IT-SECURITY

NIS-2 Action-Plan inklusive Checkliste

techbold

Liebe*r Leser*in,
NIS-2 wird bald für viele Unternehmen verpflichtend – höchste Zeit also, sich darauf vorzubereiten.

Zusammengefasst findest du in diesem Dokument einen umfassenden Überblick zu den Anforderungen der NIS-2 Richtlinie sowie eine praktische Checkliste, die dich Schritt für Schritt zur Compliance führt.

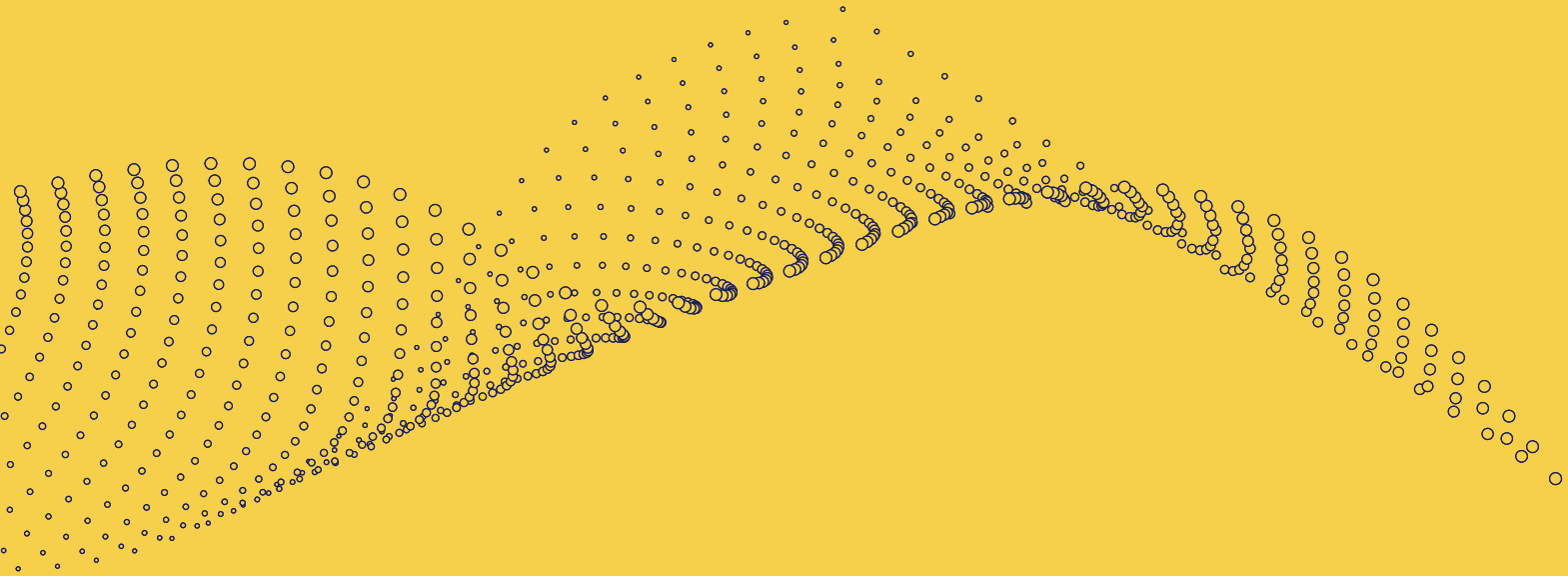
Der Überblick in Form eines Leitfadens führt in 6 übersichtlichen Schritten durch den Weg zur NIS-2 Konformität. Außerdem erklären wir spezifische Anforderungen und Begriffe von NIS-2.

Die Checkliste stellt eine praktische Hilfe dar und enthält alle Punkte, die zur Erfüllung der NIS-2-Konformität notwendig sind. Sie ist bewusst ausführlich gehalten, damit wirklich jeder Aspekt abgehakt werden kann. Zusätzliche Orientierung bieten Infokästchen, die Fachbegriffe und spezifische Anforderungen verständlich erklären.

