Leitfaden zur Prävention von Cyberrisiken

Gezielte Maßnahmen für die Informationssicherheit

Autorenteam

Peer Casper
Geschäftsführer
Smart Data Center GmbH

Mark Mickasch
Chief Compliance Officer
Funke Mediengruppe GmbH &Co. KGaA

Dr. Stephan Petri
Senior Vice President Corporate Legal
GEA Group AG

Dr. Holger Schramm
Rechtsanwalt

Mit freundlicher Unterstützung von

Prof. Dr. Jürgen Gramke
Institute for European Affairs – INEA

BSI – Bundesamt für Sicherheit in der Informationstechnik

Inhalt

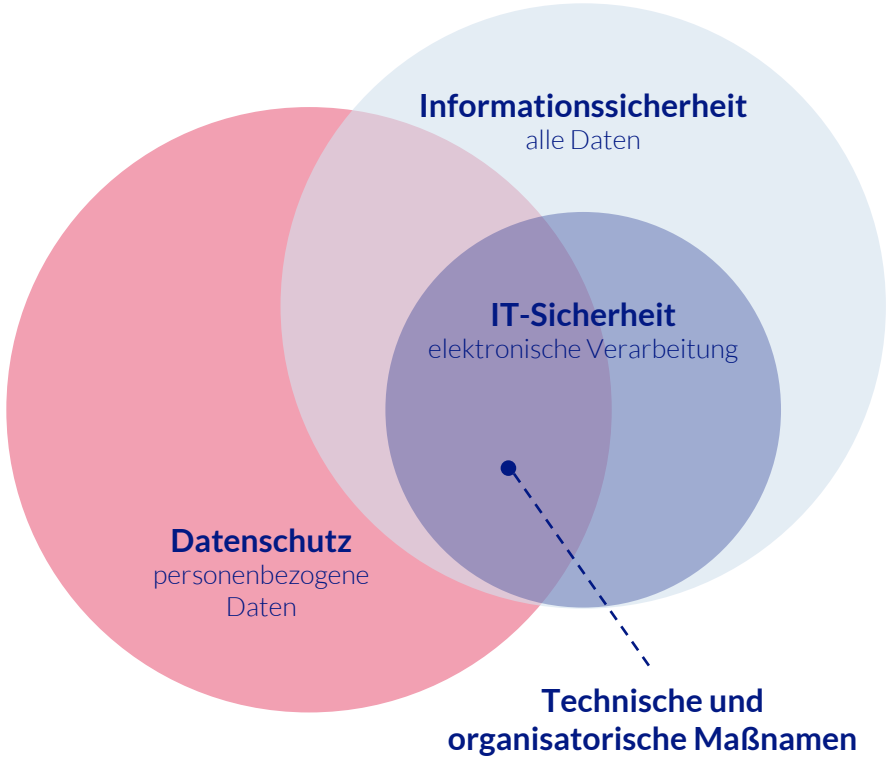
Informationssicherheit

Informationssicherheit

1. Unverzichtbarer Erfolgsfaktor

In der heutigen Informationsgesellschaft und einer Welt, in der Daten als der Rohstoff des 21. Jahrhunderts gelten, ist der Schutz von Informationen für Unternehmen, Behörden und andere Institutionen für die zukünftige Entwicklung und den Erfolg unverzichtbar.

Bei der Informationssicherheit als Oberbegriff geht es um den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit (auf Englisch „CIA Triangle“) sämtlicher Informationen. Unabhängig davon, ob sie nun wie früher in physischer Form oder heutzutage – überwiegend – in elektronischer Form existieren, wie z. B. auf Mobilgeräten, Desk- bzw. Laptops, Netzwerken oder in der Cloud.



Informationssicherheit

1. Unverzichtbarer Erfolgsfaktor

Schnittmengen der Informationssicherheit gibt es im Bereich der technischen und organisatorischen Maßnahmen, den sogenannten TOMs, mit dem Schutz von personenbezogenen Daten und für die Person, die für den Datenschutz verantwortlich ist. Diese Person beschäftigt sich in erster Linie mit der Frage, inwieweit personenbezogene Daten erhoben, gespeichert, verarbeitet und gelöscht werden dürfen, während die Informationssicherheit für die Maßnahmen zum Schutz sämtlicher Informationen verantwortlich ist.

Cybersicherheit ist – als Teil der Informationssicherheit – die IT-Sicherheit der im Cyberraum auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme.

Informationssicherheit

2. Compliance und operative Risiken

Top-5-Compliance-Risiken der Informationssicherheit

- **Geldbußen** als Folge von Gesetzesverstößen
- **Beendigung** laufender Kundenbeziehungen
- **Ausschluss** von zukünftigen Ausschreibungen
- **Verlust** einer Wettbewerbsposition
- **Haftung** von Organen bei Vorfällen im Bereich der Informationssicherheit

Top 5 operative Risiken der Informationssicherheit

- **Diebstahl/Spionage** von geistigem Eigentum
- Produktionsverlauf durch **Sabotage**
- **Manipulation** der Fertigung
- **Verlust** vertraulicher Informationen zu Strategie, Kunden und Preisen
- **Angriff** auf die Infrastruktur von Kunden über das Firmennetzwerk

→ **Reputationsverlust und finanzieller Schaden** → **Informationssicherheit kostet, keine Informationssicherheit kostet mehr.**

Informationssicherheit

3. Prävention als maßgebliche Leitungsaufgabe

Angesichts der Risiken ist die Gewährleistung einer bestmöglichen Informationssicherheit eine der maßgeblichen Leitungsaufgaben für Unternehmen, Behörden und andere Institutionen. Insbesondere Cyberkriminalität ist mittlerweile zur bitteren täglichen Realität geworden. Vor allem digitale Überfälle haben während der Verbreitung des Homeoffice – begünstigt durch schlecht gesicherte Homeoffice-Rechner – sowohl in Umfang, Häufigkeit und Intensität stark zugenommen.

