Bitdefender

WHITEPAPER

NIS 2: Unternehmen müssen handeln

NIS 2: Unternehmen müssen handeln

Im Herbst 2024 tritt NIS 2 in Kraft. Viele Unternehmen glauben, die EU-Richtlinie betreffe sie nicht, doch das kann ein gefährlicher Irrtum sein.

NIS 2? Das geht uns nichts an! So lautet bei vielen Firmen die Standardantwort, wenn sie auf die neue Richtlinie zur Netzwerk-Informationssicherheit (NIS-Richtlinie) der Europäischen Union angesprochen werden. Tatsächlich geht es sie in vielen Fällen doch etwas an. Warum, das erklärt dieser Artikel. Am Anfang soll jedoch zunächst einmal die Frage stehen, was NIS 2 ist und worum es bei der Richtlinie genau geht.

NIS 2 löst die erste NIS-Richtlinie der Europäischen Union ab. Ein Datum dafür steht bereits fest: der 18. Oktober 2024. An diesem Tag muss die neue Richtlinie in nationales Recht umgesetzt sein, wodurch sie dann auch für deutsche Unternehmen relevant ist. Seit Juli 2023 existiert mit dem NIS-2-Umsetzungs-und-Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) ein Referentenentwurf für das deutsche Gesetzespaket für die Umsetzung von NIS 2.

Wichtig ist: Unternehmen müssen jetzt handeln! Wer auch bisher schon der Cybersicherheit viel Aufmerksamkeit geschenkt und entsprechende Maßnahmen getroffen hat, muss eventuell gar nicht viel ändern oder zusätzliche Maßnahmen ergreifen. Alle anderen betroffenen Firmen stehen bei der rechtzeitigen Umsetzung der NIS-2-Richtlinie unter großem Zeitdruck.

Die Gründe für NIS 2

Die Abkürzung NIS steht für Network and Information Security. Die Richtlinie definiert eine Reihe von Maßnahmen, die in der gesamten EU ein gleichmäßig hohes Niveau bei der Cybersicherheit sicherstellen sollen. Hintergrund der Aktualisierung der bestehenden NIS-Richtlinie aus dem Jahr 2016 waren unter anderem die Erfahrungen während der Covid-19-Pandemie. In dieser Zeit zeigte sich, wie abhängig die EU-Länder mittlerweile von digitaler Technik sind und was es für die Gesellschaft bedeutet, wenn die damit verbundenen Abläufe aufgrund von unvorhergesehenen Ereignissen gestört werden.

Die EU hat dabei vor allem den gemeinsamen Binnenmarkt im Blick. Analysen hatten ergeben, dass viele in der EU tätige Unternehmen nur unzureichend gegen Cyberrisiken geschützt sind. Außerdem zeigte sich eine unterschiedliche Widerstandsfähigkeit zwischen den einzelnen Mitgliedsstaaten und auch zwischen den verschiedenen Sektoren der Wirtschaft. Es fehle zudem an einem gemeinsamen Verständnis für die wichtigsten aktuellen Bedrohungen und Herausforderungen, so die EU. Außerdem gebe es keine gemeinsame Krisenreaktion der EU-Länder, hieß es. All das gefährde eine robuste Funktion des gemeinsamen europäischen Marktes auch in Krisenzeiten.

Die NIS-2-Richtlinie definiert nun ein ganzes Bündel an Maßnahmen, die die EU weniger anfällig für Bedrohungen der Cybersicherheit machen sollen. Sie umfasst unter anderem Strategien für die nationale Cybersicherheit der einzelnen EU-Länder, sieht die Benennung von speziellen Behörden für das Cyberkrisenmanagement und die Cybersicherheit vor und verlangt außerdem die Bildung von nationalen Computer-Notfallteams (CSIRT, Computer Security Incident Response Team). Unternehmen wiederum müssen neue Regelungen zum Umgang mit Cyberzwischenfällen und zur Geschäftskontinuität beachten.

Für welche Firmen NIS 2 gilt

Die bisherige NIS-Richtlinie betraf in erster Linie Großunternehmen. Mit NIS 2 ändert sich das, die EU hat den Gültigkeitsbereich deutlich ausgeweitet. Die neue Richtlinie erfasst wesentlich größere Bereiche der Wirtschaft. Fachleute rechnen damit, dass in Deutschland rund 30.000 Unternehmen von der Richtlinie betroffen sein werden, rund 10.000 mehr als bisher.

