OBJECT FIRST

Whitepaper

Die NIS-2-Richtlinie

Was Sie beachten müssen und wie Sie die Vorschriften einhalten

NIS-2 – eine Einführung

Die Zahl der Cyberangriffe nimmt ständig zu und die Methoden von Angreifern werden immer ausgefeilter. Regierungen und internationale Organisationen verabschieden deshalb neue und überarbeitete Vorschriften, die helfen sollen, sich in wichtigen Bereichen gegen diese Gefahren zu wappnen. Innerhalb der Europäischen Union (EU) wurde hierfür die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) verabschiedet. Unternehmen in der EU müssen Maßnahmen ergreifen, um die Anforderungen der Richtlinie zu erfüllen und Risiken durch den Verstoß gegen Vorschriften und Imageschäden zu vermeiden.

Wenn Sie in der IT-Branche in der EU tätig sind, müssen Sie mit den Regelungen der NIS-2-Richtlinie vertraut sein, um Ihre Infrastruktur zu schützen und weiterhin als vertrauenswürdiger Partner Ihrer Kunden agieren zu können. Diese kurze Einführung schlüsselt die wichtigsten Elemente der Richtlinie für Sie auf, damit Sie die Vorschriften einhalten und Angreifern stets einen Schritt voraus sein können.

Was ist NIS-2?

Ziel der NIS-2-Richtlinie (Network and Information Security Directive 2) ist es, die Cybersicherheit in allen EU-Mitgliedstaaten sowie in allen Einrichtungen, die in diesen Staaten Geschäfte tätigen, zu verbessern. Sie dient dazu, den wachsenden Gefahren zu begegnen, die sich aus der Digitalisierung und der zunehmenden Zahl von Cyberangriffen ergeben.

NIS-2 erweitert den Anwendungsbereich der ursprünglichen NIS-Richtlinie, sodass nun mehr Sektoren und Einrichtungen zur Einhaltung der Vorschriften verpflichtet sind. Hierzu gehören auch Sektoren und Einrichtungen, die im EU-Binnenmarkt eine „wesentliche“ und „wichtige“ Rolle spielen. Die NIS-2-Richtlinie enthält strengere Vorgaben unter anderem in Bezug auf eine umfassende Berichterstattung über Sicherheitsvorfälle, Risikomanagementverfahren, Maßnahmen zur Gewährleistung der Rechenschaftspflicht von Unternehmen und Strategien zur Aufrechterhaltung des Betriebs.

Ist unser Unternehmen wesentlich oder wichtig?

Die NIS-2-Richtlinie teilt Unternehmen in zwei Kategorien ein: wesentliche Einrichtungen und wichtige Einrichtungen.
Wenn Sie wissen, in welche dieser Kategorien Sie fallen, können Sie Auswirkungen der NIS-2-Richtlinie auf Ihr Unternehmen verstehen.

Risiken bei Nichteinhaltung

Die NIS-2-Richtlinie sieht bei Verstößen umfangreiche Strafen vor, darunter Bußgelder in erheblicher Höhe und mögliche Rechtsstreitigkeiten.Die NIS-2-Richtlinie musste bis zum 17. Oktober 2024 von den EU-Mitgliedsstaaten in nationales Recht umgesetzt werden. Nicht alle Länder haben die Richtlinie fristgerecht umgesetzt, doch bemühen sich alle aktiv um eine Umsetzung. In einige Mitgliedsstaaten werden bereits nationale Vorschriften durchgesetzt, andere stehen kurz vor der Verabschiedung entsprechender Gesetze.

Sie müssen sich deshalb proaktiv mit den Regelungen der Richtlinie vertraut machen, die Auswirkungen auf Ihr Unternehmen ermitteln und einen Plan entwickeln, wie Sie die Einhaltung sicherstellen.

Sie fragen sich nun vielleicht, inwiefern Sie von dieser Richtlinie betroffen sind, doch zunächst müssen Sie verstehen, wer „Sie“ sind und ob die NIS-2-Vorschriften sich auf Ihr Unternehmen auswirken.

