Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Lagebild Deutschland

Stefan Becker
Bundesamt für Sicherheit in der Informationstechnik

26. April 2023

Leitsatz

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

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

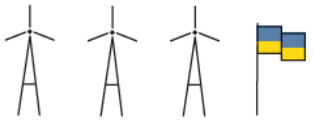
Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

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

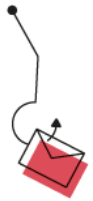
Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.

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.

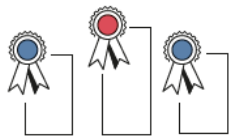
78.000
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

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 betrügerisch 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•

Quelle: BSI

Bundesamt für Sicherheit in der Informationstechnik

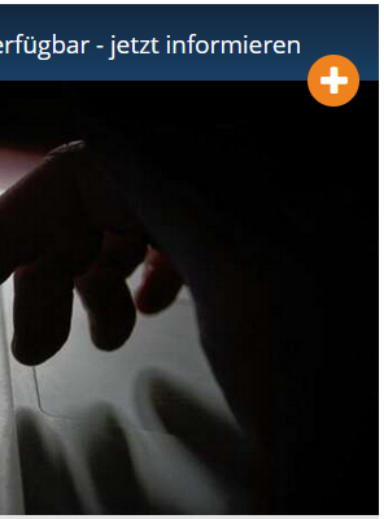
Deutschland Digital•Sicher•BSI•

Wie bedroht ist Deutschlands Cyber-Raum?

- 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.

Lesezeit Jetzt Artikel teilen: 21. April 2023 ts/ys/ba



dpa

Hacker haben offenbar das Netzwerk der Badischen Stahlwerke in Kehl angegriffen. Das Unternehmen musste reagieren und die interne Kommunikation abschalten.

Auf das Netzwerk der Badische Stahlwerke GmbH in Kehl hat es am Donnerstag einen Hackerangriff gegeben. Das bestätigte die Polizei in Offenburg. Das Unternehmen selbst weist auf seiner Homepage auf den "unautorisierten Zugriff" hin.

Demnach wurden die betroffenen Systeme abgeschaltet, weshalb Mitarbeiter vorübergehend per E-Mail und Festnetz-

Bundesamt für Sicherheit in der Informationstechnik

Meldungen & Nachrichten

Zur Übersicht

25.04.2023

Gezielter Cyberangriff auf IT-Netz des Klinikums Hochsauerland

Ende der letzten Woche haben Unbekannte mit einem gezielten und massiven Angriff versucht, Zugriff auf die IT-Infrastruktur des Klinikums Hochsauerland zu erlangen. Der unmittelbare Angriff ist dank automatisierter Sicherheitssysteme schnell erkannt und gestoppt worden. Aus Sicherheitsgründen wurden alle webbasierten Anwendungen zunächst deaktiviert und das IT-System des Klinikums vom Internet getrennt. Seither werden alle Systeme in Zusammenarbeit mit externen Forensikern überprüft. „Wir haben die Ermittlungsbehörden eingeschaltet und Strafanzeige erstattet. Die Zentral- und Ansprechstelle Cybercrime (ZAC NRW) führt nun die Ermittlungen. Auch das Landeskriminalamt NRW sowie das Bundesamt für Sicherheit in der Informationstechnik sind involviert“, so Werner Kemper, Sprecher der Geschäftsführung, Klinikum Hochsauerland.

Quelle: BSI

ZIEGLER momentan nur eingeschränkt erreichbar

10. Februar 2023 | Aktuelles aus dem Unternehmen

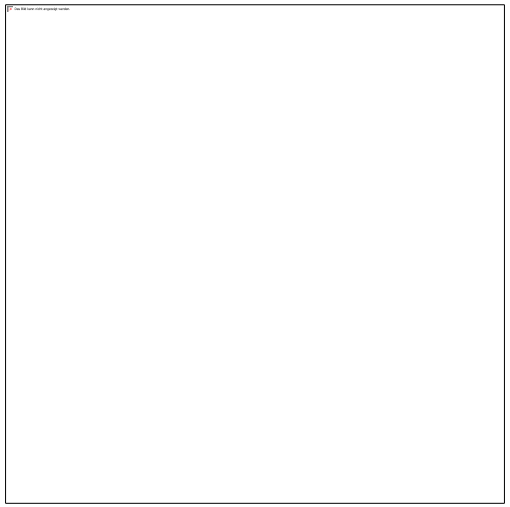
Am Donnerstag, den 09.02. wurde ZIEGLER Opfer eines Cyberangriffs. Der Angriff wurde gegen 08:00 Uhr morgens erkannt.

