



IT-SECURITY

NIS-2 Richtlinie Checkliste

Liebe*r Leser*in,

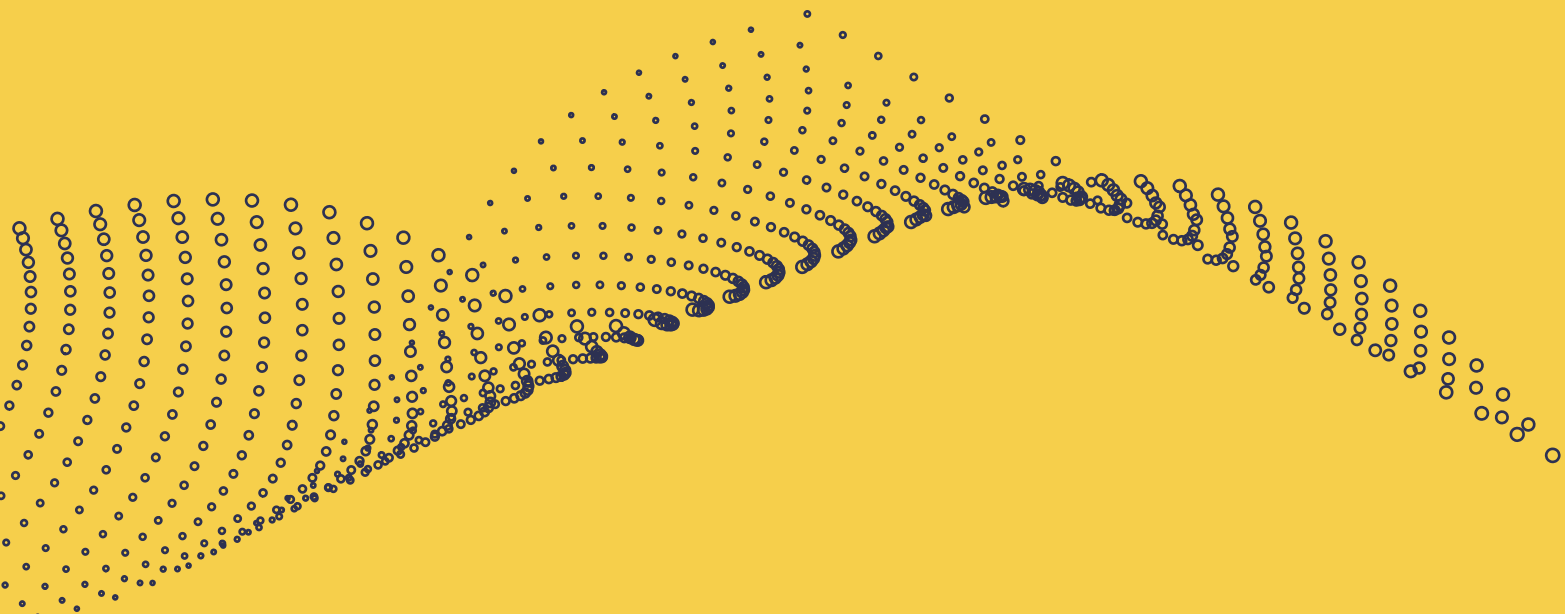
mit dieser Checkliste fassen wir dir die Punkte zur NIS-2 Compliance übersichtlich zusammen. Die Checkliste ist so aufgebaut, dass sie dem Gesetztext sowie den entsprechenden Maßnahmen strukturell folgt. Wenn du für dein Unternehmen alle Punkte abhaken kannst - herzlichen Glückwunsch, dann hast du bei der NIS-2 Umsetzung richtig gute Arbeit geleistet.

Die Checkliste kann dich auf deinem Weg zur NIS-2 Compliance begleiten und dir leicht verständlich aufzeigen, welcher Punkt als nächstes zu bearbeiten und zu berücksichtigen ist. Zwischendurch haben wir dir auch kleine Info-Kästen aufbereitet, damit hoffentlich keine Fragen zu dem vor allem technischen Begrifflichkeiten aufkommen. Oft geben wir dir auch Beispiele an die Hand, damit der Punkt auf der Checkliste angereichert und leichter verständlich ist.

Bei Fragen steht dir unser NIS-2 Expertenteam auch gerne zur Seite.

Inhaltsverzeichnis

1. Leitungsorgane	3
2. Sicherheitsrichtlinien	3
3. Risikomanagement	4
4. Verwaltung von Vermögenswerten	6
5. Personalwesen	8
6. Cybersicherheitskompetenzen und Cybersicherheitsschulungen	11
7. Sicherheit von Lieferketten	12
8. Zugangssteuerung	14
9. Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung	19
10. Kryptographie	22
11. Umgang mit Cybersicherheitsvorfällen	23
12. Betriebskontinuitäts- und Krisenmanagement	26
13. Umgebungsbezogene und physische Sicherheit	28



1. Leitungsorgane

Die Leitungsorgane einer Organisation übernehmen zentrale Aufgaben in der strategischen Steuerung und Überwachung der betrieblichen Aktivitäten. In diesem Kapitel wird untersucht, welche Rollen und Verantwortlichkeiten diese Organe innehaben und ob die Struktur der Organisation durch ein aktuelles Organigramm klar abgebildet ist. Darüber hinaus wird geprüft, ob die Zuständigkeiten der einzelnen Organe eindeutig definiert und abgegrenzt sind, um Transparenz und Effizienz sicherzustellen.

Gemäß NIS-2 versteht man unter einem Leitungsorgan eine oder mehrere natürliche Personen oder Gremien, die durch gesetzliche Vorgaben, Satzungen oder vertragliche Bestimmungen dazu befugt sind, die Geschäfte einer Einrichtung zu führen oder deren Führung zu kontrollieren. Dabei wird die tatsächliche Führungsebene erfasst. Laut den Erläuterungen zum NISG 2024 (abhängig von der finalen Gesetzgebung) zählen hierzu typischerweise Positionen wie der Vorstand, Geschäftsführer oder Aufsichtsrat einer Organisation (WKO, 10.07.24).

1.a. Rollen und Verantwortlichkeiten der Leitungsorgane

1. Organigramm und Struktur

Es gibt es ein aktuelles Organigramm, das die Struktur der Organisation klar darstellt und die Rollen und Verantwortlichkeiten der Leitungsorgane definiert.

2. Verantwortungsbereiche

Die Verantwortungsbereiche der einzelnen Leitungsorgane sind dokumentiert und klar abgegrenzt.

2. Sicherheitsrichtlinien

Das NIS-2 Gesetz versteht unter Sicherheitsrichtlinien formelle, schriftlich festgehaltene Vorgaben und Maßnahmen, die den Schutz kritischer Infrastrukturen und IT-Systeme gewährleisten sollen. Eine Sicherheitsrichtlinie definiert die strategische Sicherheitsziele, das beschreibt Risikomanagement und verweist auf alle relevanten spezifischen Sicherheitsvorgaben wie Richtlinien und Leitlinien.

Diese Richtlinien müssen regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Bedrohungslagen entsprechen. Darüber hinaus muss gewährleistet sein, dass alle Mitarbeiter die Sicherheitsrichtlinien kennen und leicht darauf zugreifen können, während die Funktionen, Aufgaben und Verantwortlichkeiten eindeutig dokumentiert und den betreffenden Personen zugewiesen sind.