Wer genau zählt nun zu dieser Gruppe? Über die Zugehörigkeit entscheiden zwei Faktoren: Der wirtschaftliche Sektor oder die Gruppe von Einrichtungen, zu denen eine Firma gehört, sowie die Unternehmensgröße. Letztere wird durch die Zahl der Mitarbeiter und die Bilanzsumme bestimmt.

Die EU teilt die von NIS 2 betroffenen Unternehmen in zwei Kategorien ein: Die eine Gruppe bezeichnet sie als „essential“ („besonders wichtig“). Sie ist weitgehend identisch mit den Unternehmen, die in Deutschland zur kritischen Infrastruktur (KRITIS) zählen. Allerdings führt NIS 2 nun eine Unterteilung dieser Gruppe in elf Klassen ein. Die zweite Gruppe, die im Vergleich mit NIS 1 jetzt neu hinzukommt, heißt bei der EU „important“ („wichtig“).

Für beide Gruppen gelten im Rahmen von NIS 2 die gleichen Regelungen. Nur bei den Strafen oder Sanktionen für etwaige Verstöße gibt es Unterschiede.

Eine besonders wichtige Rolle für die EU spielen Unternehmen, die in diesen Sektoren tätig sind:

- Energie (Strom, Gas, Öl, Heizung, Wasserstoff, Ladestationen für E-Fahrzeuge)
- Wasser (Trinkwasser- und Abwasserversorgung)
- Transport (Straßen-, Schienen-, Luft- und Schiffsverkehr)
- Bank- und Finanzwesen
- Gesundheitswesen (Gesundheitsdienstleister, Pharmazeutika, Hersteller medizinischer Geräte, Forschungseinrichtungen)
- Digitale Infrastruktur und IT-Dienste (Rechenzentren, Clouddienste, elektronische Kommunikationsdienste, Internetknoten)
- Öffentliche Verwaltung
- Raumfahrt

Hinzu kommen Unternehmen in diesen wichtigen Sektoren:

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemische Erzeugnisse (Produktion und Vertrieb)
- Lebensmittel (Produktion und Vertrieb)
- Industrie/Herstellung (Medizin- und Diagnosegeräte, Computer, Elektronik, Optik, Maschinen, Kraftfahrzeuge, sonstige Transportmittel)
- Digitale Anbieter (Online-Marktplätze, Suchmaschinen, soziale Plattformen)
- Forschungseinrichtungen

Damit ein Unternehmen zu einer der beiden Gruppen zählt, muss es eine Mindestgröße aufweisen. Sie wird nach Umsatz, Bilanzsumme und Mitarbeiteranzahl bestimmt. Die EU unterscheidet dabei zwischen mittleren und großen Unternehmen. Großunternehmen zählen zu den besonders wichtigen Firmen und zeichnen sich durch mindestens 250 Mitarbeiter, einen Umsatz von mindestens 250 Millionen Euro oder eine Gesamtbilanzsumme von mindestens 43 Millionen Euro aus. Mittlere Betriebe hingegen können sowohl zu den wichtigen als auch zu den besonders wichtigen Unternehmen gehören. Sie beschäftigen mindestens 50 Mitarbeiter, machen einen Umsatz von mehr als zehn Millionen Euro oder können auf eine Bilanzsumme von mehr als zehn Millionen verweisen.

Aber Achtung: Die Regelungen von NIS 2 können in bestimmten Fällen auch kleinere Firmen betreffen. Das gilt beispielsweise dann, wenn sie in einem der genannten Bereiche als Zulieferer oder Dienstleister arbeiten. Aber auch Unternehmen, die als einziger Anbieter in einem Mitgliedsstaat der EU tätig sind oder bei denen ein Ausfall erhebliche Konsequenzen für die Wirtschaft und die öffentliche Versorgung hätte, müssen die NIS-2-Regelungen grundsätzlich umsetzen. Last, but not least fallen auch Einrichtungen der öffentlichen Verwaltung sowie Anbieter von DNS-Diensten, TLD-Namensregistern und Betreiber öffentlicher elektronischer Kommunikationsnetze und -dienste unter die NIS-2-Richtlinie.

