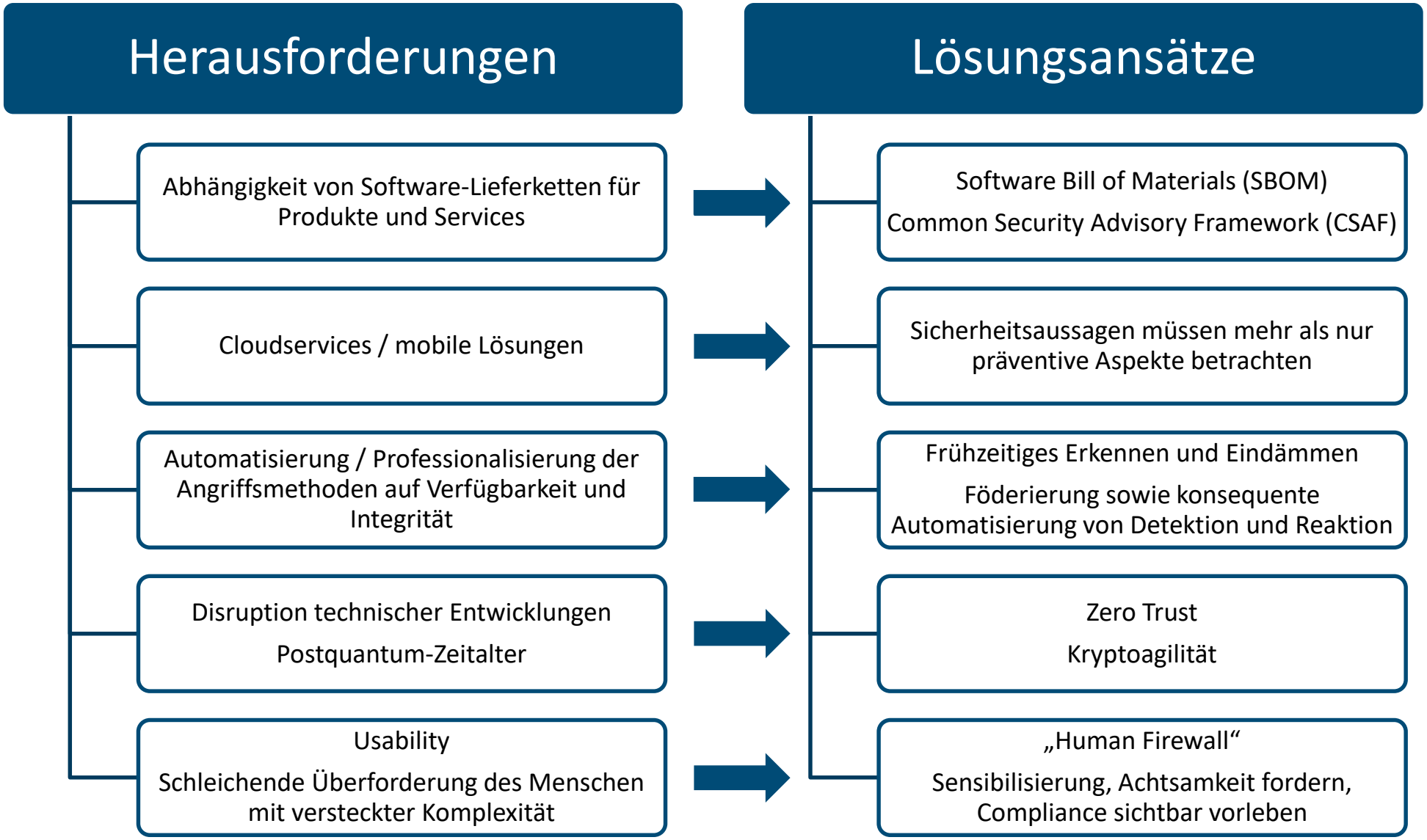
Cloud-Sicherheit – Gestohlener Microsoft-Signaturschlüssel 07/2023