Daraufhin wurden umgehend alle relevanten Systeme abgeschaltet. Das führt dazu, dass sämtliche Systeme standortübergreifend derzeit offline sind, sodass wir aktuell in unserer Arbeitsfähigkeit sowie Erreichbarkeit per Mail stark eingeschränkt sind. Das Telefonnetz ist nicht betroffen, weshalb wir weiterhin telefonisch erreichbar sind.

Deutschland Digital•Sicher•BSI•

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

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

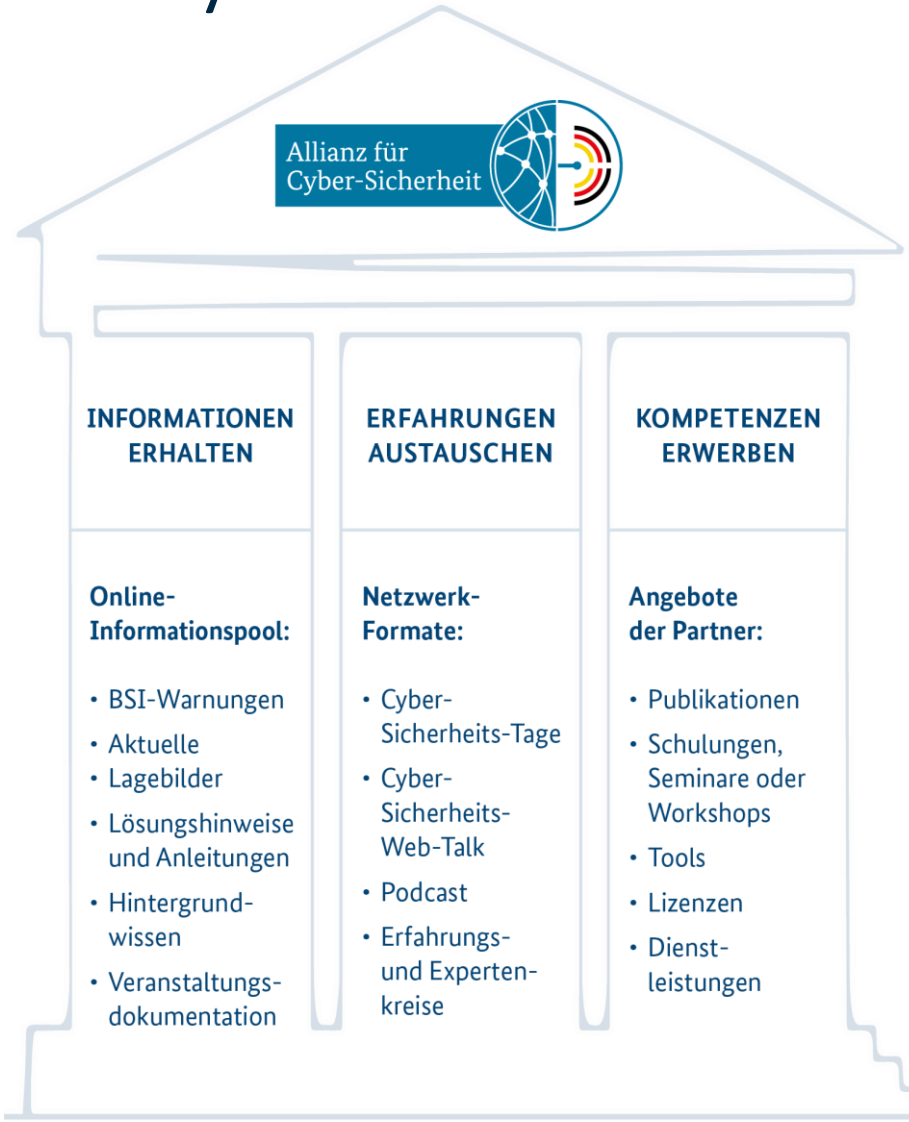
Bundesamt
für Sicherheit in der
Informationstechnik