Aus diesen Gründen sollten generell alle Unternehmen prüfen, ob und wo es in ihrer Supply Chain Abhängigkeiten von NIS-2-pflichtigen Firmen gibt.

Was NIS 2 für die betroffenen Unternehmen bedeutet

Die NIS-2-Richtlinie verlangt, dass die Betriebe eigenständig prüfen, ob sie in die Gruppe der besonders wichtigen oder der wichtigen Firmen fallen. Weder das BSI (Bundesamt für Sicherheit in der Informationstechnik) noch eine andere Behörde nimmt eine solche Einteilung vor. Stellt ein Unternehmen fest, dass es zu einer der beiden Gruppen zählt, muss es sich innerhalb von drei Monaten beim BSI melden. Unternehmen, die in mehreren EU-Mitgliedsstaaten tätig sind, müssen sich in jedem dieser Staaten bei der zuständigen Behörde registrieren lassen.

Die weiteren Pflichten umfassen:

- Eine sofortige Meldung von Sicherheitsvorfällen. Registriert eine Firma einen Cybersicherheitsvorfall, muss sie eine Meldung an die zuständige Behörde in dem EU-Staat machen, in dem sie registriert ist. Laut der NIS-2-Richtlinie muss die zuständige Behörde (in Deutschland das BSI) innerhalb von 24 Stunden informiert werden. Insbesondere für viele kleinere und mittlere Firmen dürfte diese Anforderung mit ihren knappen Zeitlimits eine große Herausforderung darstellen.

- Teilnahme am Informationsaustausch: Unternehmen, die als besonders wichtige Einrichtungen gelten, müssen aktiv am Informationsaustausch mit dem BSI teilnehmen. Diese Maßnahme soll eine effektive Kommunikation bei Sicherheitsvorfällen garantieren.

- Einhaltung der Sicherheitsanforderungen: NIS 2 verlangt von den Unternehmen zudem die Umsetzung neuer, strenger Sicherheitsanforderungen gemäß der Richtlinie. Dazu zählen unter anderem die Einführung von Sicherheitsmaßnahmen und -verfahren zum Schutz der Netzwerk- und Informationssysteme.

Die Regelungen für die praktische Umsetzung der NIS-2-Richtlinien sind sehr allgemein gehalten. Welche Pflichten auf die betroffenen Unternehmen genau zukommen, bestimmt in Deutschland das NIS-2-Umsetzungsgesetz (NIS2UmsuCG). Seit dem 7. Mai 2024 existiert ein Referentenentwurf zu diesem Gesetz, der bis zum 1. Oktober 2024 das Gesetzgebungsverfahren auf Bundesebene durchlaufen soll. Anschließend soll das BSI die Vorgaben der NIS-2-Richtlinie und damit des Umsetzungsgesetzes in Deutschland durchsetzen und bei Verstößen die im Gesetz definierten Maßnahmen ergreifen.

Da das Gesetz noch nicht endgültig formuliert und verabschiedet ist, bleibt im Moment lediglich der Rückgriff auf die Vorgaben der NIS-2-Richtlinie. Sie umfassen folgende Sicherheitsregelungen:

- NIS 2 verlangt von den Unternehmen ein Cybersicherheits-Risikomanagement. Es soll die Umsetzung von Risikoanalyse- und Sicherheitskonzepten regeln, ein Vorfallmanagement umfassen sowie die Sicherheit in den Lieferketten gewährleisten. Auf diese Weise sollen Unternehmen und Behörden Risiken frühzeitig erkennen, geeignete Sicherheitsvorkehrungen treffen und schnell auf Sicherheitsvorfälle reagieren können.

