Sensibilisierung NIS 2.0 und ISMS

TELCO TECH NETWORK SECURITY
ENGINEERED IN GERMANY

Sensibilisierung zum Aufbau und Nutzen eines ISMS

Mit wem haben Sie es zu tun?

Bernd Schulz
- Gründer, Gesellschafter und Geschäftsführer der F1 Gesellschaft für Informationstechnologien- und Managementberatung mbH (IT-Systemhaus mit Spezialisierung zum Thema IT-Security)
- Gesellschafter und Geschäftsführer der TELCO TECH GmbH (Entwickler und Hersteller von UTM Systemen (IT-Securitysysteme))
- ehemaliger Sprecher des Netzwerkes iVersiD (Intelligente Vernetzung und sicherer Datentransport)
- Zertifizierter EDV-Sachverständiger nach DIN EN ISO/IEC 17024
- Fachgutachter von IT-Forschungs- und Entwicklungsprojekten für verschiedene Projektträger

NIS 2.0?

ISO/IEC-27000?

ISMS?

Was ist das alles?
Was kommt auf unser Unternehmen zu?
Braucht mein Unternehmen das Ganze?
Hilft es uns weiter?
Was kostet unser Unternehmen das Ganze?

Sensibilisierung zum Thema NIS 2.0

Kompletter Titel:
"Richtlinie (EU) 2022/2555 des Europäischen Parlaments und Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)."

Sperriger Titel!

Was soll damit erreicht werden?

Sensibilisierung zu NIS 2.0

Zunächst zum aktuellen Sachstand:

- Die NIS2 (Netz- und Informationssysteme)-Richtlinie soll das Cybersicherheitsniveau von Netz- und Informationssystemen in der Europäischen Union erhöhen.
- Sie baut auf der ursprünglichen NIS-Richtlinie von 2016 auf und ist Teil eines größeren Maßnahmenpakets, um die Cybersicherheit in der EU zu verbessern.
- Die NIS2 erweitert unter anderem den Anwendungsbereich der NIS und verpflichtet so mehr Unternehmen und Organisationen, im Namen der Cybersicherheit aktiv zu werden.
- Innerhalb des Europäischen Parlaments war der Ausschuss für Industrie, Forschung und Energie (ITRE) federführend. Der Bericht des Berichterstatters wurde am 28. Oktober 2021 angenommen, der Rat einigte sich am 03. Dezember 2021 auf einen gemeinsamen Standpunkt zum Richtlinienentwurf.
- Die EU-Mitgesetzgeber einigten sich am 13. Mai 2022 auf einen vorläufigen Richtlinientext. Die offizielle Einigung zwischen Parlament und Rat zur Richtlinie wurde dann im November 2022 erzielt. Am 16. Januar 2023 schließlich trat die NIS2 in Kraft. ***Die Mitgliedsstaaten haben nun 21 Monate – bis zum 17. Oktober 2024 – Zeit, sie in nationales Recht zu überführen.***

Sensibilisierung zu NIS 2.0

Warum ist die NIS2 für EU-Unternehmen so relevant?

Zwar hatte die ursprüngliche NIS-Richtlinie die Cybersicherheit in den EU-Mitgliedsstaaten bereits wesentlich verbessert – die Umsetzung gestaltete sich jedoch schwierig und hatte eine starke Fragmentierung des EU-Binnenmarktes zur Folge.

Die NIS2 Richtlinie soll nun helfen, die Cybersicherheit in der EU zu vereinheitlichen!
Es erhöhen sich die Sicherheitsanforderungen an Unternehmen, adressiert wird die Absicherung von Lieferketten (Supply Chain Security), NIS2 erweitert die Berichtspflichten und gibt den zuständigen Behörden umfassendere Aufsichts- und Durchsetzungsmechanismen an die Hand.

So gibt sie beispielsweise allen EU-Mitgliedsstaaten die gleichen Sanktionsmöglichkeiten!