Folgende Gemeinsamkeiten sind hier meist festzustellen:

- Die Cyberattacken treffen die **angegriffene Institution weitgehend unvorbereitet**, ggf. trotz getroffener Schutzmaßnahmen.
- Sie bergen ein **ggf. existentielles Risiko** für den Angegriffenen, z. B. durch Betriebsunterbrechungen bzw. Wiederherstellungskosten.
- Die Angegriffenen müssen **mit hohem Zeitdruck weitreichende Entscheidungen treffen**, die auch **haftungsrelevant** sein können.
- **Cyberversicherungsschutz** ist meist nur **unzureichend verfügbar** und deckt allenfalls einen Teil des möglichen Schadens ab, der einen beachtlichen Prozentsatz des Umsatzes ausmachen kann.

Informationssicherheit

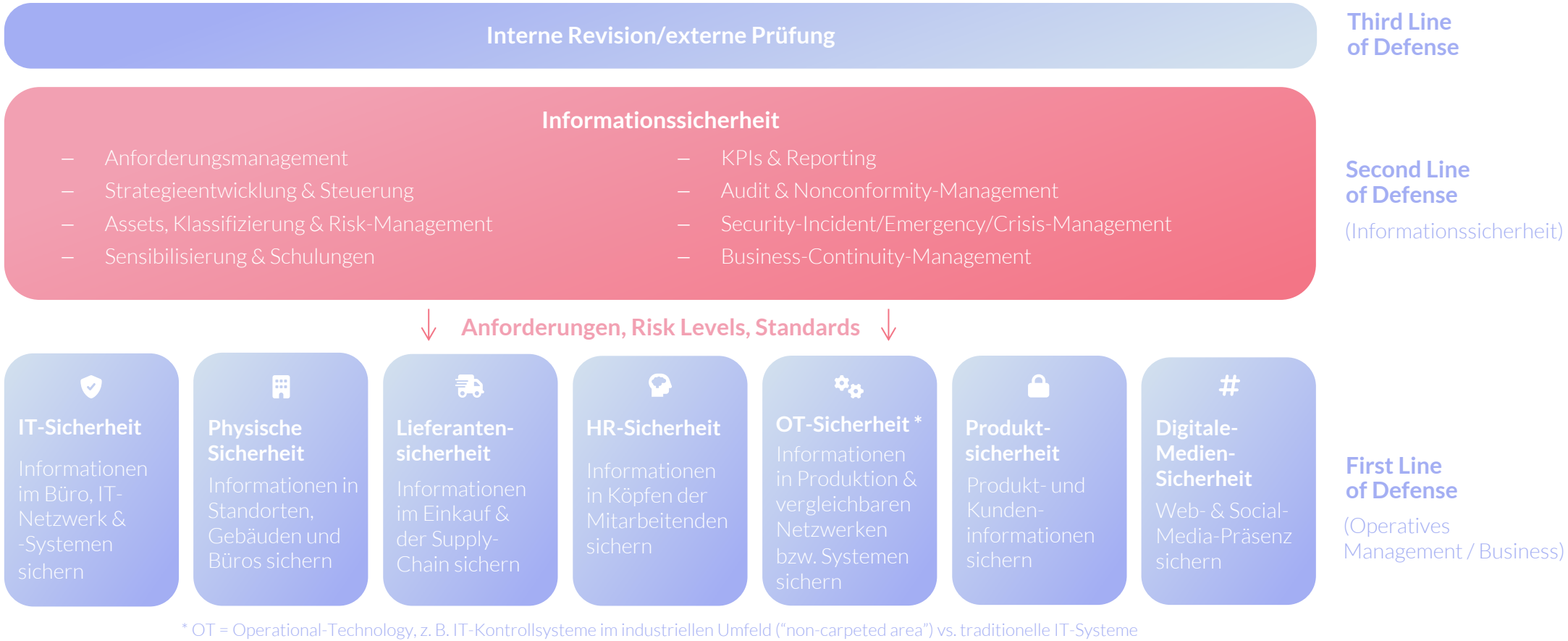
3. Prävention als maßgebliche Leitungsaufgabe

Vor diesem Hintergrund ist es unverzichtbar, für Angriffe auf die Informationssicherheit bestmöglich Vorsorge zu treffen, um den Ernstfall entweder von vornherein zu verhindern oder jedenfalls kontrollierbar zu machen.

Dieser Leitfaden soll insbesondere für Unternehmen und vergleichbare Institutionen eine praktische Hilfestellung bieten. Beschrieben werden ein empfehlenswertes Organisationsmodell mit dem klassischen 3-Lines-of-Defense-Set-Up sowie die wesentlichen Aspekte, welche zur Prävention bzw. Bewältigung von Angriffen auf die Informationssicherheit zu beachten sind.

Informationssicherheit

4. Das 3-Lines-of-Defense-Modell



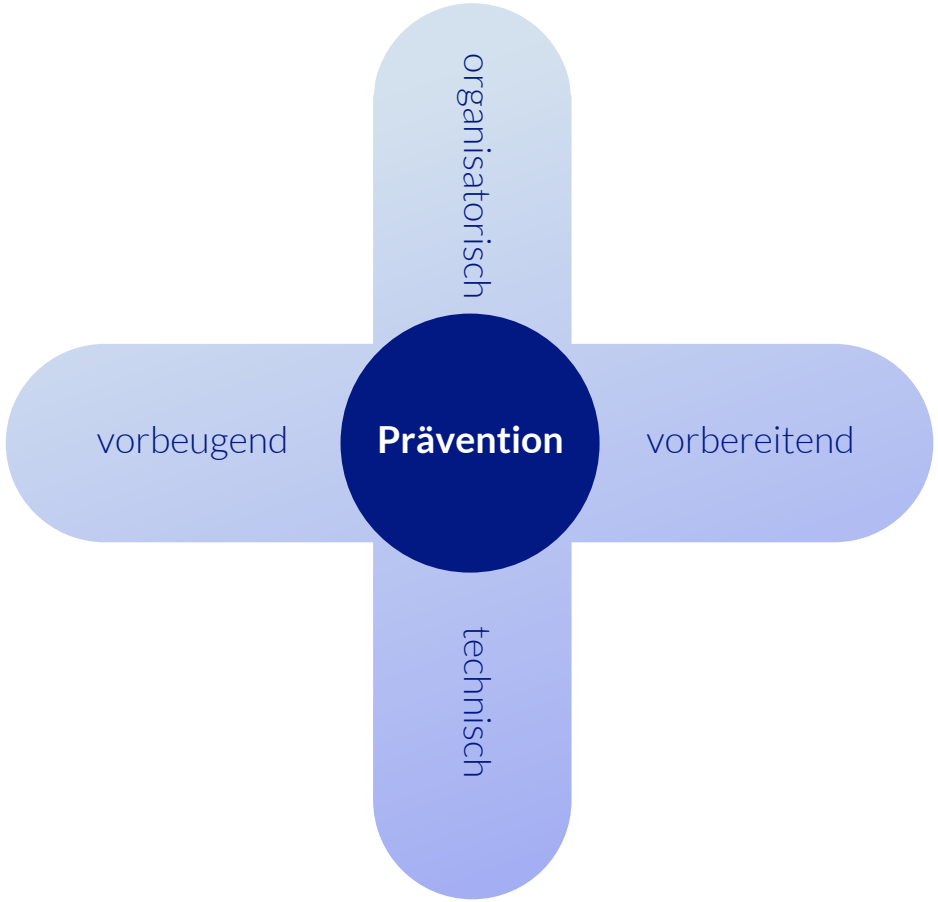
* OT = Operational-Technology, z. B. IT-Kontrollsysteme im industriellen Umfeld ("non-carpeted area") vs. traditionelle IT-Systeme

