NIS2

ist kein Kinderspiel

Leitfaden OT - Network and Information Security 2

INDUSTRIAL AUTOMATION

NIS 2 compliant

siehe Seite 3

Ab dem 17. Oktober 2024 gibt es kein Zurück mehr.

“Stellen Sie sich vor, Sie betreten einen dunklen Raum, und plötzlich erstrahlt eine Taschenlampe, die jede Ecke ausleuchtet”

Genau das ist das NIS 2 - Gesetz für Ihr Unternehmen.

NIS 2 ist keine weitere bürokratische Hürde, sondern ein klarer Schritt in Richtung einer sicheren und widerstandsfähigen Zukunft.

Jeder, der bereits einmal in einem IT-/ OT-Projekt gearbeitet hat, weiß, dass die festgelegten Umsetzungsfristen für Projekte dieser Größenordnung nie ausreichen.

Somit werden viele Unternehmen auch hier die gesetzte Frist nicht einhalten, selbst wenn sie jetzt noch mit der Umsetzung starten würden. Dafür sind die im Zusammenhang mit dem Framework diskutierten Themenfelder viel zu umfangreich.

Eines ist jedoch klar: Im Gegensatz zur DSGVO ist für das neue NIS 2 - Gesetz **keine Übergangszeit** geplant.

Somit fallen alle betroffenen Unternehmen faktisch

am Tag nach dem 17. Oktober 2024 (oder nach Regierungsbeschluss)

unter die neuen Security-Regeln und können von den Behörden entsprechend kontrolliert werden.

Auch wenn die Prüfmechanismen noch gar nicht konkret feststehen und der Gesetzgeber nicht auf einem Schlag hunderte von NIS 2 - Auditoren auf die Betriebe loslassen wird - jetzt ist dennoch der Moment, in dem Sie die Zügel in die Hand nehmen und Ihr Unternehmen auf das nächste Level heben müssen.

INDUSTRIAL AUTOMATION

NIS 2 compliant

Ab dem 17. Oktober 2024 gibt es kein Zurück mehr, oder?

Stand: 11.09.2024

(diese Seite wird laufend aktualisiert)

Das NIS 2 - Gesetz ist zwar noch nicht beschlossen, ist aber EU-weit bereits in Kraft. Österreich sollte das NIS 2-Gesetz bis Stichtag 17.10.2024 in nationales Recht umwandeln.

Das bedeutet: Die NIS2-Richtlinie ist bereits wirksam und wurde von den 27 EU-Mitgliedsstaaten beschlossen. Der Begutachtungsentwurf in Österreich wurde mittels eines Indikativantrags an den Nationalrat gestellt.

Derzeit gibt es daher zwei mögliche Szenarien, die von der Nationalratswahl im Herbst abhängen:

1. **Variante A:** Sollte der Beschluss vor der Nationalratswahl fallen, ist die Frist der **1. Juni 2025.** (bedeutet: Verstoß gegen die NIS 2 Richtlinie auf EU-Ebene)
2. **Variante B:** Ist der Beschluss vor der Sommerpause der Regierung abgeschlossen**,** bleibt der **17.10.2024** als Stichtag bestehen.

Wir müssen daher abwarten, welche Variante ihre Gültigkeit erlangt. Noch einmal **zur INFO:** die **NIS2 Richtline** ist bereits mit **16. Jänner 2023** in Kraft - es muss nur noch das Gesetz umgesetzt werden.

Die meistgestellte Frage an uns:
Welche Maßnahmen sollen bzw. müssen umgesetzt werden? Seriöserweise kann das zu diesem Zeitpunkt niemand genau beantworten, da es:

- a) noch kein endgültiges Gesetz und
- b) noch keine Detailverordnung

gibt.

Man ist gut beraten, wenn man sich bereits jetzt an der **Maßnahmen zum Risikomanagement für Cybersicherheit (Art. 21)** orientiert. Ein Informationssicherheits-managementsystem **(ISMS**) nach **ISO 27001** bietet die ideale Grundlage, um die Anforderungen von NIS-2 zu erfüllen. ISO 27001 ist ein international anerkannter Standard, der die Planung, Implementierung, Überwachung und Verbesserung der Informationssicherheit in Unternehmen systematisiert. Ebenfalls eine Orientierung bietet die **IEC 62443 2-1:** Supplay Chain security und **IEC 62443 T eil 3-3** System security requirements and security levels.

NIS Fact Sheet 9/22 - Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

Aber:

Muss man Sicherheit per Gesetz vorschreiben?

Haben **Sie** schon von der **NIS-Richtlinie (NIS 1)** und dem **NIS-Gesetz (NIS 2)** gehört? Es fordert Betreiber kritischer Infrastrukturen und wesentliche und wichtige Unternehmen dazu auf, ein hohes Sicherheitsniveau ihrer IT- und OT-Systeme sicherzustellen. Ziel ist es, Cyberangriffe zu verhindern – ein Thema, das heute relevanter denn je ist.

Primär betrifft das Gesetz große Unternehmen wie Energieversorger, Öl- und Gaskonzerne, Trinkwasserverbände sowie Banken. **Man könnte annehmen, dass diese Betriebe bereits vor NIS 2 - mit NIS 1 - alles unternommen haben, um die Sicherheit ihrer IT- / OT-Systeme zu optimieren.**

Ist es daher wirklich notwendig ein solches Gesetz zu erlassen und zusätzliche Verpflichtungen auf-zuerlegen?

Die Verantwortlichkeit für IT/OT-Sicherheit sollte nicht nur bei den IT-Abteilungen liegen, sondern auch von der Geschäftsführung aktiv unterstützt werden. Täglich liest man über Unternehmen, die durch Hacker-Angriffe erheblichen Schaden erlitten haben. Niemand möchte, dass das eigene Unternehmen in einer solchen Schlagzeile auftaucht.