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•

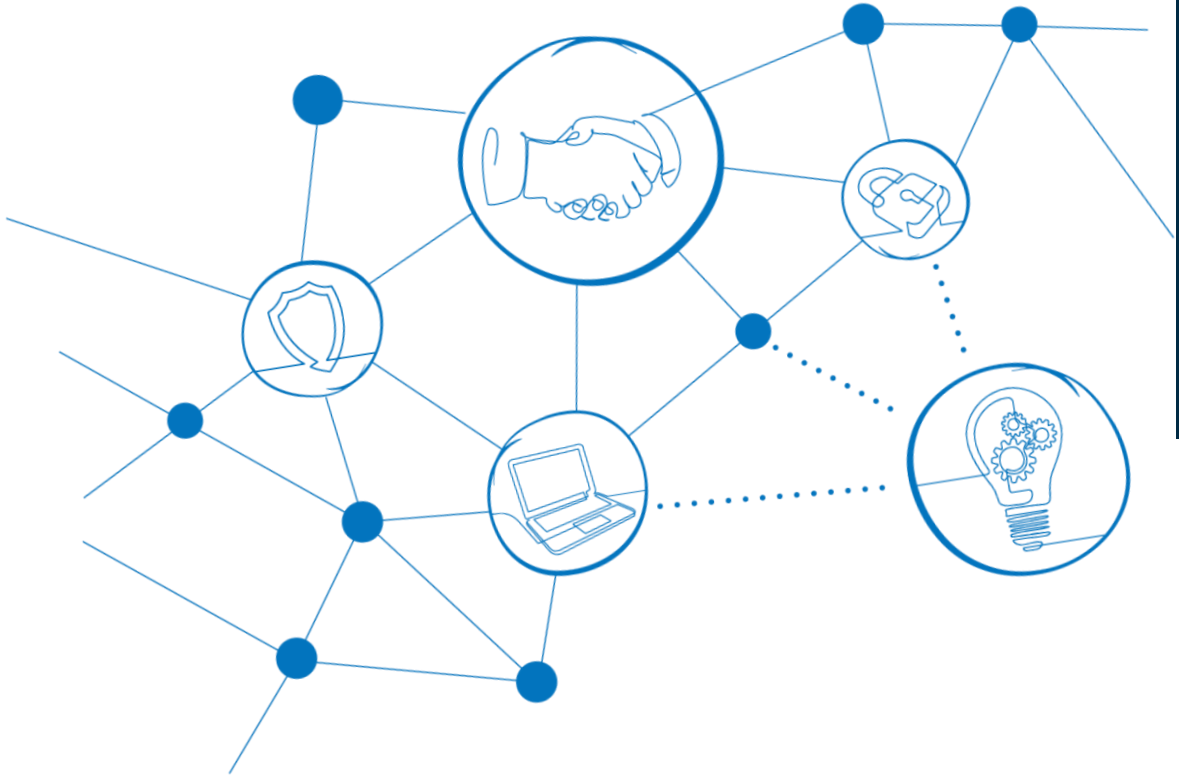
Erfahrungen austauschen

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

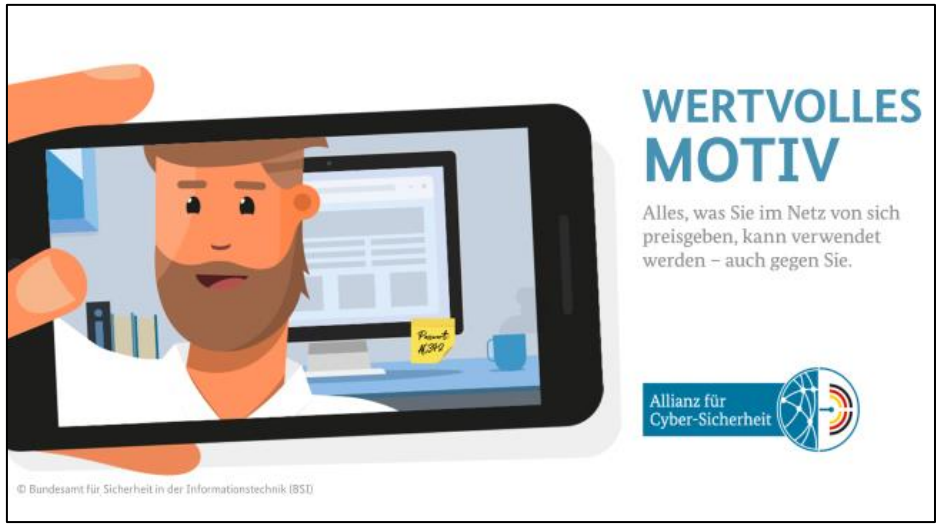
Podcast der ACS - CYBERSNACS

- Cyber-Sicherheit „to go“

Cyber-Sicherheitsfaktor Mensch

- Cyber-Sicherheit ist nur so gut, wie der Mensch, der die Systeme bedient.
- Cyber-Sicherheit betrifft alle Mitarbeitende und jede Abteilung im Unternehmen.