2.a. Sicherheitsrichtlinien

1. Existenz und Dokumentation

Es gibt eine schriftlich festgehaltene Sicherheitsrichtlinie in der Organisation.

2. Aktualisierung und Überprüfung

Die Sicherheitsrichtlinie wird regelmäßig überprüft und bei Bedarf aktualisiert.

3. Kommunikation und Verfügbarkeit

Die Sicherheitsrichtlinie ist allen Mitarbeitern bekannt und leicht zugänglich.

2.b. Funktionen, Aufgaben und Verantwortlichkeiten

1. Dokumentation von Verantwortlichkeiten

Die spezifischen Funktionen, Aufgaben und Verantwortlichkeiten in Bezug auf die Sicherheitsrichtlinien sind klar dokumentiert.

2. Zuweisung und Klarheit

Die Rollen und Verantwortlichkeiten sind klar zugewiesen und allen betroffenen Mitarbeitern bekannt.

3. Risikomanagement

Das NIS2-Gesetz definiert Risikomanagementmaßnahmen als systematische Verfahren zur Erkennung und Steuerung von Risiken, die sich auf die Sicherheit von Netz- und Informationssystemen auswirken können. Diese Maßnahmen umfassen die Entwicklung klarer Richtlinien, die regelmäßige Überprüfung ihrer Wirksamkeit sowie die Sicherstellung, dass Organisationen proaktiv auf potenzielle Bedrohungen reagieren können. Ein zentraler Aspekt ist dabei die Dokumentation und unabhängige Überprüfung der Prozesse, um eine fortlaufende Verbesserung sicherzustellen.

Ein Beispiel für ein Risiko ist Phishing. Aus der speziellen Risikomanagementrichtlinie muss klar hervorgehen, wie wahrscheinlich der Eintritt von bestimmten Phishing-Risiken ist, welche Maßnahmen es dagegen oder im Falle des Eintritts gibt, welches Budget für den Fall eingeplant wäre.

3.a. Risikomanagementrichtlinie und Risikomanagementprozess

1. Existenz einer Richtlinie

Es gibt eine dokumentierte Risikomanagementrichtlinie in der Organisation.

2. Regelmäßige Aktualisierung

Die Risikomanagementrichtlinie wird regelmäßig überprüft und aktualisiert.

3. Risikomanagementprozess

Es ist ein klar definierter Risikomanagementprozess etabliert, der die Identifizierung, Bewertung und Behandlung von Risiken umfasst.

3.b. Beurteilung der Effektivität von Risikomanagementmaßnahmen

1. Wirksamkeit der Maßnahmen

Es gibt Verfahren (z.B. spezifische Person, die Checks durchführt) zur regelmäßigen Beurteilung der Wirksamkeit der implementierten Risikomanagementmaßnahmen.

2. Ergebnisdokumentation

Die Ergebnisse der Beurteilung werden dokumentiert und analysiert.

3. Kontinuierlicher Verbesserungsprozess

Auf Basis der Beurteilung werden kontinuierliche Verbesserungen der Risikomanagementmaßnahmen umgesetzt.

3.c. Überwachung der Einhaltung von Vorgaben

1. Regelmäßige Überprüfung

Die Risikomanagementmaßnahmen werden regelmäßig überprüft und angepasst.

2. Berichterstattung

Es gibt klare Berichtswege und Verantwortlichkeiten für die Überwachung der Einhaltung der Vorgaben.

3.d. Unabhängige Überprüfungen

Derzeit gibt es aufgrund der unklaren Rechtslage keine Definition davon, wer eine unabhängige Überprüfung durchführen kann. Es gibt Stand Herbst 2024 noch keine spezifischen Auditoren, allerdings kann davon ausgegangen werden, dass ein passender IT-Dienstleister oder auch die qualifizierte Stelle der NIS-2 Behörde selbst eine unabhängige Überprüfung durchführen könnte.

1. Externe Audits

Unabhängige Überprüfungen oder externe Audits werden zur Beurteilung der Risikomanagementprozesse und -maßnahmen durchgeführt.

2. Dokumentation der Ergebnisse

Die Ergebnisse der unabhängigen Überprüfungen werden dokumentiert und analysiert.

3. Umsetzung von Empfehlungen

Die Empfehlungen aus den unabhängigen Überprüfungen werden in die Risikomanagementprozesse integriert und umgesetzt.

4. Verwaltung von Vermögenswerten

Im Rahmen der NIS-2 Richtlinie stehen Vermögenswerte (Assets) im Zentrum der Betrachtung, da sie entscheidend für die Sicherheit kritischer Infrastrukturen und digitaler Systeme sind.

Vermögenswerte umfassen nicht nur physische Güter wie Server oder Netzwerke, sondern auch immaterielle Werte wie Daten, Software und Wissen.

Im Kontext von NIS-2 ist es essenziell, diese Vermögenswerte genau zu identifizieren, zu bewerten und zu schützen, da sie Ziel potenzieller Angriffe sein können. Das Gesetz fordert von Unternehmen und Organisationen, Risiken zu minimieren und Sicherheitsmaßnahmen auf den Schutz dieser Vermögenswerte abzustimmen. Dies umfasst sowohl technische als auch organisatorische Maßnahmen.

Die Identifikation von Schwachstellen und die regelmäßige Aktualisierung der Sicherheitsstrategie stehen dabei im Vordergrund, um Gefahren frühzeitig zu erkennen und angemessen zu reagieren. Vermögenswerte bilden somit das Fundament für die Resilienz von IT-Systemen und deren Fähigkeit, Bedrohungen abzuwehren.

4.a. Inventarisierung von Vermögenswerten

1. Inventar der Systeme

Es gibt ein aktuelles Inventar aller IT-Systeme.

2. Inventar der Softwareplattformen

Es gibt ein aktuelles Inventar aller Softwareplattformen.

3. Inventar der Softwarelizenzen

Es gibt ein aktuelles Inventar aller Softwarelizenzen.

4. Inventar der Hardware-Komponenten

Es gibt ein aktuelles Inventar aller Hardware-Komponenten.

5. Inventar der IT-Prozesse

Es gibt ein aktuelles Inventar aller IT-Prozesse.

6. Regelmäßige Aktualisierung

Das Inventar wird regelmäßig aktualisiert und überprüft.

7. Rollen und Verantwortlichkeiten

Es sind klare Rollen und Verantwortlichkeiten für die Pflege und Verwaltung des Inventars festgelegt.

4.b. Klassifikation von Vermögenswerten

1. Kritikalität

Alle Vermögenswerte sind im Inventar nach ihrer Kritikalität für den Betrieb klassifiziert.

2. Sicherheitsanforderungen

Die Sicherheitsanforderungen sind für jede Klassifikationsstufe definiert und dokumentiert.

3. Überprüfung der Klassifikation

Die Klassifikation der Vermögenswerte wird regelmäßig überprüft und angepasst.

4.c. Handhabung von Vermögenswerten

1. Nutzungsrichtlinien

Es gibt Richtlinien für die Nutzung und Handhabung von IT-Vermögenswerten.

2. Zugriffsrechte

Die Zugriffsrechte auf Vermögenswerte sind klar definiert und dokumentiert.

3. Schulung

Mitarbeiter werden regelmäßig über die korrekte Handhabung von Vermögenswerten geschult.

