(secudor)

NIS2 und seine Relevanz für KMU

Ein Leitfaden zur Informationssicherheit

Klassifizierung **„Für unsere Partner“**

INHALT

PRÄAMBEL (EXECUTIVE SUMMARY)

Dieses Whitepaper beleuchtet die Relevanz der NIS2-Richtlinie speziell für kleine und mittlere Unternehmen (KMU). Es wird aufgezeigt, welche Anforderungen die Richtlinie stellt, wie diese effizient umgesetzt werden können und welche Vorteile daraus resultieren.
Dieses Dokument richtet sich an Geschäftsführer, IT-Leiter und Sicherheitsverantwortliche, die die Cybersicherheit in ihrem Unternehmen stärken wollen.

EINLEITUNG

In der digitalen Geschäftswelt sind KMU zunehmend mit Cybersicherheitsrisiken konfrontiert. Die NIS2-Richtlinie der EU soll einheitliche Cybersicherheitsstandards schaffen, die besonders für Unternehmen in kritischen Sektoren wie Energie, Gesundheit und digitale Infrastruktur von Bedeutung sind. Ein wichtiger Aspekt dabei ist die Berücksichtigung von Abhängigkeiten in der Lieferkette. Auch wenn ein Unternehmen selbst über hohe Sicherheitsstandards verfügt, kann es durch Schwachstellen bei seinen Lieferanten oder Dienstleistern gefährdet sein.

Immer mehr Auftraggeber setzen daher voraus, dass Zulieferer und Dienstleister geordnete Prozesse und Organisationen zur Begegnung von Cyberrisiken implementiert haben und dies nachweisen können. Dieses Whitepaper bietet Ihnen eine kompakte Übersicht, um die Anforderungen der NIS2-Richtlinie zu verstehen und gezielt umzusetzen.

HINTERGRUND UND KONTEXT

Die NIS2-Richtlinie betrifft Unternehmen, die in kritischen Sektoren tätig sind. Diese Unternehmen spielen eine entscheidende Rolle in der Wirtschaft und Gesellschaft, weshalb ihre Cybersicherheit von besonderer Bedeutung ist. Unternehmen müssen sicherstellen, dass sie die Richtlinie einhalten, um ihre Geschäftsprozesse und Netzwerke gegen Cyberangriffe zu schützen.

Kritische Bedeutung:

Ein Unternehmen wird als kritisch eingestuft, wenn seine Dienstleistungen oder Produkte für die Aufrechterhaltung der Gesellschaft und Wirtschaft unverzichtbar sind. KMU in Sektoren wie Energie, Transport, Gesundheit und digitale Infrastruktur sind besonders anfällig, da sie essenzielle Funktionen erfüllen.

Die NIS2-Richtlinie fordert von diesen Unternehmen die Einführung von Maßnahmen zur Risikosteuerung und Vorfallsmeldung.

KATEGORISIERUNG VON UNTERNEHMEN NACH NIS2

Der Entscheidungsbaum zur NIS2-Betroffenheit, bereitgestellt vom Bundesamt für Sicherheit in der Informationstechnik (BSI), hilft Unternehmen dabei, festzustellen, ob sie von der NIS2-Richtlinie betroffen sind und wie sie kategorisiert werden. Der Entscheidungsbaum unterscheidet u.a. zwischen wichtigen Unternehmen und besonders wichtigen Unternehmen:

Wichtige Unternehmen:

Diese sind in kritischen Sektoren tätig und überschreiten bestimmte Schwellenwerte wie eine Mitarbeiterzahl von mehr als 50 oder einen Jahresumsatz/Jahresbilanzsumme von mehr als 10 Millionen Euro. Wichtige Unternehmen müssen umfassende Sicherheitsmaßnahmen umsetzen, um den Anforderungen der NIS2-Richtlinie gerecht zu werden.

Besonders wichtige Unternehmen:

Diese Kategorie umfasst größere Unternehmen mit mehr als 250 Mitarbeitern oder einem Jahresumsatz von über 50 Millionen Euro bzw. einer Jahresbilanzsumme von mehr als 43 Millionen Euro. Diese Unternehmen haben aufgrund ihrer Größe und Bedeutung noch strengere Verpflichtungen, da ein Ausfall ihrer Dienstleistungen oder Produkte erhebliche gesellschaftliche Auswirkungen haben könnte.