OT-Security, speziell in Bereichen wie Steuerung, Messung und Automatisierung, ist besonders kritisch. Ein Hacker, der Zugang zu Maschinen oder Anlagen erhält, stellt eine potenziell größere Gefahr dar als einer, der „nur" Dateien verschlüsselt, um Lösegeld zu verlangen.

Es ist klar, dass eine fortschrittliche IT/OT-Security für jedes Unternehmen oberste Priorität haben sollte. Unsere Erfahrung zeigt, dass fast alle Kunden durch die NIS-Richtlinie Verbesserungen erzielt haben. Zwar wurde auch viel Dokumentation erstellt, die vielleicht nicht immer gelesen wurde, und manchmal sind die Maßnahmen über das Ziel hinausgeschossen. Doch letztlich profitieren viele Betriebe von erhöhter Sicherheit und einem gestärkten Bewusstsein des Managements für die Risiken.

War die Einführung eines Gesetzes notwendig?

Vermutlich. Oft braucht es einen externen Impuls, um notwendige Veränderungen zu bewirken.

Auch wenn Ihr Unternehmen nicht direkt unter das NIS-Gesetz fällt, fragen Sie sich vielleicht, wie gut Sie auf den Ernstfall vorbereitet bzw. ob Sie Lieferant sind.

Daher haben wir diesen Folder erstellt, um Sie zu sensibilisieren, die wichtigsten Informationen zusammenzufassen und Ihnen einen klaren und verständlichen Überblick über das NIS 2-Gesetz in Österreich zu bieten.

INDUSTRIAL AUTOMATION

NIS 2 compliant

NIS 2 also doch nicht ganz so neu?

Die **Cybersicherheits-Richtlinie NIS 2 ist seit Jänner 2023** in Kraft. Diese muss bis **17. Okt. 2024** in Österreich umgesetzt werden.

Ab diesem Zeitpunkt gelten für **Unternehmen in bestimmen Bereichen**, wie zB. Energie, Gesundheitswesen, Transport uvm. ganz konkrete Mindeststandards hinsichtlich IT- / OT-Sicherheit und der Meldepflicht bei Ereignissen.

Davon sind **vorwiegend mittlere und große Organisationen** betroffen – **aber auch kleine Unternehmen können betroffen sein, wenn diese als Zulieferer gelten oder wenn sie essenziell für die Aufrechterhaltung kritischer gesellschaftlicher bzw. wirtschaftlicher Aktivitäten sind.**

NIS 2 ist kein Kinderspiel:

Was steckt dahinter?

Die EU-Richtlinie **NIS 2** ist eine überarbeitete Version der NIS 1-Richtlinie, die strengere Cybersicherheitsstandards für Unternehmen mit mindestens **50 Mitarbeiter:innen und 10 Millionen Euro** Umsatz in bestimmten Sektoren vorschreibt.

NIS 2-compliant zu sein, stellt somit sicher, dass Ihr Unternehmen den strengen Sicherheitsanforderungen der EU-Richtlinie standhält.

Sie wurde als Reaktion auf die **erhöhte Bedrohung von kritischen Infrastrukturen durch digitale Angriffe** eingeführt, um solche potenziell katastrophalen Angriffe zu verhindern.

Mit der Einführung der **NIS 2** sind Unternehmen verpflichtet, sich selbst einzustufen, sich bei der zuständigen Behörde zu registrieren, Sicherheitsvorfälle zu melden und eine Reihe von Sicherheitsmaßnahmen zu ergreifen, einschließlich Risikomanagement, Sicherheit in der Lieferkette und angemessene Reaktion auf Sicherheitsvorfälle.

Insgesamt zielt NIS 2 darauf ab, die Cybersicherheitslage der Anbieter wesentlicher Dienste zu verbessern, die Meldung der Zwischenfälle und die Zusammenarbeit zu fördern und die allgemeine Widerstandsfähigkeit kritischer Sektoren in der EU zu erhöhen.

TIPP:

- **Risikomanagement** als Grundpfeiler etablieren
  (Beaufsichtigung und Durchsetzung)
- **Sicherheitsmaßnahmen** ergreifen
- **Informationssicherheitsstandards** in Lieferketten sicherstellen
- **Cybersecurity-Kompetenz** entwickeln
- **Sicherheitsvorfälle** melden und angemessen behandeln

Wen trifft NIS 2?

- **Branchen mit hoher Kritikalität (wesentlich)**
- **Branchen mit geringer Kritikalität (wichtig)**

Betroffene Unternehmenskategorien

Die Richtlinie betrifft grundsätzlich **alle Betreiber kritischer Infrastrukturen** und darüber hinaus die **Betreiber wichtiger und wesentlicher Dienste, mit Niederlassung in der EU,** egal ob öffentliche oder private Einrichtungen.

Sie müssen abhängig von Netz- und Informationssystemen sein, einen Dienst bereitstellen, der für die Aufrechterhaltung kritischer gesellschaftlicher und oder wirtschaftlicher Tätigkeiten unerlässlich ist, und, bei denen ein Sicherheitsvorfall eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirkt.

Wer konkret betroffen ist, lässt sich nicht in einem Satz sagen. Bei den **“Essential Entities” oder Branchen mit hoher Kritikalität (den wesentlichen Diensten)** sind es beispielsweise Unternehmen mit über 250 Mitarbeiter:innen, 50 Mio. Euro Umsatz oder 43 Mio. Euro Bilanzwert. Doch daneben gibt es noch die **“Important Entities” oder Branchen mit geringer Kritikalität (den wichtigen Diensten)** und **mittlere Firmen (KMU)** mit anderen Klassifizierungen. Kleine Unternehmen werden jedoch, anders als in der NIS 1 Richtlinie, mit in die Verantwortung genommen.