Wir hoffen, dass dieses Dokument dir nicht nur hilft, die NIS-2 Anforderungen zu verstehen, sondern dich auch dabei unterstützt, sie gezielt umzusetzen.

Viele Grüße,

Damian Izdebski



NIS-2 Leitfaden

Inhalt

1. Kläre deine Betroffenheit ab

1.1 Abklärung der direkten Betroffenheit

Im ersten Schritt solltest du abklären, ob du ***direkt*** unter die NIS-2 Richtlinie fällst. Das bedeutet, dass du zu den ***wesentlichen*** oder ***wichtigen*** Einrichtungen gehörst.

Zu den ***wesentlichen*** Einrichtungen zählst du, wenn du ein großes Unternehmen (> 250 Mitarbeiter oder >50 Mio. Jahresumsatz oder Jahresbilanz) besitzt und aus den Sektoren Energie, Verkehr, Bankwesen, Finanzmarkt, Gesundheit, Trinkwasser, Abwasser, Verwaltung von IKT-Diensten oder Weltraum kommst.

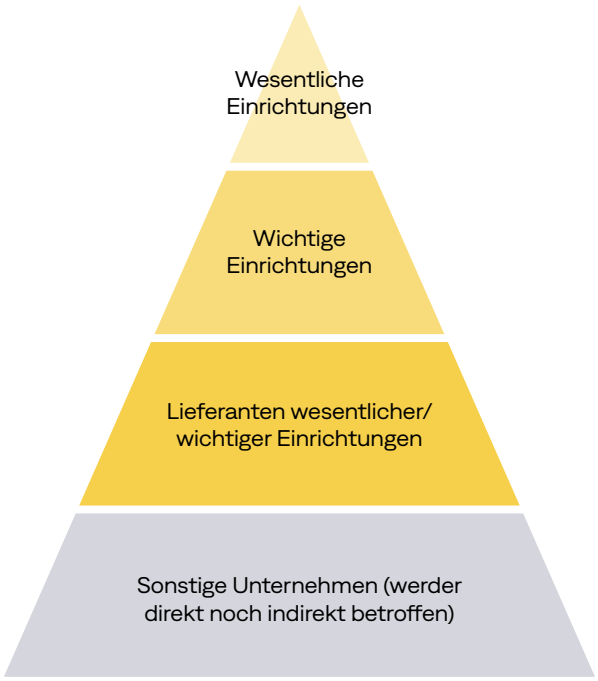
Wenn du aus den oben genannten Sektoren stammst, jedoch nur ein mittleres Unternehmen (50-250 Mitarbeiter oder 10 Mio. - 50 Mio. Euro Jahresumsatz oder Jahresbilanz) führst, giltst du als ***wichtige*** Einrichtung. Darüber hinaus gelten große und mittlere Unternehmen aus den Sektoren Post und Kurier, Abfall, Chemie, Lebensmittel, Produktion, Digitale Dienste oder Forschung als ***wichtige*** Einrichtungen.

Einen einfachen Selbsttest gibt es bei der WKO im Online Ratgeber, der auf Basis deiner Antworten in Single Choice Verfahren ermittelt, ob du unter die wesentlichen und wichtigen Einrichtungen fällst.

Wichtig zu wissen

Du musst selbst für dein Unternehmen feststellen, ob du unter NIS-2 fällst. Es wird keinen Bescheid von behördlichen Einrichtungen geben. Die NIS-2 Richtlinie ist seit 16.01.2023 auf EU-Ebene in Kraft. Das Datum für die österreichische Umsetzung des NISG und der Verordnungen ist noch unklar, jedoch wird damit spätestens Mitte 2025 gerechnet.