Mit der Erweiterung des Anwendungsbereiches auf mehr Organisationen und Sektoren versucht die NIS2, das Cybersicherheitsniveau in Europa langfristig zu erhöhen!

Sensibilisierung zu NIS 2.0

Von der NIS zur NIS2: Was hat sich geändert?

Die ursprüngliche Richtlinie zur Netz- und Informationssicherheit (NIS) wurde 2016 veröffentlicht. Ziel war die Vereinheitlichung von Cybersicherheitsmaßnahmen innerhalb der EU.

Die Richtlinie stellte eine Reihe von Anforderungen an Betreiber wesentlicher Dienste (Operators of Essential Services OES) und Anbieter digitaler Dienste (Digital Service Providers DSP), darunter Berichtspflichten bei Sicherheitsvorfällen und Vorgaben zum Risikomanagement. Die NIS-Richtlinie war damit das erste EU-weite Gesetzespapier zum Thema Cybersicherheit und stellte einen wesentlichen Schritt im Kampf gegen die EU-weite Cyberbedrohungen dar.

Die Umsetzung jedoch erwies sich für viele Unternehmen als schwierig. Manche Organisationen hatten Schwierigkeiten, überhaupt zu verstehen, was die NIS von ihnen forderte, für andere war es schwierig, die komplexen Melde- und Berichtspflichten zu erfüllen. Gleichzeitig monierten Kritiker, dass die NIS nicht genug Organisationen und Sektoren in die Pflicht nähme und dadurch generell zu kurz griffe.

Sensibilisierung zu NIS 2.0

Von der NIS zur NIS2: Was hat sich geändert?

Eine der wichtigsten Änderungen ist daher auch die Erweiterung des Anwendungsbereichs der NIS2. Sie bezieht nun eine viel größere Zahl an Organisationen und Sektoren mit ein, darunter kleine Unternehmen und digitale Plattformen. So soll sichergestellt werden, dass mehr Organisationen Anstrengungen unternehmen, um sich vor Cyberbedrohungen zu schützen.

NIS2 legt zusätzlich größeren Fokus auf das Risikomanagement in Unternehmen und verpflichtet sie, mögliche Risiken für die Cybersicherheit im Unternehmen zu identifizieren und zu bewerten.

Nur so ist es möglich, potenzielle Bedrohungen systematisch zu verstehen und mögliche Gegenmaßnahmen zu ergreifen.

NIS2 beinhaltet zudem weitere Anforderungen an die Meldung von und Reaktion auf Sicherheitsvorfälle. Das hilft Organisationen, besser mit möglichen Cyberangriffen umzugehen.

Sensibilisierung zu NIS 2.0

Von der NIS zur NIS2: Was hat sich geändert?

Ein weiterer wichtiger Punkt ist der Fokus auf die Sicherheit von Lieferketten (Supply Chain Security). Die Richtlinie fordert Unternehmen auf, die Cybersicherheit ihrer Lieferketten zu prüfen und dafür zu sorgen, dass sich auch ihre Zulieferer ausreichend vor Cyberbedrohungen schützen. Vor dem Hintergrund zurzeit häufig beobachteter Cyberangriffe auch auf große Unternehmen erhält dieser Teil der NIS2 noch einmal zusätzliches Gewicht.

Denn: Ohne einen effektiven Schutz der gesamten Lieferkette nützt auch die beste Absicherung von Einzelunternehmen wenig.

Sensibilisierung zu NIS 2.0

Wer ist von der NIS2-Richtlinie betroffen und auf wen kommen Aufgaben zu?

Sensibilisierung zu NIS 2.0

Folgende Einrichtungen werden in der Richtlinie genannt**:**

Betreiber wesentlicher Dienste (Operators of Essential Services OES): Dies sind Unternehmen, die als wesentlich für das Funktionieren von Wirtschaft und Gesellschaft angesehen werden. Dazu gehören Unternehmen der Energiebranche, der Trinkwasser- und Abwasserversorgung und Gesundheitsdienstleister. Die Größe der Organisation ist in diesem Fall irrelevant.