- **Angriff auf E-Mail-Konten** mit Hilfe eines gestohlenen Microsoft-Signaturschlüssels
- Laut Microsoft mutmaßlich durch eine staatliche chinesische Gruppe ausgeführt
- Motivation: **Spionage**
- **Betroffen ca. 25 Organisationen weltweit**; darunter Behörden in Westeuropa und eine Bundesbehörde in den USA
- Bis zum 3. Juli 2023 wurden **Maßnahmen durch Microsoft ergriffen**
- Wie der Vorfall zeigt, können auch Public Clouds erfolgreich angegriffen werden

Die Lage der IT-Sicherheit in Deutschland 2023

Wie bedroht ist Deutschlands Cyberraum?

- **Ransomware** ist weiterhin die größte Bedrohung.
- Vermehrt wurden **kleine und mittlere Unternehmen (KMU) sowie Kommunalverwaltungen und kommunale Betriebe** angegriffen.
- Mehr als **zwei erfolgreiche Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden im Durchschnitt **in jedem Monat** bekannt.
- Außerdem hat das BSI den **Ausbau einer Schattenwirtschaft** cyberkrimineller Arbeitsteilung beobachtet.


Herausforderungen
Lösungsansätze
Abhängigkeit von Software-Lieferketten für Produkte und Services
Software Bill of Materials (SBOM)
Common Security Advisory Framework (CSAF)
Cloudservices / mobile Lösungen
Sicherheitsaussagen müssen mehr als nur präventive Aspekte betrachten
Automatisierung / Professionalisierung der Angriffsmethoden auf Verfügbarkeit und Integrität
Frühzeitiges Erkennen und Eindämmen
Föderierung sowie konsequente Automatisierung von Detektion und Reaktion
Disruption technischer Entwicklungen
Postquantum-Zeitalter
Zero Trust
Kryptoagilität
Usability
Schleichende Überforderung des Menschen mit versteckter Komplexität
„Human Firewall“
Sensibilisierung, Achtsamkeit fordern, Compliance sichtbar vorleben

NIS 2: Den gemeinsamen Wirtschaftsraum cyber-sicher gestalten

Stärkere Harmonisierung der Anforderungen
Sicherheitsmaßnahmen werden europaweit einheitlicher für Wirtschaft/Verwaltung geregelt; Überarbeitungen B3S ggf. erforderlich; mehr Anforderungen (supply chain)

Ausweitung der Aufsichts- und Durchgriffsrechte
BSI wird mehr Kompetenzen ggü. Wirtschaft erhalten/weitere Aufsichts- und Durchgriffsrechte für einen Großteil der Unternehmen aus mehr NIS-Sektoren

Einheitlichere Meldepflichten
Vorfallsmeldeverfahren werden europaweit einheitlicher für Wirtschaft/Verwaltung geregelt; 3-stufiges Verfahren; zeitliche Fristen

Erweiterte Informationspflichten
mehr Vorgaben bei Überlieferung von Unternehmensdaten an das BSI; ggf. Selbstidentifizierung; bei Vorfällen: Information der Kunden zu mögl. Maßnahmen

Einheitliche Vorgaben bei Sektorrechtsakten
Anwendung horizontaler und sektoraler Anforderungen werden grundsätzlich auf EU-Ebene geregelt; NIS2 immer als Mindestsicherheit auch bei „Doppelregulierungen“

Potentiell höhere Strafen & Verantwortung CEOs
Sanktionsregime wird erweitert; höherer Bußgeldrahmen; CEOs können bei Verstößen sanktioniert werden

