NIS-2

Überblick & Orientierung

https://kritis-berater.com

Die NIS-2-Richtlinie markiert einen wichtigen Meilenstein in der Stärkung der Cybersicherheit in Europa. Sie erweitert den Anwendungsbereich und legt strengere Anforderungen fest, um den Schutz kritischer Infrastrukturen und digitaler Dienste zu gewährleisten.

Ausgangssituation

Die NIS-2-Richtlinie wurde am 27. Dezember 2022 im EU-Amtsblatt veröffentlicht und ist seit dem 16. Januar 2023 in Kraft. Alle EU-Mitgliedstaaten haben bis September 2024 Zeit, um die Richtlinie in nationales Recht umzusetzen.

Die Richtlinie unterscheidet zwischen

- "*wesentlichen Unternehmen/Einrichtunge*n"

und

- "*wichtigen Unternehmen/Einrichtungen*".

Dabei sollen in der gesamten EU einheitliche Kriterien verwendet werden, um den Anwendungsbereich festzulegen. Dadurch wird der Geltungsbereich der Richtlinie auch in Deutschland erheblich erweitert.

Die betroffenen Unternehmen und Organisationen sind verpflichtet, angemessene Maßnahmen in verschiedenen Bereichen zu ergreifen, darunter das Cyber-Risikomanagement, die Sicherheit in der Lieferkette, das Business Continuity Management, Penetrationstests, die Reaktion auf Sicherheitsvorfälle sowie die Berichterstattung an die zuständigen Behörden und die Umsetzung von Abhilfemaßnahmen.

Änderungen

Von der ursprünglichen NIS-Richtlinie zur NIS2 hat es einige Veränderungen gegeben. Die NIS-Richtlinie, die im Jahr 2016 veröffentlicht wurde, hatte das Ziel, Cybersicherheitsmaßnahmen in der gesamten EU zu vereinheitlichen.

Die Richtlinie legte Anforderungen für Betreiber wesentlicher Dienste (Operators of Essential Services, OES) und Anbieter digitaler Dienste (Digital Service Providers, DSP) fest. Dazu gehörten Meldepflichten für Sicherheitsvorfälle und Vorgaben für das Risikomanagement. Die NIS-Richtlinie war das erste EU-weite Gesetz im Bereich der Cybersicherheit und ein wichtiger Schritt im Kampf gegen Cyberbedrohungen in der gesamten EU.

Was ist NIS-2?

NIS-2 steht für die zweite Stufe der Richtlinie der Europäischen Union über Maßnahmen zur Gewährleistung eines **hohen gemeinsamen Sicherheitsniveaus von Netzwerk- und Informationssystemen**, auch bekannt als NIS-Richtlinie (Network and Information Systems Directive).

Die NIS-Richtlinie wurde entwickelt, um die Cybersicherheit in der EU zu verbessern und den Schutz kritischer Infrastrukturen und digitaler Dienste zu gewährleisten.

Die NIS-2-Anforderungen bauen auf den Bestimmungen der ersten Stufe der Richtlinie auf und zielen darauf ab, den Schutz vor Cyberbedrohungen weiter zu stärken.

Die genauen Anforderungen können je nach Mitgliedstaat variieren, da die Richtlinie in nationales Recht umgesetzt wird.

Allerdings stellte sich die Umsetzung der Richtlinie für viele Unternehmen als schwierig heraus: Einige Organisationen hatten Probleme damit, die Anforderungen der NIS überhaupt zu verstehen, während andere Schwierigkeiten hatten, die komplexen Melde- und Berichtspflichten zu erfüllen. Es gab auch Kritik daran, dass die NIS nicht genügend Organisationen und Sektoren einschloss und daher insgesamt zu begrenzt war.

Als Reaktion auf diese Herausforderungen wurde die NIS2-Richtlinie entwickelt. Diese überarbeitete Version zielt darauf ab, die Effektivität der Cybersicherheit in der EU weiter zu verbessern. Es werden strengere Anforderungen gestellt, insbesondere in Bezug auf die Identifizierung kritischer Sektoren und die Einbeziehung einer größeren Anzahl von Organisationen. Die NIS2-Richtlinie soll sicherstellen, dass Unternehmen angemessene Sicherheitsmaßnahmen ergreifen und bei Sicherheitsvorfällen effektiv reagieren.