Informationssicherheit (2nd Line of Defense)

5. Das Fundament der Prävention

Eine erfolgreiche Prävention gegen Risiken der Informationssicherheit richtet sich nach vier Dimensionen aus. Hierbei gilt:

- **Organisatorische Maßnahmen** werden in der Aufbau- und Ablauforganisation verankert.
- **Technische Maßnahmen** lassen sich durch Einsatz entsprechender Technologie erreichen.
- **Vorbeugende Maßnahmen** sichern und härten das Unternehmen, um einen Angriff zu erschweren.
- **Vorbereitende Maßnahmen** schaffen im Fall eines erfolgten Angriffs die Basis für ein schnelles, angemessenes und präzises Handeln des Unternehmens.



5.1 Vorbeugende organisatorische Maßnahmen

Geschäftsleitung/Aufsichtsorgane

- Geeignete **Governance-Struktur** sicherstellen, z. B. durch
  - das Etablieren eines 3-Lines-of-Defense-Modells mit klar zugeordneten Zuständigkeiten (Seite 14)
- Ein **Information-Security-Management-System** (ISMS) mit einem **Chief-Information-Security-Officer** (CISO) mit ausreichenden Ressourcen, direkten Berichtswegen und regelmäßiger Berichterstattung an die Verwaltung etablieren (Seite 15)
- Vorhandene IT-Systeme (einschließlich deren Schnittstellen mit anderen IT-Systemen) inventarisieren und als IT-Infrastrukturlandkarte aktuell halten (Seite 16)
- Angemessene Prozesse schaffen, diese sind z. B.
  - fortlaufende Risikoanalyse und Risikomanagement
  - On- und Off-Boarding-Prozesse von Mitarbeitenden
- ISMS regelmäßig intern prüfen bzw. extern auditieren lassen (z. B. ISO 27001)

Interne und Externe

- Alle Mitarbeitenden adressatengerecht und fortlaufend über die Risiken zur Informationssicherheit sensibilisieren (Seite 17)
- Berufliches und Privates strikt trennen
- Externe Expertise für den Notfall sichern
  - **Security-Office-Center** intern einrichten / extern beauftragen
  - IT-Dienstleister-Vereinbarungen zur Unterstützung bei Cyberangriffen, wie Distributed-Denial-of-Service (DDoS), Ransomware, Hacking der Website etc., abschließen
- Vorbild sein, wenn es um den täglichen Umgang mit Themen der Informationssicherheit geht.

5.2 Vorbeugende technische Maßnahmen

IT- und OT-Management

- Tests/Freigaben für Änderungen der IT-Infrastruktur bzw. Software vorsehen
- Aufbau eines Identity-Managements
- Außerbetriebnahme, Aussonderung, Löschung und Vernichtung von IT-Infrastruktur, Software bzw. Daten sicherstellen
- Penetrations-Tests/Phishing-Tests durchführen
- Patch-Management durchführen (Seite 19)
- Privilegierte Accounts begrenzen (Seite 20)
- Wechselseitige Systemverbindungen reduzieren
- Bei Produkt-/Technologieentwicklung zukünftige Cyberrisiken berücksichtigen (**Cyber-Security-by-Design**) (Seite 21)
- Informationssicherheit bei Lieferanten/ Subunternehmen/Kunden überprüfen (Seite 22)

IT- und OT-Technologie

- Die Gebäudesicherheit gewährleisten und Zutritts- bzw. Verhaltensregeln etablieren
- Internen und externen Netzwerkzugang absichern, z. B. über inventarisierte Geräte bzw. per VPN
- Passwortregeln vorschreiben und technisch durchsetzen (Seite 23)
- Programme zum Schutz vor Schadsoftware einsetzen
- Virenscanner benutzen / Firewall unterhalten / Netzwerke segmentieren (Netzplan)
- Sorgsamen Umgang mit Wechseldatenträgern und Cloudspeichern sicherstellen
- Ausweich-Arbeitsplätze für den Notfall schaffen (Seite 24)

5.3 Vorbereitende organisatorische Maßnahmen

Notfallpläne und Business-Continuity-Management

- Business-Continuity-Management sicherstellen
- Notfall- bzw. Alarmierungsplan aufstellen und regelmäßige Notfallübungen abhalten (Seite 26)
- Kommunikationsplan mit Mitteilungsentwürfen aufstellen (Seite 27)
- Abschluss einer Cyberversicherung prüfen (Seite 28)

Inventarisierung und Listen

- Die wichtigsten IT-Systeme und IT-Prozesse („Kronjuwelen“) definieren und priorisieren (Seite 29)
- Interne Ansprechpartner festlegen sowie Reihenfolge der Benachrichtigung bestimmen (Seite 30)
- Externe Ansprechpartner festlegen sowie Reihenfolge der Benachrichtigung bestimmen (Seite 31)
- Wesentliche Listen und Kontaktdaten offline bzw. ausgedruckt vorhalten