- Bei allen Veränderungen und neuen Prozessen sollte Cyber-Sicherheit immer grundsätzlich mitgedacht und die verantwortlichen Personen einbezogen werden.

→ Der Mensch ist der Grundstein der Cyber-Sicherheit im Unternehmen!



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?

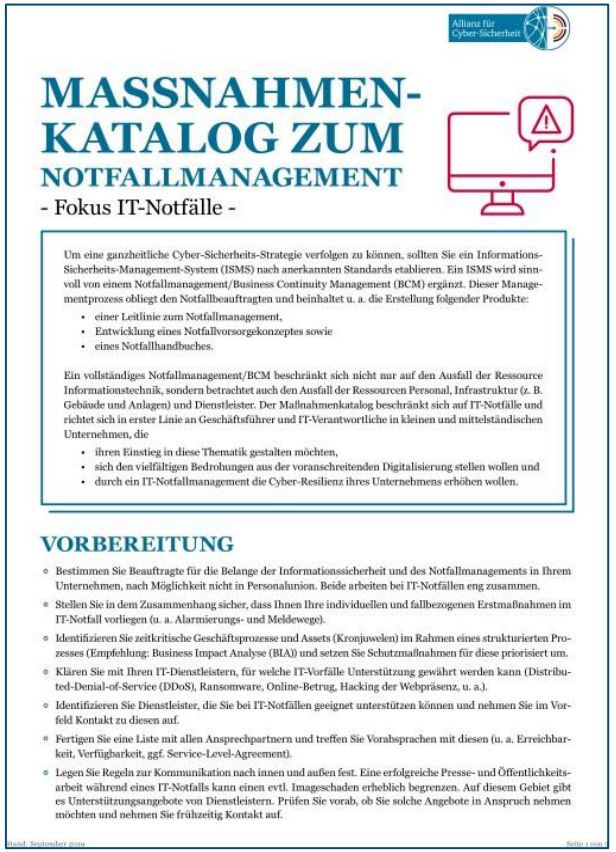
Wann ist das Ereignis eingetreten?

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:

