GPP-Blickpunkt

NIS-2 im Fokus: Neue Herausforderungen und Chancen für die Cybersicherheit in Unternehmen und Behörden.

1. Wer ist betroffen?

Ist Ihr Unternehmen auf die neuen Anforderungen vorbereitet? Die NIS-2-Richtlinie betrifft nicht nur große Konzerne, sondern auch kleinere Unternehmen mit mindestens 50 Mitarbeitenden oder einem Umsatz von über 10 Millionen Euro. Diese Unternehmen müssen jetzt handeln!

> *Es ist wichtig, dass Unternehmen jetzt handeln, um potenzielle Sanktionen zu vermeiden!*

Andrej Ditler
IT-Prüfer bei GPP

Die NIS-2-Richtlinie bringt eine erhebliche Erweiterung des Anwendungsbereichs im Vergleich zur bisherigen Regelung mit sich. Neben den bereits bekannten Betreibern kritischer Infrastrukturen (KRITIS) fallen nun auch sogenannte besonders wichtige Einrichtungen (bwE) und wichtige Einrichtungen (wE) unter die neuen Vorgaben. Das betrifft beispielsweise Unternehmen aus den Bereichen Telekommunikation, Energie, Gesundheitsversorgung und Transport.

Sind Sie unsicher, ob Ihr Unternehmen von der NIS-2-Richtlinie betroffen ist? Mit unserer kurzen Betroffenheitsanalyse können Sie das hier schnell und einfach herausfinden.

Ein wesentlicher Unterschied zur bisherigen Regelung ist, dass die NIS-2-Richtlinie auch kleinere Unternehmen mit mindestens 50 Mitarbeitenden oder einem Jahresumsatz bzw. einer Bilanzsumme von über 10 Millionen Euro erfasst, sofern diese in beschriebenen relevanten Bereichen tätig

Sehr geehrte Mandantinnen,
sehr geehrte Mandanten,
sehr geehrte Fachinteressierte,

die Europäische Union (EU) hat mit dem Regelwerk für die Netzwerk- und Informationssicherheit in der zweiten Fassung (NIS-2) die Richtlinienkompetenz zum Schutz von kritischen Infrastrukturen auf einen größeren Kreis von Unternehmen, die von der Richtlinie betroffen sind, erweitert.

Ziel der Richtline ist es, den wachsenden schwerwiegenden Cyber-/Informationssicherheitsrisiken für Organisationen und Unternehmen umfassend zu begegnen.

Hierfür wurde mit der NIS-2 Richtline das Rahmenwerk um ein umfassendes Meldewesen ergänzt, sowie die Verantwortung der Einhaltung der zu ergreifenden Maßnahmen an die gesetzlichen Vertreter und die Geschäftsführung adressiert.

Als Wirtschaftsprüfungs- und Beratungsgesellschaft, die sich auf die Kommunalwirtschaft spezialisiert hat, möchten wir diese Gelegenheit nutzen, um Sie in diesem GPP Blickpunkt über die jetzt notwendigen Maßnahmen zu informieren.

Wir wünschen Ihnen eine aufschlussreiche Lektüre und hoffen Ihnen hiermit einen übersichtlichen Einstieg in das Thema zu verschaffen.

Bremen, 15.Oktober 2024

Bernd Tameling-Meyer
Wirtschaftsprüfer
Steuerberater

Carsten Hartung
IT-Auditor IDW

sind. Besonders für diese Unternehmen stellt die Richtlinie eine Herausforderung dar, da sie bislang möglicherweise nicht die gleiche Aufmerksamkeit auf ihre Cybersicherheitsmaßnahmen gelegt haben wie größere Organisationen.

Um Unternehmen und Behörden bei der Klärung ihrer Pflichten zu unterstützen, haben wir eine Betroffenheitsprüfung entwickelt. Mit dieser Prüfung können Sie für Ihr Unternehmen schnell und präzise ermitteln, ob Sie den Anforderungen der NIS-2-Richtlinie unterliegen. Unser Ziel ist es, den Betroffenen frühzeitig Klarheit zu verschaffen und Sie bei der Umsetzung der erforderlichen Cybersicherheitsmaßnahmen zu begleiten.

Es ist wichtig, dass Unternehmen jetzt handeln, um potenzielle Sanktionen zu vermeiden und die Sicherheit ihrer IT-Infrastrukturen zu gewährleisten.

2. Meldepflichten und Sanktionen

Wann müssen Sie im Fall eines Sicherheitsvorfalls die Behörde informieren? Mit NIS-2 werden die bisherigen Anforderungen der bestehenden Richtlinie verschärft.

> *Nach NIS-2 haften Geschäftsleitungen von wichtigen und besonders wichtigen Einrichtungen für die Umsetzung und Überwachung der Risikomanagementmaßnahmen.*
>
> **Thomas Lissowski**
> IT-Prüfer bei GPP

Im Meldewesen nach NIS-2 dreht sich alles um Sicherheitsvorfälle, welche Dienste schwerwiegend gestört, finanzielle Verluste verursacht oder Personen durch Schäden beeinträchtigt haben. Ebenfalls gilt dies, wenn diese Möglichkeiten noch eintreten könnten.