Wesentliche Einrichtungen

Die NIS-2-Richtlinie klassifiziert wichtige Sektoren wie Verkehr, Finanzdienstleistungen, Gesundheitswesen und Versorgungsunternehmen (einschließlich Energieversorger) als „wesentliche Einrichtungen“ und unterstreicht damit ihre Bedeutung für das gesellschaftliche und wirtschaftliche Wohlergehen. Sie unterliegen umfangreicheren Pflichten und müssen insbesondere Sicherheitsvorfälle innerhalb von 24 Stunden melden. Damit enthält NIS-2 wesentlich strengere Vorgaben als die bisherige Richtlinie. Bei Verstößen gegen die Richtlinie drohen Unternehmen nun außerdem hohe Geldbußen und schwerwiegende Konsequenzen. Es steht für sie also einiges auf dem Spiel, wenn sie die strengeren Gesetzesvorschriften nicht einhalten.

Wenn Ihr Unternehmen mehr als 250 Mitarbeiter beschäftigt, einen Jahresumsatz von 50 Millionen Euro erwirtschaftet und in eine der folgenden Kategorien fällt, ist es eine wesentliche Einrichtung:

- Digitale Infrastruktur
- Energie
- Finanzdienstleistungen
- Gesundheitswesen
- Öffentliche Verwaltung
- Weltraum
- Verkehr
- Wasserversorgung (Trinkwasser und Abwasser)

Wichtige Einrichtungen

Mit der NIS-2-Richtlinie wird die neue Kategorie der „wichtigen Einrichtungen“ eingeführt. Damit wird der Anwendungsbereich auf Sektoren wie Postdienstleistungen, Abfallbewirtschaftung und das verarbeitende Gewerbe bzw. die Herstellung von Waren ausgeweitet. Dies bedeutet, dass diese Sektoren ihre Sicherheitsmaßnahmen überprüfen und ergänzen müssen, um die NIS-2-Vorschriften einzuhalten.

Für wichtige Einrichtungen gelten zwar weniger strenge Pflichten und Strafen bei Nichteinhaltung als für wesentliche Einrichtungen, doch sollten sie die Herausforderung, diese Anforderungen zu erfüllen, nicht unterschätzen.

Wenn Ihr Unternehmen mehr als 50 Mitarbeiter beschäftigt, einen Jahresumsatz von 10 Millionen Euro erwirtschaftet und in eine der folgenden Kategorien (einschließlich der für wesentliche Einrichtungen geltenden Kategorien) fällt, ist es eine wichtige Einrichtung:

- Chemische Stoffe
- Lebensmittel
- Verarbeitendes Gewerbe/Herstellung von Waren
- Postdienstleistungen
- Forschung
- Abfallbewirtschaftung

Wesentliche Einrichtungen

Fällt Ihr Unternehmen in eine der Kategorien „wesentliche Einrichtungen“ oder „wichtige Einrichtungen“, müssen Sie als Nächstes prüfen, was die NIS-2-Vorschriften für Ihr Unternehmen bedeuten und welche Auswirkungen sie haben können.

Erste Schritte

Die NIS-2-Richtlinie hebt darauf ab, dass Unternehmen eine umfassende Cybersicherheitsstrategie benötigen. Die Regelungen sind sehr detailliert und wir empfehlen betroffenen Unternehmen in den Mitgliedstaaten, sich mit den einzelnen Artikeln der Richtlinie vertraut zu machen. Um Sie dabei zu unterstützen, die Auswirkungen der Richtlinie auf Ihr Unternehmen zu bewerten, haben wir die zehn Cybersicherheitsmaßnahmen, die Sie mindestens ergreifen sollten, für Sie zusammengefasst.