Sektoren mit hoher Kritikalität:

- **Energie**
- **Verkehr**
- **Bankwesen*)**
- **Finanzmarktinfrastrukturen*)**
- **Gesundheitswesen**
- **Trinkwasser**
- **Abwasser**
- **Digitale Infrastruktur**
- **Verwaltung von IKT-Diensten B2B**
- **öffentliche Verwaltung**
- **Weltraum**

Sonstige kritische Sektoren:

- **Post- und Kurierdienste**
- **Abfallbewirtschaftung**
- **Chemie**
- **Lebensmittel**
- **verarbeitendes/herstellendes Gewerbe**)**
- **Anbieter digitaler Dienste**
- **Forschung (fakultativ)**
- im **Finanzsektor** hat die Verordnung (EU) 2022/2554, kurz **DORA** Vorrang vor NIS 2

Ab wann gilt ein Unternehmen als “groß“ oder “mittel“?

Die Einstufung einer Einrichtung als “mittleres” oder als “großes” Unternehmen richtet sich nach der **Anzahl der Mitarbeiter:innen**, dem **Jahresumsatz** und der **Jahresbilanzsumme**

Großes Unternehmen:

Eine Einrichtung gilt als “groß”, wenn wenn sie zumindest **250 Mitarbeiter:innen beschäftigt oder wenn sie einen Jahresumsatz von über 50 Millionen Euro erzielt UND sich die Jahresbilanzsumme auf über 43 Millionen Euro beläuft.**

Mittleres Unternehmen:

Eine Einrichtung gilt als „mittleres Unternehmen“, wenn sie zumindest **50 Mitarbeiter:innen beschäftigt, ODER wenn sie einen Jahresumsatz von über zehn Millionen Euro erzielt UND sich die Jahresbilanzsumme auf über zehn Millionen Euro beläuft, sofern sie nicht bereits als großes Unternehmen gilt.**

ACHTUNG:

Bei **Unternehmen mit einer komplexeren Struktur (z.B. Tochtergesellschaft im Konzern)** ist eine Einzelfallprüfung erforderlich. Für die Beurteilung wird neben der Unternehmensgröße (d.h. Mitarbeiterzahl und Umsatz- bzw. Bilanzzahl) berücksichtigt, ob es sich um ein eigenständiges Unternehmen, Partnerunternehmen (Beteilungen an anderen Unternehmen ab 25 % bis 50 %) oder verbundenes Unternehmen (Beteiligungen an anderen Unternehmen über 50 %) handelt.

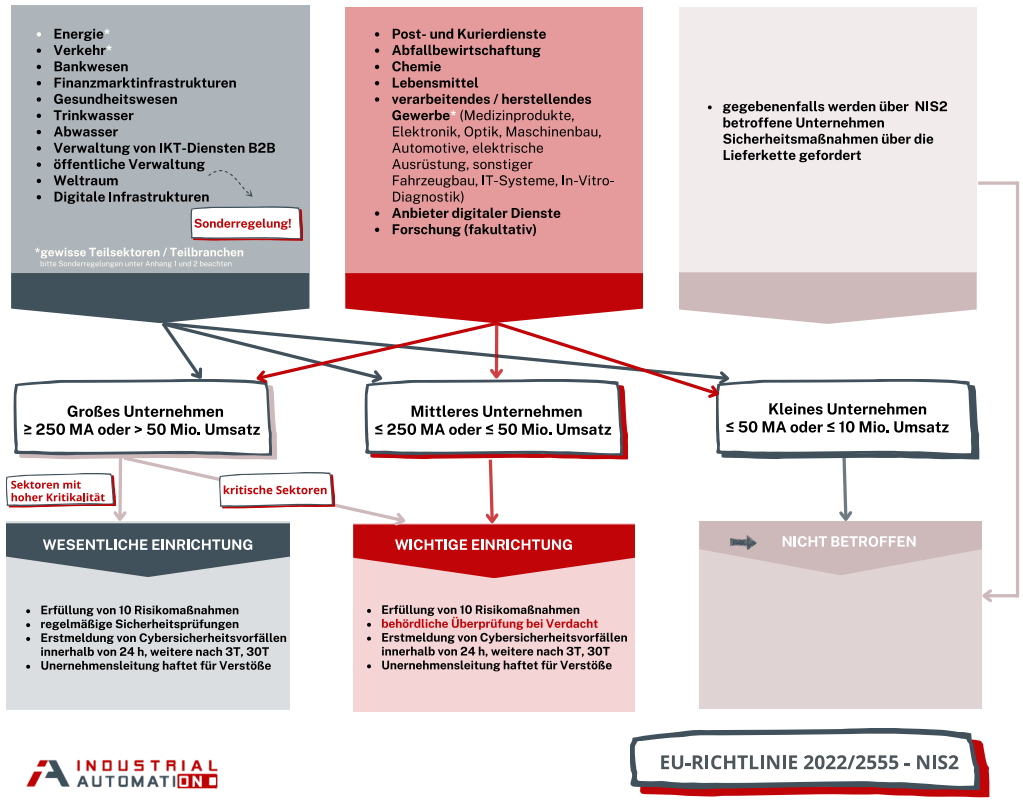
Sind auch kleine Unternehmen betroffen?

