BDJ

VERSICHERUNGSMAKLER

NIS 2-RICHTLINIE VERSCHÄRFT – BESTEHT AUCH FÜR SIE HANDLUNGSBEDARF?

10 RELEVANTE FAKTEN FÜR IHR UNTERNEHMEN

Die Cyberkriminalität ist international wie national anhaltend hoch und gilt als eines der größten Geschäftsrisiken. Das bestätigt die sehr beträchtliche Anzahl (9 von 10 Betrieben) betroffener Unternehmen. Aus diesem Grund hat die EU mit der Richtlinie NIS 2 die Anforderungen an die IT-Sicherheit ebenso verschärft wie die persönliche Haftung des Managements. Für die Umsetzung bleibt nicht mehr viel Zeit.

INHALT DER NIS-RICHTLINIE

Die ursprüngliche NIS-Richtlinie mit dem Hauptziel, Europas Widerstandsfähigkeit gegen Cyberkriminalität zu stärken und die Reaktionsfähigkeit zu verbessern, wurde bereits 2016 verabschiedet und musste bis Mai 2018 von allen EU-Mitgliedstaaten in nationales Recht umgesetzt werden. Die NIS 2-Richtlinie wurde Ende 2022 erstmals veröffentlicht und ist im Januar 2023 in Kraft getreten. Sie ist noch nicht in deutsches Recht umgesetzt, und bei diversen Punkten gibt es Diskussionsbedarf. Bis zum 17.10.2024 muss die Richtlinie allerdings ratifiziert sein, so dass die betroffenen Unternehmen ab 18. Oktober zur Anwendung verpflichtet sein werden.

›››

FÜR WEN BESTEHT HANDLUNGSBEDARF?

Genau in dieser Frage liegt eines der Hauptprobleme, denn durch die Verschärfung der Richtlinie hat sich die Bandbreite und Anzahl der betroffenen Unternehmen immens erhöht. NIS1 wandte sich zunächst an Betreiber kritischer Infrastrukturen (KRITIS), z. B. Unternehmen der Energieversorgung, Gesundheit und Transport. Schätzungen zufolge müssen durch diese Ausweitung nun rund 30.000 zusätzliche Betriebe in Deutschland den Anforderungen entsprechen, für die ursprünglich kein Handlungsbedarf bestand. Dazu zählen beispielsweise Zulieferer in diversen Branchen. Hinzu kommt eine deutliche Herabsetzung der Mitarbeiterzahl und des Jahresumsatzes der betroffenen Unternehmen.

In vielen Fällen bedarf es einer fachgerechten Prüfung, um festzustellen, inwieweit der eigene Betrieb dazuzählt, denn nicht immer ist diese Einschätzung eindeutig. So können beispielsweise Hersteller von Nischenprodukten in einem der nun relevanten Sektoren inbegriffen sein, wenn der Umsatz die neue Grenze von 10 Millionen Euro übersteigt.

Es besteht jetzt Handlungsbedarf! Prüfen Sie, ob Ihr Unternehmen betroffen ist, um im Bedarfsfall rechtzeitig die geforderten Maßnahmen bis zum Oktober dieses Jahres in Gang zu setzen.

WELCHE MASSNAHMEN MÜSSEN ERGRIFFEN WERDEN

Unternehmen, die von NIS 2 betroffen sind, müssen umfangreiche Schutzvorgaben erfüllen. Dazu zählen in erster Linie folgende Maßnahmen:

KONZEPTE DER RISIKOBEWERTUNG, RISIKOANALYSE UND INFORMATIONSSICHERHEIT

- Konzepte für Risikoanalyse und Sicherheit für Informationssysteme
- Erkennung, Analyse, Eindämmung und Reaktion auf Vorfälle (z. B. DER, XDR, SIEM, SOC)
- Backup-Management und Wiederherstellung, Krisenmanagement (z. B. BCM, Notfallplan, 3-2-1 Backup Strategie)
- Sicherheit in der Lieferkette (z. B. Absicherung der Fern- / Fremdzugriffe)
- Sicherheit bei Erwerb, Entwicklung und Wartung der IT-Systeme
- Bewertung der Wirksamkeit der Risikomanagementmaßnahmen
- Cyberhygiene (z. B. Updates) und Schulungen Tests und Phishing-Simulationen in der Cyber Security
- Einsatz von Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Asset Management
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung
- Sichere Sprach-, Video- und Text-Kommunikation, ggf. auch im Notfall