Übersicht zur Betroffenheit von NIS-2



Betroffene Unternehmen	NIS-2-Verpflichtung	Prüfregime	Nachweise
Wesentliche Einrichtungen	Ja	Ex Ante (regelmäsige und gezielte Audits)	Prüfung durch: • qualifizierte Stelle oder Behörde
Wichtige Einrichtungen	Ja	Ex Post (bei begründetem Verdacht)	Prüfung durch: • qualifizierte Stelle oder Behörde
Lieferanten wesentlicher/ wichtiger Einrichtungen	Ja	indirekt (Einforderung von Maßnahmen vom NIS-2 betroffenen Kunden	• ISO27001, TISAX, Cyber Trust Label
Sonstige Unternehmen (werder direkt noch indirekt betroffen)	Nein	-	• Nicht erforderlich • Basismaßnahmen der IT-Sicherheit werden empfohlen

Konsequenzen bei Nicht-Einhaltung

Ob dein Unternehmen eine ***wesentliche*** oder eine ***wichtige Einrichtung*** ist, macht bei der Umsetzung der geforderten Sicherheitsmaßnahmen keinen Unterschied. Der Unterschied besteht in den möglichen Sanktionen.

Bei ***wesentlichen*** Einrichtungen drohen bei Nichterfüllung Sanktionen bis zu 10 Mio. Euro oder 2 % des Gesamtjahresumsatzes des Unternehmens. Bei ***wichtigen*** Einrichtungen 7 Mio. Euro oder 1,4 % des Gesamtjahresumsatzes des Unternehmens.

1.2 Abklärung der indirekten Betroffenheit:

Wenn du ***direkt*** nicht betroffen bist, kannst du trotzdem ***indirekt*** betroffen sein. ***Indirekt*** betroffen bist du, wenn dein Unternehmen Lieferant einer ***wesentlichen*** oder ***wichtigen*** Einrichtung bist. Hierbei greift, was sich in der NIS-2 Richtlinie „Sicherheit der Lieferkette“ nennt. Unter diesen Umständen fällst du unter die NIS-2 Richtlinie und musst mindestens Basismaßnahmen umsetzen, um die Sicherheit der Lieferkette aufrecht zu erhalten.

Zusammenfassung:

1 **Mit dem online WKO-Selbsttest abklären, ob du *direkt* von NIS-2 betroffen bist.**

2 **Deine Lieferkette überprüfen, ob du *indirekt* von NIS-2 betroffen bist.**

2. Plane deine Ressourcen ein und kläre Verantwortlichkeiten

2.1 Personelle Ressourcen

Intern

Zunächst braucht es eine zentrale Rolle innerhalb des Unternehmens, die sich um die operative Umsetzung von NIS-2 und dessen Einhaltung kümmert. Dies ist eine zeitintensive Aufgabe und sollte ressourcentechnisch nicht unterschätzt werden. Besonders eignen sich Personen, die mit den Bereichen Organisation, IT oder Recht vertraut sind. Auch Personen mit einem Hintergrund im Bereich Qualitätsmanagement eignen sich für diese zentrale Position.

Denn durch die verschiedenen Bereiche (IT, Recht, Organisation), die von NIS-2 betroffen sind, findet die Umsetzung von Maßnahmen bereichsübergreifend statt. Das bedeutet, dass die Umsetzung einer technischen Maßnahme weitreichende organisatorische Auswirkungen haben kann.

Extern

Vor allem ***wesentliche*** und ***wichtige*** Einrichtungen sollten sich rechtliche, technische und/oder organisatorische Partner ins Haus holen, sofern sie die Bereiche nicht intern durch eigene Abteilungen abdecken. Externe Berater sind in ihren jeweiligen Bereichen auf NIS-2 spezialisiert und können wertvolle Impulse geben, um Konformität sicherzustellen. Außerdem helfen sie bei der Umsetzung bestimmter Maßnahmen.

BEISPIEL 1:

Eine technische Maßnahme umfasst, dass ein von mehreren Personen genutztes Postfach auf einzelne Postfächer aufgeteilt wird, damit nicht alle Personen Zugang zu sensiblen Informationen haben. Im Zuge der technischen Umsetzung muss sich die Abteilung auch organisatorisch umstellen und Prozesse neu definieren.

