# Allianz für Cyber-Sicherheit

## Netzwerke schützen Netzwerke

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# 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

# Werden Sie Teil eines starken Netzwerks!

Allianz für Cyber-Sicherheit

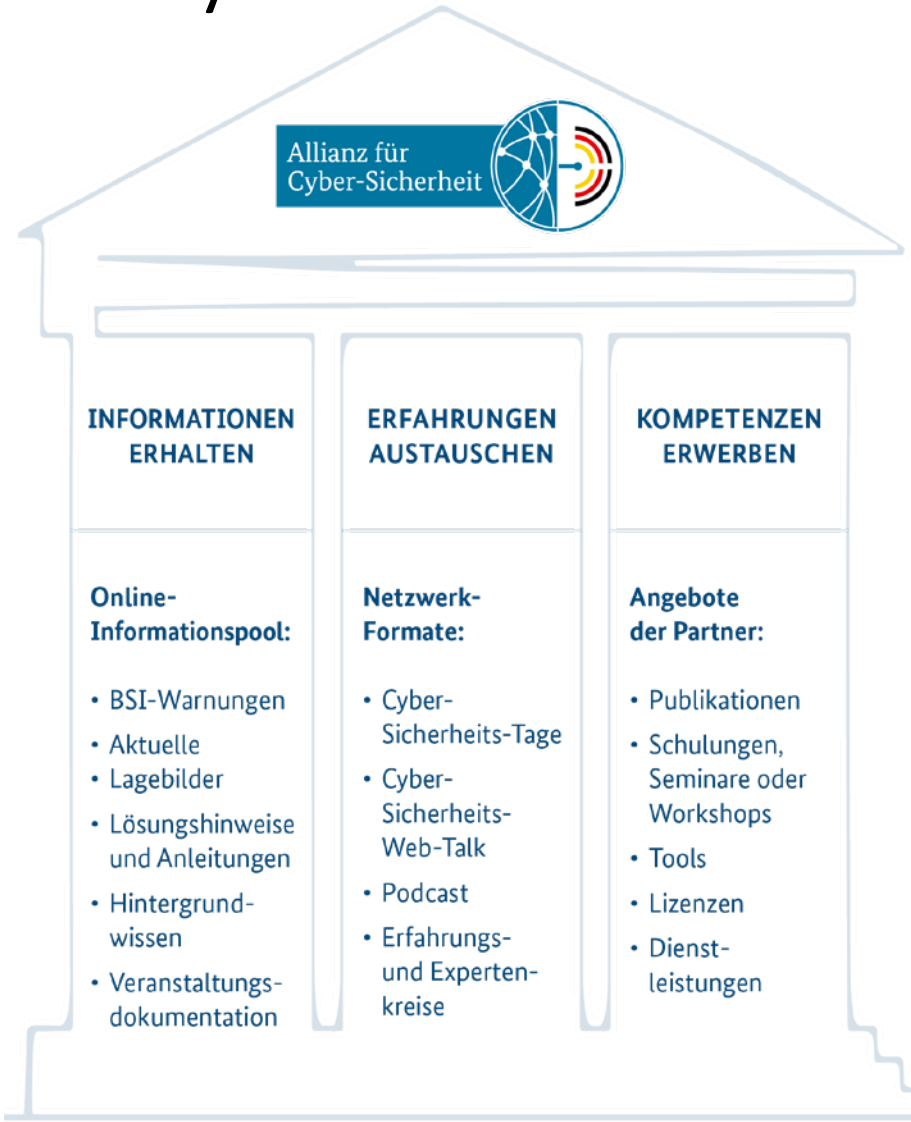
**Als Teilnehmer der Allianz für Cyber-Sicherheit profitieren Sie von…**

- der Expertise des BSI und der Partner der Allianz für Cyber-Sicherheit,
- dem vertrauensvollen Erfahrungsaustausch mit anderen Unternehmen und Institutionen zu Themen wie Angriffsvektoren, geeigneten Schutzmaßnahmen, Tipps zum Sicherheitsmanagement, Vorfallsbehandlung etc. sowie
- den exklusiven und für alle Teilnehmer kostenfreien Partner-Angeboten zum Ausbau Ihrer Cyber-Sicherheitskompetenz.
- dem Newsletter mit den aktuellsten Publikationen, Ereignissen und Terminen.

