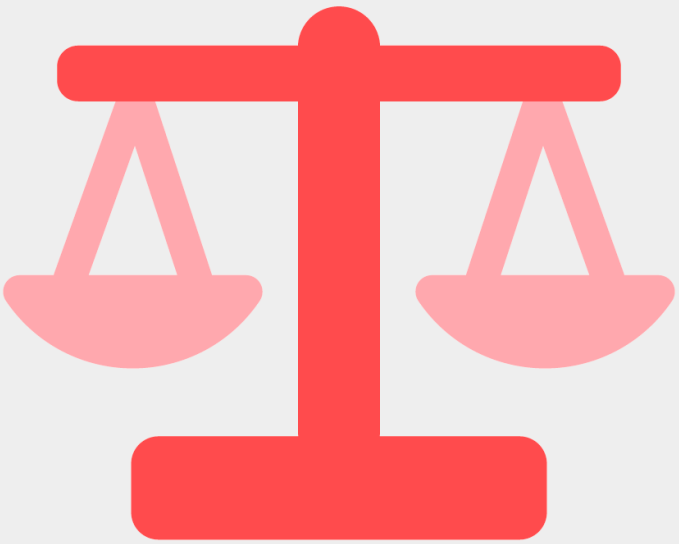
keepit

Was ist die NIS2-Richtlinie?

Das müssen Sie wissen



Was ist die NIS2-Richtlinie? Das müssen Sie wissen

Am 10. November 2022 (veröffentlicht am 27. Dezember 2022) verabschiedete das EU-Parlament mit der NIS2-Richtlinie eine neue Rechtsvorschrift, die die Cyber-Resilienz in der gesamten Europäischen Union verbessern soll. NIS2 enthält unter anderem auch klare Anforderungen an die Datensicherung und Notfallwiederherstellung.

Die Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) ist eine Antwort auf die wachsende Gefährdung Europas durch Cyberbedrohungen sowie darauf, dass wir mit zunehmender Vernetzung immer anfälliger für Cyberangriffe werden. Mit der neuen Richtlinie wollen die Regulierungsbehörden einheitliche Regeln für Unternehmen schaffen und dafür sorgen, dass die Strafverfolgungs- und Justizbehörden effizient arbeiten können und die EU-Bürger für das Thema Cybersicherheit sensibilisiert werden.

Keepit unterstützt die EU-Initiative zum Schutz unserer digitalen Infrastruktur, unserer sensiblen Geschäftsdaten und unserer personenbezogenen Daten.

Welchen Zweck verfolgt die NIS-Richtlinie?

Im Vergleich zur ersten NIS-Richtlinie erweitert NIS2 sowohl die Anforderungen an die Cybersicherheit als auch die Sanktionsmöglichkeiten, um das Sicherheitsniveau in den Mitgliedstaaten zu vereinheitlichen und zu optimieren. Für eine Reihe von Sektoren werden die Anforderungen deshalb strenger.

Wie der Wissenschaftliche Dienst des Europäischen Parlaments (EPRS) in einem Briefing zur NIS-Richtlinie konstatiert, nimmt nicht nur die Zahl der Cyberangriffe weltweit rapide zu, sondern auch ihr Ausmaß, ihre Raffinesse und die verursachten Kosten. Angesicht dessen, so der EPRS weiter, hat die Kommission „einen Vorschlag vorgelegt, um die ursprüngliche NIS-Richtlinie zu ersetzen und damit die Sicherheitsanforderungen zu verschärfen, die Sicherheit der Lieferketten zu gewährleisten, die Meldepflichten zu straffen und striktere Aufsichtsmaßnahmen sowie strengere Durchsetzungsregelungen einzuführen."

Was also hat dazu geführt, dass die Anforderungen erweitert werden müssen? Der WEF Global Risks Report 2023 beschreibt den Grund wie folgt:

> *„Die immer stärkere Verflechtung zwischen Technologien und kritischen gesellschaftlichen Aufgaben setzt die Bevölkerung unmittelbaren inneren Bedrohungen aus, einschließlich solcher, die die Funktionsfähigkeit der Gesellschaft zu zerrütten versuchen."*

keepit

Für welche Sektoren und Einrichtungen gilt NIS2?

Die Richtlinie gilt insbesondere für Unternehmen und Einrichtungen in zwei Arten von Sektoren, nämlich „wesentlichen“ und „wichtigen“.