4.d. Umgang mit Wechseldatenträgern

1. Richtlinien für Wechseldatenträger

Es gibt spezifische Richtlinien für den Umgang mit Wechseldatenträgern (z.B. USB-Sticks, externe Festplatten).

2. Sicherheitsmaßnahmen

Sicherheitsmaßnahmen wie Verschlüsselung und Virencans sind für Wechseldatenträger implementiert.

3. Protokollierung

Die Nutzung von Wechseldatenträgern wird protokolliert und überwacht.

4.e. Rücknahme oder Löschung von Vermögenswerten

1. Richtlinien für Rücknahme/Löschung

Es gibt dokumentierte Prozesse für die sichere Rücknahme oder Löschung von Vermögenswerten.

2. Datensicherheit

Daten auf Vermögenswerten werden sicher gelöscht oder zerstört, um eine Wiederherstellung zu verhindern.

3. Nachweisdokumentation

Die Schritte der Rücknahme oder Löschung von Vermögenswerten werden dokumentiert und nachverfolgt.

5. Personalwesen

Auch das Personal spielt in der NIS-2 eine Rolle, so muss festgelegt sein, dass Zugriffsrechten bei Stellenwechsel oder Austritt verändert werden. Außerdem braucht es Maßnahmen zum Umgang mit Sicherheitsverstößen und Sensibilisierungsprogramme für Mitarbeiter.

5.a. Sicherheit im Personalwesen

1. Vertrauenswürdigkeit der Mitarbeiter

Es gibt Verfahren, um sicherzustellen, dass Mitarbeiter vertrauenswürdig und sich ihrer Verantwortung bewusst sind.

Beispiel eines Verfahrens für die Vertrauenswürdigkeit:

Hintergrundüberprüfungen:

Es wird empfohlen, dass Organisationen vor der Einstellung von Mitarbeitern, insbesondere in sicherheitskritischen Positionen, Hintergrundprüfungen durchführen. Dies kann auch die Überprüfung von Vorstrafen, Qualifikationen und Berufserfahrung umfassen.

Regelmäßige Nachprüfungen:

Auch nach der Einstellung kann es sinnvoll sein, regelmäßige Überprüfungen der Vertrauenswürdigkeit durchzuführen, um sicherzustellen, dass Mitarbeiter weiterhin den Sicherheitsanforderungen entsprechen.

2. Schulung und Sensibilisierung

Es gibt ein Schulungsprogramm für sicherheitsrelevante Themen, das alle Mitarbeiter umfasst.

3. Spezielle Trainingsprogramme

Mitarbeiter mit spezifischer Verantwortung für Netz- und Informationssysteme werden in einem speziellen Sicherheitstrainingsprogramm geschult.

5.b. Hintergrundüberprüfung

1. Durchführung von Hintergrundüberprüfungen

Es werden Hintergrundüberprüfungen für Mitarbeiter in sicherheitsrelevanten Positionen durchgeführt.

! Was umfasst eine Hintergrundüberprüfung?

Beispielsweise:

- Identitätsprüfung
- Überprüfung des Strafregisters
- Berufs- und Ausbildungsnachweise
- Referenzen von früheren Arbeitgebern

2. Regelmäßige Überprüfung

Die Hintergrundüberprüfungen werden regelmäßig aktualisiert oder bei veränderten Positionen erneut durchgeführt.

3. Dokumentation der Überprüfungen

Die Ergebnisse der Hintergrundüberprüfungen werden dokumentiert und sicher aufbewahrt.

5.c. Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses

1. Sicherheitsmaßnahmen bei Beendigung

Es gibt definierte Verfahren zur Sicherstellung, dass alle Zugangsrechte und privilegierten Zugriffe bei Beendigung des Arbeitsverhältnisses entfernt werden.

2. Umgang mit Wechseln innerhalb der Organisation

Zugriffsrechte und Verantwortlichkeiten werden überprüft und angepasst, wenn ein Mitarbeiter eine neue Position innerhalb der Organisation einnimmt.

3. Rückgabe von Unternehmensressourcen

Es gibt klare Prozesse für die Rückgabe von Unternehmensressourcen wie Schlüssel, Ausweise und IT-Geräte bei Beendigung oder Wechsel des Beschäftigungsverhältnisses.

5.d. Umgang mit Verstößen gegen die Sicherheitsrichtlinie

1. Meldeverfahren für Verstöße

Es gibt ein klares Verfahren für das Melden und Dokumentieren von Verstößen gegen die im Unternehmen vorhandenen Sicherheitsrichtlinien.

2. Disziplinarmaßnahmen

Es sind Disziplinarmaßnahmen für Verstöße gegen die Sicherheitsrichtlinie definiert und diese werden konsequent umgesetzt.

3. Sensibilisierung und Prävention

Mitarbeiter werden regelmäßig über die Konsequenzen von Verstößen gegen die Sicherheitsrichtlinie informiert und sensibilisiert.

6. Cybersicherheitskompetenzen und Cybersicherheitsschulungen

In einer zunehmend vernetzten Welt sind nicht nur technische Systeme, sondern vor allem die Menschen, die sie bedienen, ein entscheidender Faktor für die Sicherheit. Ohne ausreichende Schulungen und Kompetenzen bleiben viele Mitarbeitende anfällig für Cyberangriffe, die häufig auf menschliches Fehlverhalten abzielen, wie Phishing oder Social Engineering.

Schulungen befähigen die Belegschaft, Bedrohungen frühzeitig zu erkennen, richtig zu reagieren und Risiken zu minimieren. Daher sind gezielte Schulungsprogramme und der kontinuierliche Ausbau von Cybersicherheitsfähigkeiten unerlässlich, um die Widerstandsfähigkeit eines Unternehmens zu stärken.

6.a. Vermittlung von Cybersicherheitskompetenzen

1. Kompetenzentwicklung für Leitungsorgane

Es gibt spezielle Schulungen zur Entwicklung von Cybersicherheitskompetenzen von Leitungsorganen, um sicherzustellen, dass sie ihre Aufsichtspflichten wirksam wahrnehmen können.

Beispiele für notwendige Cybersicherheitskompetenzen

- **Risikobewertung:**
Fähigkeiten zur Identifizierung und Bewertung von Cyber Risiken, die die Organisation betreffen könnten.
- **Management von Cybersicherheitsmaßnahmen:**
Verständnis von Best Practices für die Implementierung und Überwachung von Sicherheitsmaßnahmen.
- **Reaktion auf Sicherheitsvorfälle:**
Kenntnisse über Notfallpläne und Reaktionsstrategien bei Cyberangriffen.

2. Regelmäßige Weiterbildung

Es gibt einen festgelegten Plan zur regelmäßigen Weiterbildung der Leitungsorgane im Bereich Cybersicherheit.

3. Dokumentation der Schulungen

Die durchgeführten Schulungen und die erworbenen Kompetenzen der Leitungsorgane werden dokumentiert.

6.b. Cybersicherheitsschulungen

1. Schulungsangebote für Mitarbeiter

Es werden allen Mitarbeitern, basierend auf ihrer Rolle und ihrem Arbeitsbezug zu Netz- und Informationssystemen, regelmäßig Cybersicherheitsschulungen angeboten.