5.4 Vorbereitende technische Maßnahmen

Monitoring und Back-up-Strategie

- Angemessenes Monitoring durchführen (Seite 33)
- Back-up-Strategie definieren und umsetzen (Seite 34)
- Recovery-Tests durchführen (Seite 35)

Protokollierung

- Protokollierung und Detektion sicherstellen (Seite 36)

Maßnahmenblätter

5.1 Vorbeugende organisatorische Maßnahmen

5.2 Vorbeugende technische Maßnahmen

5.3 Vorbereitende organisatorische Maßnahmen

5.4 Vorbereitende technische Maßnahmen

5.1.1 Vorbeugende organisatorische Maßnahmen

Governance-Struktur sicherstellen

Maßnahmen
- In der Geschäftsordnung festlegen, wer in der Geschäftsführung/Vorstand für ISMS zuständig ist.
- 3-Lines-of-Defense-Modell mit klaren Verantwortlichkeiten etablieren (z. B. 1. operativer Manager, 2. CISO, 3. interne Revision)
- Die notwendigen personellen Ressourcen und Sachmittel für das ISMS und den CISO im jährlichen Budget und Mittelfristplanung zur Verfügung stellen
- Direkte Berichtslinie bzw. Vortragsrecht des CISO an den zuständigen Geschäftsführer/Vorstand etablieren
- ISMS Board/Steering-Committee mit Beteiligung relevanter Unternehmensfunktionen mit regelmäßigen (mind. quartärliche) Sitzungen etablieren
- Regelmäßige (mind. monatliche) Jour-Fixe-Termine des CISO mit zuständigem Geschäftsführer/Vorstand sicherstellen
- Regelmäßige (mind. quartärliche) sowie anlassbezogene Sofort-Berichterstattung des CISO an Geschäftsführung/Vorstand sicherstellen
- Regelmäßige (mind. jährliche) sowie anlassbezogene Sofort-Berichterstattung des CISO an Aufsichtsrat bzw. zuständige Aufsichtsratsausschüsse sicherstellen
- Regelmäßige (mind. 2-jährliche) interne und/oder externe Audits in Bezug auf die First Line und die Second Line of Defense anhand gängiger Standards durchführen
- Audit-Ergebnisse der Prüfung in Verantwortung der Geschäftsführung umsetzen
- Für rasche Integration neu erworbener Geschäftsaktivitäten in das ISMS ist Sorge zu tragen
- Forensik-Teams für den Notfall definieren

Ergebnis
- Dokumentierte Zuordnung von Verantwortungen für Informationssicherheit innerhalb und jenseits der Geschäftsführung bzw. Aufsichtsorgane

Weiterführende Information
- BSI-Standard 200-1 "Managementsysteme für Informationssicherheit (ISMS) – www.bsi.bund.de/gs-standards

5.1.2 Vorbeugende organisatorische Maßnahmen

ISMS mit CISO etablieren

Maßnahmen
- CISO mit Verantwortung für ISMS und hinreichender Expertise und Unabhängigkeit (einschließlich Zutrittsrecht zu allen Bereichen, in denen Informationstechnik eingesetzt wird) benennen, der mit eigenen personellen Ressourcen und Sachmitteln ausgestattet ist (eigenes Budget neben dem IT-Budget).
- Mitverantwortlichkeit des operativen Managements als First Line of Defense für Informationssicherheit bis hinunter zu den Einzelgesellschaften bzw. Reporting-Units durch entsprechende Rollenzuweisung sicherstellen – regelmäßige Sitzungen des Program-Leadership-Teams mit allen relevanten Verantwortlichen abhalten
- Regelmäßige (mind. jährliche) Risikoanalyse durchführen, Maßnahmen ableiten und umsetzen. Dazu gehört eine entsprechende Nachverfolgung der Maßnahmen durch CISO und ggf. Eskalation zur Geschäftsführung/Vorstand bei mangelnder Umsetzung.
- Angemessenes ISMS-Richtlinienwerk mit erforderlichen Durchgriffsrechten des CISO erlassen (ggf. unter Beteiligung des Betriebsrats) und regelmäßig aktualisieren
- Strategischen Mittelfristplan (3-5 Jahre) zur Fortentwicklung des ISMS aufstellen und verfolgen
- Berücksichtigung von Querschnittsthemen sicherstellen (z. B. Datenschutz)

Ergebnis
- CISO und ISMS mit Expertise und hinreichendem Budget

Weiterführende Information
- IT-Grundschutz-Kompendium – www.bsi.bund.de/gs-kompendium
- Online-Kurs - Informationssicherheit mit IT-Grundschutz – www.bsi.bund.de/grundschutzkurs

5.1.3 Vorbereitende technische Maßnahmen

Aktuelle IT-Infrastrukturlandkarte gewährleisten

Maßnahmen
- Ein Schaubild der System- und Schnittstellenlandschaft mit Netzwerkübergängen (IT-Infrastrukturlandkarte) erstellen
- Ein IT-Asset-Register führen und mit dem Schaubild der System- und Schnittstellenlandschaft abgleichen
- Einen Systemsteckbrief pro System mit technischen, fachlichen und organisatorischen Angaben erstellen, einschließlich des Vitalitätsgrads (Kronjuwelen) und der Sensitivität (Schadenpotential)
- IT-Infrastrukturlandkarte und IT-Asset Register kontinuierlich pflegen und aktualisieren

Ergebnis
- IT-Infrastrukturlandkarte und IT-Asset-Register zur Ausfallfolgeabschätzung und Krisenreaktion

Weiterführende Information
- Universität Potsdam: Architekturen betrieblicher Anwendungssysteme. Aufnahme und Visualisierung von IT-Landschaften wi.uni-potsdam.de