(Referenz NIS-2 Gesetz: Maßnahme 8. Zugangssteuerung b) Verwaltung von Zugriffsberechtigungen)

BEISPIEL 2:

In deinem Unternehmen werden technische Maßnahmen umgesetzt. Dafür muss es einen zentralen Ansprechpartner geben, an den sich Mitarbeiter wenden können. Dieser steht bei Fragen und für Erklärungen zur Verfügung. Beispielsweise weiß dieser Ansprechpartner, wie der Zugang zu einer Anwendung oder Dokumenten geregelt ist oder kann Auskünfte geben, z.B. wo und wie in Zukunft Passwörter abgespeichert werden dürfen.

(Referenz NIS-2 Gesetz:
Maßnahme 2. Sicherheitsrichtlinien
b) Funktionen, Aufgaben und Verantwortlichkeiten)

2.2 Verantwortlichkeit der Leitungsorgane

Für die Einhaltung der Pflicht von NIS-2 sind im Unternehmen die Leitungsorgane zuständig. Obwohl die Aufgaben der operativen Umsetzung durch interne oder externe personelle Ressourcen durchgeführt werden dürfen, obliegt den Leitungsorganen die Pflicht sicherzustellen, dass die Einhaltung von NIS-2 erfolgt.

Nach NIS-2 ist ein Leitungsorgan eine oder mehrere natürliche Personen oder Verwaltungsorgane, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung oder innerhalb der Einrichtung zur Überwachung der Geschäftsführung berufen sind. Erfasst werden soll die tatsächliche Leitungs- und Geschäftsführungsebene. Laut Erläuterungen zum NISG 2024 (vorbehaltlich Gesetzgebung) sind dies etwa der Vorstand, Geschäftsführer oder Aufsichtsrat der jeweiligen Einrichtung (WKO, 10.07.24).

2.3 Monetäre Ressourcen

Im Rahmen der NIS-2 Richtlinie wird von einem risikobasierten Ansatz gesprochen. Die Aufwendung der (monetären) Ressourcen und der Grad der Umsetzung müssen verhältnismäßig an dein Unternehmen angepasst und vernünftig sein. Daher gibt es keine Formel für die pauschale Berechnung der Kosten.

Ein guter Anfangspunkt ist die Durchführung eines internen Audits und/oder eines Beratungsgespräches mit Dienstleistern. Diese erheben den Status Quo und geben Einblick in erste Handlungsvorschläge inklusive Kostenschätzung.

Bei der Kostenschätzung kommt es darauf an, welche IT-Sicherheitsmaßnahmen dein Unternehmen schon umsetzt und welche Auswirkungen ein IT-Sicherheitsvorfall haben könnte.

!

Wichtig zu wissen

Selbst wenn du als Leitungsorgan Rollen intern und extern vergibst, bist du angehalten, Maßnahmen zu billigen und die Umsetzung sicherzustellen. Als Führungsorgan können dich bei Nichteinhaltung rechtliche Folgen treffen.

Zusammenfassung:

1 **Mindestens eine interne Rolle sollte für die operative Umsetzung der NIS-2 verantwortlich sein.**

2 **Sinnvoll ist die Zusammenarbeit mit externen Beratern in den Bereichen IT, Recht und Organisation.**

3 **Monetär ist eine Berechnung pauschal schwierig, da es auf verschiedene Variablen (Unternehmensgröße, vorhandene Maßnahmen & Prozesse) ankommt.**

3. Führe eine Risikoanalyse in Bezug auf NIS-2 durch

3.1 Durchführung einer Risikoanalyse

Eine Risikoanalyse kannst du intern oder extern durchführen lassen. Die durchführende Instanz sollte ein Fachverständnis für die Bereiche IT, Organisation und Recht aufweisen und darüber hinaus geschult sein, Risikoanalysen durchzuführen.