Gerade für kleinere und mittlere Betriebsgrößen kann dieses Maßnahmenpaket problematisch sein. Wer inhouse nicht über die entsprechende IT-Expertise verfügt, muss personell gezielt aufstocken beziehungsweise externe Dienstleister in Anspruch nehmen, um die geforderten Maßnahmen in der vorgegebenen Zeit erfüllen zu können.

Wichtig: Künftig muss ein Cyber-Schaden der betroffenen Unternehmen direkt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden, innerhalb von 24 Stunden mit einem vorläufigen Bericht, innerhalb von 72 Stunden mit einem vollständigen Bericht samt einer Bewertung und spätestens nach einem Monat mit einem ausführlichen Abschlussbericht – so der aktuelle Stand.

CYBERSICHERHEIT WIRD KÜNFTIG ZUR CHEFSACHE

Geschäftsführer, Vorstände und Aufsichtsräte haften schon jetzt mit ihrem Privatvermögen im Falle von vorsätzlichen oder fahrlässigen Pflichtverletzungen. Diese Haftung wird im aktuellen Gesetzesentwurf nun deutlich präzisiert: Die Geschäftsleiter sind verpflichtet, die geforderten Maßnahmen zu billigen und zu überwachen. Außerdem müssen sie regelmäßig an Schulungen persönlich teilnehmen und eine Teilnahme auch weiteren Mitarbeitern anbieten.

›››

Die Haftung nach NIS 2 bezieht sich auf alle „Leitungsorgane“, wobei noch unklar ist, wer hierunter zu subsumieren ist

Neu ist: Ein Verzicht der Einrichtung auf Ersatzansprüche aufgrund einer Verletzung der Pflichten oder ein Vergleich zwischen Unternehmen und Leistungsorgan über diese Ansprüche ist unwirksam.

HOHE GELDBUSSEN DROHEN

Bei Verstößen drohen hohe Geldbußen bis zu zwei Prozent des weltweiten Umsatzes bzw. bis zu einer Höhe von sieben Millionen Euro für „wesentliche Einrichtungen“ und bis 1,4 Prozent des weltweiten Umsatzes bzw. bis zu einer Höhe von zehn Millionen Euro für „wichtige Einrichtungen“.

UMSETZUNG IN EIGENEM INTERESSE

Auch wenn es einen hohen Aufwand bedeutet, sollte die Umsetzung der Richtlinie im Interesse aller beteiligten Seiten liegen. Nur eine stark ausgeprägte und solide Cyberabwehr sowie effiziente Handlungsvorgaben können langfristig und dauerhaft vor großen wirtschaftlichen Schäden schützen.

WARUM DIE CYBERVERSICHERUNG NUN UMSO WICHTIGER IST

Natürlich geht es bei der Absicherung durch eine Cyberversicherung um die Deckung des verursachten Schadens, der oft erst später in seiner vollen Größe sichtbar wird. Dennoch bietet die Cyberversicherung – gerade in Hinsicht auf die verschärften NIS 2-Anforderungen – noch deutlich mehr Unterstützung und Sicherheit, denn die IT-Forensik ist darin inbegriffen.

So stehen Ihnen bei einem entsprechenden Abschluss ab dem Moment des Schadeneintritts umfassende Assistance-Dienstleistungen für die Handlungsfähigkeit im Notfall zur Verfügung. Über eine 24/7-Hotline erhalten Sie Zugriff auf ein Netzwerk von IT-Experten, die Ihnen auch bei der Umsetzung genau dieser nun so elementaren Anforderungen zur Seite stehen.