Inhalte einer effektiven Cybersicherheitsschulung

Beispielsweise:

- Erkennung von Phishing-Angriffen
- Passwortsicherheit
- Datenschutz und Informationssicherheit

2. Evaluierung der Schulungseffektivität

Es gibt Verfahren zur Evaluierung der Effektivität der Schulungen, z.B. durch Tests oder Simulationen.

7. Sicherheit von Lieferketten

Im NIS-2 Gesetz steht die Sicherheit der Lieferkette im Vordergrund, da viele Unternehmen auf externe Partner und Dienstleister angewiesen sind.

Unter der Sicherheit der Lieferkette versteht man den Schutz vor Cyberangriffen und Störungen in Bezug auf alle Abläufe, Systeme und Beteiligten, die zur Lieferung von Produkten und Dienstleistungen beitragen.

NIS-2 fordert, dass nicht nur Risiken im eigenen Unternehmen, sondern auch bei Zulieferern berücksichtigt werden, da Angriffe auf diese ebenfalls schwere Folgen haben können. Unternehmen müssen daher ihre Lieferketten regelmäßig prüfen, Schwachstellen aufdecken und Sicherheitsmaßnahmen ergreifen, um Risiken zu verringern.

7.a. Richtlinie zur Sicherheit von Lieferketten

1. Existenz einer Lieferkettensicherheitsrichtlinie

Es gibt eine dokumentierte Richtlinie zur Sicherheit von Lieferketten, die die Anforderungen an Lieferanten und Dienstleister klar definiert.

Inhalte einer Lieferketten- sicherheitsrichtlinie

Beispielsweise:

- Risikobewertung
- Sicherheitsanforderungen
- Vertragsgestaltung

2. Überprüfung und Aktualisierung

Die Lieferkettensicherheitsrichtlinie wird regelmäßig überprüft und aktualisiert.

3. Umsetzung der Sicherheitsanforderungen

Die definierten Sicherheitsanforderungen werden bei allen relevanten Lieferanten konsequent umgesetzt und überprüft.

7.b. Lieferantenverzeichnis

1. Vollständigkeit des Lieferantenverzeichnisses

Es gibt ein aktuelles und vollständiges Verzeichnis aller Lieferanten und Dienstleister.

2. Klassifikation der Lieferanten nach Kritikalität

Die Lieferanten sind im Verzeichnis nach ihrer Kritikalität für die Organisation und die von ihnen bereitgestellten Dienste klassifiziert.

Klassifikation von Lieferanten

→ **Hohe Kritikalität:**

Lieferanten, deren Ausfall oder Sicherheitsvorfall erhebliche Auswirkungen auf den Betrieb der Organisation haben könnte.

→ **Mittlere Kritikalität:**

Lieferanten, die wichtige, aber nicht betriebsentscheidende Dienste bereitstellen.

→ **Geringe Kritikalität:**

Lieferanten, deren Einfluss auf den Betrieb minimal ist.

3. Periodische Überprüfung des Verzeichnisses

Das Lieferantenverzeichnis wird regelmäßig überprüft und bei Bedarf aktualisiert.

4. Sicherheitsmaßnahmen für kritische Lieferanten

Für Lieferanten mit hoher Kritikalität werden spezifische Sicherheitsmaßnahmen implementiert und regelmäßig überprüft.

8. Zugangssteuerung

In dieser Maßnahme geht es darum, sicherzustellen, dass der Zugriff auf Netz- und Informationssysteme streng kontrolliert und gesichert ist. Dies beinhaltet die Erstellung einer Zugangssteuerungsrichtlinie, die Verwaltung von Zugriffsberechtigungen, den sicheren Umgang mit privilegierten und administrativen Zugängen sowie die Implementierung von Identifikations-, Authentifikations- und Multi-Faktor-Authentifizierungssystemen.

8.a. Zugangssteuerungsrichtlinie

1. Existenz einer Zugangssteuerungsrichtlinie

Es gibt eine dokumentierte Richtlinie, die die Zugangssteuerung und -verwaltung klar definiert.

Inhalte einer Zugangssteuerungsrichtlinie

→ **Minimalrechtsprinzip:**

Zugriffsbeschränkungen basierend auf dem Bedarf, um das Risiko unautorisierter Zugriffe zu minimieren.

→ **Regelmäßige Überprüfung:**

Vorgaben zur periodischen Überprüfung der Zugriffsrechte.

→ **Protokollierung:**

Anforderungen zur Protokollierung und Überwachung aller Zugriffsaktivitäten.

2. Überprüfung und Aktualisierung

Die Zugangssteuerungsrichtlinie wird regelmäßig überprüft und aktualisiert, um mit den aktuellen Bedrohungen und Systemanforderungen Schritt zu halten.

8.b. Verwaltung von Zugriffsberechtigungen

1. Dokumentation der Zugriffsberechtigungen

Alle Zugriffsberechtigungen werden systematisch dokumentiert, einschließlich der Zuweisung und Überprüfung von Zugriffsrechten.

2. Regelmäßige Überprüfung

Die Zugriffsrechte werden mindestens einmal jährlich überprüft und bei Bedarf angepasst.

3. Aufbewahrung von Zugriffsdaten

Die Daten über Zugriffsberechtigungen werden sicher aufbewahrt und sind diese für Prüfungen leicht zugänglich.

8.c. Privilegierte und administrative Zugänge

In diesem Kapitel bezieht sich der Begriff „privilegierte und administrative Zugänge“ auf spezielle Zugriffsrechte, die es bestimmten Benutzern oder Administratoren ermöglichen, tiefgreifende Änderungen und Konfigurationen an Netzwerken, IT-Systemen und sensiblen Anwendungen vorzunehmen. Solche Zugänge gehen über die normalen Benutzerrechte hinaus und umfassen in der Regel höhere Befugnisse, die zur Verwaltung und Kontrolle von IT-Infrastrukturen erforderlich sind.

Privilegierte Zugänge:

- Diese beinhalten erweiterte Zugriffsrechte, die es Nutzern ermöglichen, kritische Systemänderungen vorzunehmen oder auf sensible Daten zuzugreifen.
- Privilegierte Konten werden häufig für spezifische Aufgaben benötigt, wie die Verwaltung von Servern, Datenbanken, Firewalls oder die Konfiguration sicherheitsrelevanter Systeme.

Administrative Zugänge:

- Dies sind spezielle Konten, die für Systemadministratoren reserviert sind und den vollen Zugriff auf IT-Infrastrukturen gewähren.
- Mit diesen Zugängen können Administratoren Systemänderungen vornehmen, Benutzerrechte verwalten, Systemeinstellungen konfigurieren und Sicherheitsmaßnahmen implementieren.
- Sie unterliegen besonderen Sicherheitsanforderungen, da ein unkontrollierter Zugang zu diesen Konten ein erhebliches Sicherheitsrisiko darstellen kann.

Die im Kapitel beschriebene Zugangssteuerung stellt sicher, dass diese privilegierten und administrativen Zugänge nach dem Minimalrechtsprinzip zugewiesen werden, also nur für genau die Aufgaben, für die sie unbedingt benötigt werden. Zudem müssen diese Zugänge dedizierte, personalisierte Konten verwenden, um eine klare Verantwortungszuweisung und Protokollierung aller administrativen Aktivitäten zu gewährleisten.

1. Minimalrechtsprinzip für administrative Zugänge

Administrative und privilegierte Zugänge werden nach dem Minimalrechtsprinzip zugewiesen.