Für wichtige und besonders wichtige Einrichtungen gilt: Maximal 24 Stunden nach Kenntnisnahme eines Sicherheitsvorfalls muss eine Erstmeldung erfolgen. Diese soll unter anderem Ihre Einschätzung enthalten, ob der Vorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist.

Spätestens 72 Stunden nach Kenntnisnahme ist ein Update zur Erstmeldung abzugeben, um die Informationen aus der Erstmeldung zu bestätigen oder zu korrigieren, sowie eine erste Bewertung des Sicherheitsvorfalls abzugeben.

Dauert der Sicherheitsvorfall nicht mehr an, muss innerhalb eines Monats nach dem Update der Erstmeldung eine Abschlussmeldung über Schweregrad, Auswirkung, Beschreibung und Ursache des Vorfalls abgegeben werden. Ferner muss genannt werden, welche Maßnahmen bereits getroffen wurden oder noch anhalten. Dauert der Sicherheitsvorfall noch an, muss stattdessen eine Fortschrittsmeldung abgegeben werden. Die Abschlussmeldung muss in diesem Fall spätestens einen Monat nach abgeschlossener Bearbeitung des Sicherheitsvorfalls eingereicht werden.

Betreiber kritischer Anlagen (ehemals KRITIS-Betreiber) müssen bei Sicherheitsvorfällen prüfen, ob diese Auswirkungen auf ihre Anlagen haben oder haben könnten. In diesem Fall sind Meldungen über die Art der Anlage, die betroffene kritische Dienstleistung und deren Auswirkungen erforderlich.

Darüber hinaus können seitens der Behörden Zwischenmeldungen über relevante Statusaktualisierungen verlangt werden. Details zum Meldeverfahren und der geforderten Inhalte werden auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI) veröffentlicht.

Die möglichen Strafen für Verstöße gegen die NIS-2 sind gravierend: Unternehmen können mit Geldbußen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes belegt werden, wobei der höhere Betrag fällig wird. Ein Compliance-Verstoß könnte also erhebliche finanzielle Schäden und Imageverluste bedeuten.

Nach NIS-2 haften Geschäftsleitungen von wichtigen und besonders wichtigen Einrichtungen für die Umsetzung und Überwachung der Risikomanagementmaßnahmen für Cybersecurity nach § 30 des NIS-2-Umsetzungsgesetzes.

Sollte diese Pflicht verletzt werden, haftet die Geschäftsleitung persönlich für die verursachten Schäden gegenüber der Einrichtung.

3. Bausteine der NIS-2-Richtlinie

Die NIS-2-Richtlinie fordert von Organisationen eine klare Struktur im Bereich der Cybersicherheit.

Im Gegensatz zu bisherigen Vorgaben wird nun ein noch stärkerer Fokus auf die regelmäßige Überprüfung der IT-Sicherheitsmaßnahmen gelegt.

Dominik Giourtzakis
IT-Prüfer bei GPP

Die wichtigsten Bausteine der NIS-2-Richtlinie umfassen Maßnahmen zum Risikomanagement, zur Behandlung von Sicherheitsvorfällen und zur Sicherstellung der Business-kontinuität. Im Gegensatz zu bisherigen Vorgaben wird nun ein noch stärkerer Fokus auf die regelmäßige Überprüfung der IT-Sicherheitsmaßnahmen gelegt. Es müssen technische als auch organisatorische Maßnahmen dafür sorgen, dass die kritische IT und Dienstleistungen vor wesentlichen Störungen geschützt werden. Hierbei wird der Geltungsbereich im Vergleich zu früheren Regelungen deutlich erweitert.

Wichtige Aspekte der Richtlinie sind zudem der gezielte Einsatz von Verschlüsselung und sicheren Kommunikationskanälen sowie die Durchführung von Schulungen zur Informationssicherheit. Diese Maßnahmen helfen, sowohl interne als auch externe Sicherheitsrisiken zu minimieren.

Nach unserer Einschätzung sind Unternehmen gut beraten, ihre bestehenden Sicherheitsmaßnahmen kritisch zu überprüfen, um den gestiegenen Anforderungen der NIS-2-Richtlinie gerecht zu werden. Der neue risikobasierte Ansatz der Richtlinie erfordert, dass Unternehmen ihre Sicherheitsstrategien regelmäßig evaluieren und anpassen. Dies ist entscheidend, um Sanktionen zu vermeiden und eine robuste Sicherheitskultur zu etablieren.“

4. Wie kann ich mich schützen?

Die NIS-2-Richtlinie erfordert umfassende Sicherheitsmaßnahmen, von der Einführung eines ISMS über technische und organisatorische Vorkehrungen bis hin zur kontinuierlichen Überwachung und Optimierung.

Mit NIS-2 kommen viele neue Anforderungen auf Sie zu, doch wir sind uns sicher, dass Sie diese mit den richtigen Maßnahmen stemmen können!