# 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•

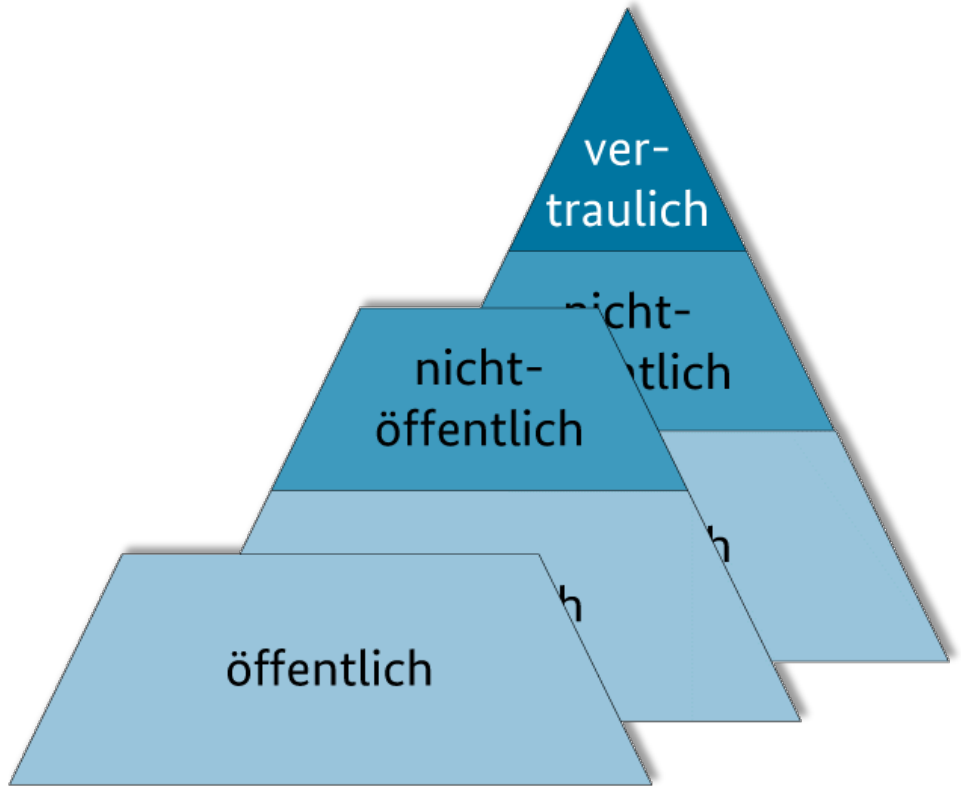
# Informationen erhalten

**Informationspool**

- Vertrauliche Dokumente
- Warnverteiler des BSI

- Nicht öffentliche Dokumente
- Informationen zur aktuellen Lage
  (z.B. Themenlagebilder, Warnmeldungen)
- Angebote der Partner (z.B. Schulungen, Seminare)