Einrichtungen in folgenden Sektoren werden als wesentlich eingestuft:

- Energie (Elektrizität, Fernwärme, Öl, Gas, Wasserstoff)
- Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr)
- Bankwesen (Kreditinstitute)
- Finanzmarktinfrastrukturen (Marktplätze)
- Gesundheitswesen (Gesundheitsdienstleister, Arzneimittelhersteller etc.)
- Trink- und Abwasser
- Digitale Infrastruktur (u. a. Anbieter von Cloud-Diensten, Anbieter von Rechenzentrumsdiensten, DNS [Domain-Name-System]-Diensteanbieter, TLD [Top-Level-Domain]-Vergabestellen, Anbieter öffentlicher Kommunikationsnetze)
- Anbieter von IKT (Informations- und Kommunikations)-Dienstleistungen
- Anbieter von Managed Services und Managed Security Services
- Öffentliche Verwaltung
- Weltraum

Öffentliche und private Einrichtungen in folgenden Sektoren werden als „wichtig“ eingestuft:

- Post- und Kurierdienste
- Abfallwirtschaft
- Herstellung, Produktion und Vertrieb von chemischen Stoffen
- Herstellung, Verarbeitung und Vertrieb von Lebensmitteln
- Produktion von elektronischen Geräten, Maschinen, Kraftfahrzeugen etc.
- Anbieter bestimmter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen und soziale Netzwerke)
- Forschung (Hochschul- und Forschungseinrichtungen).

Wenn Ihr Unternehmen eine Dienstleistung erbringt, die unerlässlich ist, um kritische gesellschaftliche und/oder wirtschaftliche Aktivitäten aufrechtzuerhalten – wie zum Beispiel Transportdienstleistungen –, werden Sie per Gesetz als „Betreiber wesentlicher Dienste“ eingestuft.

Diese Einstufung wird Ihre technischen und organisatorischen Strukturen und Funktionen erheblichen Belastungen aussetzen, da Sie dann gesetzlich verpflichtet sind, umfassende Risikomanagement- und Sicherheitsmaßnahmen umzusetzen und einzuhalten.

NIS2-Anforderungen, Risikomanagement und Sicherheitsmaßnahmen

Die derzeitige NIS-Richtlinie verpflichtet die betroffenen Einrichtungen dazu, geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheitsrisiken zu steuern und bei einem Sicherheitsvorfall den Schaden zu begrenzen.

NIS2 hält diese Bestimmungen aufrecht und legt zusätzliche Anforderungen für angemessene Sicherheitsmaßnahmen fest. Diese müssen nun mindestens Folgendes umfassen:

- Konzepte für Risikoanalysen und die Sicherheit von Informationssystemen
- Bewältigung von Sicherheitsvorfällen
- Maßnahmen zur Aufrechterhaltung des Betriebs, wie Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement
- Sicherheit der Lieferkette, einschließlich Lieferantenmanagement/Sicherheit bei Lieferanten
- Sicherheitsmaßnahmen beim Erwerb, der Entwicklung und Wartung von Netz- und Informationssystemen
- Konzepte und Verfahren, um die Wirksamkeit von Maßnahmen zur Bewältigung von Cybersicherheitsrisiken zu bewerten
- Grundlegende Cyberhygiene und Schulungen zur Cybersicherheit
- Vorgaben für den Einsatz von Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrollen und Asset Management
- Absicherung der internen Kommunikationssysteme

NIS2 zuverlässig bewältigen

Eine dedizierte Backup- und Datenmanagement-Lösung kann Ihrem Unternehmen helfen, robuste Maßnahmen zum Schutz und zur Verwaltung von Daten für Ihre SaaS-Workloads umzusetzen, etwa für Microsoft 365 und Salesforce.

Keepit bietet Ihnen umfassende Dienste zur Sicherung Ihre SaaS-Daten. Diese können Ihnen helfen, die Anforderungen der NIS2-Richtlinie zu erfüllen, und dienen dabei dem Gesamtziel, die Kontinuität Ihrer Geschäftsabläufe sicherzustellen.

Sie selbst müssen allerdings entscheiden, welche Geschäftsfunktionen unerlässlich sind, und feststellen, ob Sie diese kritischen Funktionen auch bei Notfällen oder Störungen aufrechterhalten können. Dementsprechend sollten Sie dann die verfügbaren Finanzmittel zuweisen. Lesen Sie dazu unseren Artikel: Data Compliance Makes Third-Party Security a Must (in englischer Sprache verfügbar).

Governance

Mit NIS2 werden auch die Governance-Bestimmungen verschärft. Für Verstöße gegen die Richtlinie sollen nicht nur das betroffene Unternehmen als juristische Person, sondern auch Mitglieder der Leitungsorgane haftbar gemacht werden können.