Für detaillierte Informationen zur Klassifizierung und zur Überprüfung, ob Ihr Unternehmen unter die NIS2-Richtlinie fällt, steht der Entscheidungsbaum zur NIS2-Betroffenheit zur Verfügung.

Eine Übersicht über die spezifischen Sektoren und Kategorien, die unter die NIS2-Richtlinie fallen, finden Sie außerdem in Anhang 2 der NIS2-Richtlinie. Zusätzlich bietet das BSI einen Schnell-Check zur NIS2-Pflicht an, um Unternehmen eine erste Orientierung zu geben.

VERANTWORTLICHKEITEN IM UNTERNEHMEN

Geschäftsführung:

Trägt die oberste Verantwortung für die Einhaltung und Umsetzung der NIS2-Richtlinie. Sie ist dafür verantwortlich, die strategische Ausrichtung des Unternehmens zu bestimmen und sicherzustellen, dass die notwendigen Ressourcen bereitgestellt werden, um die Anforderungen der Richtlinie zu erfüllen.
Die Geschäftsführung muss das Thema Cybersicherheit zur Priorität machen und entsprechende Budgets sowie Personal bereitstellen.

Chief Information Security Officer (CISO) oder IT-Sicherheitsbeauftragter:

Diese Person übernimmt die operative Verantwortung für die Implementierung der Sicherheitsmaßnahmen. Der CISO oder IT-Sicherheitsbeauftragte entwickelt das Sicherheitskonzept, überwacht die Einhaltung der Richtlinie und koordiniert die Umsetzung der Maßnahmen.
Sie spielen eine zentrale Rolle, indem sie die technischen und organisatorischen Sicherheitsanforderungen in die Praxis umsetzen und die gesamte IT-Sicherheitsstrategie des Unternehmens überwachen.

Fachabteilungen und Mitarbeiter:

Die IT-Abteilung ist verantwortlich für die technische Umsetzung der Sicherheitsmaßnahmen, das Personalwesen unterstützt durch Schulungen und Sensibilisierungskampagnen, und die Rechtsabteilung überwacht die Einhaltung gesetzlicher Vorschriften. Alle Mitarbeiter des Unternehmens sind verpflichtet, die Sicherheitsrichtlinien in ihrer täglichen Arbeit einzuhalten. Jede Abteilung muss aktiv mitarbeiten und die vom CISO bzw. IT-Sicherheitsbeauftragten vorgegebenen Maßnahmen unterstützen.

LÖSUNGSANSÄTZE UND EMPFEHLUNGEN

KMU sollten die folgenden Schritte zur Umsetzung der NIS2-Richtlinie in Betracht ziehen. Basis hier kann die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) wie z.B. ISO 27001 sein.

Bestandsaufnahme und Risikoanalyse:

Erfassen Sie den aktuellen Stand und identifizieren Sie potenzielle Risiken, einschließlich der Abhängigkeiten in der Lieferkette.

Implementierung der Maßnahmen:

Setzen Sie technische und organisatorische Maßnahmen um.

Entwicklung eines Sicherheitskonzepts:

Erstellen Sie ein maßgeschneidertes Konzept zur Risikosteuerung, das auch Maßnahmen zur Absicherung der Lieferkette umfasst.

Schulungen und Sensibilisierung:

Schulen Sie Mitarbeiter regelmäßig in Sicherheitsfragen.
Es besteht die Verpflichtung zur laufenden Schulung und Sensibilisierung der Geschäftsführung, Führungskräfte und Beschäftigten. Stellen Sie entsprechendes Schulungsmaterial zur Verfügung.

Einbindung von Lieferanten und Dienstleistern:

Stellen Sie sicher, dass auch Ihre Lieferanten und Dienstleister geordnete Prozesse zur Begegnung von Cyberrisiken implementiert haben. Fordern Sie entsprechende Nachweise ein, um sicherzustellen, dass Ihre gesamte Lieferkette über ein angemessenes Sicherheitsniveau verfügt.