Kleine Unternehmen, d.h. Unternehmen, die **weniger als 50 Mitarbeiter:innen beschäftigen oder die entweder einen Jahresumsatz von höchstens 10 Mio. Euro erzielen bzw. deren Jahresbilanzsumme sich auf höchstens 10 Mio. Euro beläuft, fallen nicht unter NIS 2.**

Dabei gibt es jedoch **Ausnahmen** – folgende Unternehmen fallen unabhängig von ihrer Größe in den Anwendungsbereich:

- Vertrauensdiensteanbieter
- Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
- TLD-Namenregister und DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern
- Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essenziell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.

Zusätzlich müssen auch **Dienstleister und Lieferanten** von betroffenen Unternehmen Sicherheitsvorkehrungen einhalten.



Was sind die Unterschiede, ob ein Unternehmen als wesentlich oder wichtig gilt?

Ob man als Unternehmen eine wesentliche oder eine wichtige Einrichtung im Sinne der Richtlinie ist, macht bei der Umsetzung der geforderten Sicherheitsmaßnahmen (siehe unten) keinen Unterschied. Es gibt jedoch Unterschiede bei der Aufsicht und den Sanktionen:

“Essential Entities” oder Branchen mit hoher Kritikalität (den wesentlichen Diensten)

- regelmäßige und gezielte Sicherheitsprüfungen („ex-ante“)
- Stichprobenkontrollen
- Bußgeldrahmen 10 Mio. Euro oder 2 Prozent des weltweiten Umsatzes (je nachdem, welcher Betrag höher ist)

“Important Entities” oder Branchen mit geringer Kritikalität (den wichtigen Diensten)

- Überprüfungen nur bei begründetem Verdacht („ex-post“)
- Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen
- Bußgeldrahmen 7 Mio. Euro oder bei 1,4 Prozent des weltweiten Umsatzes

INDUSTRIAL AUTOMATION

NIS 2 compliant

Was gilt für die „Digitale Infrastruktur“?

Für den Sektor „Digitale Infrastruktur“ gibt es Ausnahmeregelungen für den Anwendungs-bereich und die Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen.

Auf diese möchten wir hier nicht näher eingehen, da wir uns als Industrial Automation GmbH mit OT-Security befassen.

Was gibt die Richtlinie Unternehmen vor?

Betroffene Einrichtungen müssen sich **binnen 3 Monaten nach Inkrafttreten des NISG 2024 registrieren**. Es sind Risikomanagementmaßnahmen zu treffen und Berichtspflichten zu beachten.

Die Leitungsorgane (Geschäftsführer:in bei GmbH, Vorstand und Aufsichtsrat bei Aktiengesellschaft) haben die Einhaltung der Risikomanagementmaßnahmen sicherzustellen und zu beaufsichtigen, haften der Einrichtung für den schuldhaft verursachten Schaden und müssen an für diese spezifisch gestalteten Cybersicherheitsschulungen teilnehmen.

Welche Risikomanagement-maßnahmen sind zu treffen?

10 Mindestmaßnahmen:

- Konzept Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaß-nahmen
- Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle
- Multi-Faktor-Authentifizierung

Dabei zu berücksichtigen sind:

- **der Stand der Technik**
- **europäische und internationalen Normen**
- **Kosten der Umsetzung**
- **bestehendes Risiko**

Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

- Zunächst gilt es für **Verantwortliche**, die unternehmensinternen kritischen Infrastrukturen und Dienstleistungen zu **identifizieren** und auf ihr **Sicherheitsniveau** zu prüfen.
- Sind diese bekannt, müssen im nächsten Schritt umfassende **Sicherheitsvorkehrungen** für diese getroffen werden. Wichtig ist, dass diese sowohl in der Unternehmensstrategie als auch **dediziert auf der Prozessebene gedacht, gelebt und umgesetzt** werden. Eine **gute Orientierung liefern Standards**, beispielsweise die **ISO 27001** Zertifizierung. **Identifizieren Sie in der Industrial Ethernet-Netzwerk Infrastruktur den managebaren Switch/Router zwischen den Bereich Leitstand, SCADA, Historien und den Steuerungen, Controllern sowie Aktoren und Sensoren**
- Um die eingeführten Maßnahmen langfristig aufrecht zu erhalten, müssen **neben der Implementierung auf Prozessebene** ein **System zur Überwachung von Sicherheitsvorfällen sowie Vorgänge und Verantwortlichkeiten für die Meldepflicht** von einem Vorfall eingerichtet werden. Insbesondere das Einhalten der Meldepflicht von sicherheitsrelevanten Vorfällen an die nationale Behörde für Cybersicherheit muss hier gewährleistet sein
- Auch wenn die Meldewege definiert wurden, sind Sicherheitsvorfälle zu jedem Zeitpunkt zu vermeiden. Die intern festgelegten **IT- / OT-Sicherheitsrichtlinien müssen dafür regelmäßig geprüft werden und an die äußere Bedrohungslage angepasst werden**
- Damit die IT-Sicherheit unternehmensweit eingehalten wird, ist sowohl **Aufklärung als auch Sensibilisierung der eigenen Mitarbeiter** unerlässlich. Relevanz und Bedrohlichkeit sowie gängige Einfallstore für Kriminelle und die eigene Kompetenz und Verantwortung muss jedem einzelnen Mitglied Ihrer Organisation bewusst sein
- Überprüfen Sie ebenfalls **Online-Dienstleister**, die für Ihr Unternehmen tätig sind, um sicherzustellen, dass auch hier keine Fehler und Sicherheitslücken in der Verarbeitung Ihrer Daten entstehen.

Was auf Firmen zukommt:

Von den Unternehmen fordert das **NIS 2 Gesetz** umfangreiche **technische, operative und organisatorische Maßnahmen**. Dazu gehört ein **Risikomanagement für Netzwerke und die Sicherheit der Lieferkette**. **Ebenso Pläne, um auf Angriffe oder Anomalien schnell reagieren und so die Geschäftskontinuität sicherstellen zu können**.