Die zehn Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Zu den wichtigsten Bestimmungen der Richtlinie gehört Artikel 21, in dem zehn Risikomanagementmaßnahmen im Bereich der Cybersicherheit aufgeführt sind. Mitgliedstaaten müssen sicherstellen, dass wesentliche und wichtige Einrichtungen geeignete technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen. Diese Maßnahmen dienen dazu, die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste zu verhindern oder möglichst gering zu halten. Sie müssen unter Berücksichtigung der neuesten Technologien, relevanter Standards und der Kosten für die Umsetzung ein Sicherheitsniveau gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit von Sicherheitsmaßnahmen müssen Unternehmen das Ausmaß ihrer Risikoexposition, ihre Größe und die potenziellen Auswirkungen von Sicherheitsvorfällen berücksichtigen. Unter anderem müssen sie den Schweregrad und die Eintrittswahrscheinlichkeit von Sicherheitsvorfällen sowie deren gesellschaftliche und wirtschaftliche Auswirkungen bewerten.

In der NIS-2-Richtlinie sind zehn Cybersicherheitsmaßnahmen aufgeführt, die die betroffenen Einrichtungen umsetzen müssen:

1. Bewältigung von Sicherheitsvorfällen
2. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
3. Prozesse zur Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
6. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
7. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
8. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
9. Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung
10. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Meldepflichten

Die NIS-2-Richtlinie verweist wiederholt darauf, dass die Meldung von Sicherheitsvorfällen von entscheidender Bedeutung ist. Wesentliche Einrichtungen müssen Verfahren für die zeitnahe Meldung erheblicher Cybersicherheitsvorfälle einrichten und dabei besondere Meldefristen einhalten. Hierzu gehört unter anderem ein vorläufiges Frühwarnsystem zur Meldung von Vorfällen innerhalb von 24 Stunden.

Die NIS-2-Richtlinie betont auch die Verantwortung von Unternehmen: Die Leitungsorgane von Einrichtungen sind verpflichtet, sich mit den Cybersicherheitsmaßnahmen des Unternehmens vertraut zu machen und sich aktiv an deren Umsetzung zu beteiligen. Personen mit Leitungsaufgaben drohen bei Sicherheitsverletzungen Strafen. Sie können möglicherweise haftbar gemacht werden oder es kann ihnen sogar die Wahrnehmung von Leitungsaufgaben vorübergehend untersagt werden.

Sanktionen

Die NIS-2-Richtlinie enthält neue, wesentlich anspruchsvollere Regelungen und sieht in manchen Fällen auch höhere oder vollkommen neue Geldbußen vor.

Die EU-Mitgliedstaaten können jedoch selbst noch höhere Geldbußen verhängen. Wesentlichen Einrichtungen drohen Strafzahlungen von bis zu 10 Millionen Euro oder 2 % ihres weltweiten Vorjahresumsatzes, je nachdem, welcher Betrag höher ist. Wichtige Einrichtungen müssen mit Strafzahlungen von bis zu 7 Millionen Euro oder 1,4 % ihres weltweiten Vorjahresumsatzes rechnen, je nachdem, welcher Betrag höher ist.

Das ist aber noch nicht alles

Diese drei Abschnitte zeigen zahlreiche Verpflichtungen aus der NIS-2-Richtlinie auf, sind jedoch keine vollständige Beschreibung der darin enthaltenen Vorschriften. Wir empfehlen allen Unternehmen, die in der Europäischen Union geschäftlich tätig sind, sich gemeinsam mit ihren Teams mit den Anforderungen der gesamten Richtlinie vertraut zu machen, um die Vorgaben und Auswirkungen dieser umfangreichen Gesetzesvorschriften zu verstehen.

Wie Lösungen von Object First Cybersicherheit gewährleisten

Die NIS-2-Richtlinie stellt eine wesentliche Weiterentwicklung der in der EU geltenden Sicherheitsvorschriften dar. Ihre Umsetzung in den Rechenzentren wichtiger und wesentlicher Einrichtungen könnte ein wichtiger Schritt hin zu mehr Sicherheit bedeuten. Im Rahmen dieser Einführung möchten wir Ihnen auch Empfehlungen an die Hand geben, wie Sie Ihre Ziele zur Umsetzung der NIS-2-Vorschriften effizient erreichen können.