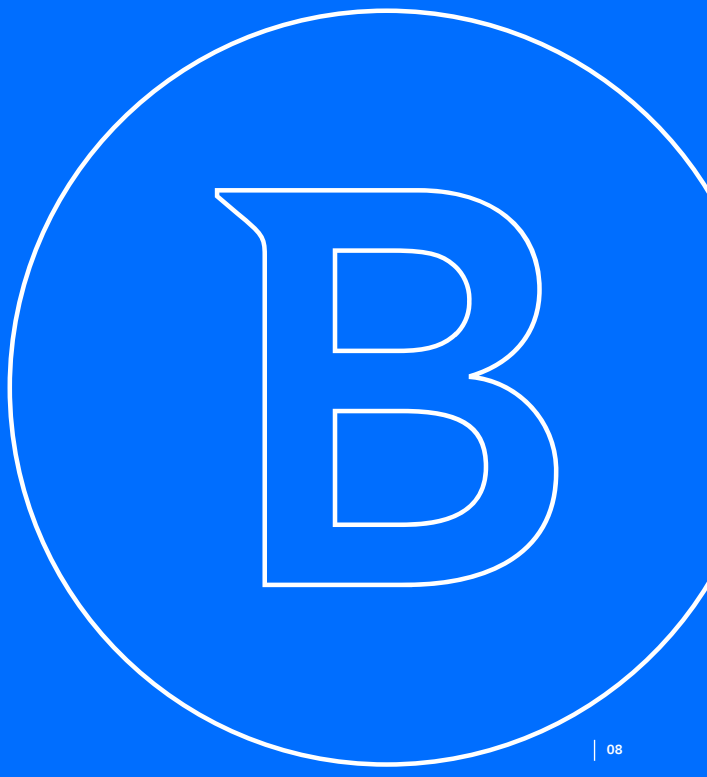
- Außerdem müssen die Unternehmen technische und organisatorische Maßnahmen (TOM) treffen, um die Cybersicherheit zu gewährleisten. Laut der NIS-2-Richtlinie müssen sie stets dem aktuellen Stand der Technik angepasst werden.

- Auf den Punkt Meldepflichten sind wir in diesem Artikel bereits eingegangen. Gravierende Sicherheitsvorfälle müssen innerhalb von 24 Stunden nach ihrer Entdeckung gemeldet werden. Innerhalb von 72 Stunden nach der Meldung muss gegebenenfalls eine Aktualisierung und erste Bewertung erfolgen. Spätestens einen Monat nach Bekanntwerden des Vorfalls muss dem BSI ein abschließender Bericht vorliegen.

Stellt sich nach einem Cybersicherheitsvorfall heraus, dass ein Unternehmen die Richtlinien von NIS 2 nicht eingehalten hat, drohen hohe Strafen. Auf besonders wichtige Unternehmen können Bußgelder von bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes zukommen – je nachdem, welcher Wert höher ist. Wichtige Unternehmen zahlen bis zu sieben Millionen Euro oder 1,4 Prozent des Jahresumsatzes. Um die große Bedeutung der Richtlinie zu unterstreichen, hat die EU NIS 2 zur Chefsache erklärt. Für eventuelle Strafzahlungen haftet deshalb der Geschäftsführer mit seinem Privatvermögen.

Doch Vorsicht:

Gerade diese Regelung kann auch negative Auswirkungen haben. Denn die Geschäftsführung gerät damit in Versuchung, lediglich auf die Compliance mit den NIS-2-Richtlinien zu achten, dafür jedoch die effektive Sicherheit des Unternehmens zu vernachlässigen. Hilfreich in solchen Fällen ist der Blick von außen beispielsweise durch ein Beratungsunternehmen. Auf diese Weise lässt sich sicherstellen, dass bei der Umsetzung von NIS 2 die Balance zwischen Compliance und Security gewahrt bleibt.



Technische Lösungen für die Anforderungen der NIS-2-Richtlinie

Zu den wesentlichen Punkten bei NIS 2 gehören die schnelle Erkennung von Cybersicherheitsvorfällen, das Vorfall-Management und die sofortige Meldung an die Behörden. Für diese Anforderungen setzen Unternehmen in der Regel SIEM-Systeme ein (SIEM: Security Information and Event Management). Diese Software sammelt mithilfe von verteilten Agenten die Daten aus den Netzwerk- und Sicherheitssystemen des Unternehmens ein, führt sie zusammen und bereitet sie übersichtlich auf, oft in Form von Diagrammen.