Das Risikomanagement sieht beispielsweise monatliche interne Sicherheitsprüfungen vor. Veraltete Software etwa auf Unternehmenscomputern und Anlagen sind ein potentielles Sicherheitsrisiko, das es zu identifizieren und zu bewerten gilt. Als Konsequenz muss die Software schnellstmöglich upgedatet oder gar entfernt werden. Diese proaktive Herangehensweise kann potentielle Risiken frühzeitig erkennen und beheben, denn nicht jeder “Angriff”, jede Kommunikation erfolgt aus und mit “fremden” Netzwerken. Anomalien zu erkennen ist das A&O eines sicheren Assetmanagements.

Gleiche Szenarien finden sich für das Lieferkettenmanagement.

Hier geht es darum, auch die Zulieferer einzubinden. Das Unternehmen wird zum Beispiel vertraglich festlegen, dass der Zulieferer regelmäßige Sicherheitsprüfungen durchführt, Richtlinien einhält und im Falle von Sicherheitsvorfällen angemessen reagiert.

Was bedeutet “Sicherheit in der Lieferkette”?

Von **NIS 2** betroffene Einrichtungen müssen die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern beachten.

Sie müssen die spezifischen Schwachstellen der einzelnen unmittelbaren (Dienste-)Anbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.

Daher betrifft das NIS 2 Gesetz fast alle Unternehmen.

Solche Maßnahmen minimieren das Risiko von Cyberangriffen und Anomalien innerhalb der Lieferkette und stärken die Cybersicherheit und den Fortbestand des eigenen Unternehmens. Sie können noch so gut abgesichert sein - zukünftig werden **80% der Angriffe über die Lieferkette** einfallen.

INDUSTRIAL AUTOMATION

NIS 2 compliant

Beispiel einer Lieferkette:

Teil 1: Hardware / Firmware:

- **Waver Herstellung --> Chip Paketierer --> Chip Lieferanten --> Modul Assemblierer --> Modul Lieferant --> Automobile Zulieferer --> Automobil Hersteller**

Teil 2: Software / Kommunikation:

- **Integrator in das Fahrzeug-Betriebssystem --> Datenanbindung in die Cloud des Herstellers (mit Sublieferanten) --> Hersteller der Handy App --> Datenanbindung aus der Cloud an die Handy App**

Teil 3: Betrieb / Support:

- **Benutzerverwaltung, Überwachung, Datenauswertung --> 1st, 2nd & 3rd Level Support, Updates (nur Software, ggf. Firmware), ...**

Vor der Behörde muss nachgewiesen werden können, dass sämtliche zumutbaren Maßnahmen innerhalb der Lieferkette ergriffen wurden und **man die Lieferanten unter Kontrolle hat**.

Langjährige Partnerschaften sind daher oft problematisch, da diese meist nicht mehr hinterfragt werden.

Mögliche Maßnahmen:

- sinnvoll anwendbare, prüfbare, erfüllbare Vorgaben in Ausschreibungen, Verträgen, SLA's etc
- ein etablierter, kontinuierlicher, pro-aktiver Prozess für das Lieferanten - Management inkl. KPI's
- ein zuverlässiges und aktuelles IT-Inventar inkl. virtueller und ausgelagerter IT-Assets
- eine aktuelle, überprüfbare Hardware - und Software-Stücklisten (Bill of Materials), ggf. mit Aussagen zur Integrität der nachgelagerten Kette und enthaltene Sub-Elemente
- prüfbare Signaturen für fremdbezogene und eigene Software-Artefakte
- proaktive Meldung und Auswertung von Schwachstellen (Vulnerability Exploitability eXchange)

Supply Chain Risk Management leicht erklärt:

Stellen Sie sich das Supply Chain Management bei einem großen Automobilhersteller wie Audi vor:

- **Planung**: Audi plant die Produktion detailliert, um die Nachfrage zu decken.
- **Beschaffung**: Sie wählen und überwachen sorgfältig Lieferanten für Autoteile wie Motoren, Getriebe und Elektronik.
- **Produktion**: In den Audi-Fabriken werden die Teile montiert und die Autos gebaut.
- **Logistik**: Die fertigen Fahrzeuge werden effizient an Händler weltweit verteilt.
- **Retourenmanagement**: Rückläufer oder defekte Fahrzeuge werden bearbeitet, um Kundenzufriedenheit sicherzustellen.
- **Integration und Koordination**: Audi koordiniert alle Schritte nahtlos, um konsistente Qualität zu gewährleisten.
- **Supply Chain Risk Management**: Audi identifiziert und minimiert Risiken in der Lieferkette, wie den Ausfall eines Zulieferers, um Produktionsunterbrechungen zu vermeiden.
- **Haftungsfragen**: Wenn ein Auto von Audi einen Defekt aufweist, kann Audi nicht einfach den Zulieferer des defekten Teils verantwortlich machen. Audi selbst trägt die Haftung gegenüber den Kunden. Daher muss Audi sicherstellen, dass alle Glieder der Lieferkette höchsten Standards genügen.