Zero-Trust-Datenresilienz

In Abschnitt 89 der Einführung zur NIS-2-Richtlinie wird darauf verwiesen, dass Unternehmen unter anderem durch Umsetzung von Zero-Trust-Grundsätzen ihre Sicherheit erhöhen können. Die Zero-Trust-Grundsätze zielen darauf ab, die Sicherheit von produktiven Anwendungen und Infrastrukturen zu gewährleisten. Im Reifegradmodell dieser Grundsätze sind Backup-Software und Backup-Storage jedoch nicht berücksichtigt.

Veeam und Numberline haben kürzlich eine Studie zum Thema **Zero-Trust-Datenresilienz (ZTDR)** veröffentlicht. Dabei handelt es sich um ein umfassendes Datenschutzkonzept, das die Sicherheitsprinzipien von Zero Trust auf die Backup-Umgebung eines Unternehmens ausweitet. Wichtige Elemente von ZTDR sind die Trennung von Backup-Software und Backup-Storage, die Verwendung mehrerer Resilienzzonen sowie ein verschlüsselter Immutable Backup-Storage. Mit diesem Ansatz können Unternehmen Risiken minimieren, den Datenschutz verbessern und ihre Sicherheit erhöhen. Unternehmen sollten sich mit dem Konzept der ZTDR vertraut machen, da es ein zuverlässiges Framework für den Schutz ihrer Daten vor Cyberbedrohungen bietet, insbesondere vor Ransomware- und Datenexfiltrationsangriffen. Es gewährleistet eine höhere Sicherheit und besseren Datenschutz als herkömmliche Sicherheitsmodelle und sollte auf der Checkliste von Administratoren, die sich auf die Umsetzung der NIS-2-Richtlinie vorbereiten, nicht fehlen. Weitere Informationen zur ZTDR finden Sie in unserem **Whitepaper**.

Immutable Backup-Datenspeicher

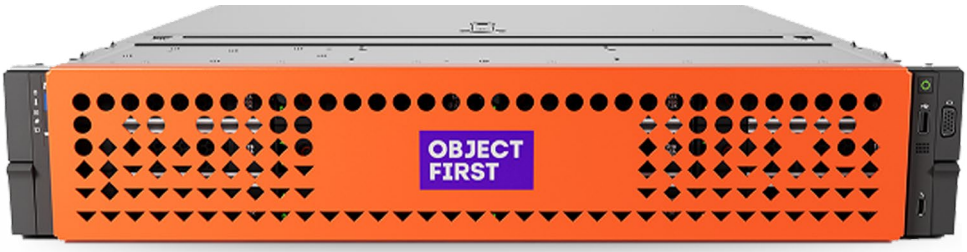
Der Begriff „Immutability“ – also die Unveränderlichkeit von Daten – kommt überraschenderweise in der NIS-2-Richtlinie nicht vor. Der wichtigste Aspekt der Datensicherung besteht in der Möglichkeit, die gesicherten Daten wiederherstellen zu können. Mit Immutable Storage ist die Wahrscheinlichkeit einer erfolgreichen Wiederherstellung wesentlich höher. Die meisten Angriffe nehmen heute zunächst die Backup-Infrastruktur ins Visier. Damit soll Unternehmen die Möglichkeit genommen werden, ihre Daten wiederherzustellen, um sie so zur Zahlung des Lösegelds zu zwingen.