5.1.4 Vorbeugende organisatorische Maßnahmen

Alle Mitarbeitenden sensibilisieren

Maßnahmen
- Alle Mitarbeitenden, die über Systemzugänge verfügen, hierarchieunabhängig sowohl bei Einstellung als auch später regelmäßig (z. B. alle sechs Monate und bei aktuellem Bedarf) über das Thema Informationssicherheit informieren zu:
  - Allgemeinen Themen: Arten von Cyberangriffen und deren Häufigkeit, mögliche Risiken und Schäden für das Unternehmen, IT-Sicherheitspolitik des Unternehmens etc.
  - Individuellen Pflichten: Passwortbildung, Umgang mit Wechseldatenträgern, Umgang mit unklaren E-Mails/Anhängen (z. B. wer ist zu informieren / wer kann helfen)
- Externe Dienstleister/Leiharbeitskräfte wie oben sensibilisieren, aber zusätzliche schriftliche Bestätigungen, Vertraulichkeitsvereinbarungen einholen
- Auf geeignete Kommunikationsmittel achten! (online, per Video, Präsenzveranstaltung, ggf. – in Absprache mit Betriebsrat – auf Betriebsversammlung, schriftlich – nicht jeder hat ständig einen PC-Arbeitsplatz!)
- Spezifische Mitarbeitenden-Gruppen für ergänzende Sensibilisierungsmaßnahmen identifizieren und schulen, z. B. Assistenzen, R&D, Rechnungswesen etc.
- Sensibilisierungsmaßnahmen durch CISO-Organisation in Zusammenarbeit mit HR durchführen
- Hundertprozentige Abdeckung der relevanten Mitarbeitenden und externen Dienstleister / Leiharbeitskräfte bei Sensibilisierungsmaßnahmen anstreben und Schulungsteilnahmen dokumentieren

Ergebnis
- Übersicht über die geschulten Mitarbeitenden

Weiterführende Information
- Online-Kurs - Informationssicherheit mit IT-Grundschutz – www.bsi.bund.de/grundschutzkurs
- "Fortschrittliche Angriffe - Neue Qualität aktueller Angriffe und Prognose" – www.bsi.bund.de/ransomware

Maßnahmenblätter

5.1 Vorbeugende organisatorische Maßnahmen

5.2 Vorbeugende technische Maßnahmen

5.3 Vorbereitende organisatorische Maßnahmen

5.4 Vorbereitende technische Maßnahmen

5.2.1 Vorbeugende technische Maßnahmen

Patch-Management durchführen

Maßnahmen
- Aktuelle Übersicht aller IT-Systeme inklusive der zu aktualisierenden Systeme in einer Inventarliste bereithalten (Inventur der Assets als Voraussetzung)
- Auto-Update-Funktionen der IT-Assets nutzen, wo immer möglich (i. d. R. bei Desktop-Systemen)
- Sicherheitsrelevante Patches und Fehlerbehebungen regelmäßig und zeitnah installieren
- Angemessenes Patch-Intervall für jedes relevante IT-System festlegen, sofern nicht jeweils ein sofortiges Patch erforderlich ist.
- Unternehmensweiten Patch-Day einführen
- Priorisierung notwendiger Patches und sofortige Installation bei sicherheitsrelevanten Patches vornehmen
- Tests der Patch-Einspielungen durchführen
- Systeme austauschen, die nicht mehr aktualisierbar sind oder Mitigationsmaßnahmen treffen (z. B. Separation der Systeme vom übrigen Netzwerk)

Ergebnis
- Dokumentation über alle Systeme und ihren Patch-Stand

Weiterführende Information
- Patch-Management: Schließen Sie Sicherheitslücken auf Knopfdruck! – www.datenschutz-praxis.de

5.2.2 Vorbeugende technische Maßnahmen

Privilegierte Accounts begrenzen

Maßnahmen
- Rollen und Berechtigungsstrukturen definieren und eindeutige Kennung von privilegierten Nutzern/Administratoren sicherstellen
- Gewährleisten, dass jeder Nutzer unter seiner eigenen Kennung arbeitet
- Prozesse für die (erweiterte/privilegierte) Berechtigungsvergabe definieren
- Technisches Privileged-Identity-Management (PIM) einführen zur Verwaltung der privilegierten Nutzer und Administratoren, „Need-to-have"-Prinzip)
- Hierarchie von privilegierten Nutzern und deren Rechten schaffen (Differenzierung im Active-Directory)
- Zugriff von Administratoren auf Accounts protokollieren und überwachen, um Auffälligkeiten zu prüfen (Session-Protokolle)
- Regeln für privilegierte Nutzer/Administratoren aufstellen, die ihnen nur die für deren Tätigkeit unbedingt notwendigen Zugriffe erlauben.
- „Gruppenaccounts" (ein Account mit mehreren Usern) eliminieren bzw. weitestmöglich minimieren
- Privilegierte und nicht-privilegierte Accounts trennen (keine Superuser-Rechte für User-Accounts)

Ergebnis
- Session-Protokolle weisen Auffälligkeiten auf => Zugriffsrechte weiter einschränken
- Anzahl der privilegierten Nutzer weiter differenzieren und reduzieren

Weiterführende Information
- Privilegierte Nutzer richtig verwalten – https://www.computerwoche.de/a/privilegierte-nutzer-richtig-verwalten,2547804
- ISO 27001 Anforderung und ISO 27002 Code of Practice
- Sarbanes-Oxley Act / SAS70/SSAE16 oder Basel II

5.2.3 Vorbeugende organisatorische Maßnahmen

Cyber-Security-by-Design sicherstellen

Maßnahmen
- Mindestanforderung an die Informationssicherheit bei der Entwicklung, Einführung und Pflege von Assets definieren, z. B. spezifische Vorgaben für die Software-Erstellung bzw. Webanwendungen
- Prozesse mit wirksamen Kontrollen für den Lebenszyklus von Assets definieren, einführen und überwachen (z. B. Bedarfsanalyse, Entwicklung, Einführung, Testverfahren, Produktivsetzung, Änderungsverfahren, Dekommissionierung)
- Dokumentation und regelmäßige Überprüfung aller Maßnahmen durchführen

Ergebnis
- Regelwerk-Mindestanforderung
- Katalog der Risikoprozesse und Prozesskontrollen für die Informationssicherheit

Weiterführende Information
- TeleTrusT - Bundesverband IT-Sicherheit e.V. – www.teletrust.de
- Software development with Data Protection by Design and by Default – www.datatilsynet.no
- Software and Hardware Weaknesses – http://cwe.mitre.org/data/index.html
- Open Web Application Security Project – OWASP Top Ten für Web-Anwendungen