In beiden Fällen ist wichtig, die komplette Analyse schlüssig zu dokumentieren.

Wenn du einen externen Berater für die Risikoanalyse wählst, achte mindestens auf diese zwei Kriterien bei der Auswahl:

- → Ein gutes Fundament ist eine Zertifizierung nach anerkannten Standards wie z.B. ISO 27001
- → Der Dienstleister oder Berater kennt sich in deinem Markt/deiner Branche aus und hat Beispielkunden in ähnlichen Situationen betreut

Zuerst identifiziert die Risikoanalyse alle Assets (z.B. Clients, Server, Patente). Im nächsten Schritt überprüft der Analysierende, welcher Schaden entsteht, wenn Assets ausfallen und wie hoch die Eintrittswahrscheinlichkeit dafür ist.

Generell hängt die Risikoanalyse von Unternehmensgröße und Umfeld ab, sollte aber so detailliert wie möglich sein.

Außerdem kann man die NIS-1 zurate ziehen. Denn zu NIS-1 gibt es bereits diverse Verordnungen und Best Practices, die eine Basis für NIS-2 bilden. NIS-2 ist eine Erweiterung der NIS-1 und wird diese Richtlinie ersetzen. Eine Orientierung für die Aspekte einer Risikoanalyse und Best Practices bietet das NIS Factsheet 09/22.

Zusammenfassung:

1 **Die Risikoanalyse kann intern oder extern durchgeführt werden. Der Durchführende sollte Fachwissen vorweisen und sich an aktuellen Standards orientieren.**

2 **Der Umfang der Analyse hängt von Faktoren wie Unternehmensgröße und Umfeld ab. Jedoch gilt: Je detaillierter, desto besser.**

3 **Die Risikoanalyse muss ausführlich dokumentiert und intersubjektiv nachvollziehbar gestaltet sein.**

Wichtig zu wissen

Achtung: Bei der Risikoanalyse ist zu beachten, dass ein vernünftiger Aufwand betrieben wird. Das bedeutet, dass im Verhältnis zu deinem Unternehmen und seinem Impact eine passende Risikoanalyse durchgeführt wird. In einem Rechtsstreit muss glaubhaft gemacht werden können, dass die Risikoanalyse mit „due diligence“ (mit gebührender Sorgfalt) durchgeführt wurde. Es gibt immer Interpretationsspielraum, was das Ausmaß einer Analyse angeht. Daher sollte sich der Analysierende fachkundig auskennen, sorgfältig arbeiten und den Prozess ausführlich dokumentieren.

4. Ermittle Maßnahmen

4.1 Berater für die Ermittlung von Maßnahmen

In den drei Bereichen (IT, Recht, Organisation) gibt es verschiedene Spezialisten, die erfassen, welche Lücken in deinem Unternehmen in Bezug auf NIS-2 Compliance zu schließen sind. Gute Anhaltspunkte für die Vertrauenswürdigkeit bei der Auswahl deines Dienstleisters sind:

- **IT:** IT-Dienstleister und Security Anbieter, die anerkannte Zertifizierungen besitzen
- **Recht:** Rechtsanwälte, die sich auf IT-Recht/ Digitalisierung spezialisiert haben
- **Organisation:** z.B. ISO-Berater

Wichtig zu wissen

Stand jetzt (November 2024) wird noch diskutiert, ob man mit einer ISO 27001 Zertifizierung kausal NIS-2 konform ist. Denn die beiden überschneiden sich stark. Allenfalls ist eine ISO 27001 Zertifizierung ein guter Anhaltspunkt, um in die NIS-2 Konformität zu starten.

4.2 Eine Übersicht von Maßnahmen aus dem österreichischen Gesetzesentwurf

In Österreich umfasst der NIS-2 Gesetzesentwurf derzeit 13 Themengebiete für Risikomanagementmaßnahmen. Diese umfassen unter anderem folgende, wichtige Punkte:

→ **SICHERHEITSRICHTLINIE**
Organisationen müssen eine an ihre Ziele angepasste Sicherheitsrichtlinie erstellen, regelmäßig überprüfen und bei Bedarf aktualisieren.