Bereits der Fragebogen, der im Rahmen des Abschlusses einer Cyberversicherung auszufüllen ist, kann unter Umständen verdeutlichen, wie viele Punkte Sie bereits erfüllen oder wo Sie im Rahmen der künftigen Anforderungen möglicherweise noch aktiv werden sollten.

DIE WICHTIGSTEN NEUEN PUNKTE IN DER ÜBERSICHT

- Umsetzung bis zum 17.10.2024
- betrifft: Unternehmen ab 50 Mitarbeitern oder 10 Millionen EUR Jahresumsatz und bestimmter Sektortätigkeit (insgesamt nun 18 Sektoren, davon dann elf „wesentliche“ und 7 „wichtige“, s. Übersicht weiter unten)

ALS „WESENTLICHE UNTERNEHMEN“ GELTEN:

- Energie (auch Lieferkette betroffen wie Verkauf, Betreiber, Verteiler, Zulieferer)
- Luft-, Schienen, Straßen- und Schiffsverkehr
- Bankwesen / Gesundheitswesen / Digitale Infrastruktur

ALS „WICHTIGE UNTERNEHMEN“ GELTEN:

- Hersteller aus den Bereichen Medizin, Computer, Elektronik, Maschinen, Transportmittel etc.
- Abfallwirtschaft / Chemische Erzeugnisse / Lebensmittel etc.

VERPFLICHTEND SIND FOLGENDE MASSNAHMEN IM BEREICH DES RISIKOMANAGEMENTS:

- Ergreifung von technischen und organisatorischen Maßnahmen (TOM) auf dem aktuellen Stand der Technik zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme etc.
- Grundlegende und ausreichende Schulungen im Bereich der Cybersicherheit für verantwortliche Geschäftsleiter
- Konzepte in Hinsicht auf Risikoanalyse und Sicherheit für Informationssysteme

›››

- Bewältigung von Sicherheitsvorfällen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung

WEITERE PFLICHTEN FÜR BETROFFENE UNTERNEHMEN UND EINRICHTUNGEN:

- Meldepflicht ans BSI
  - Erste Meldung 24 Std. nach Entdeckung
  - Erste Bewertung 72 Std. nach Entdeckung
  - Abschlussbericht innerhalb eines Monats nach Entdeckung (Cyberversicherungen bieten entsprechende Sachverständige)
- Registrierungspflicht (muss spätestens bis 18.10. erfolgt sein)
- Mögliche zusätzliche Nachweispflicht für besonders wichtige Einrichtungen wie ein regelmäßiger Nachweis bzgl. der Einhaltung bestehender IT-Standards

PFLICHTEN FÜR DIE VERANTWORTLICHEN GESCHÄFTSLEITER:

- Billigung bzw. Überwachung der zur Einhaltung der Richtlinie ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- Teilnahme an regelmäßigen Schulungen zum Erwerb ausreichender Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die Dienste des jeweiligen Unternehmens

DIE GENANNTEN 18 SEKTOREN IN DER GESAMTÜBERSICHT:

SEKTOREN MIT HOHER KRITIKALITÄT:

- Energie
- Verkehr
- Bankwesen
- Finanzmarkt-infrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)
- Öffentliche Verwaltung
- Weltraum

SONSTIGE KRITISCHE SEKTOREN:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe / Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

WAS BDJ FÜR SIE TUN KANN

Prüfen Sie zunächst, ob Sie zu den Unternehmen gehören, die die NIS 2-Richtlinie umsetzen müssen. Gerne stehen wir Ihnen dazu in folgenden Bereichen zur Seite:

Sie wollen eine Cyber-Versicherung abschließen oder wissen, inwieweit Ihre bestehende Versicherung im Hinblick auf die NIS 2 Anforderungen unterstützt?

Für die Managerhaftung schließen Unternehmen regelmäßig eine D&O Versicherung ab. Diese kann durch eine persönliche D&O Versicherung ergänzt werden, die der Manager selbst vereinbart.

Gern beraten wir Sie individuell und persönlich!