Kurz gesagt, Audi stellt sicher, dass jeder Schritt in der Lieferkette effizient, zuverlässig und qualitativ hochwertig ist, um die bestmöglichen Fahrzeuge an die Kunden zu liefern und Haftungsrisiken zu minimieren.

denn:

- **50% - 80% aller Informationssicherheitsverletzungen haben Ihren Ursprung in der Lieferkette**
- **45% aller Cybervorfälle wurden früheren Partnern zugeschrieben**
- **71% der Unternehmen haben NICHT die volle Transparenz Ihrer Lieferketten**
- **59% der Unternehmen verfügen NICHT über ein Verfahren zur Bewertung der Cybersicherheit von Drittanbietern, mit denen sie Daten oder Netzwerke tauschen**
- **40% der Angriffskampagne zielen auf den Industrie- und Dienstleistungssektor ab (jeweils 20%)**

Quelle: Supply Chain Risk Management aas / InfoGuard

Was ist jedoch Informationssicherheit? Datensicherheit?

Informationssicherheit ist ein Konzept der Informationsverarbeitung, das sich mit dem Schutz von Daten vor **unbefugtem Zugriff und Manipulation** befasst. Um die Informationssicherheit zu gewährleisten, müssen **bestimmte Schutzziele** erreicht werden, darunter **Vertraulichkeit, Integrität und Verfügbarkeit**. Die Vertraulichkeit stellt sicher, dass Daten nur von autorisierten Benutzern eingesehen und verwaltet werden. Die Integrität verhindert, dass Daten unbemerkt verändert oder manipuliert werden können. Die Verfügbarkeit sicherstellt, dass Daten jederzeit zur Verfügung stehen, wenn sie benötigt werden. **Informationssicherheit ist ein wesentlicher Aspekt der IT- / OT-Sicherheit und schützt Unternehmen vor Risiken, die durch Datenverlust oder -diebstahl entstehen können.**

Schutzziele der IT- / OT-Sicherheit

Diese umfassen alle Maßnahmen, die getroffen werden, um Daten vor schädlichen Einflüssen zu schützen. Dabei spielen sowohl **externe Bedrohungen** als auch **interne Risiken** eine Rolle.

Um die Schutzziele der Informationssicherheit zu erfüllen, muss ein Unternehmen seine IT- / OT-Sicherheit entsprechend aufstellen und kontinuierlich weiterentwickeln.

- **Vertraulichkeit (Confidentiality):** Unbefugte Dritte können auf sensible personenbezogene Daten oder Know-How zugreifen, was zu Identitätsdiebstahl, finanziellen Verlusten und Rufschädigung der betroffenen Personen führen kann.Die Vertraulichkeit von Informationen kann durch technische und organisatorische Maßnahmen gewährleistet werden. Beispielsweise können Daten verschlüsselt werden oder es kann eine Zugangskontrolle eingerichtet werden. Die Einhaltung der Vertraulichkeit ist jedoch nicht immer einfach, da autorisierte Personen häufig Zugang zu denselben Informationen haben. Darüber hinaus können schutzwürdige Informationen auch an unternehmensexterne Personen weitergegeben werden, zum Beispiel an Geschäftspartner oder Kunden.

- **Integrität (Integrity):** Hackerangriffe können die Integrität der Daten beeinträchtigen, indem sie Daten verändern oder löschen. Dies kann die Verlässlichkeit und Genauigkeit der Daten infrage stellen. Zu den möglichen Bedrohungen zählen zum Beispiel: physische Zerstörung, Verlust, unbefugte Veränderung, unbefugter Lesezugriff. Die Abschätzung von Schwere und Häufigkeit erfolgt in Abhängigkeit vom jeweiligen Kontext und kann unterschiedlich ausfallen. So ist beispielsweise eine höhere Häufigkeit an Bedrohungen zu erwarten, wenn die Datenbank oder Datei im Internet verfügbar ist.

- **Verfügbarkeit (Availability):** Durch den Angriff können Daten unzugänglich oder zerstört werden, was die Geschäftskontinuität und den Zugriff auf wichtige Informationen behindern kann. Das bedeutet, dass Informationen jederzeit und an jedem Ort verfügbar sein müssen. Dies ist wichtig, damit Benutzer auf ihre Daten zugreifen können, wenn sie es brauchen. Wenn ein System nicht verfügbar ist, kann es zu Ausfällen und Beeinträchtigungen der Leistung kommen. Aus diesem Grund ist die Verfügbarkeit eines der wichtigsten Schutzziele in der Informationssicherheit. Um die Verfügbarkeit des Systems sicherzustellen, müssen Sicherheitsmaßnahmen getroffen werden, um sicherzustellen, dass keine schädlichen Einflüsse die Verfügbarkeit des Systems beeinträchtigen.

INDUSTRIAL AUTOMATION

NIS 2 compliant

Welche Herausforderungen gibt es bei der Implementierung von Maßnahmen zum Schutz von Daten?

Die Hauptherausforderung bei der Implementierung von Maßnahmen zur Informations- und Datensicherheit ist die **Abwägung zwischen den Kosten und dem Schutzbedürfnis**. Oft sind die Kosten für einen vollständigen Schutz höher als das Risiko eines Angriffs.

Zudem müssen die **richtigen Maßnahmen identifiziert werden**, um effektiv zu sein.

Dies erfordert ein **Verständnis der Bedrohungslage sowie der Schwachstellen des Unternehmens**.

Ohne dieses Wissen könnten teure Sicherheitsmaßnahmen implementiert werden, die keinen wirklichen Schutz bieten und darüber hinaus schwierig in bestehende Systeme und Prozesse zu integrieren sind.

Darüber hinaus gibt es noch "erweiterte" Schutzziele, die bei besonderen Anforderungen mit einbezogen werden.

- **Authentizität (Authenticity)**
- **Nichtabstreitbarkeit (Non-Repudiation)**
- **Verlässlichkeit (Reliability)**

Erkennen - Reagieren - Handeln

Mit der Umsetzung des **NIS 2** Gesetzes sind Kosten und oft umfangreiche strukturelle Anpassungen verbunden. Das hört sich nicht nur teuer an, es ist teuer.