→ **BEWÄLTIGUNG VON VORFÄLLEN**
Eine Richtlinie für den Umgang mit Sicherheitsvorfällen muss erstellt werden, die den Ablauf der Vorfallserkennung und -bewältigung regelt. Die Maßnahmen müssen dokumentiert und nach einem Vorfall analysiert werden.

→ **BUSINESS CONTINUITY**
Ein Notfallplan zur Betriebsfortführung und Wiederherstellung muss erstellt, regelmäßig getestet und durch sichere Backups unterstützt werden.

→ **SICHERE BESCHAFFUNG UND NUTZUNG VON IT-PRODUKTEN**
IT-Produkte müssen sicher beschafft, konfiguriert und aktualisiert werden. Organisationen müssen für sichere Softwareentwicklung und -nutzung sorgen.

→ **KONTROLLE DER EFFEKTIVITÄT**
Sicherheitsmaßnahmen müssen regelmäßig durch Assessments und Tests auf ihre Wirksamkeit überprüft und verbessert werden.

→ **VERSCHLÜSSELUNG**
Daten müssen je nach Schutzbedarf verschlüsselt werden, mit sicherem Management der kryptographischen Schlüssel.

→ **ZUGRIFFSKONTROLLE**
Es muss eine Access Control Policy etabliert werden, die den Zugang zu IT-Ressourcen regelt, insbesondere durch Multi-Faktor-Authentifizierung und regelmäßige Überprüfungen der Zugriffsrechte.

→ **PHYSISCHE SICHERHEIT**
Organisationen müssen durch Zugangskontrollen, Überwachung und Maßnahmen gegen physische Gefahren wie Feuer oder Überschwemmungen geschützt werden.

→ **RISIKOMANAGEMENT**
Ein Risikomanagement-Framework ist erforderlich, das Risiken identifiziert, bewertet und behandelt. Regelmäßige Überprüfungen und ein Compliance-Monitoring sind notwendig.

→ **MONITORING & LOGGING**
Aktivitäten in IT-Systemen müssen überwacht und in einem zentralen Event-Log aufgezeichnet werden. Die Logs sind vor unbefugtem Zugriff zu schützen und regelmäßig zu sichern.

→ **SICHERHEIT DER LIEFERKETTE**
Organisationen müssen die Sicherheit in ihrer Lieferkette durch Auswahlkriterien, Verträge und regelmäßige Überprüfungen der Dienstleister sicherstellen.

→ **NETZWERKSICHERHEIT**
Das Netzwerk muss durch Segmentierung, aktuelle Diagramme, Zugriffskontrollen und sichere Protokolle geschützt werden.

→ **SECURITY AWARENESS**
Mitarbeitende müssen über IT-Sicherheit und Cyberhygiene geschult werden. Spezielle Trainings sind für bestimmte Rollen erforderlich.

→ **ASSET MANAGEMENT**
Ein Inventar aller wichtigen Assets muss erstellt, laufend aktualisiert und entsprechend des Schutzbedarfs klassifiziert werden.

→ **PERSONELLE SICHERHEIT**
Sicherheitsrichtlinien müssen von allen Mitarbeitenden, Zulieferern und der Geschäftsführung verstanden und befolgt werden. Hintergrundprüfungen können für bestimmte Funktionen erforderlich sein.

4.3 Beispiele für Maßnahmen im Detail

Multi-Faktor-Authentifizierung

→ Bei der Multi-Faktor-Authentifizierung wird der Zugriff auf Systeme und Anwendungen durch mehrere unabhängige Merkmale abgefragt. Zu diesen Merkmalen zählen zum Beispiel Passwörter, Biometrie (wie Fingerabdruck) oder das Vorhandensein eines Hardwarekeys oder einer App. Alle Mitarbeiter brauchen Zugriff auf die Möglichkeit eine Multi-Faktor-Authentifizierung durchzuführen.

