NIS2 im Sektor „Verarbeitendes Gewerbe/Herstellung von Waren“

NIS	NIS2
• Betreiber wesentlicher Dienste • Anbieter digitaler Dienste • **Sektorbasiert**	• Wesentliche Einrichtunge • Wichtige Einrichtungen • **Sektor- und größenbasiert**
• 30 Einrichtungsarten • 7 Sektoren	• 67 Einrichtungsarten • 18 Sektoren
• “Nur” risikobasiert. Keine Verpflichtung zum Nachweis der Einhaltung	• Obligatorisches Risikomanagement • Überwachung/Inspektion (vor Ort) • Sicherheitsscans und Audits • Sicherheit der Lieferkette
• Sanktionen nach Mitgliedstaaten	• Persönliche Verantwortung der Unternehmensleitung • Schwere Strafen • Formalisierte Berichterstattung

Bild 1: Vergleich von NIS und NIS2

Am 16. Januar 2023 wurde die NIS2-Richtlinie (EU 2022/2555) wirksam, mit dem Ziel, die Cybersicherheitsmaßnahmen in der gesamten Europäischen Union zu stärken. Sie legt einen gemeinsamen Rahmen von Cybersicherheitsanforderungen für Unternehmen und Mitgliedstaaten fest, wobei die Umsetzung durch die Mitgliedstaaten bis zum 17. Oktober 2024 erfolgen muss.

Im Vergleich zur ursprünglichen NIS-Richtlinie führt NIS2 zusätzliche Maßnahmen und Anforderungen im Bereich der Cybersicherheit ein:

- Die Sicherheit der Lieferkette wird zur Priorität.
- Ein verpflichtendes Cyber-Risikomanagement wird eingeführt.
- Unternehmen müssen Mitarbeiter schulen und regelmäßige Cybersicherheitsaudits durchführen.
- Bei Verstößen wird die Unternehmensleitung persönlich haftbar gemacht.
- Empfindliche Strafen drohen bei Nichteinhaltung.
- Formale Meldefristen für die Reaktion auf Vorfälle sind nun vorgesehen.

Autor:
Udo Schneider
Micro_ IoT
Security Evangelist Europe
Trend Micro Deutschland
www.trendmicro.com

NIS im Vergleich zu NIS2

Bild 1 stellt NIS und NIS2 gegenüber.

NIS2 erweitert den Anwendungsbereich auf eine breitere Palette von Sektoren und senkt die Schwelle für betroffene Einrichtungen: Mehr Branchen fallen nun unter die Vorschriften und die Auswahlkriterien für erfasste Einrichtungen wurden angepasst, was zu einer größeren Anzahl von betroffenen Einrichtungen führt.

Neue Sektoren

NIS2 führt zahlreiche neue Sektoren und Subsektoren ein. Im Sektor „Verarbeitendes Gewerbe/Herstellung von Waren“ sind für Unternehmen, die in den Bereichen Automatisierung, Herstellung oder Mess-, Steuer- und Regelungstechnik tätig sind, insbesondere die Subsektoren „Herstellung von elektrischen Ausrüstungen“ und „Maschinenbau“ von Interesse. Die meisten Teilsektoren sind in der NACE Rev. 2 [1] durch entsprechende Verweise näher spezifiziert. Im Falle der „Herstellung von elektrischen Ausrüstungen“ ist dies der Abschnitt C Abteilung 27, im Falle des „Maschinenbaus“ der Abschnitt C Abteilung 28. Betrachtet man die darunter aufgeführten Wirtschaftszweige, so fallen zwei Dinge auf: Erstens werden eine Vielzahl von Wirtschaftszweigen erfasst, die zweitens auch auf den zweiten Blick nicht „kritisch“ sind. Gerade hier zeigt sich, dass NIS2 nicht als Richtlinie nur für „kritische“ Bereiche missverstanden und dementsprechend ignoriert werden darf. Als Geschäftsführung ist man gut beraten, hier explizit zu prüfen, ob man von NIS2 betroffen ist – unabhängig davon, was einem das Bauchgefühl sagt. Man tut auch gut daran, das Ergebnis der Prüfung auch im negativen Fall entsprechend zu dokumentieren.

Einheitliche Kriterien

Im Unterschied zur ursprünglichen NIS-Richtlinie führt NIS2 klare, EU-weit gültige Kriterien ein, um Einrichtungen zu regulieren oder von der Regulierung auszunehmen. NIS2 erweitert die regulierten Sektoren erheblich, auch auf Bereiche, die nicht intuitiv als „kritisch“ betrachtet würden. Die Begriffe „Betreiber wesentlicher Dienste“ und „Anbieter digitaler Dienste“ werden durch „Wesentliche Einrichtungen“ und „Wichtige Einrichtungen“ ersetzt. Dies reflektiert den erweiterten Fokus von NIS2 über die „kritische Infrastruktur“ hinaus.