Auch bei kleinen Unternehmen liegen die Kosten im fünfstelligen Bereich, wenn noch KEINE Basis für OT-Sicherheit vorhanden ist. Die anfallenden Kosten lassen sich nicht generell beziffern und variieren daher nach bereits vorhandener IT-Infrastruktur, nach dem Sektor, der Branche, nach Neustrukturierung der Unternehmensprozesse, der Unternehmensgröße und spezifischen Anforderungen.

doch:

Was passiert, wenn Unternehmen die Regelung nicht einhalten?

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

Leitungsorgane, die ihre Pflichten nach **NISG** verletzen, haften der Einrichtung für den schuldhaft verursachten Schaden.

Begriff Leitungsorgan:

Leitungsorgan ist eine oder sind 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.

Aufgaben der Leitungsorgane

Die Leitungsorgane

- haben die Einhaltung der im **NISG** geforderten Risikomanagementmaßnahmen sicherzustellen und zu beaufsichtigen
- müssen an spezifisch für Leitungsorgane gestalteten Cybersicherheitsschulungen teilnehmen (allgemeine Cybersicherheitsschulungen wie z.B. Schulungen für Mitarbeiter sind nicht ausreichend). Die Teilnahme an den Schulungen muss entsprechend dokumentiert werden (Inhalt der Schulungen und Schulungsangebote siehe unten).
- haben den Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, damit diese ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste erwerben können.

Welche Berichtspflichten sind zu beachten?

Bei **erheblichen Cybersicherheitsvorfällen** gibt es ein dreistufiges Meldeverfahren an das zuständige **CSIRT (Cybersecurity Incident Response Team).**

Fristen

- **Unverzüglich, innerhalb von 24 Stunden:** Frühwarnung (ggf. Verdacht auf rechtswidrige und schuldhafte Handlung oder grenzüberschreitende Auswirkungen)
- **Unverzüglich, jedenfalls innerhalb von 72 Stunden:** Meldung (Schweregrad, Auswirkungen, ggf. Komprimittierungsindikatoren)
- **Spätestens einen Monat nach Frühwarnung:** Abschlussbericht (Beschreibung Vorfall, einschließlich Schweregrad und Auswirkungen, Art der Bedrohung, Ursachen, Abhilfemaßnahmen)

Auf Ersuchen des CSIRT oder der Behörde Zwischenberichte über Statusaktualisierungen.

Data Breach

Sollte es im Zuge des Cybersicherheitsvorfalls auch zu einer Verletzung des Schutzes personenbezogener Daten (data breach) gekommen sein, sind zusätzlich die **Melde- und Berichtspflichten nach DSGVO** zu beachten. Dem Bericht "Cost of a Data Breach" zufolge führt eine durchschnittliche Datenschutzverletzung zu einem Geschäftsverlust von 1,42 Millionen US-Dollar.

Freiwillige Meldungen nach NIS

Weiters gibt es die Möglichkeit der **freiwilligen Meldung** von (Beinahe-)Cybersicherheitsvorfällen, und -bedrohungen an das CSIRT, das die Meldungen zusammenfasst und an die Cybersicherheitsbehörde weiterleitet.

Watchlist Internet

Melden Sie betrügerischen Nachrichten und Internetfallen auch an die **Watchlist Internet**. So können andere Unternehmen rechtzeitig gewarnt werden.

Welche weiteren Auswirkungen haben Cyberangriffe auf Unternehmen?

- Betriebsunterbrechungen
- Datendiebstahl
- Datenlöschung
- Datenveröffentlichung
- Systemdeaktivierung

sekundäre Kosten wie:

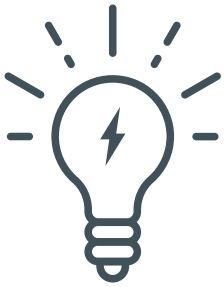
- Lieferengpässe und -schwierigkeiten
- Pönalzahlungen
- Auswirkungen in der Lieferkette - sekundäre Opfer
- Erpressungs- bzw. Lösegelder
- Mitarbeiterkosten (Urlaub, Überstunden, arbeitsrechtliche Gehalts- und Lohnfortzahlungen bei verschuldeter Arbeitsverhinderung

Sind wir alle echt?

“Bist du ein Deepfake? Oder versuchst du, mich mit Psychologie zu manipulieren?“

Damit Ihre Daten sicher bleiben. Damit Ihr Unternehmen störungsfrei läuft. Damit Sie es Hackern nicht so einfach machen. Damit Sie geschützt sind. Damit der Mensch nicht immer die Schwachstelle bleibt:

Awarness-Tipps:



Technische Awarness (Basics)

- lange unterschiedliche Passwörter
- Udates / Patches
- Accee & Identity Management, Firewall, Antivirus
- 2-Factor-Authentification / MFA
- keine fremden W-Lans, Sticks oder Anhänge

Psychologische Awarness (Keynotes, Workshops, Online)

- Psychology of Cybercrime: Emotion + Zeitdruck + Ausnahme
- Deepfakes: call back, Code-Wort, Sicherheitsfragen stellen

Physische Awarness:

- nie Laptop oder Smartphone entsperrt liegen lassen
- Sichtschutzfolie für Smartphone & Laptop
- Windows + L bei jedem Kaffee (Bildschirm sperren)
- Hotel Safe nutzen, Büro abschließen
- keine Dokumente im Drucker liegen lassen (!)

INDUSTRIAL AUTOMATION

NIS 2 compliant

Welche Computer-Notfallteams im Sinne des NIS 2 Gesetzes gibt es in Österreich?