Die Cybersicherheitsmaßnahmen nach Artikel 21 der NIS-2-Richtlinie sehen konkret Verfahren für Backup, Cyberhygiene und Verschlüsselung vor. Diese Sicherheitsmaßnahmen können jedoch von Angreifern umgangen oder außer Kraft gesetzt werden. Ein Immutable Storage-Ziel, das den Best Practices von ZTDR entspricht – keine Administratorrechte, eine Trennung der Backup-Architektur von der Backup-Software und Storage mit S3 Object Lock im Compliance-Modus , sorgt hingegen für stärkere Resilienz gegenüber Angriffen. Um jedoch eine Wiederherstellung zu *garantieren*, ist absolute Immutability erforderlich. So kann niemand – auch kein Administrator mit weit gefassten Rechten oder ein Angreifer mit Zugriff auf den Backup-Storage – Ihre Daten ändern oder löschen.

Einhaltung von RTO-Vorgaben

In der Richtlinie wird mehrfach darauf verwiesen, wie wichtig eine Wiederherstellungsstrategie ist. Diese sollte auch einen Plan für eine schnelle Wiederherstellung und das Testen von Wiederherstellungsszenarien beinhalten, bevor es zu einem Cyberangriff kommt. Wir empfehlen allen Unternehmen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, ihre derzeitige Datensicherungsumgebung auf den Prüfstand zu stellen und ihre Wiederherstellungsszenarien zu testen, um ihre tatsächlichen Ziele für den Wiederherstellungspunkt (RPOs) und ihre Wiederherstellungszeiten (RTOs) besser einschätzen zu können. Ein entscheidender Aspekt der von NIS-2 geforderten Reaktionsfähigkeit besteht darin zu ermitteln, wie weit der Wiederherstellungspunkt zurückliegt (d. h. wie groß der entsprechende Datenverlust ist) und wie lange die Wiederherstellung der Daten dauert.

Bestens geschützt mit Ootbi (Out-of-the-Box Immutability)



Object First möchte allen Veeam-Kunden in der EU helfen sicherzustellen, dass ihr Backup-Storage die NIS-2-Standards nicht nur erfüllt, sondern sogar übertrifft. Deshalb hat Object First Ootbi entwickelt, die beste Storage-Lösung für Veeam. Ootbi von Object First bietet Ransomware-Schutz und integrierte Immutability. Damit steht Unternehmen ein sicherer, unkomplizierter und leistungsfähiger Backup-Storage mit absoluter Immutability zur Verfügung.

Durch diesen ultimativen Ransomware-Schutz profitieren Sie und Ihr Unternehmen von einfacher Resilienz.

Object First basiert auf Best Practices für Zero Trust. Unabhängige Tests bestätigen, dass die Lösung sicher ist und sich auch ohne spezielle Sicherheitskenntnisse einfach implementieren und verwalten lässt. Sie ist ausreichend leistungsfähig, um eine Sofortwiederherstellung zu unterstützen, und kann gemeinsam mit Ihrem Unternehmen wachsen.

Fazit

Die am 17. Oktober 2024 in Kraft getretene NIS-2-Richtlinie wurde von den Mitgliedstaaten in nationales Recht umgesetzt. Wie bei jedem umfangreichen Regelwerk bringt diese Umsetzung für die Verantwortlichen in wichtigen und wesentlichen Einrichtungen viel Arbeit mit sich, um zu gewährleisten, dass gegen das Unternehmen keine Geldbußen wegen Nichteinhaltung der Vorschriften verhängt werden. Entsprechende Schulungen der Mitarbeiter sind ein wichtiger erster Schritt, um die Anforderungen dieser Richtlinie zu erfüllen. Nehmen Sie sich bitte Zeit, um die vollständige NIS-2-Richtlinie zu lesen, falls Ihr Unternehmen davon betroffen ist. Nur so können Sie sicherstellen, dass alle Verantwortlichen ausführlich über die Folgen für Ihr Unternehmen informiert sind. Die Umsetzung der NIS-2-Richtlinie mag zunächst mit erheblichem Aufwand verbunden sein, doch können Sie dadurch Unterbrechungen des Geschäftsbetriebs aufgrund von Cyberangriffen verringern.

Simply Resilient for Veeam

1.0_20251118

OBJECT FIRST