2. Dedizierte administrative Konten

Für administrative Aufgaben werden ausschließlich dedizierte, personalisierte Konten verwendet, die nicht für andere Aufgaben genutzt werden.

3. Protokollierung und Überwachung

Administrative Aktivitäten werden umfassend protokolliert und regelmäßig überwacht, um mögliche Sicherheitsvorfälle schnell zu erkennen.

8.d. Systeme und Anwendungen zur Systemadministration

1. Verwendung von dedizierten Systemen

Systeme und Anwendungen werden zur Systemadministration ausschließlich für administrative Tätigkeiten verwendet.

In diesem Kontext bezieht sich der Begriff „dedizierte Systeme“ auf spezielle IT-Systeme und Anwendungen, die ausschließlich für administrative Aufgaben und Systemverwaltungszwecke verwendet werden. Diese Systeme sind für administrative Nutzer vorgesehen und dienen der Verwaltung von Netzwerken, Servern und anderen IT-Infrastrukturen.

Die Verwendung von dedizierten Systemen stellt sicher, dass administrative Aufgaben klar von anderen Tätigkeiten getrennt werden, um die Sicherheit zu erhöhen. Das bedeutet, dass administrative Konten und Systeme nicht für alltägliche oder weniger sicherheitskritische Aufgaben genutzt werden. Dies minimiert das Risiko, dass Administratorenzugänge durch Sicherheitslücken in anderen Anwendungen oder durch unautorisierte Zugriffe gefährdet werden.

Im Rahmen des NIS-2 Gesetzes ist es essenziell, dass solche dedizierten Systeme nach aktuellen Sicherheitsstandards konfiguriert und von anderen Netzwerken isoliert sind, um die Gefahr von Cyberangriffen weiter zu verringern.

2. Sichere Konfiguration

Diese Systeme werden nach den aktuellen Sicherheitsstandards konfiguriert und regelmäßig überprüft

3. Isolierung von administrativen Systemen

Die administrativen Systeme sind logisch oder physisch von anderen Netzwerken isoliert, um das Risiko von Angriffen zu minimieren?

8.e. Identifikation

1. Eindeutige Benutzeridentifikation

Es sind eindeutige Konten für alle Benutzer oder automatisierten Prozesse eingerichtet, die auf Netz- und Informationssysteme zugreifen.

2. Deaktivierung nicht genutzter Konten

Nicht mehr benötigte oder inaktive Benutzerkonten werden regelmäßig deaktiviert.

8.f. Authentifikation

1. Sicherer Authentifikationsmechanismus

Es gibt einen sicheren Authentifikationsmechanismus, um den Zugriff auf Ressourcen zu schützen.

Sichere Authentifizierungsmechanismen sind Verfahren und Technologien, die gewährleisten, dass nur autorisierte Benutzer Zugang zu IT-Systemen, Netzwerken und Ressourcen erhalten. Sie stellen sicher, dass Benutzer eindeutig identifiziert und authentifiziert werden, bevor sie auf sensible Daten oder Systeme zugreifen können. Dabei wird sichergestellt, dass die Identität der Benutzer zuverlässig überprüft wird, um unautorisierten Zugriff zu verhindern.

Beispiele sicherer Authentifizierungsmechanismen:

1. *Passwortbasierte Authentifizierung:*

→ *Starke Passwörter:*

Die Verwendung von komplexen, ausreichend langen Passwörtern, die regelmäßig geändert werden, ist eine Grundvoraussetzung für die Sicherheit.

→ *Passwort-Richtlinien:*

Organisationen implementieren häufig Richtlinien zur Passwortsicherheit, um Schwächen in diesem Bereich zu vermeiden (z. B. Mindestlänge, Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).

2. *Multi-Faktor-Authentifizierung (MFA):*

→ MFA kombiniert mehrere Authentifizierungsfaktoren, wie etwas, das der Benutzer *weiß* (z. B. Passwort), etwas, das er *besitzt* (z. B. ein Token oder ein Smartphone), und etwas, das er *ist* (z. B. ein Fingerabdruck).

→ Beispiele: Eine Kombination aus Passwort und einem Einmalcode, der per SMS oder App verschickt wird, oder die Verwendung eines biometrischen Scans wie Fingerabdruck oder Gesichtserkennung.

3. *Biometrische Authentifizierung:*

→ Hierbei werden einzigartige, individuelle Eigenschaften des Benutzers verwendet, um die Identität zu bestätigen, wie Fingerabdrücke, Gesichtserkennung, Iris- oder Stimmerkennung.

→ Biometrische Authentifizierung ist besonders sicher, da sie schwer zu fälschen ist und keine physischen Elemente wie ein Passwort oder eine Karte benötigt.

4. Hardwarebasierte Authentifizierung:

- Sicherheits-Token oder Smartcards, die physisch von Benutzern getragen werden und bei der Anmeldung an ein System in einen Kartenleser eingesteckt oder per USB verbunden werden müssen.
- Diese Methode ist besonders sicher, da die physische Komponente für den Zugang erforderlich ist.

5. Einmalpasswörter (One-Time Passwords, OTP):

- Ein OTP wird bei jeder Anmeldung neu generiert und kann nur für eine begrenzte Zeit verwendet werden. Es wird oft als Teil der Multi-Faktor-Authentifizierung verwendet.
- Diese Passwörter können per App, E-Mail oder SMS an den Benutzer gesendet werden.

6. Public-Key-Infrastructure (PKI):

- PKI verwendet kryptografische Schlüsselpaare (öffentlicher und privater Schlüssel), um Benutzer zu authentifizieren. Benutzer können sich mit einem privaten Schlüssel, der sicher auf einem Gerät gespeichert ist, authentifizieren, während der öffentliche Schlüssel für die Verifizierung genutzt wird.

Wichtige Aspekte sicherer Authentifizierungsmechanismen:

- **Regelmäßige Änderung der Authentifizierungsdaten:**
Passwörter und Zugangsdaten sollten regelmäßig geändert werden, um Sicherheitslücken zu minimieren.
- **Sichere Speicherung von Authentifizierungsdaten:**
Passwörter und andere Authentifizierungsdaten müssen sicher und verschlüsselt aufbewahrt werden.
- **Protokollierung und Überwachung:**
Authentifizierungsprozesse sollten überwacht und protokolliert werden, um verdächtige Zugriffsversuche frühzeitig zu erkennen.

2. Regelmäßige Änderung der Authentifizierungsdaten

Es gibt Vorgaben zur regelmäßigen Änderung der Authentifizierungsdaten, insbesondere bei sensiblen Systemen.

Einsatzbereiche für Multi-Faktor-Authentifikation (MFA)

Beispielsweise:

- VPN-Zugang
- Firewall-Administration
- Mailboxen
- Cloud-Dienste
- Server-Management
- Datenbanken
- Remote Desktop Service

9. Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung

Diese Maßnahme umfasst eine breite Palette von Sicherheitsaspekten, die sicherstellen, dass Netz- und Informationssysteme während ihres gesamten Lebenszyklus - von der Beschaffung über die Entwicklung bis hin zum Betrieb und zur Wartung - sicher betrieben werden. Dies schließt die sichere Konfiguration von Systemen, das Management von Änderungen, den Umgang mit Schwachstellen, die Durchführung von Sicherheitstests und das Patchmanagement ein.