Laufendes Awareness Training

→ Es muss ein nachweisbares Training aller Mitarbeitenden auf den Umgang mit Daten und Möglichkeiten des Datenmissbrauchs von Dritten erfolgen. Die Schulungen sind von Online-Training bis Inhouse-Training möglich.

→ Außerdem müssen neue Mitarbeiter beim Onboarding nachweislich eine Schulung im Bereich Cyber-Security-Awareness und Datenmissbrauch absolvieren.

→ Für Leitungsorgane sind spezifisch gestaltete Cybersicherheitsschulungen vorgesehen.

Geschäftskontinuität: Vorliegen eines Disaster Recovery Plans

→ Aus IT-Sicht sollte für die Geschäftskontinuität ein Disaster Recovery Plan für die IT-Landschaft vorliegen. Damit im Falle eines Vorfalls ein detaillierter Plan besteht, was organisatorisch und technisch zu tun ist. Mindestens einmal pro Jahr sollte ein Test des Disaster Recovery Plans stattfinden.

→ Darüber hinaus muss der Disaster-Recovery-Plan up to date gehalten werden, damit alle aktuellen Prozesse und Systeme im Notfallplan vermerkt sind.

Geschäftskontinuität: Technische Maßnahmen

→ Die Geschäftskontinuität verlangt, dass technische Maßnahmen wie bspw. Backups bestehen. Die Risikoanalyse determiniert vorab Variablen wie den Aufbewahrungszeitraum von Backups. Im Sinne der Geschäftskontinuität sollten neue Technologien und Veränderungen immer unter NIS-2 Konformität aufgestellt werden.

Überprüfung der eigenen Zulieferer (Lieferkette)

→ Im Zuge der Sicherheit aller, müssen Unternehmen ihre Lieferanten und deren Basismaßnahmen in der Cybersecurity überprüfen. Dies geht am einfachsten über eine jährliche Einforderung von NIS-2 anerkannten Zertifikaten oder Cybertrust Labels.

→ Organisatorisch sollte ein Prozess eingeführt werden, der einen jährlichen Reminder ausschickt und alle Lieferanten in einem System (wie beispielsweise Cybertrust) mitsamt ihrer NIS-2 Konformitäts-Bestätigung ablegt. Unternehmen sind angehalten, die NIS-2 Konformität ihrer Lieferkette jährlich und vor dem Start einer Zusammenarbeit zu prüfen.

Wichtig zu wissen

Das Cyber Trust Austria Label stellt eine wichtige Unterstützung zur Erreichung von NIS-2 Compliance dar. Einerseits dient es als Nachweis der eigenen Basissicherheitsmaßnahmen (und im Fall des Silber oder Gold Labels sogar einer fortgeschrittenen Sicherheit) und andererseits kann es im Management des Lieferantenrisikos (Third Party Risk Management) ein wesentliches Element zum Nachweis der erforderlichen Sicherheit ihrer Lieferanten sein (Cybertrust, 11.10.24).

5. Maßnahmen umsetzen

5.1 Implementierung von ausgewählten Maßnahmen

Mit einer Umsetzung sollte definitiv nicht bis zum Inkrafttreten des österreichischen Gesetzes gewartet werden.

Viele Maßnahmen, wie bspw. ***Notfallpläne*** und ***Business-Kontinuität***, brauchen Vorlaufzeit und vorhergegangene Maßnahmen, wie bspw. das ***Assetmanagement*** oder ***Recovery Pläne***. Diese Vorlaufzeiten können unter Umständen recht lange dauern. Deswegen ist ein sofortiger Start sinnvoll – sofern nicht schon geschehen. Unternehmen sollten jetzige Anhaltspunkte, wie bspw. die NIS-2 EU-Richtlinie, die NIS-1 Verordnungen, die ISO 27001 Zertifizierung und Cybertrust Labels nutzen, um mit der Umsetzung zu starten.