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html

NIS-2-Betroffenheitsprüfung

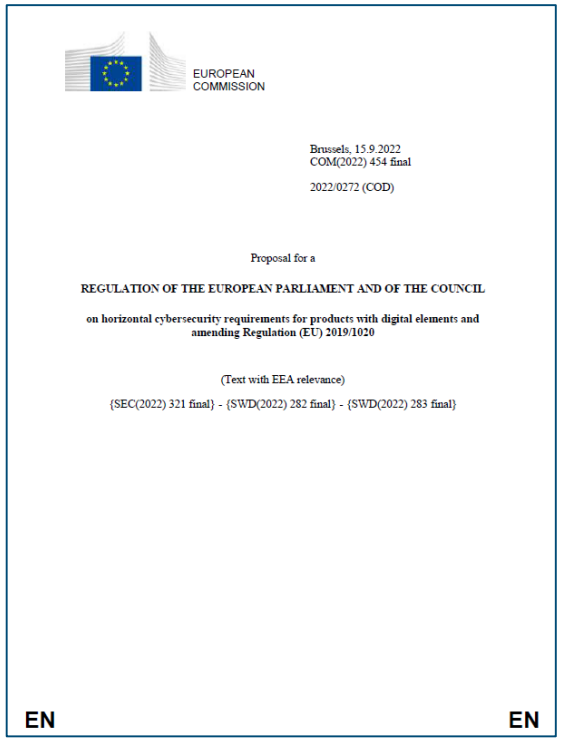
Sind Sie unsicher, ob Ihr Unternehmen von der NIS-2-Richtlinie der EU betroffen ist?
Die › **NIS-2-Betroffenheitsprüfung** des BSI bietet Ihnen in wenigen Schritten dafür eine erste Orientierung.

Die NIS-2-Betroffenheitsprüfung stellt Ihnen konkrete, an der Richtlinie orientierte Fragen, um Ihr Unternehmen einzuordnen. Die Fragen sind kurz und präzise gehalten und werden bei Bedarf im Kleingeschriebenen tiefer gehend erläutert.

Nachdem Sie den Fragenkatalog durchlaufen haben, erhalten Sie ein auf Ihren Angaben basierendes Ergebnis. Dieses gibt eine automatisierte Ersteinschätzung, ob Ihr Unternehmen von der NIS-2-Richtlinie betroffen ist - und erläutert Ihnen, was dieser Status bedeutet und welche Pflichten durch den EU-Gesetzgeber vorgezeichnet sind.

Cyber Resilience Act

- **Europäische Kommission** hat am 15. September 2022 den **Entwurf** veröffentlicht
- CRA regelt den **Marktzugang** in Form von **horizontalen europäischen Cyber-Sicherheitsanforderungen** für ein breites Spektrum **digitaler Produkte und Dienste**
- Beinhaltet sind Anforderungen für Produkte über deren **gesamten Lebenszyklus** hinweg
- CRA wird als Teil des New Legislative Framework in ein **bestehendes Ökosystem** mit Fokus auf „**safety**“ erstmals um „**security**“-Aspekte erweitert



EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EN EN

In Cyber-Sicherheit investieren >

Ist aktive Gestaltung der Zukunftsfähigkeit!