Die NIS2-Richtlinie ist derzeit noch nicht in deutsches Recht umgesetzt worden.

(Stand 15.07.2024)

Die NIS1-Richtlinie wurde jedoch im Rahmen des IT-Sicherheitsgesetzes umgesetzt und führte zur entsprechenden Anpassung des Bundesgesetzes über die Sicherheit in der Informationstechnik (BSIG) in Deutschland, insbesondere im Bereich **kritischer Infrastrukturen (KRITIS).**

Es wird erwartet, dass die NIS2-Richtlinie in einem zukünftigen IT-Sicherheitsgesetz 3.0 umgesetzt wird, was wiederum zu einer Erweiterung der KRITIS-Sektoren führen wird.

Wichtig:

In der Gesetzgebung für kritische Infrastrukturen (KRITIS) ist nicht die Größe und der monetäre Umsatz relevant, sondern vielmehr die Art der erbrachten kritischen Dienstleistung und der Versorgungsgrad der Bevölkerung. Bisher wurde dies immer auf eine bestimmte Anlage und nicht auf das gesamte Unternehmen bezogen.

Ein Beispiel hierfür ist der Bereich Gesundheit und Pharma. Wenn ein Unternehmen an einem Standort pro Jahr 4,65 Millionen Packungen verschreibungspflichtiger Arzneimittel lagert, herstellt oder vertreibt, dann fällt es gemäß Anhang 5 der BSI-KritisV (Gesetze im Internet) unter die KRITIS.

Es ist wahrscheinlich, dass dies auch bei der NIS2-Richtlinie beibehalten wird.

Zusammenfassend lässt sich sagen, dass die NIS2-Richtlinie erst relevant wird, wenn sie in deutsches Recht überführt wird.

Anforderungen

Wie oben bereits erwähnt legt die NIS-2-Richtlinie Anforderungen für "wesentliche Unternehmen" und "wichtige Unternehmen" fest. Der Hauptunterschied besteht darin, dass "wichtige Unternehmen" geringere Geldstrafen erhalten und einer reaktiven Aufsicht unterliegen, während "wesentliche Unternehmen" einer proaktiven Aufsicht unterstellt sind.

Die EU strebt an, einheitliche Kriterien zu verwenden, anstatt unterschiedliche Schwellenwerte festzulegen, um den Anwendungsbereich der Richtlinie zu bestimmen. Dies bedeutet, dass mittlere und große Unternehmen unter die Regulierung fallen, basierend auf Kriterien wie Mitarbeiterzahl, Umsatz und Bilanzsumme. Dadurch wird der Anwendungsbereich der Richtlinie in Deutschland erheblich erweitert.

⇒ Für "wesentliche Einrichtungen" können Geldstrafen von mindestens zehn Millionen Euro oder zwei Prozent des Jahresumsatzes verhängt werden, je nachdem, welcher Betrag höher ist.
⇒ Bei "wichtigen Einrichtungen" liegen die Bußgelder bei mindestens sieben Millionen Euro oder 1,4 Prozent des Jahresumsatzes.

Die betroffenen Unternehmen und Organisationen sind verpflichtet, angemessene Maßnahmen in Bereichen wie Cyber-Risikomanagement, Sicherheit in der Lieferkette, Business Continuity Management, Penetrationstests, Reaktion auf Vorfälle sowie Berichterstattung an die zuständigen Behörden und Umsetzung von Abhilfemaßnahmen zu ergreifen.

Die NIS-2-Richtlinie erweitert das Thema Cybersicherheit und -Resilienz auch auf eine breite Masse von Unternehmen in Europa und insbesondere in Deutschland, und es wird erwartet, dass dies zu einem wichtigen Thema wird.

Ist mein Unternehmen / meine Institution betroffen?