5.2.4 Vorbeugende organisatorische Maßnahmen

Informationssicherheit bei Kunden, Zulieferern, Subunternehmern überprüfen

Maßnahmen
- Mindeststandards für Informationssicherheit in Bezug auf Kunden, Zulieferer, Subunternehmer (z. B. ISO) festlegen
- Maßnahmenplan zur regelmäßigen Überprüfung der Einhaltung der Standards erstellen
- Alle Maßnahmen dokumentieren, auch durch den Zulieferer/Subunternehmer/Kunden
- Zuordnung und Priorisierung der Kunden, Zulieferer, Subunternehmer nach Kritikalität gewährleisten
- Schulung von ausgewählten Mitarbeitenden der Zulieferer/Subunternehmer/Kunden durchführen
- Bestellung eines Sicherheitsbeauftragten bzw. Ansprechpartner beim Zulieferer/Subunternehmer/Kunden sicherstellen
- Auditrechte bei Lieferanten einräumen lassen und ausüben

Ergebnis
- Ranking der Geschäftspartner nach Kritikalität bei Informationssicherheit anhand von Fragelisten/Checklisten
- Maßnahmenplan und Umsetzungsfortschritt

Weiterführende Information
- ISO - ISO/IEC 27036-1:2014 - Information security for supplier relationships - Part 1: Overview and concepts www.iso.org/standard/59648.html

5.2.5 Vorbeugende technische Maßnahmen

Passwortregeln vorschreiben

Maßnahmen
- Zwei-Faktor-Authentifizierung oder andere starke Authentifizierungsmethoden (z. B. Fingerprint) vorschreiben
- Systeme so konfigurieren, dass nur Passworte mit mindestens 12 Zeichen (bestehend aus Klein- und Großbuchstaben mit Zahlen und Sonderzeichen) möglich sind.
- Passwort bei gegebenen Anlässen schnellstmöglich ändern
- Passwortgeneratoren/-manager einführen
- Triviale Passworte abweisen (z. B. Passwort123#, keine Wortwiederholungen, keine Tastaturmuster)
- Verhindern, dass auf verschiedenen Systemen das gleiche Passwort verwendet werden kann (Ausnahme: Single-Sign-On).

Ergebnis
- Erweiterung der Übersicht der IT-Infrastrukturlandkarte um den Grad der technisch erzwungenen Passwortregeln je System:
  weiß: Systeme, bei denen ein Benutzerlogin nicht notwendig ist.
  rot: keine der Passwortregeln technisch erzwungen
  gelb: teilweise Einhaltung der Passwortregeln technisch erzwungen
  grün: vollständige Einhaltung aller Passwortregeln technisch erzwungen

Weiterführende Information
- Sichere Passwörter erstellen – www.bsi.bund.de

5.2.6 Vorbeugende technische Maßnahmen

Ausweich-Arbeitsplätze schaffen

Maßnahmen
- Sicheres mobiles Arbeiten ermöglichen, sodass Mitarbeitende zu jeder Zeit von jedem Ort aus in Bezug auf Computernutzung, Telefonie und Dokumentenzugang arbeitsfähig sein können, z. B. möglich über virtualisierte Arbeitsplätze.
- Die Ausweich-Arbeitsplätze regelmäßig auf Sicherheit und technische Funktionsfähigkeit überprüfen
- Regelmäßige Notfallübungen durchführen sowie einen regelmäßigen Verbesserungsprozess zu den Ergebnissen der Notfallübungen sicherstellen

Ergebnis
- Übersicht aller Mitarbeitenden zu der Sicherheit und Funktionsfähigkeit ihrer Ausweich-Arbeitsplätze

Weiterführende Information
- Sicherer Fernzugriff auf das interne Netz (ISi-S) – www.bsi.bund.de

Maßnahmenblätter

5.1 Vorbeugende organisatorische Maßnahmen

5.2 Vorbeugende technische Maßnahmen

5.3 Vorbereitende organisatorische Maßnahmen

5.4 Vorbereitende technische Maßnahmen

5.3.1 Vorbereitende organisatorische Maßnahmen

Notfall- und Alarmierungsplan erstellen

Maßnahmen
- Handbuch für Notfälle (Information-Security-Event, Incident, Emergency, Crisis-Management) aufstellen und regelmäßig auf Aktualität überprüfen
- Krisenstab unter Einbindung aller relevanten Unternehmensfunktionen und unter Leitung eines Krisenmanagers definieren und im Fall der Fälle aktivieren
- Abläufe und Kommunikationswege für entsprechende Notszenarien festlegen, einschließlich virtueller oder tatsächlicher Besprechungsraum inklusive Ausweichorte
- Notfallpläne regelmäßig üben

Ergebnis
- Aktuelle Notfallpläne, die auch in Probesimulationen geübt werden
- Protokoll der Notfallübung mit Verbesserungsmaßnahmen, die umgesetzt werden

Weiterführende Information
- Business Continuity Management gemäß BSI Standard 200-4 (Entwurf)

5.3.2 Vorbereitende organisatorische Maßnahmen

Kommunikationsplan erstellen

Maßnahmen

- **Externe Kommunikation vorbereiten**
    1. Allgemein: durch Pressesprecher oder definiertes Mitglied der Geschäftsführung
    2. Operative Ebene (Kunden, Lieferanten etc.):
    - Leiter der entsprechenden Abteilung/Einheit unter Verwendung der vom Pressesprecher bzw. Geschäftsführung/Vorstand festgelegten Sprachregelung
    - CISO bzw. zuständige Funktionsverantwortliche mit z. B. BSI, Versicherungen, externen Dienstleistern zur Bewältigung der Lage
    - Rechtsabteilung, insbesondere in Hinblick auf mögliche Ad-hoc-Mitteilungen und Behördenmeldungen
- **Interne Kommunikation vorbereiten**
  Vorgesetzte mit ihren Mitarbeitenden unter Verwendung der vom Geschäftsführung/Vorstand festgelegten Sprachregelung
- Liste von Ansprechpartnern offline oder als Ausdruck hinterlegen (physische Trennung)

Ergebnis

- Vorliegen eines Kommunikationsplans nach außen und nach innen mit entsprechenden Mitteilungsentwürfen