Allianz für Cyber-Sicherheit

Netzwerke schützen Netzwerke

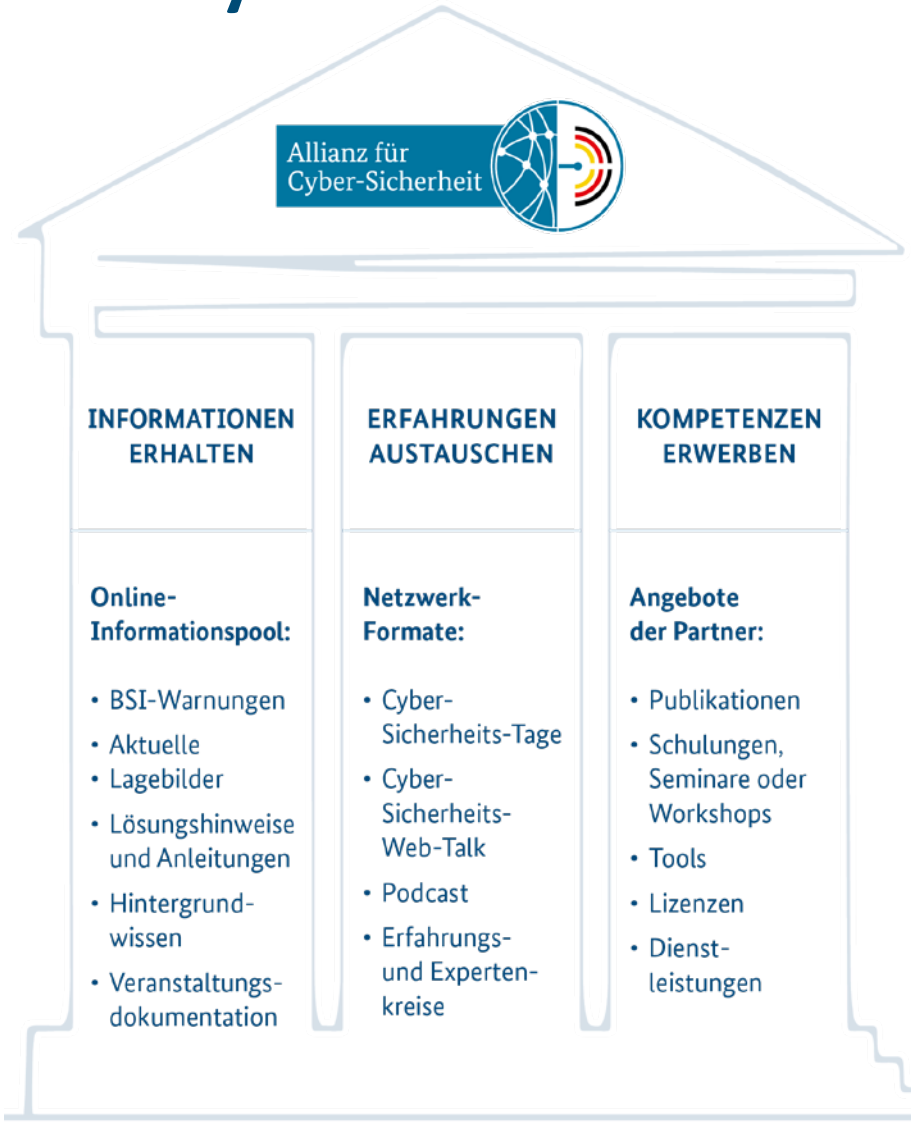
Bundesamt
für Sicherheit in der
Informationstechnik

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•

Lösungen zur Vereinheitlichung der Informationsweitergabe innerhalb der Lieferkette

Software Bill of Materials (SBOM)

- Digitaler „Beipackzettel“ für alle verwendeten Softwarekomponenten
- Für Hersteller und OEMs

Common Security Advisory Framework (CSAF)

- Aktuell nutzen Hersteller von Software kein einheitliches Format für Informationen über Patches und Updates
- Fokus Endkunden
- Viele Systeme haben keine Möglichkeiten zu automatischen Updates
- Durch CSAF wird manueller Aufwand minimiert, insbesondere in der Produktion
- **Erfolg durch Ihre Unterstützung!**

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?

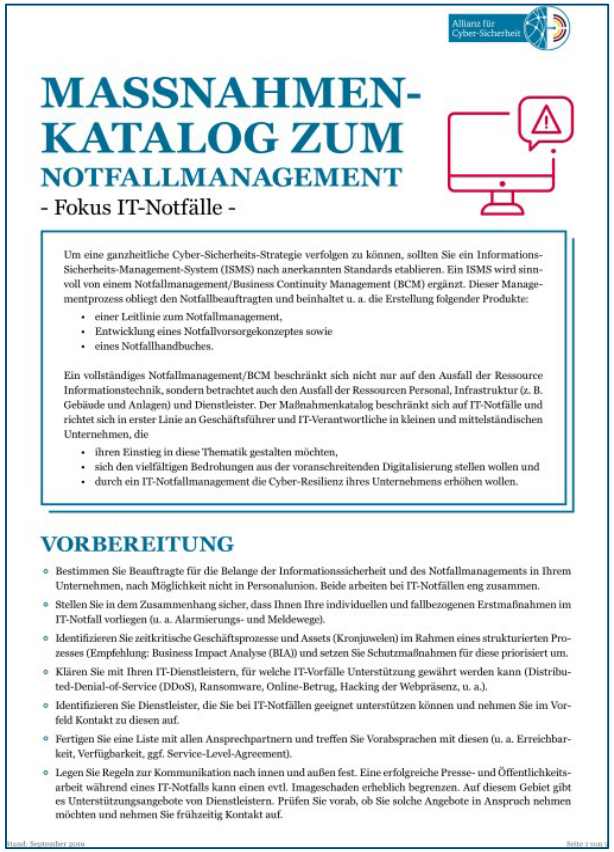
Wann ist das Ereignis eingetreten?

