IT-SECURITY

NIS-2 Action-Plan für Unternehmer

techbold.at

techbold

Liebe*r Leser*in,

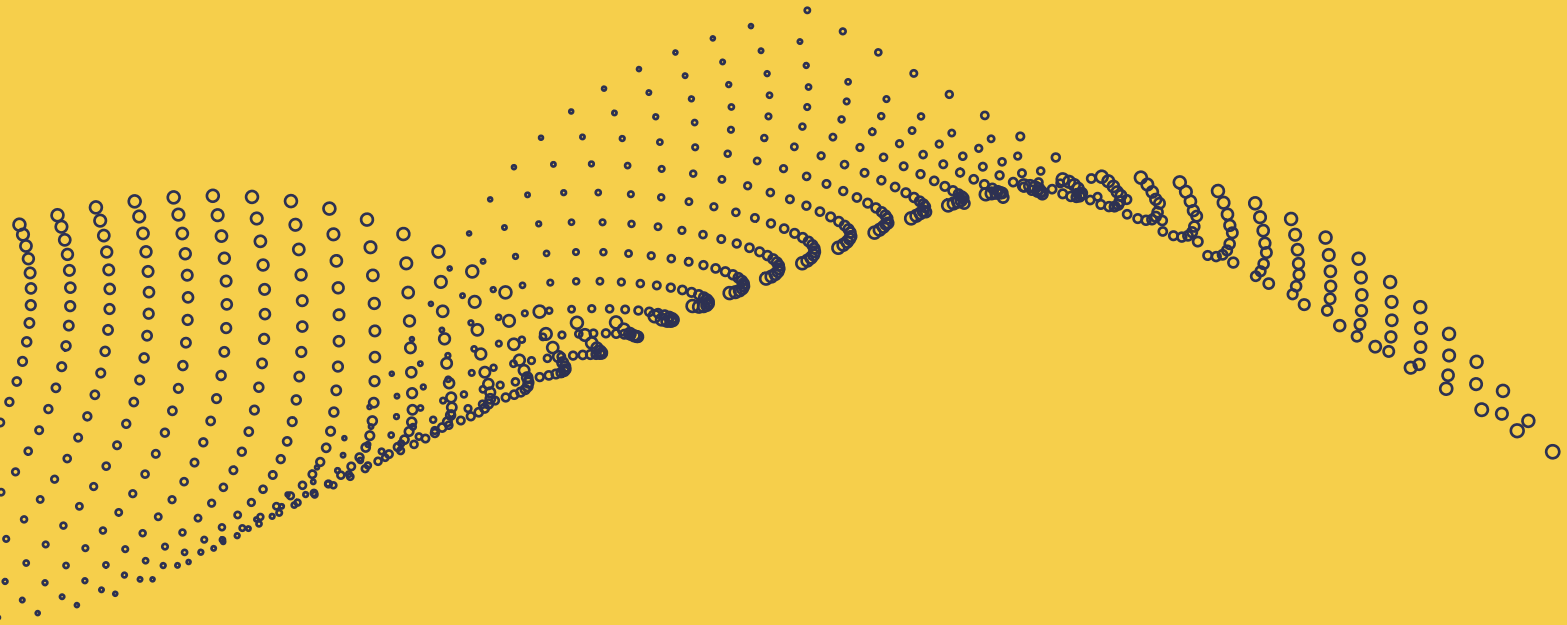
NIS-2 ist in aller Munde – und das mit gutem Recht. Denn die Umsetzung von Maßnahmen wird bald zur Pflicht für Unternehmer. Das lässt nur noch ein kurzes Zeitfenster offen, um sich mit dem Thema auseinanderzusetzen und dein Unternehmen vorzubereiten.

Und trotzdem: oft findet man im Internet schwammige Artikel zum Thema NIS-2, die keine wirklich Handlung – keinen konkreten Action-Plan – hergeben. Manchmal findet man Artikel, die sich im Fachjargon verlieren.

Deswegen wollen wir dir mit diesem Leitfaden aufschlüsseln, was unter einzelne Handlungsschritte fällt und wo du ansetzen kannst. Und dir damit einen greifbaren Plan an die Hand geben.

Viele Grüße,

Damian Izdebski



Inhaltsverzeichnis

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.

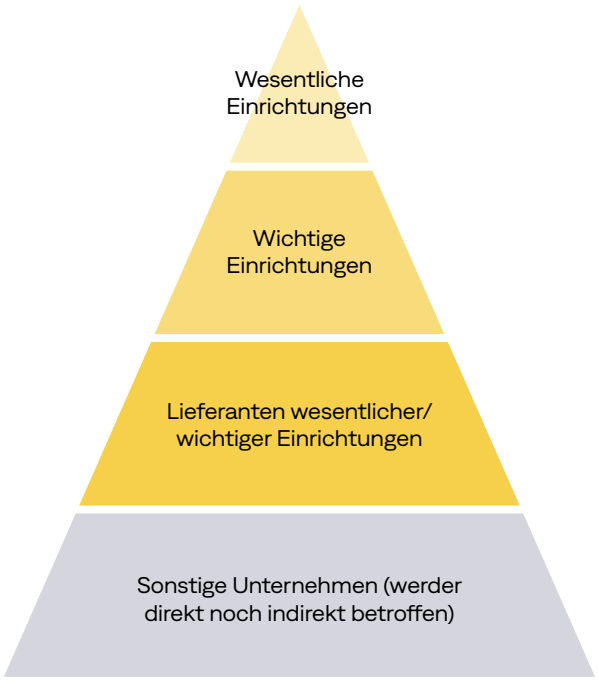
Wenn du aus den oben genannten Sektoren stammst, jedoch nur ein mittleres Unternehmen (50-250 Mitarbeiter oder 10 Mio. - 50 Mio. Euro Jahresumsatz oder Jahresbilanz) führst, giltst du als ***wichtige*** Einrichtung. Darüber hinaus gelten große und mittlere Unternehmen aus den Sektoren Post und Kurier,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

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