Zunächst ist es wichtig zu beachten, dass die Behörden keine direkte Mitteilung darüber machen, ob die NIS-2-Richtlinie auf ein Unternehmen oder eine Institution zutrifft.

Es liegt in der Verantwortung des Unternehmens, anhand bestimmter Kriterien, die sowohl Branchenelemente als auch Größenüberlegungen berücksichtigen, selbst zu beurteilen, ob sie betroffen sind. In einigen Fällen kann ein Unternehmen aufgrund seiner Größe und seines Marktanteils in einem bestimmten Sektor sogar als "wesentlich" eingestuft werden.

Die NIS2-Richtlinie betrifft eine breite Palette von Unternehmen und Organisationen in verschiedenen wesentlichen und wichtigen Sektoren. Diese Einrichtungen werden verpflichtet, Maßnahmen zu ergreifen, um ihre Systeme vor Cyberangriffen zu schützen und im Falle eines Vorfalls eine schnelle Wiederherstellung zu gewährleisten.

Zu den betroffenen Einrichtungen gehören:

- **Betreiber wesentlicher Dienste (Operators of Essential Services OES):** Dies sind Unternehmen, die als wesentlich für das Funktionieren der Wirtschaft und Gesellschaft angesehen werden. Dazu gehören Unternehmen in den Bereichen Energie, Trinkwasser- und Abwasserversorgung sowie Gesundheitsdienstleister. Die Größe des Unternehmens spielt dabei keine Rolle.

- **Anbieter digitaler Dienste (Digital Service Providers DSP):** Dies sind Unternehmen, die Online-Dienste anbieten, wie zum Beispiel Online-Marktplätze, Cloud Computing-Anbieter und Suchmaschinen. DSPs müssen die Anforderungen der NIS2-Richtlinie nur erfüllen, wenn sie bestimmte Größenkriterien überschreiten. Dabei wird zwischen mittleren Unternehmen (50 oder mehr Mitarbeiter und ein Jahresumsatz von mindestens 10 Millionen Euro) und großen Unternehmen (250 oder mehr Mitarbeiter und ein Jahresumsatz von mindestens 50 Millionen Euro) unterschieden.

Die NIS2-Richtlinie deckt eine Vielzahl von wesentlichen und wichtigen Sektoren ab, darunter Energie, Verkehr, Bankwesen, Gesundheitswesen, Trinkwasser- und Abwasserversorgung, digitale Infrastruktur, öffentliche Verwaltung und viele weitere.

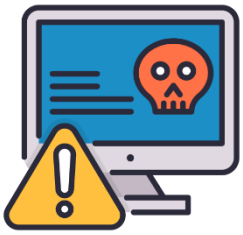
wesentliche Sektoren	wichtige Sektoren
Energie Verkehr Bankwesen Finanzmarktinfrastruktur Gesundheitswesen Trinkwasser Abwasser Digitale Infrastruktur Verwaltung von IKT-Diensten Öffentliche Verwaltung Weltraum	Post- und Kurierdienste Abfallbewirtschaftung Chemische Stoffe Lebensmittel Verarbeitendes Gewerbe/Herstellung von Waren Anbieter digitaler Dienste Forschungseinrichtungen

Unternehmen, die nicht unter die spezifischen Kriterien der NIS2-Richtlinie fallen, können dennoch ihre Cybersicherheitsmaßnahmen entsprechend ausrichten und ihre Systeme effektiv vor Angriffen schützen. Es liegt im Interesse aller Unternehmen, ihre Cybersicherheit zu verbessern und so zur Stärkung der gesamten digitalen Sicherheitslandschaft beizutragen.

Neue Herausforderungen und Handlungsbedarf

Die Einführung der NIS2-Richtlinie durch die Europäische Union markiert einen entscheidenden Schritt im Kampf gegen die zunehmende Cyberkriminalität weltweit. Diese Richtlinie bringt jedoch nicht nur strengere Anforderungen an die Cybersicherheit mit sich, sondern auch erweiterte rechtliche Konsequenzen für Unternehmen, die den neuen Standards nicht entsprechen.