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 sinnvoll von einem Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

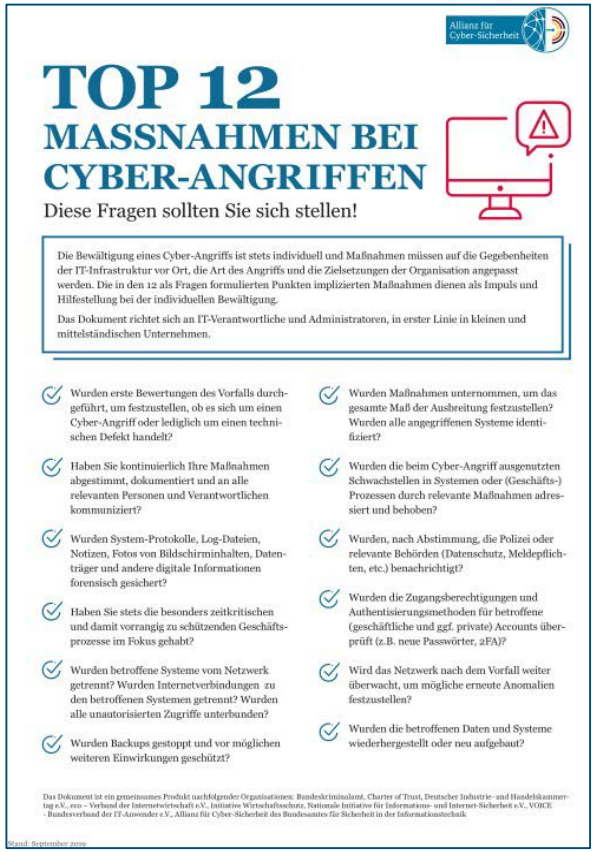
- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

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 zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) im Rahmen eines strukturierten Prozesses (Empfehlung: Business Impact Analyse (BIA)) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, für welche IT-Vorfälle Unterstützung gewährt 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 eines 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 festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, 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 zeitkritischen 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 (geschäftliche 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 aufgebaut?

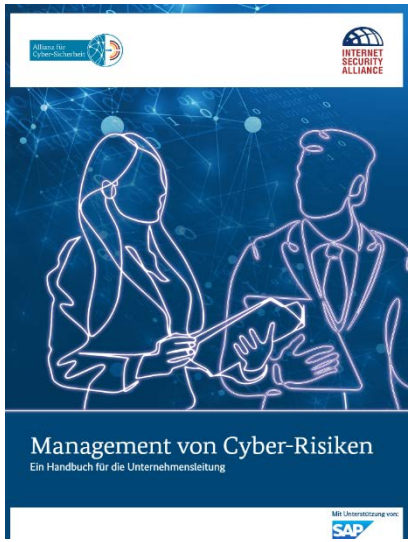
Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag e.V., eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VOICE – Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik

„Management Blitzlicht“ – C-SCRM

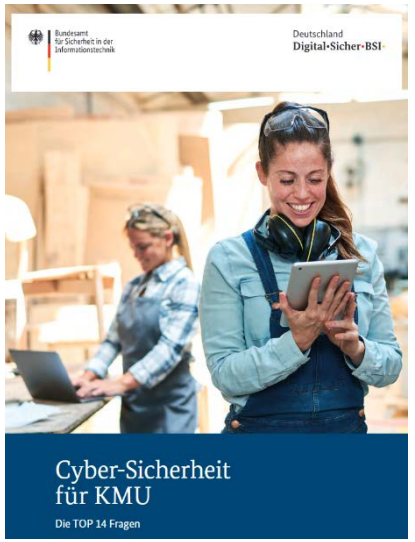
- Grundlagen des Cyber-Supply Chain Risk Management
- 5 Maßnahmenempfehlungen