Anbieter digitaler Dienste (Digital Service Providers DSP): Dies sind Unternehmen, die Online-Dienste anbieten, also beispielsweise Online-Marktplätze, Cloud Computing-Anbieter und Suchmaschinen. DSPs müssen nur dann die Vorgaben der NIS2 erfüllen, wenn sie eine bestimmte Größe überschreiten. Dabei wird unterschieden zwischen:

Mittlere Unternehmen: DSPs mit 50 oder mehr Mitarbeitern und einem Jahresumsatz von mindestens 10 Millionen Euro

Große Unternehmen: DSPs mit 250 oder mehr Mitarbeitern und einem Jahresumsatz von mindestens 50 Millionen Euro

Sensibilisierung zu NIS 2.0

wesentliche Sektoren

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastruktur
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Öffentliche Verwaltung???
- Weltraum

wichtige Sektoren

- Post- und Kurierdienste
- Abfallbewirtschaftung

Sensibilisierung zu NIS 2.0

Was fordert die NIS 2 - Richtlinie?

Die NIS2 orientiert sich am „All-hazard approach“ (dt. „All-Gefahren-Ansatz“).
Ziel ist, alle Netzwerke, Informationssysteme und die physischen Umgebungen dieser Systeme vor Sicherheitsvorfällen zu schützen.
Die Anforderungen umfassen unter anderem:

- Konzepte für Maßnahmen
- Vorfallsmanagement
- Aufrechterhaltung des Betriebs (Business Continuity)
- Sicherheit der Lieferkette (Supply Chain Security)
- Schulung und Training
- Management von Anlagen (Asset Management)
- Dokumentationspflichten

Sensibilisierung zu NIS 2.0

Welche Sanktionen drohen im Zusammenhang mit der NIS 2?

Das Nicht-Einhalten der NIS2-Vorgaben kann empfindliche Strafen nach sich ziehen. Geldbußen in Höhe von bis zu 10 Millionen Euro bzw. 2 % des Vorjahresumsatzes (weltweit) sind möglich, je nachdem, welcher Betrag höher ist.

In besonders schweren Fällen können Geldbußen bis zu 20 Millionen Euro oder 4 % des Vorjahresumsatzes weltweit verhängt werden, je nachdem, welcher Betrag höher ausfällt.

Die nationalen Behörden können zusätzlich weitere Sanktionen erlassen.

Möglich sind beispielsweise Zwangsgelder, um wesentliche oder wichtige Einrichtungen dazu zu zwingen, einen festgestellten Verstoß gegen die Richtlinie zu unterlassen.

Sensibilisierung zu NIS 2.0

Welche Auswirkungen hat die NIS2 für deutsche Unternehmen?

Die EU-Mitgliedsstaaten haben noch 7 Monate Zeit, die Richtlinie in nationales Recht umzusetzen. Für deutsche Unternehmen heißt das: Spätestens im Herbst 2024 werden eine Vielzahl neue Regularien auf die deutsche Wirtschaft zukommen. Hier gilt es, frühzeitig Maßnahmen zu ergreifen und die Vorgaben der NIS2 – schon aus Eigeninteresse – möglichst genau umzusetzen.

Sensibilisierung zu NIS 2.0

Welche Vorteile hat die NIS2 für Ihr Unternehmen?

Risikomanagement:
Die NIS2 verpflichtet Unternehmen, regelmäßige Risikobewertungen ihrer IT-Systeme durchzuführen, potenzielle Risiken und Schwachstellen zu identifizieren und Abwehr- und Gegenmaßnahmen zu implementieren. Befolgen Sie diese Vorgabe, schützen Sie Ihr Unternehmen effektiv vor Cybersicherheitsrisiken und minimieren die Wahrscheinlichkeit für einen Cyberangriff.