- Cyber-Sicherheits-Empfehlungen
- Meldestelle



# 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“

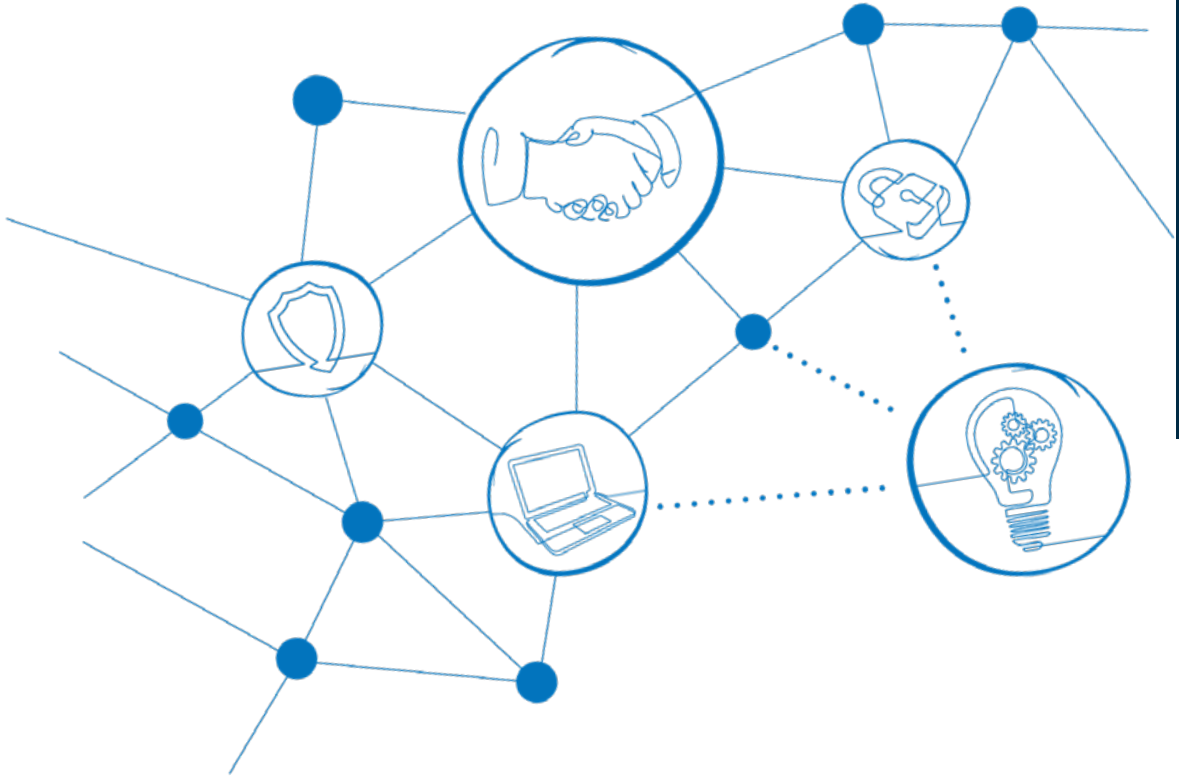
# Erfahrungen austauschen

**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**

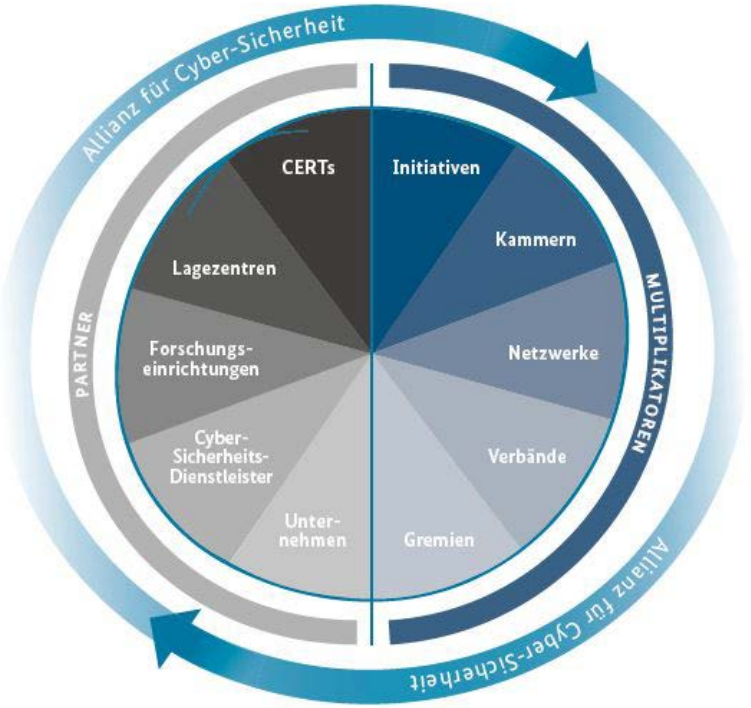
Die Partner der Allianz für Cyber-Sicherheit (ACS) aus Wirtschaft und Forschung bringen ihre Expertise zu unterschiedlichen Aspekten der Informationssicherheit regelmäßig in Form von Partner-Angeboten in das Netzwerk ein.

Beispiele:

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

# Aktiv für mehr Cyber-Sicherheit – als Partner oder Multiplikator

Rund 145 Partner und 114 Multiplikatoren engagieren sich im Rahmen der Initiative und leisten so einen wertvollen Beitrag für mehr Cyber-Sicherheit am Wirtschaftsstandort Deutschland.



# 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?

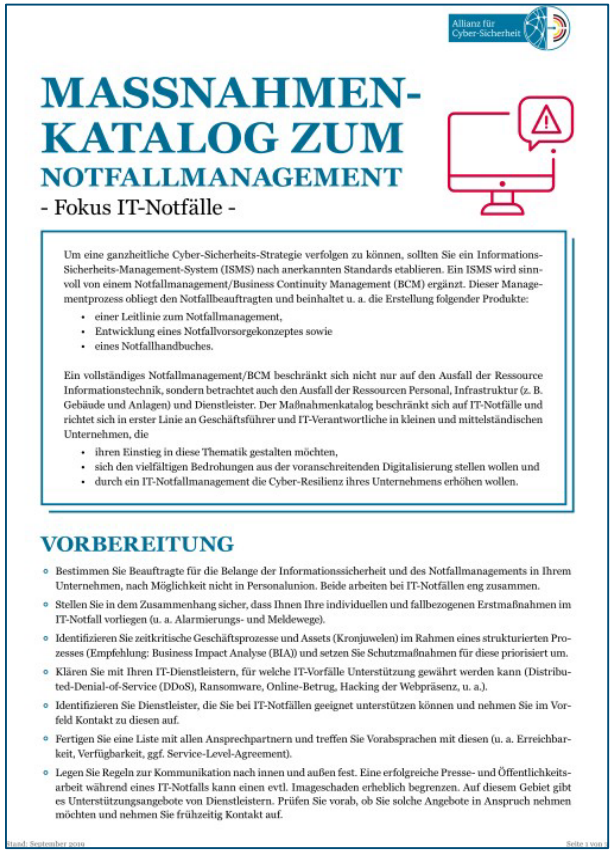
Wann ist das Ereignis eingetreten?