„KMU Angebote“

- **Cyber-Sicherheit muss Chefinnen- und Chefsache sein!**
  - Zum Teil des Risiko-Managements machen
  - SBOM bei Zulieferern einfordern
  - Budget für IT-Sicherheit erhöhen
- **CyberRisikoCheck für Klein- und Kleinstunternehmen**
  - Niedrige Kosten für Unternehmen und Fördermöglichkeit
  - Niedrigschwelliges Angebot zur Erhöhung der Cyber-Sicherheit
- **Umsetzung IT-Grundschutz**



https://www.bsi.bund.de/dok/1086750



https://www.bsi.bund.de/dok/1070672

Quelle: BSI

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

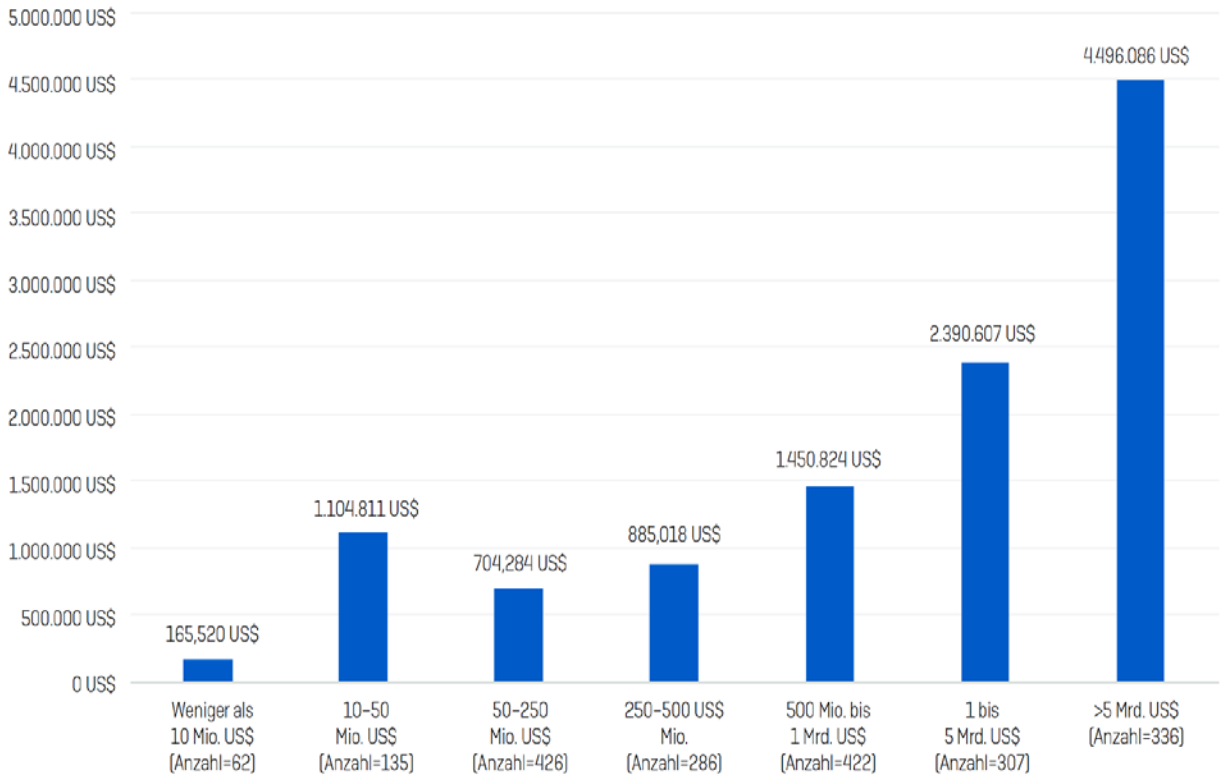
Podcast der ACS - CYBERSNACS

- Cyber-Sicherheit „to go“

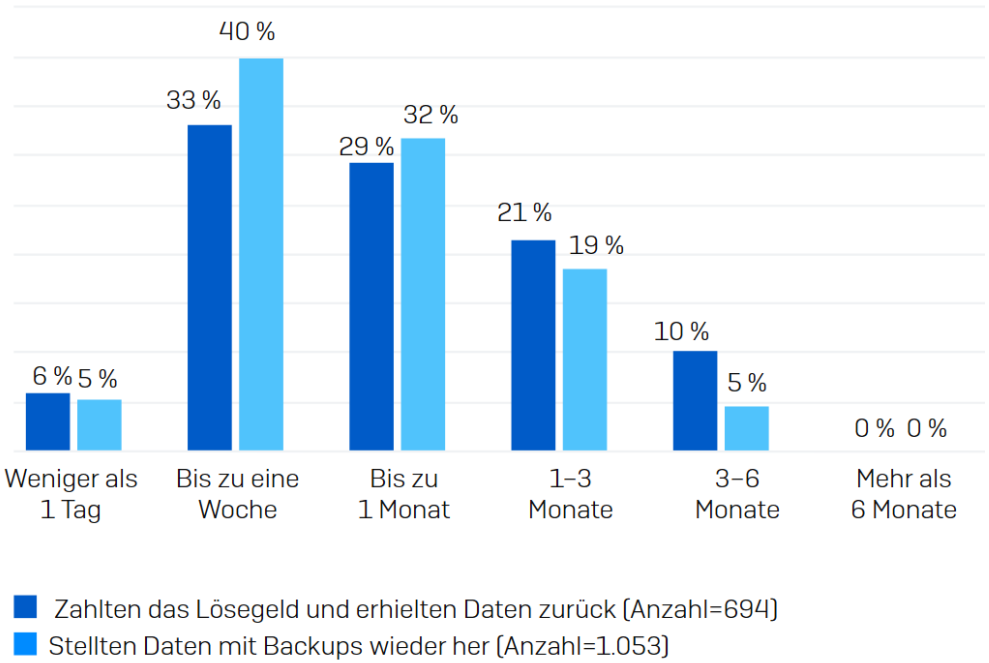
Cybersicherheit rechnet sich! Beispiel Ransomware

Zahlten das Lösegeld und erhielten Daten zurück	Stellen Daten mit Backups wieder her
750.000 US$ Median	375.000 US$ Median
2,6 Mio. US$ Durchschnitt	1,62 Mio. US$ Durchschnitt

Wiederherstellungskosten nach Methode



Durchschn. Bereinigungskosten nach Umsatz



Ausfallzeiten nach Methode der Datenwiederherstellung

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Quelle: Sophos Ransomware-Report 2023: https://assets.sophos.com/X24WTUEQ/at/svpmfvq7h6748rmrvrp8njb/sophos-state-of-ransomware-2023-wpde.pdf
Befragung von 3000 IT-/Cybersecurity-Entscheidern in Unternehmen und Organisationen mit 100-5000 Mitarbeitenden aus 14 Ländern.

Allianz für Cyber-Sicherheit

Sie möchten die Cyber-Sicherheit in Ihrem Unternehmen erhöhen?