Vorfallsmanagement:
Die Richtlinie enthält Vorgaben zum Vorfallsmanagement in Unternehmen, darunter Berichtspflichten und Reaktionspläne. Das hilft Ihrem Unternehmen, schnell und effektiv auf Sicherheitsvorfälle zu reagieren, negative Auswirkungen zu minimieren und ähnliche Vorfälle für die Zukunft zu verhindern.

Technische und organisatorische Maßnahmen:
Die Richtlinie verpflichtet Unternehmen auch, geeignete technische und organisatorische Maßnahmen für die Absicherung ihrer Netz- und Informationssysteme einzurichten. Dazu gehören Maßnahmen zur Zugriffskontrolle, Verschlüsselung und die Einführung von digitalen Überwachungssystemen. Die Umsetzung solcher Maßnahmen hilft Unternehmen, das Risiko von Cyberangriffen und Datenlecks zu verringern.

Sensibilisierung zu NIS 2.0

Welche Vorteile hat die NIS2 für Ihr Unternehmen?

Business Continuity:
Pläne zur Aufrechterhaltung des Betriebs, darunter Backup- und Wiederherstellungspläne, helfen, den Geschäftsbetrieb auch im Fall eines Sicherheitsvorfalls fortzuführen, Ausfallzeiten zu minimieren und kritische Dienste aufrechtzuerhalten. Hier empfiehlt sich die Implementierung eines Business Continuity Managementsystems (BCM).

Sicherheit der Lieferkette (Supply Chain Security):
Die NIS2 enthält auch Vorgaben zur Absicherung der Lieferkette (Zulieferer und Dienstleister). Nehmen Unternehmen die Supply Chain Security mit in den Blick, senken sie proaktiv das Risiko von Cyberangriffen über eben diese Lieferkette.

Sensibilisierung zu NIS 2.0

Wie hilft die NIS2 Unternehmen, mit Cybergefahren umzugehen und die Risiken zu minimieren?

Geringeres Risiko von Cyberangriffen:
Mit der Umsetzung der NIS2-Vorgaben verringern Sie das Risiko von Cyberangriffen und Datenlecks enorm. Das ist deshalb relevant, weil solche Vorfälle nicht nur intern hohe Kosten verursachen – hinzu kommen möglicherweise Strafzahlungen von behördlicher Seite oder teure Rechtsstreitigkeiten. Je geringer das Risiko von Cyberangriffen, desto geringer das Risiko hoher Kosten.

Besseres Management von Sicherheitsvorfällen:
Die NIS2 macht Vorgaben zum Vorfallsmanagement in Unternehmen, z.B. zu Dokumentationsspflichten und Reaktionsplänen. Ein klares und durchdachtes Vorfallsmanagement hilft Unternehmen, Sicherheitsvorfälle schnell einzudämmen und ihre negativen Folgen abzumildern. Das wiederum minimiert die Kosten, die durch Ausfallzeiten, verminderte Produktivität und Reputationsschäden entstehen können.

Verbesserte Business Continuity:
Die NIS2 verpflichtet Unternehmen dazu, Pläne für die Aufrechterhaltung des Betriebes (Business Continuity-Pläne) zu entwickeln, z.B. Backup- und Wiederherstellungspläne. Robuste Business Continuity-Pläne helfen, Kosten durch Ausfallzeiten zu minimieren und sicherzustellen, dass kritische Prozesse auch im Fall eines Sicherheitsvorfalls weiterlaufen.

Höhere Effizienz und Produktivität:
Die Vorgaben der NIS2 können Unternehmen helfen, ihre Sicherheitsprozesse zu optimieren und den Aufwand für das Management der Informationssysteme zu verringern. Das wiederum steigert Effizienz und Produktivität und spart somit zusätzlich Kosten.

Sensibilisierung zum Thema NIS 2.0

Danke für die Aufmerksamkeit!

Bernd Schulz
Geschäftsführer
bschulz@telco-tech.de

TELCO TECH NETWORK SECURITY ENGINEERED IN GERMANY