Kontinuierliche Verbesserung:

Überwachen und optimieren Sie die Sicherheitsmaßnahmen fortlaufend, insbesondere im Hinblick auf externe Abhängigkeiten.

FOLGEN BEI NICHTEINHALTUNG DER NIS2-RICHTLINIE

Die Nichteinhaltung der NIS2-Richtlinie kann für KMU erhebliche Konsequenzen haben, sowohl rechtlicher als auch finanzieller Natur.

NIS2 ist Chefsache

Bei Verstößen gegen die Pflichten haftet die Geschäftsleitung gegenüber ihrer Einrichtung nach den jeweils geltenden gesellschaftsrechtlichen Vorschriften für schuldhaft verursachte Schäden. Die Nichteinhaltung könnte somit nicht nur zu Sicherheitsrisiken, sondern auch zu persönlicher Haftung der Geschäftsleitung führen.

1. Bußgelder:

Bei Nichteinhaltung der NIS2-Richtlinie drohen empfindliche Geldstrafen. Die Bußgelder können bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes des Unternehmens betragen – je nachdem, welcher Betrag höher ist.
Dies macht eine rechtzeitige und vollständige Umsetzung der Richtlinie unerlässlich.

2. Reputationsschäden:

Ein Verstoß gegen die NIS2-Richtlinie kann das Vertrauen von Kunden, Partnern und Investoren erheblich beeinträchtigen.
Dies kann zu einem Verlust von Geschäftsmöglichkeiten und Marktanteilen führen.

3. Betriebsunterbrechungen:

Mangelnde Cybersicherheit kann zu erheblichen Betriebsunterbrechungen führen, insbesondere wenn ein Unternehmen von einem Cyberangriff betroffen ist.
Die daraus resultierenden Kosten und Schäden können existenzbedrohend sein.

4. Rechtliche Konsequenzen:

Neben Bußgeldern können auch rechtliche Konsequenzen drohen, wenn durch die Nichteinhaltung der NIS2-Richtlinie Schäden bei Dritten entstehen.
Dies kann zu Schadensersatzforderungen und weiteren rechtlichen Auseinandersetzungen führen.

FALLBEISPIELE

Im Folgenden werden vier Fallbeispiele aus den Projekten der secudor GmbH aufgeführt, die veranschaulichen, wie die Vorgaben der kommenden NIS2-Richtlinie in der Praxis angewendet werden können:

Fallbeispiel 1:
Unternehmen im Bereich Automatisierungstechnik

Ein Unternehmen im Bereich Automatisierungstechnik, das in der Entwicklung und Wartung von Steuerungssystemen für die Industrie tätig ist, erkannte, dass es unter die kommende NIS2-Richtlinie fallen wird.
Da diese Steuerungssysteme in zahlreichen kritischen Infrastrukturen verwendet werden, führte das Unternehmen eine detaillierte Risikoanalyse durch und entwickelte ein Sicherheitskonzept, das unter anderem den Schutz vor Cyberangriffen auf Steuerungssysteme sowie die Sicherstellung der Systemverfügbarkeit und des operativen Betriebs umfasste. Die Implementierung dieser Maßnahmen stärkte die Resilienz des Unternehmens und erhöhte das Vertrauen der Kunden in die Zuverlässigkeit der Automatisierungstechnik.

Fallbeispiel 2:
Krankenhaus im ländlichen Raum

Ein Krankenhaus im ländlichen Raum erkannte die kritische Bedeutung seiner IT-Infrastruktur für die Patientenversorgung. In Hinblick auf die potenziellen Anforderungen der NIS2-Richtlinie führte das Krankenhaus eine Reihe von Sicherheitsmaßnahmen ein, darunter die Verschlüsselung sensibler Patientendaten und die Einführung eines Incident-Response-Plans.
Diese Maßnahmen stellten sicher, dass das Krankenhaus auf mögliche Cyberangriffe vorbereitet ist und die Versorgung der Patienten auch im Falle eines Sicherheitsvorfalls nicht gefährdet wird.