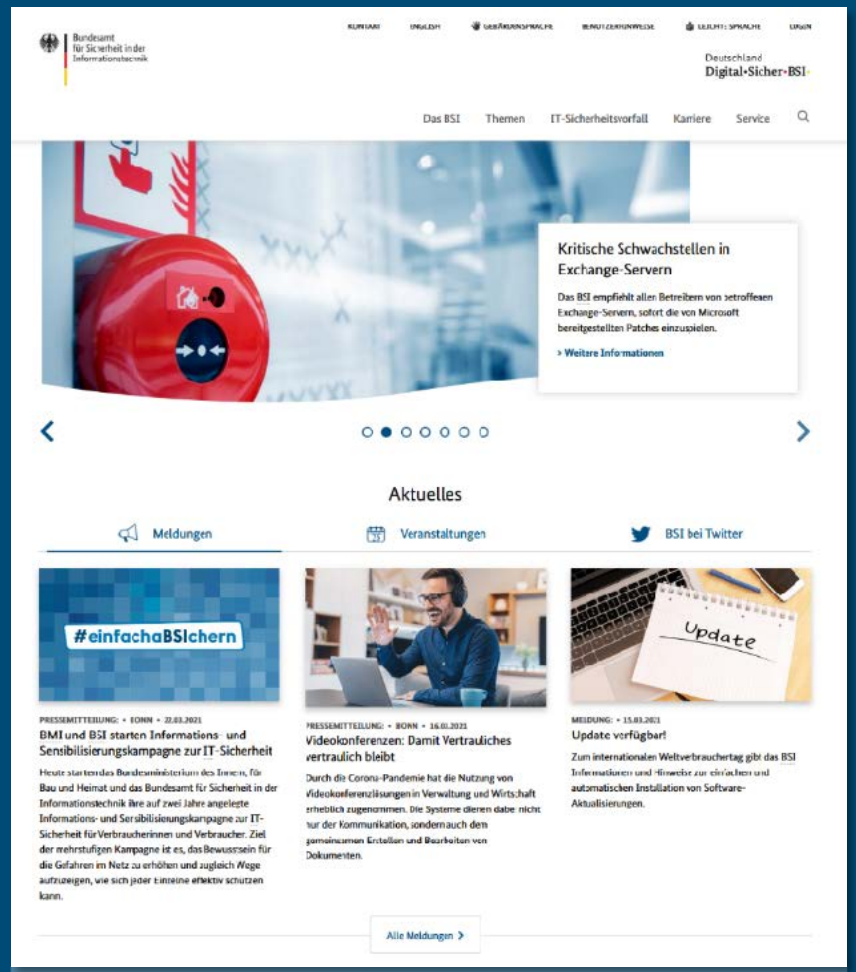
Werden Sie Teil eines starken Netzwerks!

12 Jahre Netzwerke schützen Netzwerke

www.allianz-fuer-cybersicherheit.de

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•



Direktlink zum Angebot für KMU:

www.bsi.bund.de/kmu

- Tipps und Tricks für die Zielgruppe KMU
- Kontaktmöglichkeit bei Sicherheitsvorfällen
- Abomöglichkeit KMU-Newsletter

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI

Führen Sie einen CyberRisikoCheck durch!!!

www.cyberrisikocheck.de

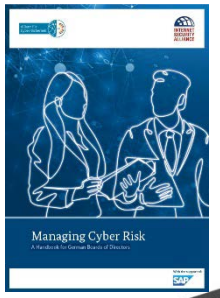
Angebote des BSI

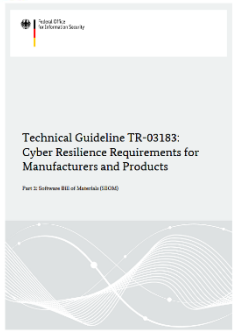
- Handbuch „Management von Cyber-Risiken“ + Toolkit
  - Insbesondere Tool C: „Risiken in der Lieferkette und gegenüber Dritten“
  - https://www.allianz-fuer-cybersicherheit.de/dok/cyberriskmanagement

- „Cyber Risiko Check“ für kleine und mittlere Unternehmen (DIN SPEC 27076)
  - KMU machen einen Großteil der Lieferkette aus!
  - https://www.bsi.bund.de/dok/crc

- SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette
  - https://www.bsi.bund.de/dok/TR-03183

- Common Security Advisory Framework (CSAF)
  - Maschinenverarbeitbare Security Advisories -> Zeit sparen, schneller handeln!
  - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html





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

Informationen:

Stefan Becker

Referatsleiter – W23 Allianz für Cyber-Sicherheit und Cyber-Sicherheit für große Unternehmen

Kontakt

stefan.becker@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

Sie finden uns auch in Sozialen Netzwerken.

Twitter

www.twitter.com/CyberAllianz