9.a. Konfigurationsmanagement

1. Dokumentation der Systemkonfiguration

Die Konfiguration aller relevanten Netz- und Informationssysteme wird strukturiert dokumentiert und regelmäßig aktualisiert.

2. Systemhärtung

Sicherheitsmaßnahmen zur Systemhärtung (z.B. Deaktivierung nicht benötigter Dienste, Minimierung der Angriffsfläche) werden konsequent umgesetzt.

9.b. Änderungsmanagement

1. Prozesse für Änderungsanfragen

Es gibt einen formalen Prozess zur Beantragung, Überprüfung und Genehmigung von Änderungen an Netz- und Informationssystemen.

2. Überwachung und Dokumentation von Änderungen

Alle Änderungen an den Systemen werden dokumentiert und überwacht, um unautorisierte oder fehlerhafte Änderungen zu verhindern.

9.c. Umgang mit Schwachstellen und deren Offenlegung

1. Schwachstellenmanagement

Es gibt ein etabliertes Verfahren zur Identifizierung, Bewertung und Behebung von Schwachstellen in Netz- und Informationssystemen.

2. Offenlegung von Schwachstellen

Identifizierte Schwachstellen werden zeitnah offengelegt und geeignete Maßnahmen ergriffen, um diese zu beheben.

9.d. Sicherheitstests

1. Regelmäßige Sicherheitstests

Es werden regelmäßig Sicherheitstests (z.B. Penetrationstests, Schwachstellenscans) durchgeführt, um die Integrität und Sicherheit der Systeme zu gewährleisten.

2. Testprotokolle

Die Ergebnisse der Sicherheitstests werden dokumentiert und in die kontinuierliche Verbesserung der Sicherheitsmaßnahmen eingebunden.

9.e. Patchmanagement

Ein *Patch* ist ein Software-Update, das Fehler, Sicherheitslücken oder Schwachstellen in einem Programm oder Betriebssystem behebt. Patches werden von Entwicklern bereitgestellt, um die Funktionalität oder Sicherheit eines Systems zu verbessern, indem bekannte Probleme korrigiert werden.

Im Kontext der IT-Sicherheit spielen Patches eine entscheidende Rolle, da sie oft kritische Sicherheitslücken schließen, die von Angreifern ausgenutzt werden könnten. Das *Patchmanagement* umfasst den Prozess der regelmäßigen Überprüfung, Installation und Überwachung solcher Updates, um sicherzustellen, dass alle Systeme auf dem neuesten Stand und vor bekannten Bedrohungen geschützt sind.

1. Regelmäßiges Einspielen von Patches

Patches und Sicherheitsupdates werden regelmäßig eingespielt, um bekannte Schwachstellen zu beheben.

2. Patchmanagement-Prozess

Es gibt einen definierten Prozess für das Patchmanagement, der sicherstellt, dass alle relevanten Systeme auf dem neuesten Stand gehalten werden.

9.f. Sicherheit bei der Beschaffung von IKT-Diensten und IKT-Produkten

IKT-Dienste und IKT-Produkte beziehen sich auf Informations- und Kommunikationstechnologie-Dienstleistungen und -Produkte, die für den Betrieb von IT-Systemen und Netzwerken notwendig sind.

- IKT-Dienste umfassen alle Leistungen, die mit der Bereitstellung, Verwaltung und Wartung von IT-Infrastrukturen, Netzwerken und Anwendungen verbunden sind. Beispiele hierfür sind Cloud-Dienste, IT-Support, Datenverwaltung und Netzwerksicherheit.
- IKT-Produkte beinhalten Hardware und Software, die in einer Organisation genutzt werden, wie Server, Computer, Netzwerkausrüstung, Betriebssysteme und spezielle Anwendungen.

1. Sicherheitsanforderungen bei der Beschaffung

Bei der Beschaffung von IKT-Diensten und -Produkten werden klare Sicherheitsanforderungen definiert und überprüft.

2. Lieferantenaudit

Lieferanten werden auf ihre Fähigkeit geprüft, die festgelegten Sicherheitsstandards einzuhalten.

9.g. Sichere Softwareentwicklung

1. Sicherheitsrichtlinien für die Softwareentwicklung

Es sind Sicherheitsrichtlinien für den gesamten Softwareentwicklungsprozess (z.B. sichere Codierungsstandards) implementiert.

2. Code-Reviews und Sicherheitsprüfungen

Regelmäßige Code-Reviews und Sicherheitsprüfungen werden durchgeführt, um Sicherheitslücken im Entwicklungsprozess frühzeitig zu erkennen.

9.h. Netzwerksegmentierung

1. Segmentierung nach Schutzbedarfwicklung

Das Netzwerk ist abhängig vom Schutzbedarf physisch oder logisch segmentiert, um die Auswirkungen von Sicherheitsvorfällen zu minimieren.

2. Schnittstellen zwischen Segmenten

Schnittstellen zwischen Netzwerksegmenten werden streng kontrolliert und überwacht.

9.i. Netzwerksicherheit

1. Filterung des Netzwerkverkehrs

Der ein- und ausgehende Netzwerkverkehr sowie der interne Verkehr wird gefiltert und auf das notwendige Minimum beschränkt?

2. Regelmäßige Aktualisierung der Filterregeln

Die Filterregeln für den Netzwerkverkehr werden regelmäßig überprüft und aktualisiert.

9.j. Schutz vor bösartiger und unautorisierter Software

1. Malware-Schutz

Systeme sind mit aktuellen Antiviren- und Antimalware-Programmen ausgestattet und regelmäßig überprüft.

2. Kontrolle der Softwareinstallation

Es gibt Richtlinien zur Installation von Software, die sicherstellen, dass nur autorisierte und geprüfte Software verwendet wird.

10. Kryptographie

In dieser Maßnahme geht es darum, die Vertraulichkeit, Authentizität und Integrität von Informationen durch den angemessenen Einsatz kryptographischer Verfahren sicherzustellen. Eine klare Kryptographierichtlinie ist wichtig, um den Einsatz von Verschlüsselungstechnologien und Schlüsselmanagement in der Organisation zu steuern und zu überwachen.

10.a. Kryptographierichtlinie

1. Existenz einer Kryptographierichtlinie

Es gibt eine dokumentierte Richtlinie, die den Einsatz von Kryptographie und Schlüsselmanagement in der Organisation regelt.

2. Einsatz von Verschlüsselungsverfahren

Es werden geeignete kryptographische Verfahren verwendet, um die Vertraulichkeit, Authentizität und Integrität von Daten zu schützen.

Beispiele für den Einsatz von Kryptographie

- **Verschlüsselung von Daten auf Wechseldatenträgern:** Alle Daten, die auf externen Medien wie USB-Sticks oder externen Festplatten gespeichert werden, sollten verschlüsselt sein.
- **Verschlüsselung sensibler Daten während der Übertragung:** Sensible Daten sollten während der Übertragung über Netzwerke durch Technologien wie Transport Layer Security (TLS) oder Open Secure Shell (OpenSSH) geschützt werden.
- **Verschlüsselung sensibler Daten im Ruhezustand:** Daten, die auf Servern, Anwendungen und Datenbanken gespeichert werden, sollten durch Speicher- oder Anwendungsschichtverschlüsselung geschützt werden.
- **Verwendung von S/MIME für E-Mails**

3. Schlüsselmanagement

Es gibt Verfahren und Tools zur sicheren Verwaltung von Verschlüsselungsschlüsseln, einschließlich der Erzeugung, Speicherung, Verteilung und Entsorgung von Schlüsseln.