Unternehmensgröße

Die Unternehmensgröße ist ein weiterer Aspekt (Bild 2). NIS2 orientiert sich an der „Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen“ (EU 32003H0361) [2] mit einem „Size-Cap“-Schwellenwert. Unternehmen mit mehr als 50 Beschäftigten in einem Sektor fallen unter NIS2. In bestimmten Sektoren/Ausnahmen können jedoch auch kleinere Unternehmen betroffen sein!

Selbstregistrierung

Ein oft übersehener Punkt betrifft die Selbstregistrierung. Während Unternehmen unter NIS (oder den lokalen Umsetzungen) von staatlicher Seite informiert wurden, dass sie die regulatorischen Anforderungen erfüllen müssen, besteht unter NIS2 eine Pflicht zur Selbst-

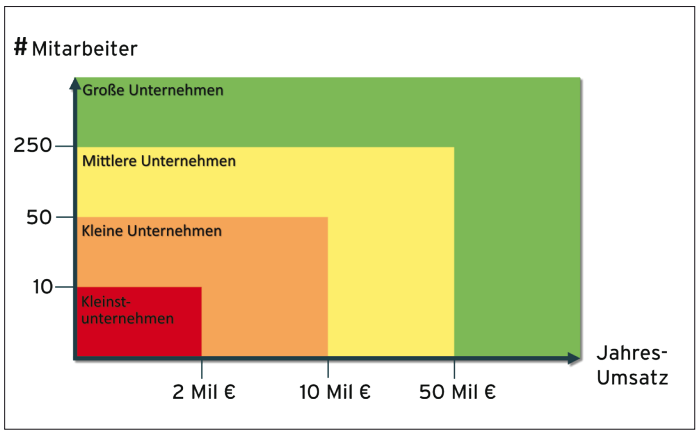

Bild 2: Kategorisierung der Unternehmensgröße für NIS2 nach EU-Vorgaben
© Trend Micro

registrierung. NIS2 sieht vor, dass Mitgliedstaaten eine (Online-)Plattform bereitstellen müssen, auf der sich Unternehmen registrieren können. Die Prüfung, ob ein Unternehmen unter NIS2 fällt, obliegt jedoch dem Unternehmen selbst.

Lieferkette

Ein weiterer bedeutender Aspekt der NIS2-Richtlinie betrifft die Sicherung der Lieferkette. Unternehmen, die unter NIS2 fallen, sind verpflichtet, die Risiken entlang ihrer Lieferkette zu evaluieren. Bei Bedarf sollen sie durch geeignete Maßnahmen, aber auch durch Diversifizierung oder einen Lieferantenwechsel diese Risiken mindern. Es ist zu erwarten, dass die Anforderungen von NIS2 künftig vertraglich in die Lieferkette integriert werden. Auch Unternehmen, die nicht unmittelbar von NIS2 betroffen sind, könnten potenziell zur Einhaltung verpflichtet sein. Dies nicht aus rechtlicher Verpflichtung, sondern aufgrund der vertraglichen Vorgaben, um ihre Lieferbeziehungen nicht zu gefährden.

Kritische Fertigung?

Böse Stimmen behaupten, dass NIS2 auch Bereiche regelt, die nicht kritisch sind. Insbesondere bei der Herstellung von Gütern oder im verarbeitenden Gewerbe mag die „Kritikalität“ auf den ersten Blick nicht ersichtlich sein. Es ist jedoch ein Trugschluss zu glauben, dass NIS2 sich auf kritische Unternehmen konzentriert. Vielmehr adressiert NIS2 die Resilienz in der EU – und das viel ganzheitlicher als NIS. Man könnte auch sagen, dass NIS2 den Fokus von NIS übernommen hat – aber den Begriff wesentlich breiter (insbesondere ökonomisch) interpretiert und damit auch nachgelagerte Unternehmen in der zweiten, dritten, vierten, usw. Reihe der Lieferkette mit einbezieht.

Ökonomisch positiv formuliert könnte man sagen, dass heute praktisch jedes Unternehmen in einer Lieferkettenbeziehung zum Sektor „Verarbeitendes Gewerbe/Herstellung von Waren“ steht. Dies ist für die Unternehmen in diesem Sektor wirtschaftlich sehr positiv. Aber genau diese Abhängigkeit bedingt auch, dass der Sektor entsprechend im Fokus steht und mit NIS2 reguliert wird.

Neue betroffene Unternehmen

Im Gegensatz zu anderen Sektoren, bei denen lediglich die Teilsektoren erweitert wurden, ist der Sektor „Verarbeitendes Gewerbe/Herstellung von Waren“ in der NIS2 neu. Dementsprechend gab es bisher wenig regulatorischen Druck, sich mit den entsprechenden Anforderungen zu beschäftigen. Mit NIS2 ändert sich dies nun schlagartig. Unabhängig vom Teilsektor darf auch nicht übersehen werden, dass Unternehmen ab einer Größe von 50 Mitarbeitern potenziell betroffen sind. NIS2 betrifft also keineswegs nur „die Großen“.