Die Geschäftsleitung muss deshalb alle Maßnahmen prüfen und gutheißen, die das Unternehmen zum Schutz gegen Cyber-Risiken trifft, und deren Umsetzung und Pflege überwachen. Das gilt beispielsweise auch für die Backup-Strategie des Unternehmens – doch worauf kommt es dabei an? Lesen Sie dazu unseren Blogbeitrag zur 3-2-1-Backup-Regel (in englischer Sprache verfügbar).

Um zu gewährleisten, dass die Mitglieder der Geschäftsleitung über ausreichendes Know-how verfügen, müssen sie regelmäßig an spezifischen Schulungen teilnehmen. Diese sollen die nötigen Kenntnisse, Einblicke und Fähigkeiten vermitteln, um die Risiken und die Managementpraktiken im Bereich Cybersicherheit verstehen und bewerten zu können, ebenso wie deren Auswirkungen auf die Geschäftstätigkeit der Einrichtung.

Aufsicht, Durchsetzung und Sanktionen

Gemäß der NIS2-Richtlinie müssen die zuständigen Behörden der Mitgliedsstaaten die Einhaltung der Sicherheitsanforderungen und Meldepflichten, die die Richtlinie vorsieht, anhand konkreter Vorfälle überwachen. Die zuständigen Behörden sind auch befugt, bestimmte Anordnungen zu erlassen.

Welche Folgen drohen, wenn die Vorschriften nicht eingehalten werden?

Die zuständigen Behörden können unter anderem Verwarnungen aussprechen und Anordnungen erteilen. Zudem können sie Personen mit Führungsverantwortung (CEOs oder anderen hochrangigen Mitgliedern der Geschäftsleitung) die Ausübung von Leitungsaufgaben in der Einrichtung zeitweise untersagen oder verlangen, dass sie untersagt wird.

Auch sonst verschärft NIS2 das Sanktionsregime. Die zuständige Behörde in den Mitgliedstaaten muss nicht nur sicherstellen, dass Verstöße mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen geahndet werden – sie hat nun auch die konkrete Möglichkeit, Geldbußen zu verhängen, wenn die Einrichtung die Anforderungen an das Risikomanagement nicht erfüllt oder die Meldepflichten nicht einhält.

Mit folgenden Geldbußen ist – als Mindest-Höchstsatz – zu rechnen:

Wesentliche Einrichtungen:
bis zu 10 Mio. Euro oder 2 % des gesamten, weltweit erzielten Jahresumsatzes des Unternehmens

Wichtige Einrichtungen:
bis zu 7 Mio. Euro oder 1,4 % des gesamten, weltweit erzielten Jahresumsatzes des Unternehmens

Ab wann müssen Sie NIS2 umsetzen? Zeitplan und wichtige Daten

Die EU-Mitgliedstaaten haben nun 20 Monate Zeit, die neue Richtlinie in nationales Recht umzusetzen. Möchten Sie mehr über die wichtigen Termine und den Zeitplan rund um NIS2 erfahren? Dann besuchen Sie bitte https://www.nis-2-directive.com/.

Was sind die nächsten Schritte? Weiterführende Lektüre

Wir empfehlen, dass Sie sich und Ihr Unternehmen zunächst über die rechtlichen Anforderungen informieren und dann damit beginnen, bestehende Compliance-Lücken beim Risikomanagement und den Maßnahmen zur Minderung der Risiken zu ermitteln. Das Briefing des EU-Parlaments zu der neuen Richtlinie finden Sie hier.

Für alle, die sich eingehender mit dem Thema befassen möchten, hat das EU-Parlament den vollständigen Text des Vorschlags zur NIS2-Richtlinie im PDF-Format bereitgestellt.

Über Keepit

Keepit ist die weltweit einzige unabhängige, anbieterneutrale Cloud für den Schutz von SaaS-Daten. Tausende von Unternehmen weltweit vertrauen auf Keepit, um ihre Cloud-Daten zu schützen und zu verwalten.

Führende Analysten sind sich einig: Keepit ist die schnellste und sicherste SaaS-Lösung für Backups und Wiederherstellung in Unternehmen.

Keepit – dedizierter SaaS-Datenschutz, auf den die Kunden bauen.
Besuchen Sie keepit.com.

Gartner peerinsights ★★★★★
TrustRadius ★★★★½
Capterra ★★★★½
G2 ★★★★★