Weiterführende Information

- Checkliste Organisatorisches - https://bsi.bund.de

5.3.3 Vorbereitende organisatorische Maßnahmen

Abschluss einer Cyberversicherung prüfen

Maßnahmen
- Als Geschäftsführung/Vorstand (schon aus Haftungsgründen) über den Nutzen einer Cyberversicherung entscheiden
  - Die Entscheidung auf Basis einer Risikoanalyse oder eines Risk-Audits fällen
  - Eine etwaige ablehnende Entscheidung dokumentiert begründen
- Die Versicherungsbedingungen, die beachtet werden müssen, den relevanten Unternehmensfunktionen und Mitarbeitenden im Unternehmen zur Kenntnis bringen.
- Auflagen der Versicherung im Zeitplan umsetzen und dauerhaft einhalten
- Versicherungsmakler für die Auswahl und Kommunikation mit der Versicherung einschalten
- Versicherungsumfang/-leistung auch unter Berücksichtigung der Betriebsunterbrechungsversicherung näher definieren
- Kontinuierliches Monitoring der Risikolage im Hinblick auf Vertragsverlängerungen durchführen

Ergebnis
- Dokumentierte Geschäftsführer-/Vorstandsentscheidung zum Einkauf von Cyberversicherungsschutz
- Maßnahmenplan für die Umsetzung der Versicherungsbedingungen

Weiterführende Information
- Cyber-Versicherung: Der Schutz vor Hacker-Angriffen? – www.gruender.de/versicherungen/cyber-versicherung/
- Betriebsunterbrechungsversicherung

5.3.4 Vorbereitende organisatorische Maßnahmen

„Kronjuwelen“ auflisten und priorisieren

Maßnahmen
- Die Systeme aus der IT-Infrastrukturlandkarte, welche verantwortlich für den Großteil der Unternehmensergebnisses sind oder deren Daten einer besonderen Vertraulichkeit unterliegen (z. B. besondere personenbezogene Daten, wie etwa Gesundheitsdaten oder Daten des Zahlungsverkehrs), identifizieren und im Business-Continuity-Management priorisieren
- Ausreichende Kommunikation zwischen IT-Administration und Controlling sicherstellen
- Besondere Schutzmaßnahmen (aktuellste Patches) auf diesen „Kronjuwel-Systemen“ gewährleisten
- Redundante Datenhaltung für diese „Kronjuwel-Systeme“ vorsehen

Ergebnis
- Liste der „Kronjuwelen“, also der Systeme, die für die Unternehmensergebnisse von größter Bedeutung sind
- Besondere Sicherung der „Kronjuwelen“-Systeme

Weiterführende Information
- Die „Kronjuwelen“ der IT-Infrastrukturlandkarte vor Bedrohungen schützen – www.it-daily.net

5.3.5 Vorbereitende organisatorische Maßnahmen

Interne Ansprechpartner auflisten

Maßnahmen

- Eine Liste aller internen Ansprechpartner (Krisenstab, IT etc.) erheben und offline bzw. ausgedruckt bereithalten
  - bei IT-Ansprechpartnern mit Zuordnung zu den IT-Bereichen, Systemen, Aufgaben und Verantwortlichkeiten
- Diese Liste mit der Infrastrukturlandkarte und Übersicht der IT-Infrastrukturlandkarte abgleichen und den Abdeckungsgrad feststellen bzw. komplettieren
- Notfall-Kontaktkanäle (z. B. Messenger-Dienst) unter Berücksichtigung des Datenschutzes erheben und bereithalten
- Hinreichende Erreichbarkeit (auch außerhalb normaler Bürozeiten) gewährleisten, ggf. mit Bereitschaftsplan
- Für den Fall der Nichtverfügbarkeit von relevanten Mitarbeitenden Vertretungslösungen sicherstellen

Ergebnis

- Erweiterung der Übersicht der IT-Infrastrukturlandkarte um den oder die Notfall-IT-Kontakte:
  rot: keine Notfall-IT-Kontakte bekannt
  gelb: Notfall-IT-Kontakte bekannt, aber Bereitschaft nicht sichergestellt
  grün: Notfall-IT-Kontakte bekannt und Bereitschaft und Erreichbarkeit sichergestellt

5.3.6 Vorbereitende organisatorische Maßnahmen

Externe Ansprechpartner auflisten

Maßnahmen
Kontaktliste über folgende externe Institutionen erstellen:
- IT-Support wie
  - Forensik-Unternehmen
  - Hardwareaustausch
  - Softwaresupport
  - IT-Dienstleister (z. B. bei Cloud-Services)
- Kommunikationsexperten
- Rechtsberatung
- Behördenkontakte wie
  - Polizei, Bundes- bzw. Landeskriminalämter, Europol bei EU-grenzüberschreitendem Sachverhalt
  - Verfassungsschutz
  - Datenschutzbehörden
  - Sonstige Aufsichtsbehörden

Ergebnis
- Bereithaltung der aktuellen Kontaktliste offline bzw. ausgedruckt

Weiterführende Information
- Krisenkommunikation – https://bsi.bund.de

Maßnahmenblätter

5.1 Vorbeugende organisatorische Maßnahmen

5.2 Vorbeugende technische Maßnahmen

5.3 Vorbereitende organisatorische Maßnahmen

5.4 Vorbereitende technische Maßnahmen

5.4.1 Vorbereitende technische Maßnahmen

Angemessenes Monitoring durchführen

Maßnahmen
Technische Monitoring-Maßnahmen:
- Log-Dateien mind. 30 Tage vorhalten (Grundlage für Forensik)
- Log-Dateien regelmäßig nach Auffälligkeiten durchsuchen (automatisiert, ggf. über Dienstleister möglich)
- Teilnahme der Mitarbeitenden an den Sensibilisierungsmaßnahmen überwachen und dokumentieren – regelmäßig durchgeführte Maßnahmen an Geschäftsführung/Vorstand sowie Aufsichtsgremien berichten
- Test-E-Mails an Mitarbeitende (insbesondere solche mit privilegierten Zugriffsrechten) verschicken, um deren Verständnis zur richtigen Handhabung zu überprüfen