In der Praxis und speziell unter Berücksichtigung der Vorgaben der NIS-2-Regelungen haben diese Systeme jedoch zwei Nachteile:

- In der Hilfestellung des BSI zur Gefahrenerkennung spricht das Bundesamt von einer Protokollierung sicherheitsrelevanter Vorfälle. Ein Protokoll bedeutet jedoch immer, dass Daten über einen gewissen Zeitraum hinweg gesammelt und anschließend als Paket an den definierten Empfänger weitergegeben werden. Da die Agenten eines SIEM-Systems ihre Protokolle in der Regel nicht im exakt gleichen Moment, sondern über einen gewissen Zeitraum hinweg verteilt weiterleiten, treten vermutlich teilweise deutliche Verzögerung ein.

- Die Protokolle von IT-Systemen liegen in der Regel in Form von Logdateien vor. Abhängig von dem System, aus dem sie stammen, enthalten sie auch personenbezogene Daten. Für die Speicherung dieser Daten gelten in der EU die Vorschriften der Datenschutzgrundverordnung (DSGVO). Aus ihr lässt sich ableiten, dass beispielsweise Telekommunikationsunternehmen sämtliche Daten, die sie nicht zur Missbrauchsbekämpfung benötigen, unverzüglich löschen müssen. Das Sammeln und Protokollieren der Daten sämtlicher Systeme und Anwendungen, wie es in dem genannten BSI-Dokument beschrieben wird, muss daher unter datenschutzrechtlichen Aspekten höchst kritisch betrachtet werden.

Die beiden angeführten Argumente bedeuten nicht, dass sich SIEM-Systeme grundsätzlich nicht für die Erfüllung der NIS-2-Vorgaben eignen. Sie sind jedoch in vielen Fällen überdimensioniert und zu schwerfällig, um sicherheitsrelevante Vorfälle sofort unter Einhaltung der Datenschutzregelungen bewältigen zu können.

Zu diesen Lösungen zählt in vielen Konstellationen ein Security Operations Center (SOC), in dem ein Team von Sicherheitsspezialisten rund um die Uhr das Netzwerk und die allgemeine Sicherheitslage eines Unternehmens überwacht, analysiert und

bei der Erkennung von Sicherheitsvorfällen die Gegenmaßnahmen koordiniert. Dazu gehört selbstverständlich auch die von NIS 2 geforderte Meldung ans BSI. Unternehmen, denen die Ressourcen fehlen, um ein eigenes SOC aufzubauen, können auf Anbieter wie Bitdefender zurückgreifen, die einen MDR-Sicherheitsservice (MDR: Managed Detection and Response) anbieten. Über ihn erhalten die Firmen Zugriff auf ein weltweites Netzwerk von SOCs, die einen regionalen Support anbieten, um eingehende Sicherheitswarnungen zu analysieren und mit geeigneten Maßnahmen darauf zu reagieren.

Verfügbare Hilfestellungen für Unternehmen

Zahlreiche Security-Anbieter und Beratungsfirmen werben derzeit mit einer Hilfestellung für die Umsetzung der NIS-2-Richtlinie, wie jede Google-Suche bestätigt. Von offizieller Seite ist die „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ des BSI als kostenloser Download erhältlich. Die Autoren sprechen darin zwar die Betreiber kritischer Infrastrukturen (KRITIS) an, die Empfehlungen lassen sich jedoch auch auf andere Unternehmen übertragen, die unter die NIS-2-Richtlinie fallen.

Dieses Dokument enthält jedoch keine konkreten Handlungsanweisungen. Denn wie die Autoren bereits im Einleitungsteil betonen, geht es vielmehr darum, einen „qualitativen Rahmen“ zu definieren, „innerhalb dessen gleichwertige und individuelle Alternativen, unter Berücksichtigung ihrer Angemessenheit, möglich sind“.

Unternehmen sollten bei diesen Ratgebern immer berücksichtigen, dass sie sich an die Gesamtheit aller von NIS 2 betroffenen Betriebe wenden und nicht auf die speziellen Umstände in einer einzelnen Branche oder gar die Situation im eigenen Haus zugeschnitten sind.