Fallbeispiel 3:
Cloud-Dienstleister

Ein Dienstleister, der Cloud-Services anbietet, musste aufgrund seiner zentralen Rolle in der IT-Infrastruktur seiner Kunden die eigenen Services und Prozesse auf Basis der möglichen Anforderungen der NIS2-Richtlinie umsetzen. Das Unternehmen führte strenge Zugangskontrollen, regelmäßige Penetrationstests und ein kontinuierliches Monitoring der Systeme ein. Weiterhin setzte der Dienstleister die Anforderungen der Informationssicherheit nach ISO 27001 bis zur Zertifizierungsreife mit der secudor GmbH um.
Diese Maßnahmen halfen dem Dienstleister, nicht nur die Einhaltung der NIS2-Richtlinie zu gewährleisten, sondern auch seine Marktposition zu stärken, indem er als zuverlässiger Partner für seine Kunden auftritt.

Fallbeispiel 4:
Trinkwasserversorger

Ein regionaler Trinkwasserversorger, der für die Versorgung einer großen Bevölkerungsgruppe verantwortlich ist, stellte die Notwendigkeit fest, seine IT-Systeme gegen potenzielle Cyberangriffe zu sichern.
Im Rahmen der jetzt schon absehbaren NIS2-Umsetzung wurden Sicherheitsstandards angehoben, eine 24/7-Überwachung der Wasserversorgungssysteme eingeführt und Notfallpläne für den Fall eines Angriffs entwickelt. Diese proaktiven Maßnahmen stellten sicher, dass die Wasserversorgung selbst bei einem Cyberangriff stabil bleibt und keine Gefahr für die öffentliche Gesundheit entsteht.

SCHLUSSFOLGERUNG

Die NIS2-Richtlinie ist ein wichtiger Schritt, um die Cybersicherheit in KMU zu erhöhen. Eine gezielte Umsetzung der Anforderungen stärkt nicht nur die Sicherheit, sondern auch das Vertrauen von Kunden und Partnern. Die secudor GmbH unterstützt Sie bei der effizienten Umsetzung der NIS2-Richtlinie und der Verbesserung Ihrer Informationssicherheit.

Hierzu bietet die secudor GmbH folgendes Vorgehen:

- NIS2-Readiness-Check (Interview & Bewertung)
- Gap-Analyse zur bestehenden IT-Sicherheit
- Workshop für Führungskräfte: NIS2 verstehen & richtig reagieren
- Erstellung eines Maßnahmenplans
- Begleitung bei Aufbau eines ISMS / NIS2-konformen Systems

QUELLEN

BSI - Bundesamt für Sicherheit in der Informationstechnik. (2024). Schnell-Check zur NIS2-Pflicht.
Verfügbar unter: https://betroffenheitspruefung-nis-2.bsi.de/

BSI - Bundesamt für Sicherheit in der Informationstechnik. (2024). Entscheidungsbaum zur NIS2-Betroffenheit.
Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.pdf?__blob=publicationFile&v=7

BSI - Bundesamt für Sicherheit in der Informationstechnik:
Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-FAQ/FAQ-zu-NIS-2_node.html

KONTAKT/IMPRESSUM

secudor GmbH
Am Schulhof 1
91757 Treuchtlingen

Email:
beratung@secudor.de

Website:
www.secudor.de

Geschäftsführer:
Joachim A. Hader

ÜBER SECUDOR GMBH

Wir verstehen die spezifischen Herausforderungen kleiner und mittlerer Unternehmen (KMU). Wir bieten Ihnen nicht nur theoretisches Wissen, sondern einen praxiserprobten, standardisierten Prozess zur Implementierung eines robusten Informationssicherheitsmanagementsystems (ISMS). Dieses Whitepaper ist Ausdruck unserer tiefgreifenden Expertise im Bereich Informationssicherheit und der NIS2-Richtlinie. Unser ganzheitlicher Ansatz integriert Informationssicherheit und Unternehmenssteuerung und macht uns zu Ihrem idealen Partner, um NIS2-Anforderungen effizient, wirtschaftlich und nachhaltig zu meistern.

Möchten Sie den nächsten Schritt gehen? Als Whitepaper-Leser erhalten Sie mit dem Code „NIS-2 Whitepaper CRC“ einen kostenlosen Cyber-Risiko-Check angelehnt an den BSI-Standard – perfekt als Ausgangspunkt für Ihre NIS2-Compliance.