Ob du die Maßnahmen durch interne Rollen- und Aufgabenverteilung umsetzt, ist von den Behörden nicht vorgegeben. Allerdings musst du während der Umsetzung ein schriftlich ausreichendes Protokoll anfertigen.

5.2 Nicht-Einhalten von NIS-2 Konformität

Kurz zusammengefasst: Es besteht die Gefahr von Sanktionen, insbesondere Strafzahlungen sowie rechtlichen Konsequenzen. Darüber hinaus besteht das Risiko, dass Kunden nicht mehr mit deinem Unternehmen zusammenarbeiten dürfen, weil es ein zu großes Sicherheitsrisiko birgt und sie selbst sanktioniert würden.

Zusätzlich ist bekannt, dass ***wesentliche*** Einrichtungen stichprobenartig überprüft werden. ***Wichtige*** Einrichtungen werden bei begründetem Verdacht auditiert.

Generell wird die Behörde bei gemeldeten Vorfällen unter anderem auf die Fahrlässigkeit schauen.

Beispiel: Ein Unternehmen, welches eine umfassende Risikoanalyse durchgeführt und passende Maßnahmen umgesetzt hat, wurde gehackt. In diesem Fall war keine Fahrlässigkeit im Spiel – das Unternehmen hat versucht, sich bestmöglich zu schützen. Es wird aus dem Angriff gelernt und Maßnahmen werden ergänzt. Hätte das Unternehmen in der Risikoanalyse ein mögliches Risiko erfasst, jedoch keine Maßnahmen umgesetzt, so kann ihm dies als Fahrlässigkeit ausgelegt werden.

Zusammenfassung:

1 **Die Implementierung der Maßnahmen kann intern und / oder extern erfolgen.**

2 **Nicht-Einhalten von NIS-2 kann hohe Sanktionen haben.**

3 **Regelmäßige IT-Audits zeigen Anpassungsbedarf von Maßnahmen.**

6. Überprüfe deine IT laufend

6.1 Kontinuierliche Überprüfung

Eine kontinuierliche Überprüfung im technischen Bereich bedeutet eine Überprüfung der IT-System-Architektur, die mindestens einmal pro Jahr mittels Schwachstellen-analyse, Penetrationstest-Test oder IT-Audit durchgeführt wird.

6.2 Audits

Dein Unternehmen sollte mindestens einmal pro Jahr ein internes Audit durchführen, welches unter anderem die Einhaltung der NIS-2 Richtlinie überprüft.

Auch externe Audits, wie beispielsweise die ISO 27001, sind passend, um deine Prozesse und Systeme fortlaufend konform zu halten.

6.3 Berichterstellung

Ein jährlicher Bericht dokumentiert die Analyse, Erstellung sowie die Einhaltung von Maßnahmen. Dieser ist schriftlich abzulegen und gewährleistet durch eine detaillierte Beschreibung intersubjektive Nachvollziehbarkeit.

Diese Berichte müssen nicht an eine Behörde versendet werden – außer, dein Unternehmen wird explizit dazu aufgefordert.

Wichtig zu wissen

Disclaimer: Updates und andere Aktualisierungen im technischen Bereich müssen natürlich häufiger durchgeführt werden.

Zusammenfassung:

1. **Die IT-System-Architektur muss mindestens jährlich geprüft werden.**
2. **Interne und externe Audits unterstützen NIS-2 Konformität.**
3. **Berichte sollten jährlich verfasst, abgelegt und nachvollziehbar gestaltet werden.**

NIS-2 Checkliste

Inhalt

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 Virenscans 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 Cyberrisiken, 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 ge ändert 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 Vorfallsmeldungen ☐

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 Sicherheits-richtlinien 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 egelmäßig 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 zu 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, Klimaanlagen 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 Klimaanlagen 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 1 925 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

Stand: 11.2024