Hinzu kommen die Herausforderungen bei der praktischen Umsetzung der Ratschläge, denn IT-Spezialisten zählen zu den stark gesuchten Fachkräften. Vielen Firmen fehlt deshalb schlicht und ergreifend das qualifizierte Personal, um die NIS-2-Regelungen so perfekt umzusetzen, wie es die Anleitungen fordern.

Fazit

Der Security-Anbieter Bitdefender hat zehn Empfehlungen für Unternehmen veröffentlicht, die sich auf die Einführung der NIS-2-Richtlinie vorbereiten möchten:

1. Überprüfen Sie, ob die NIS-2-Richtlinie für Ihre Organisation oder einen Ihrer direkten Geschäftspartner Gültigkeit besitzt.
2. Identifizieren Sie die kritische IT-Ausstattung in Ihrem Unternehmen.
3. Entwickeln Sie eine Risikomanagement-Strategie.
4. Setzen Sie passende Sicherheitsmaßnahmen um.
5. Setzen Sie Verfahren für das Vorfallmanagement (Incident Response Procedures) um.
6. Führen Sie regelmäßige Sicherheitstests durch.
7. Schulen Sie Ihre Belegschaft.
8. Berücksichtigen Sie auch die Risiken, die von anderen Parteien in der Lieferkette ausgehen.
9. Dokumentieren Sie sämtliche Maßnahmen und Vorfälle.
10. Erfüllen Sie die gesetzlichen Meldepflichten.

Der erste Schritt sollte auf jeden Fall die Überprüfung sein, ob das eigene Unternehmen zu den von NIS 2 betroffenen Betrieben zählt. Falls ja, dann empfiehlt sich das Arbeiten an einer Risikomanagement-Strategie, während parallel dazu die IT die für Cybersicherheitsvorfälle besonders exponierte Hardware und Software im Unternehmen identifiziert und Sicherheitsmaßnahmen dafür entwickelt. An dieser Stelle wie auch bei den folgenden Schritten sollten Unternehmen externe Berater hinzuziehen. Auch bei der Umsetzung von Sicherheitsmaßnahmen und eines Vorfallmanagements geben erfahrene Sicherheitsfirmen wie Bitdefender wertvolle Hilfestellungen.

NIS 2 stellt hohe Anforderungen an Unternehmen, darunter die Verpflichtung, selbst zu prüfen, ob sie zu den Betroffenen zählen, für die das neue Gesetz gilt. Wer hier eine falsche Entscheidung trifft und die Anforderungen von NIS 2 ignoriert, läuft Gefahr, bei einem Sicherheitsvorfall nicht nur den Schaden zu haben, sondern zusätzlich noch zu einer hohen Geldstrafe verurteilt zu werden. Leider sind die amtlichen Informationen und Hilfestellungen zur Umsetzung des Gesetzestextes oftmals unnötig kompliziert formuliert, sodass die Firmen häufig juristische Beratung benötigen.

Über Bitdefender

Bitdefender ist ein weltweit führender Anbieter von Cybersicherheitslösungen zur Abwehr, Erkennung und Reaktion auf Bedrohungen. Bitdefender schützt mehrere Millionen von Endverbrauchern sowie IT-Umgebungen in Unternehmen und im öffentlichen Sektor. Die Lösungen sind in hohem Maße anerkannt als Mittel, Bedrohungen zu beseitigen, die Privatsphäre, digitale Identitäten und Informationen zu schützen sowie die Resilienz der IT gegenüber Cyberbedrohungen zu stärken. Dank umfangreicher Investitionen in Forschung und Entwicklung entdecken die Bitdefender Labs minütlich Hunderte neuer Bedrohungen und validieren täglich Milliarden von Bedrohungsanfragen. Das Unternehmen hat in seiner Geschichte bedeutende Innovationen in den Bereichen Anti-Malware, IoT-Sicherheit, Verhaltensanalyse und künstliche Intelligenz entwickelt. Seine Technologie wird von mehr als 180 der weltweit bekanntesten Technologiemarken lizenziert. Bitdefender wurde 2001 gegründet und hat Kunden in über 170 Ländern mit Niederlassungen auf der ganzen Welt. Weitere Informationen finden Sie unter www.bitdefender.de.

Trusted. Always.

Kontaktieren Sie uns:

sales-dach@bitdefender.com