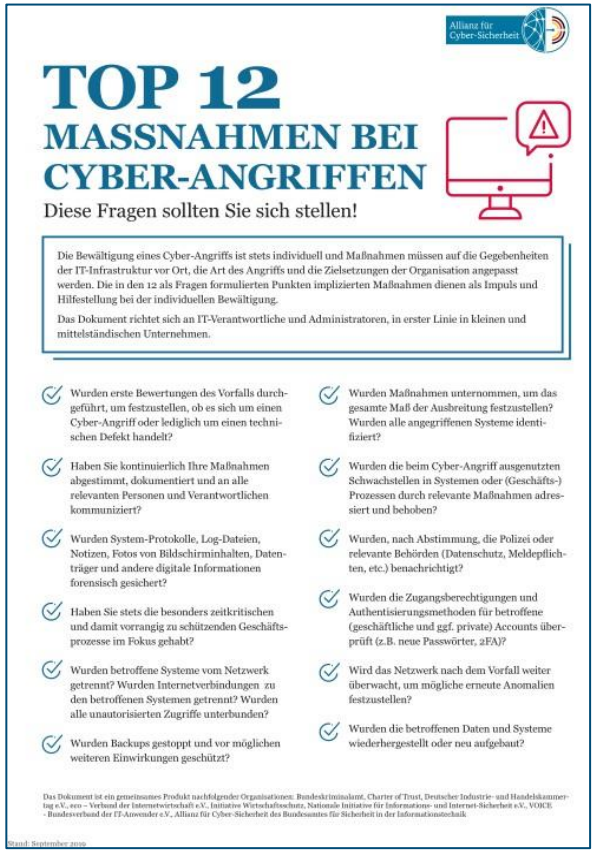
- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

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

Stand: September 2019

Management von Cyber-Risiken:

Ein Handbuch für die Unternehmensleitung

6 grundlegende Prinzipien für das Management:

Prinzip 1: Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmensweiten **Risikomanagements** verstehen

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

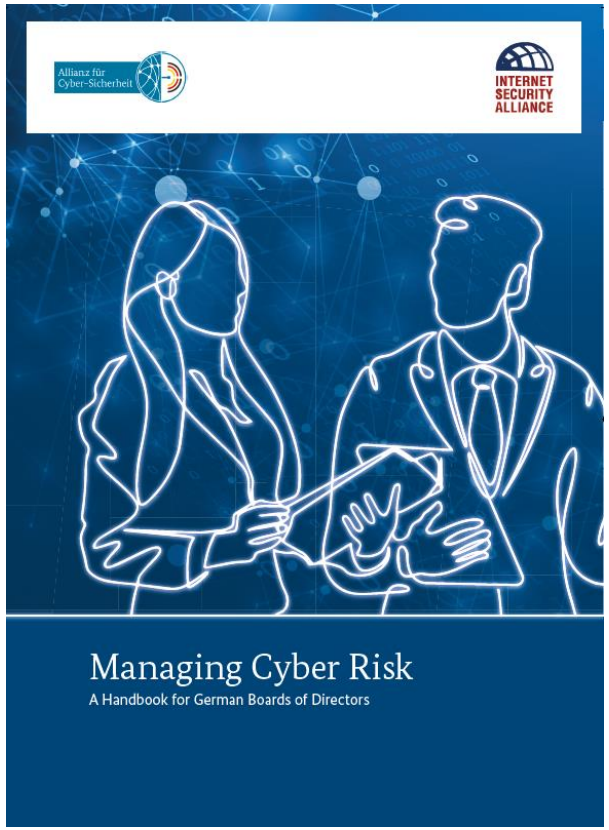
Prinzip 3: Zugang zur **Cybersicherheitsexpertise** sowie regelmäßigen Austausch sicherstellen

Prinzip 4: Umsetzung geeigneter **Rahmenbedingungen und Ressourcen** für das Cyberrisikomanagement sicherstellen

Prinzip 5: **Risikoanalyse** erstellen sowie Definition von **Risikobereitschaft** in Abhängigkeit von Geschäftszielen und -strategien formulieren

Prinzip 6: Unternehmensweite **Zusammenarbeit** und den Austausch von Best Practice fördern

https://www.allianz-fuer-cybersicherheit.de/dok/cyberriskmanagement



Informationen:

Stefan Becker
Referatsleiter – WG22 Cyber-Sicherheit für die Wirtschaft

Kontakt

stefan.becker@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185 – 189
53175 Bonn
www.bsi.bund.de
www.allianz-fuer-cybersicherheit.de
www.upkritis.de

Sie finden uns auch in Sozialen Netzwerken.

Twitter

www.twitter.com/CyberAllianz

UP KRITIS

www.upkritis.de