Herausforderungen



- Betriebsunterbrechungen und Datenpannen wurden als die größten Geschäftsrisiken in Deutschland identifiziert.
- Mangelnde Reaktion auf Sicherheitsvorfälle kann das Vertrauen von Kunden und Partnern gefährden und langfristig die finanzielle Stabilität eines Unternehmens beeinträchtigen.

Erforderliche Maßnahmen:

- Implementierung eines umfassenden Informationssicherheits-Managementsystems (ISMS), welches alle Unternehmensbereiche und -prozesse abdeckt.
- Entwicklung detaillierter Pläne zur Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen, einschließlich der Meldung innerhalb kurzer Fristen.
- Durchführung kontinuierlicher Schulungen zur Sensibilisierung aller Mitarbeiter für Sicherheitsprinzipien und spezifische Anforderungen ihres Arbeitsbereichs.

Dringender Handlungsbedarf:

- Unternehmen sollten unverzüglich mit der Vorbereitung auf die NIS2-Richtlinie beginnen, da die Zeit bis zur Deadline begrenzt ist.
- Eine Gap-Analyse ist der erste Schritt, um festzustellen, welche Maßnahmen zur Einhaltung der NIS2-Richtlinie erforderlich sind.
- Trotz eventuell begrenzter Mittel müssen Unternehmen die erforderlichen Maßnahmen ergreifen, um ihre Cybersicherheit zu verbessern und das Risiko von Sicherheitsvorfällen zu minimieren – besonders vor dem Hintergrund, dass ein Fachkräftemangel im Bereich der Cybersicherheit herrscht, ist schnelles Handeln, gegebenenfalls mit externer Unterstützung, unabdingbar!

Wie kann ich mich und mein Unternehmen vorbereiten?

ISMS nach ISO 27001 als optimale Vorbereitung:

Ein Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 ist der Schlüssel zur Erfüllung der Anforderungen von NIS2. Es wurde von führenden NIS2-Regulatoren als bestens geeignet bestätigt und bietet eine solide Grundlage für die Cybersicherheit Ihres Unternehmens.

Checkliste für IT-Verantwortliche:

Um sicherzustellen, dass Ihre IT-Systeme den Anforderungen von NIS2 entsprechen, folgen Sie unserer Checkliste in 10 Schritten zur Cyberresilienz und Compliance. Diese praktische Anleitung hilft Ihnen dabei, die erforderlichen Maßnahmen zu ergreifen und Ihr Unternehmen vor Cyberbedrohungen zu schützen.

Schulungen für Mitarbeiter:

Neben technologischen Maßnahmen ist die regelmäßige Schulung aller Mitarbeiter entscheidend für die Sicherheit Ihrer IT-Systeme. Sensibilisieren Sie Ihr Team für korrektes Verhalten im Umgang mit Cybergefahren, um Sicherheitsvorfälle effektiv zu behandeln und die Compliance mit NIS2 sicherzustellen.

Fristen für Vorfalls-Meldungen:

Beachten Sie die sehr kurzen Fristen für die Meldung von Sicherheitsvorfällen gemäß NIS2. Richten Sie Mechanismen zur Erkennung und Meldung von Sicherheitsvorfällen ein, um den Anforderungen der Richtlinie gerecht zu werden und die erforderlichen Meldungen innerhalb der vorgegebenen Fristen abzugeben.

Es ist wichtig zu beachten, dass der Anwendungsbereich der NIS-2-Richtlinie über die bisher bekannten kritischen Infrastrukturen hinausgeht!

Im Energiesektor zum Beispiel waren bisher nur Unternehmen betroffen, die Strom- und Gasenergie erzeugen, liefern oder regulieren. Mit der Einführung von NIS-2 ist zu erwarten, dass auch die Lieferkette, wie beispielsweise Hersteller von Windturbinen und Betreiber von Ladestationen für Elektrofahrzeuge, den Anforderungen unterliegen werden.

OPTIQUM GmbH
Siegburger Straße 223
D-50679 Köln

+49 221 82 95 91 0
info@optiqum.de