4. Regelmäßige Überprüfung und Aktualisierung

Die Kryptographierichtlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass die verwendeten kryptographischen Verfahren den aktuellen Sicherheitsanforderungen entsprechen.

11. Umgang mit Cybersicherheitsvorfällen

Die Behandlung von Cybersicherheitsvorfällen ist ein zentraler Aspekt der Cybersicherheit, um die Sicherheit von Netz- und Informationssystemen zu gewährleisten. Diese Maßnahme umfasst die Entwicklung und Umsetzung von Richtlinien und Prozessen für den Umgang mit Sicherheitsvorfällen, die Überwachung und Protokollierung von sicherheitsrelevanten Ereignissen, die Meldung und Analyse von Vorfällen sowie die Reaktion und Nachbereitung, um aus Vorfällen zu lernen und die Sicherheit kontinuierlich zu verbessern.

11.a. Richtlinie zum Umgang mit Cybersicherheitsvorfällen

1. Existenz einer Vorfallsrichtlinie

Es gibt eine dokumentierte Richtlinie für den Umgang mit Cybersicherheitsvorfällen, die Rollen, Verantwortlichkeiten und Prozesse klar definiert.

Inhalte einer Vorfallsrichtlinie

- **Rollen und Verantwortlichkeiten:** Festlegung von Schlüsselpersonen für das Incident Handling, einschließlich primärer Verantwortlicher und Backup-Personen.
- **Kommunikationsplan:** Mechanismen für die Kommunikation während eines Vorfalls, z.B. alternative Kommunikationswege bei Ausfall der primären Systeme.
- **Reaktionsprozesse:** Schritte zur schnellen Eindämmung und Behebung eines Vorfalls.

2. Regelmäßige Aktualisierung und Übung

Die Vorfallsrichtlinie wird regelmäßig überprüft, aktualisiert und durch Übungen getestet.

11.b. Überwachung und Protokollierung

1. Implementierung von Überwachungsmechanismen

Es sind Mechanismen zur kontinuierlichen Überwachung von Netzwerken und Systemen implementiert, um sicherheitsrelevante Ereignisse in Echtzeit zu erkennen.

2. Protokollierung sicherheitsrelevanter Ereignisse

Sicherheitsrelevante Ereignisse sind umfassend protokolliert, einschließlich Zeitstempel, Benutzeraktionen und Netzwerkverkehr.

! Wichtige Aspekte der Protokollierung

- **Zentralisierte Protokollierung:** Alle Logs sollten zentral gesammelt und gesichert werden, um eine konsolidierte Analyse zu ermöglichen.
- **Speicherfristen:** Audit Logs sollten mindestens 90 Tage aufbewahrt werden, um eine gründliche Nachverfolgung zu gewährleisten.
- **Zeitsynchronisation:** Standardisierte Zeitsynchronisation für alle Logs, um eine korrekte Chronologie zu gewährleisten.

11.c. Meldung von Ereignissen

1. Etablierung eines Meldesystems

Es gibt ein klar definiertes System zur internen und externen Meldung von Sicherheitsvorfällen, das auch Kontakte zu Behörden und Dienstleistern umfasst.

2. Kontaktinformationen für Vorfallmeldungen

Aktuelle Kontaktinformationen sind für alle relevanten Stakeholder (z.B. interne Teams, Drittanbieter, Behörden) verfügbar und überprüft.

11.d. Korrelation und Analyse von Ereignissen

1. Korrelation von sicherheitsrelevanten Ereignissen

Es wird ein System zur Korrelation und Analyse von Logs eingesetzt, um Sicherheitsvorfälle schnell zu erkennen und zu bewerten.

2. Datenschutz und Vertraulichkeit

Bei der Korrelation und Analyse von sicherheitsrelevanten Daten sind Maßnahmen zur Wahrung der Vertraulichkeit implementiert?

11.e. Reaktion auf Cybersicherheitsvorfälle

1. Reaktionsprozesse bei Vorfällen

Es gibt etablierte Prozesse zur schnellen und effektiven Reaktion auf Sicherheitsvorfälle, einschließlich der Dokumentation und Koordination aller Maßnahmen.



Schlüsselkomponenten der Vorfallsreaktion

- **Incident Response Team (IRT):** Ein dediziertes Team, das auf Vorfälle reagiert und sie bearbeitet.
- **Forensische Untersuchung:** Sicherstellung, dass forensische Fähigkeiten vorhanden sind, entweder intern oder durch Dienstleister.
- **Kommunikationsstrategie:** Festlegung von internen und externen Kommunikationswegen während eines Vorfalls.

2. Übung von Vorfallsreaktionen

Es werden regelmäßig Übungen zur Vorfallsreaktion durchgeführt, um die Effektivität der Prozesse zu testen und zu verbessern.

11.f. Erkenntnisse nach Cybersicherheitsvorfällen

1. Post-Incident Reviews

Nach jedem Vorfall werden Post-Incident Reviews durchgeführt, um die Ursachen zu analysieren und Verbesserungsmaßnahmen abzuleiten.

2. Integration von Erkenntnissen

Die aus Vorfällen gewonnenen Erkenntnisse werden in die Sicherheitsrichtlinien und -prozesse integriert, um zukünftige Vorfälle zu verhindern.

12. Betriebskontinuitäts- und Krisenmanagement

Die Sicherstellung der Betriebskontinuität und das effektive Krisenmanagement sind entscheidende Faktoren, um die Erbringung wesentlicher Dienste auch während und nach einem Sicherheitsvorfall aufrechtzuerhalten. Diese Maßnahme umfasst die Erstellung und Pflege von Notfallwiederherstellungsplänen, das Management von Backups und Redundanzen sowie die Organisation eines effizienten Krisenmanagements.

12.a. Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne

1. Existenz von Betriebskontinuitätsplänen

Es gibt dokumentierte Betriebskontinuitätspläne, die Strategien zur Wiederherstellung wesentlicher Dienste nach einem Sicherheitsvorfall definieren.



Bestandteile eines Betriebskontinuitätsplans

- **Ziele und Richtlinien:** Definition der Ziele für die Wiederherstellung und Aufrechterhaltung wesentlicher Dienste.
- **Business Impact Analyse (BIA):** Regelmäßige Durchführung einer BIA zur Bewertung der Auswirkungen potenzieller Vorfälle auf Netz- und Informationssysteme.
- **Notfallhandbuch:** Detaillierte Anweisungen und Prozesse für den Umgang mit Sicherheitsvorfällen und die schnelle Wiederherstellung des Betriebs.

2. Regelmäßige Überprüfung und Tests

Die Betriebskontinuitäts- und Notfallpläne werden regelmäßig getestet und aktualisiert, um ihre Wirksamkeit sicherzustellen.

12.b. Backup-, Redundanz- und Wiederherstellungsmanagement

1. Automatisierte Backups

Es werden regelmäßig automatisierte Backups für alle relevanten Unternehmensdaten durchgeführt.

2. Sicherung der Backup-Daten

Backup-Daten werden mit denselben Sicherheitsmaßnahmen geschützt wie die Originaldaten (z.B. durch Verschlüsselung).