Nationales Computer-Notfallteam:

CERT.at – Computer Emergency Response Team Austria

- Webseite: www.cert.at
- Telefon: +43 1 505 64 16-78
- Verpflichtende und freiwillige NIS-Meldungen: nis.cert.at
- E-Mail-Adresse für Sicherheitsvorfälle: reports@cert.at
- E-Mail-Adresse für andere Anfragen: team@cert.at

Computer-Notfallteam im Sektor öffentliche Verwaltung:

GovCERT.at – Computer Emergency Response Team Austria für die öffentliche Verwaltung

- Webseite: www.govcert.gv.at
- Telefon: +43 1 505 64 16-930 (govCERT Teil technische und operative Leistungen)
- Verpflichtende und freiwillige NIS-Meldungen: nis.govcert.gv.at
- E-Mail-Adresse für Sicherheitsvorfälle: reports@govcert.gv.at
- E-Mail-Adresse für andere Anfragen: team@govcert.gv.at

Sektorenspezifisches Computer-Notfallteam im Sektor Energie:

AEC – Austrian Energy CERT

- Website: www.energy-cert.at
- Telefon: +43 1 505 64 16-92
- Verpflichtende und freiwillige NIS-Meldungen: nis.energy-cert.at
- E-Mail-Adresse für Sicherheitsvorfälle: reports@energy-cert.at
- E-Mail-Adresse für andere Anfragen: team@energy-cert.at

Die Anforderungen und Fristen ändern sich derzeit leider noch.

Daher finden Sie nachfolgend einige Links, über die Sie sich in Österreich Unterstützung holen können. Insbesondere für KMUs gibt es auch Informationen über Förderungen:

Cyber-Trust Austria

TÜV Austria

NIS.GV.AT

WKO - Cybersicherheitsrichtlinie NIS 2

Parlamentskorrespondenz 692 v. 19.06.24

Bundeskanzleramt NIS 2 Büro

Europäische Kommission

Diese Ressourcen können Ihnen helfen, sich auf die kommenden Änderungen vorzubereiten und mögliche Förderungen zu nutzen.

Diese Links zählen gleichzeitig als Quellenangaben für diesen Folder.

Warum tun wir das, was wir tun?

Maschinen, Produktionsanlagen, Steuerungen, Messgeräte – eine Vielzahl unterschiedlichster Geräte kommen in der Produktion heutzutage zum Einsatz. **All diese Anlagen können über mehr oder weniger standardisierte Schnittstellen miteinander und mit übergeordneten Leitsystemen, Produktionsplanungs- und -Steuerungssystemen, ERP-Tools … sprich mit allen möglichen im Betrieb vorhandenen Automatisierungsebenen, kommunizieren.**

Heterogene und seit Jahrzehnten gewachsene Landschaften sind dabei eher die Regel denn die Ausnahme.

Viele verschiedene Hersteller, Ansprechpartner, Systempartner und Wartungsunternehmen spielen hier mit. Verschiedenste Betriebssysteme, unterschiedliche Protokolle und Bussysteme und diverse Programmiersprachen gelangen hier zum Einsatz.

Viele Systeme sind für IT- / OT- Verhältnisse „alt". Während IT- Geräte gerne im 3- bis 5-Jahresintervall ausgetauscht werden, müssen OT-Systeme oft 15 bis 20 Jahre lang ihren Dienst versehen.

All diese Umstände stellen eine große Herausforderung für einen sicheren, zuverlässigen und reibungslosen Betrieb derart komplexer Kommunikationssysteme dar. **Daher gibt es uns**.

Seit über 20 Jahren sind wir in Österreich Ihr Experte für intuitive Automatisierungs- und Sicherheitssoftware in der Produktionsbranche. Wir bieten hochwertige Automatisierungs-software für die operative Technologie (OT), basierend auf offenen Standards.

Unser Ziel ist es, Ihre Automatisierungsprozesse mit unseren Lösungen nachhaltig zu verbessern, denn unsere eingesetzten Tools sind perfekt auf Ihre Anforderungen abgestimmt und integrieren sich nahtlos in Ihre Infrastruktur, um Ihre Produktivität und Betriebssicherheit zu steigern.

Entwickelt von Automatisierungsexperten für Automatisierungsfachleute: Schnell und einfach zu implementieren, kosteneffizient und benutzerfreundlich.

Wir packen gerne an. Je komplexer ein Thema, desto größer die Herausforderung und umso mehr Spaß haben wir bei der Arbeit.

Hands-on: in allen Branchen mitten im Geschehen. So lieben wir das.

INDUSTRIAL AUTOMATION

NIS 2 compliant

Wie lernen wir uns kennen?

In einer Stunde beleuchten wir online viele verschiedene Aspekte der IT- (und speziell **OT**)-**Security** und Sie erhalten einen guten Überblick, wo Sie bereits gut aufgestellt sind.

Online - unkompliziert.

Und vielleicht findet sich auch das eine oder andere Thema, wo Sie noch etwas verbessern können.

Nehmen Sie Kontakt mit uns auf!

Wir freuen uns auf das Gespräch mit Ihnen!

Industrial Automation GmbH

AT-6020 Innsbruck
Technikerstraße 1 - 3

Tel: +43 512 27 22 71 - 00
Mail: office@automation.team

Onlinetermin buchen

Industrial Automation Suisse GmbH

CH-8808 Pfäffikon SZ
Churerstraße 16

Tel: +41 55 56 002 - 00
Mail: office.ch@automation.team

Onlinetermin buchen

NEW NEW NEW

Büro Italien

IT-39032 Campo Tures
Via Unterwalburgen 15B

Tel: +39 0474 86 93 - 99
Mail: support@scada.online

Onlinetermin buchen