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:

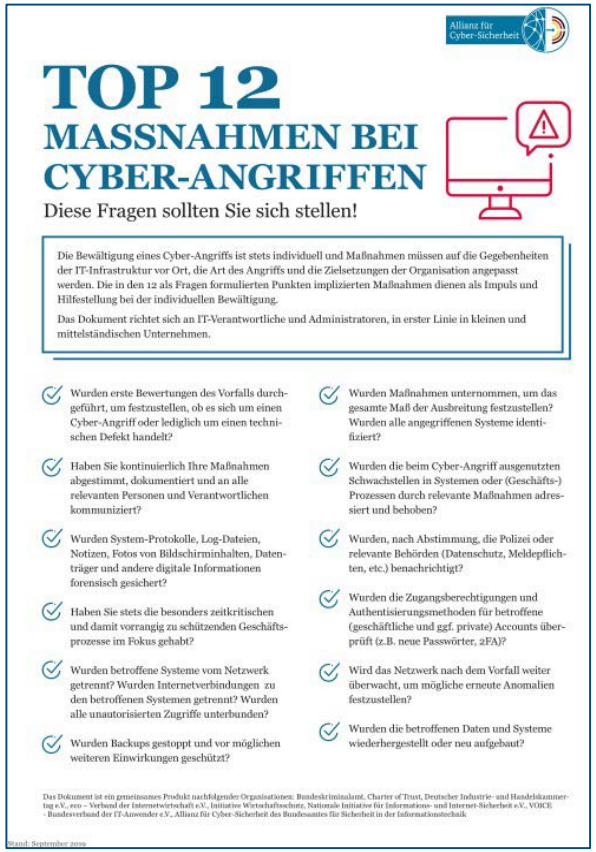
- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

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

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

# 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

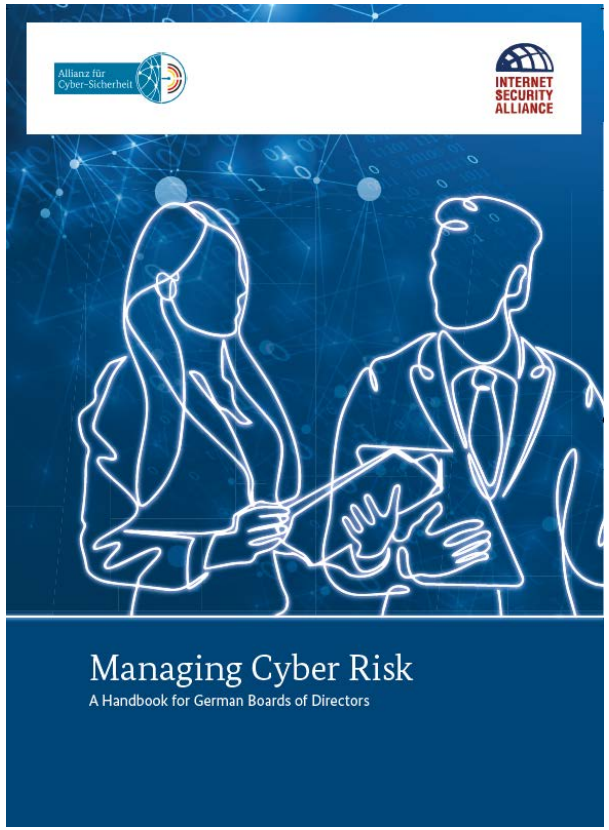
Prinzip 3: Zugang zur **Cybersicherheitsexpertise** sowie regelmäßigen Austausch sicherstellen

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



Allianz für Cyber-Sicherheit

**Sie möchten die Cyber-Sicherheit in Ihrem Unternehmen erhöhen?**

# Werden Sie Teil eines starken Netzwerks!

13 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 87
53175 Bonn

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