Wichtige Aspekte des Backup-Managements

- **Isolierte Backups:** Backups sollten in einer isolierten Umgebung gespeichert werden, z.B. offline, in der Cloud oder an einem externen Standort.
- **Wiederherstellungstests:** Regelmäßige Tests der Backup-Wiederherstellung sollten mindestens vierteljährlich durchgeführt werden, um die Integrität und Verfügbarkeit der Daten sicherzustellen.

3. Redundanzmanagement

Redundanzmechanismen sind implementiert, um kritische Systeme und Daten bei einem Ausfall sofort verfügbar zu halten.

12.c. Krisenmanagement

1. Krisenmanagementplan

Es gibt einen umfassenden Krisenmanagementplan, der die Organisation und Verantwortlichkeiten für den Umgang mit Krisen klar definiert.

2. Koordination mit externen Partnern

Es sind Prozesse zur Koordination von Krisenmanagementaktivitäten mit externen Partnern (z.B. CERTs, Behörden, ISPs) etabliert und regelmäßig getestet.

3. Alarmierungs- und Kommunikationspläne

Alarmierungs- und Kommunikationspläne sind definiert und getestet, um sicherzustellen, dass alle relevanten Parteien im Krisenfall schnell informiert werden.

Elemente eines effektiven Krisenmanagements

- **Schlüsselfunktionen:** Bestimmung der Verantwortlichkeiten für IT, Sicherheit, PR, Recht und andere relevante Bereiche.
- **Kommunikationsmechanismen:** Festlegung primärer und sekundärer Kommunikationswege, um sicherzustellen, dass auch bei einem Ausfall des primären Kanals eine Kommunikation möglich ist.
- **Krisenübungen:** Regelmäßige Übungen, um die Krisenbewältigungsstrategien zu testen und zu verbessern.

13. Umgebungsbezogene und physische Sicherheit

Die umgebungsbezogene und physische Sicherheit spielt eine entscheidende Rolle beim Schutz von Netz- und Informationssystemen. Diese Maßnahme zielt darauf ab, unbefugten physischen Zugang zu verhindern, Umgebungsgefahren abzuwehren und die kontinuierliche Verfügbarkeit durch gesicherte Versorgungseinrichtungen sicherzustellen.

13.a. Sicherheitsperimeter und physische Zutrittskontrollen

1. Existenz von Sicherheitsperimetern

Es gibt einen definierten und gesicherten Sicherheitsperimeter um kritische Bereiche, z.B. durch Zäune, Mauern oder andere physische Barrieren zu schützen.

2. Physische Zutrittskontrollen

Physische Zutrittskontrollen sind implementiert, um den Zugang zu sicherheitskritischen Bereichen wie Rechenzentren oder Serverräumen zu kontrollieren.

Bestandteile eines physischen Sicherheitskonzepts

- **Sicherheitszonen:** Definition von Sicherheitszonen innerhalb des Gebäudes (z.B. allgemeiner Bereich, eingeschränkter Bereich, Hochsicherheitsbereich).
- **Zutrittskontrollsysteme:** Einsatz von Zugangskontrolltechnologien wie RFID-Karten, biometrischen Scannern oder PIN-Codes zur Sicherung der Zugänge.
- **Überwachung:** Einsatz von Überwachungskameras und Bewegungsmeldern zur kontinuierlichen Überwachung sicherheitsrelevanter Bereiche.

3. Überwachung und Protokollierung

Zutrittsversuche und tatsächliche Zugriffe u sicherheitskritischen Bereichen werden protokolliert und überwacht?

13.b. Schutz vor umgebungsbezogenen Gefährdungen

1. Umgebungsschutzmaßnahmen

Es sind Maßnahmen zum Schutz vor umgebungsbezogenen Gefährdungen wie Feuer, Wasser oder extremen Witterungsbedingungen implementiert.

2. Standortauswahl und bauliche Maßnahmen

Bei der Auswahl des Standorts und der Bauplanung wurde auf die Minimierung von Umgebungsrisiken geachtet, z.B. Hochwasserschutz, Schutz vor Erdbeben oder Absicherung gegen Einflüsse durch benachbarte Industrieanlagen.

! Wichtige Schutzmaßnahmen

- **Brandschutz:** Implementierung von Brandschutzsystemen wie Rauchmeldern, Feuerlöschern und automatischen Löschanlagen (z.B. Sprinkleranlagen, CO2-Löschanlagen).
- **Wasserschutz:** Absicherung gegen Wasserschäden durch bauliche Maßnahmen wie erhöhte Serverräume oder wasserfeste Abdichtungen.
- **Schutz vor Erschütterungen:** Absicherung gegen Erschütterungen durch Verkehrswege oder Bauarbeiten in der Nähe.

13.c. Versorgungseinrichtungen

1. Sicherung der Versorgungseinrichtungen

Versorgungseinrichtungen wie Strom- und Wasserversorgung, Klimaanlage und Kommunikationsverbindungen sind gegen Ausfälle und Sabotage gesichert?

2. Redundanz und Notstromversorgung

Redundanzsysteme und Notstromversorgungen, wie z.B. unterbrechungsfreie Stromversorgungen (USV) und Dieselgeneratoren, sind implementiert, um den kontinuierlichen Betrieb im Falle eines Ausfalls sicherzustellen.

! Kritische Versorgungseinrichtungen

- **Stromversorgung:** Implementierung von USV-Anlagen und Notstromgeneratoren, um Ausfälle in der Stromversorgung zu überbrücken.
- **Kühlungssysteme:** Sicherstellung der Kühlung kritischer IT-Infrastrukturen durch redundante Klimaanlage und Backup-Systeme.
- **Kommunikationsverbindungen:** Nutzung redundanter Kommunikationswege, um die Erreichbarkeit und Datenübertragung auch bei Ausfällen zu gewährleisten.

Über techbold

Wir sind der Spezialist für sichere IT-Systeme

techbold hat sich auf die Errichtung und Betreuung von sicheren IT-Infrastrukturen für den Mittelstand spezialisiert und ist der perfekte Partner für alle Unternehmen, die sowohl IT-Security Lösungen als auch alle IT-Dienstleistungen und Services aus einer Hand beziehen möchten.

Mit unserem rund 170-köpfigen Team verantworten wir die IT-Systeme von über 900 Kunden aus 27 Branchen in 10 europäischen Ländern. Von großen Schulen, über die Amerikanische Handelskammer bis zu einem der modernsten Tiernahrungsproduzenten in Europa. Aber auch viele renommierte Kanzleien, Finanzunternehmen und Steuerberater zählen zu unseren Kunden.



Evelyn Heinrich
Head of Account Management

+43 699 1925 38 17
+43 59 555 520
ehe@techbold.at



Mario Novak
Head of New Business

+43 664 800 80 501
+43 59 555 501
mno@techbold.at

techbold Wien
techbold secure IT GmbH
Dresdner Straße 89, 1200 Wien
+43 59 555 | office@techbold.at

techbold Oberösterreich
techbold secure IT GmbH
Business Center Plus City, 5. OG
Plus-Kauf-Straße 7, 4061 Pasching
+43 59 555 | office@techbold.at

techbold Burgenland
techbold secure IT GmbH
Werner von Siemens-Straße 1, 7343 Neutal
+43 59 555 | office@techbold.at