Ergebnis
- Berichterstattung über durchgeführte Monitoring-Maßnahmen

5.4.2 Vorbereitende technische Maßnahmen

Back-up-Strategie definieren und umsetzen

Maßnahmen
- Geschäftskritische Daten identifizieren
- Maximal akzeptable Zeiten für Datenverlust für Datenkategorien definieren und Back-up-Strategie daran anpassen (mind. alle 24 Stunden)
- Mindestens drei Datenkopien, zwei davon mit Speicherung auf mind. 2 Medienarten und eines an externem Standort, vorhalten (3-2-1-Regel)
- Dauerhaftes Monitoring der Back-up-Systeme und automatisierte Persistenz-Prüfungen der Back-ups durchführen
- Regelmäßige Rücksicherungstests durchführen (mind. 1x jährlich)
- Regelmäßig aktualisierte verschlüsselte Kopien existenzieller Daten erstellen und ohne Verbindung zum Unternehmensnetzwerk speichern
- Unterbrechungsfreie Stromversorgung sicherstellen
- Schriftliche Offline-Kopie essentieller Daten vorhalten

Ergebnis
- Minimierung von Datenverlusten
- Sicherstellung von Kommunikationsfähigkeit im Krisenfall

Weiterführende Information
- CON.3 Datensicherungskonzept / Backup – https://www.bsi.bund.de
- Datensicherung und Datenverlust – https://bsi.bund.de

5.4.3 Vorbereitende technische Maßnahmen

Recovery-Tests durchführen

Maßnahmen
- Business-Continuity und Desaster-Recovery-Pläne aufstellen
- Notfälle regelmäßig (mind. jährlich) mit Beteiligung der Hauptverantwortlichen im definierten Krisenstab üben
- Notwendige Anpassungen, die aus den Ergebnissen der Notfallübungen resultieren, zeitnah umsetzen
- Anlaufpläne (zur Herstellung des Notfallbetriebes und zur Rückkehr in den Normalbetrieb) testen
- Reihenfolge der Wiederanlaufsequenz testen

Ergebnis
- Vorliegen von Test- und Ergebnisprotokollen
- Maßnahmenliste

Weiterführende Information
- Business Continuity Management gemäß BSI Standard 200-4 (Entwurf)

5.4.4 Vorbereitende technische Maßnahmen

Protokollierung und Detektion sicherstellen

Maßnahmen
- SOC (Security-Operations-Center) einführen, das z. B. SIEM (Security-Information & Event-Management), Advance-Threat-Protection, IT-Security-Monitoring und IT-Risk-Detection umfasst
- Protokolldateien (Logs) von Betriebssystemen, Datenbanken und Anwendungen aufbewahren, idealerweise in einem SIEM-System unter Beachtung angemessener Aufbewahrungsfristen
- Zeitstempel synchron halten (NTP)
- Protokollsammlungen mit zentral verwalteter Infrastruktur für das Log-Management gewährleisten
- Zuordnungswerkzeuge nutzen, um eine ganzheitliche Sicht zu erlangen und die Anzahl der Fehlalarme zu reduzieren
- Zur Vereinfachung der Protokollprüfung durch die Erstellung von Berichten automatische Berichtsfunktionen verwenden
- Protokolle regelmäßig prüfen und analysieren
- Automatisierung eines Großteils des Protokollanalyseprozesses einführen
- Prüfungsverfahren durchführen, die eine Echtzeitüberwachung entsprechender Protokollereignisse beinhalten.
- Ein Alarmsystem auf Basis von Prioritäten erstellen
- Basiszusammenstellung typischer Protokolleinträge entwickeln, um ungewöhnliche oder unnormale Ereignisse oder Aktivitäten erkennen zu können

Ergebnis
- Alarmierung und Mitigation bei Anomalitäten
- Richtlinienkonforme Aufbewahrung von Protokolldaten

Weiterführende Information
- Telekommunikationsgesetz – https://www.gesetze-im-internet.de/
- Best Practices für das Log-Management – www.infopoint-security.de
- Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen – www.bsi.bund.de/

Publikationen und Quellen

Relevante Publikationen und Quellen :

Publikationen des Bundesamts für Sicherheit in der Informationstechnik:

- Die Lage der IT-Sicherheit in Deutschland: www.bsi.bund.de/lageberichte
- Fortschrittliche Angriffe - Neue Qualität aktueller Angriffe und Prognose: www.bsi.bund.de/ransomware
- BSI-Standards: www.bsi.bund.de/gs-standards
    - BSI-Standard 200-1 Managementsysteme für Informationssicherheit
    - BSI-Standard 200-2 IT-Grundschutz-Methodik
    - BSI-Standard 200-3 Risikomanagement
    - BSI-Standard 200-4 Business Continuity Management (Entwurf)
- IT-Grundschutz-Kompendium: www.bsi.bund.de/gs-kompendium
- Online-Kurs - Informationssicherheit mit IT-Grundschutz www.bsi.bund.de/grundschutzkurs
- Allianz für Cyber-Sicherheit: www.allianz-fuer-cybersicherheit.de

Publikationen der International Organization for Standardization (Hrsg.):

- ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary, ISO/IEC JTC 1/SC 27, 2018
- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC JTC 1/SC 27, 2013
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls, ISO/IEC JTC 1/SC 27, 2013
- ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management, ISO/IEC JTC 1/SC 27, 2018

Relevante Publikationen und Quellen :

Weitere Publikationen:

- BUJ Bundesverband der Unternehmensjuristen: www.buj-verband.de/buj/news/buj-bluepaper-it-sicherheit-guideline-fuer-unternehmensjuristen/

Podcasts:

- BSI – Cybersnacs Podcast: www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Netzwerk-Formate/Medien/Cyber-Sicherheits-Podcast/cyber-sicherheits-podcast_node.html
- Logbuch Netzpolitik: https://logbuch-netzpolitik.de/

Standards:

- VDS10000 für KMU: https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10000-informations-sicherheit-fuer-kmu
- CISIS12 für Behörden und KMU anlog zu ISO27001: https://cisis12.de/
- ISO27001: www.iso.org/isoiec-27001-information-security.html

Förderung:

- go-digital: Den Mittelstand auf dem Weg in die digitale Zukunft begleiten: www.innovation-beratung-foerderung.de/INNO/Navigation/DE/go-digital/go-digital.html