Sofern diese Unternehmen derzeit kein (wie auch immer geartetes) ISMS (Information Security Management System) implementieren, müssen sie möglicherweise vor dem Inkrafttreten der lokalen Umsetzung ihren IT-(Security-)Betrieb grundlegend überdenken. Das reaktive Handeln bei Anforderungen, Vorfällen und Angriffen sollte einem strukturierten, risikobasierten und dokumentierten IT-Betrieb weichen – eine anspruchsvolle Aufgabe, insbesondere für diejenigen, die erst jetzt damit beginnen.

Alles in Echtzeit

NIS2 betrachtet Cybersecurity ähnlich wie andere Unternehmensbereiche. Während es beispielsweise im Rechnungswesen üblich ist, betriebswirtschaftliche Kennzahlen in Echtzeit zur Verfügung zu haben, erweitert NIS2 diesen Ansatz auf die Cybersicherheit. Status, Risiken und betriebliche Kennzahlen müssen jederzeit verfügbar sein, nicht nur im Fall eines Vorfalls. Mit „Turnschuh-Administration“, „Security-Feenstaub“ und „Dokumentation machen wir später“ ist es unmöglich, diese Art von Kennzahlen zeitnah zu erhalten. Das bedeutet, insbesondere für kleinere Unternehmen, erhebliche Veränderungen in den Prozessen, der Organisation, dem (IT-)Betrieb und der Wahrnehmung der IT.

Standards und Implementation

Angesichts der ursprünglichen NIS-Richtlinie im Zusammenhang mit kritischen Infrastrukturen mag es überraschen, dass das (Cyber-)Risikomanagement in NIS2 einen starken Fokus auf IT aufweist. Während zum Beispiel die ENISA für NIS nicht nur Mappings auf IT-Standards wie die ISO/IEC27001-Reihe und NIST CSF, sondern auch auf OT-Standards wie ISO/IEC62443 [3] erstellt hat, spricht die NIS2-Richtlinie bisher ausschließlich von ISO27000:

[...] Maßnahmen zum Schutz dieser Systeme [...] in Übereinstimmung mit europäischen und internationalen Normen wie denen der ISO/IEC 27000er Reihe [...].

Dies ist umso bedauerlicher, als andere Normen wie z. B. die ISO/IEC62443 im OT-Bereich deutlich konkretere Umsetzungsvorgaben machen. Leider gibt es noch keine branchenspezifischen Sicherheitsstandards (B3S) des BSI für den Bereich „Verarbeitendes Gewerbe/Herstellung von Waren“. Es ist jedoch davon auszugehen, dass bis zum Inkrafttreten der NIS2-Umsetzung in Deutschland zumindest Handlungsempfehlungen des BSI [4] veröffentlicht werden. Es ist jedoch nicht empfehlenswert, mit der Umsetzung bis zu deren Veröffentlichung zu warten. Insbesondere da 80 Prozent der geforderten Maßnahmen seit Jahren „Standard“ und entsprechend dokumentiert sind. Das bedeutet, es empfiehlt sich in jedem Fall, sich zeitnah mit den grundlegenden Anforderungen auseinanderzusetzen, um dann, wenn entsprechende branchenspezifische Anforderungen veröffentlicht werden, auf deren Basis die restlichen 20 Prozent umzusetzen.

Fazit

Die NIS2-Richtlinie der Europäischen Kommission verbessert die Schwächen der ursprünglichen NIS-Richtlinie und erweitert den Rahmen für Risikomanagement, Anforderungen, Berichtspflichten und Sanktionen. Dies fördert eine Nivellierung des Wettbewerbs in der EU und unterstützt den europäischen Binnenmarkt. Unternehmen, die neu von NIS2 betroffen sind, stehen vor großen Herausforderungen, insbesondere wenn sie ihren IT-Betrieb noch nicht strukturiert betreiben. Die Umsetzung erfordert nicht nur technische Maßnahmen, sondern auch prozessuale und organisatorische Veränderungen. Mit dem größeren Anwendungsbereich von NIS2 steigt die Anzahl der direkt und indirekt betroffenen Unternehmen erheblich. Unternehmen, die direkt von NIS2 betroffen sind, haben es leichter, NIS2-konforme Waren und Dienstleistungen zu beschaffen. Selbst wenn der Lieferant nicht direkt betroffen ist, liegt es oft in seinem wirtschaftlichen Interesse, Konformität sicherzustellen.

Links

[1] https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-ra-07-015

[2] https://eur-lex.europa.eu/eli/reco/2003/361/oj

[3] https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services

[4] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html ◄