Tizian Stemmer
IT-Prüfer bei GPP

Hierfür empfehlen wir Ihnen zunächst, mindestens zwei Personen innerhalb Ihres Unternehmens zu benennen, welche die Verantwortung für die Koordination der Informationssicherheit nach der Richtlinie übernehmen. Ebenfalls sollte eine erste Bestandsaufnahme Ihrer Informationssicherheit erfolgen. Für die Umsetzung der Sicherheitsstandards nach der NIS-2-Richtlinie ist die Einführung eines Informationssicherheitsmanagementsystems (ISMS) unerlässlich, um die bestehenden Standards zu verbessern. Dies umfasst regelmäßige Risikobewertungen zur Identifizierung potenzieller Bedrohungen.

Im nächsten Schritt sollten sowohl technische Maßnahmen, wie die Implementierung von Firewalls und Intrusion Detection Systemen als auch organisatorische Maßnahmen, wie Zugangskontrollen und Schulungen für Mitarbeiter, umgesetzt werden. Vergessen Sie nicht, auch Ihre IT-Lieferkette abzusichern, da Angriffe oft über Dritte erfolgen.

Ein weiterer wesentlicher Aspekt ist die Überwachung und das Incident Management. Implementieren Sie Systeme zur kontinuierlichen Überwachung und Protokollierung sicherheitsrelevanter Ereignisse. Zudem sollten Prozesse zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen entwickelt und getestet werden. Diese Maßnahmen müssen den aktuellen technischen Standards entsprechen und Konzepte zur Risikoanalyse, Sicherheitsvorfallbewältigung sowie zur Betriebskontinuität und Krisenmanagement umfassen.

Die interne und externe Kommunikation ist ebenfalls von großer Bedeutung. Stellen Sie sicher, dass alle Mitarbeiter über die Sicherheitsrichtlinien und -verfahren informiert sind und diese verstehen. Etablieren Sie zudem Kommunikationskanäle zu relevanten Behörden und Partnern, um im Falle eines Sicherheitsvorfalls schnell und effektiv reagieren zu können. Auch Stellvertretungsregelungen sollten eindeutig definiert und formalisiert werden.

Abschließend sind regelmäßige Überprüfungen und Verbesserungen der Sicherheitsmaßnahmen unerlässlich. Dies beinhaltet Sicherheitsaudits und Penetrationstests, um die Wirksamkeit der implementierten Maßnahmen zu überprüfen. Nutzen Sie die Ergebnisse dieser Überprüfungen, um die Sicherheitsvorkehrungen kontinuierlich zu optimieren. Die NIS-2-Richtline ist flexibel formuliert, sodass Unternehmen angemessene Maßnahmen entsprechend ihrer Risikolage und Infrastruktur ergreifen können. Diese werden anhand von Kriterien wie Gefährdungslage, Unternehmensgröße, Kosten und Auswirkungen definiert.

5. Wie geht es weiter?

Die NIS-2 Richtlinie wurde im Dezember 2022 von den Gremien der EU veröffentlicht und die Mitgliedstaaten der EU haben bis zum 17. Oktober 2024 Zeit, diese Richtlinie in nationales Recht umzusetzen. Das nationale Gesetzgebungsverfahren ist zum jetzigen Zeitpunkt noch nicht abgeschlossen, aktuell liegt der verabschiedete Referentenentwurf vom Juli 2024 vor.

Der Bundestag hat sich mit dem Antrag des Ausschusses für Inneres und Heimat am 09. Oktober 2024 zum Thema „Cyberresilienz stärken und kritische Infrastrukturen wirksam schützen – NIS-2 Richtlinie unverzüglich umsetzen“ beschäftigt. Es ergeben sich für betroffene Unternehmen unmittelbar folgende Handlungsnotwendigkeiten:

1. **Betroffenheitsüberprüfung**
   Führen Sie die oben genannte Betroffenheitsprüfung durch!
2. **IT Compliance Berichterstattung**
   Diskutieren Sie mit den Verantwortlichen die Ergebnisse der Betroffenheitsüberprüfung und starten Sie eine IT-Compliance-Berichterstattung zu wesentlichen IT-Prozessen, -Dienstleistungen und betroffenen Lieferketten.
3. **Security-Awareness-Programm**
   Entwickeln Sie eine Strategie zum Umgang mit einem IT-Sicherheitsvorfall. Schulen Sie Ihre MitarbeiterInnen im sicheren Umgang mit IT-Systemen.
4. **FIT-GAP-Analyse**
   Identifizieren Sie im Rahmen einer Lückenanalyse die kritischen Prozesse, die für die Bereitstellung Ihrer wesentlichen Dienste verantwortlich sind und stellen Sie fest, ob Ihre bisherigen angewandten Cyber-Sicherheitsmaßnahmen ausreichend und wirksam sind und die NIS-2 Anforderungen erfüllen.

Unternehmen und Organisation haben insgesamt mit Beginn der Maßnahmen bis zu 24 Monate Zeit die Richtlinien nach NIS-2 zu erfüllen. Der Beginn dieser Maßnahmen und der Projektplan müssen bei einer Überprüfung nachgewiesen werden. Gerne begleiten wir Sie im Rahmen von Informationsvermittlung und Beratungsdienstleistungen zu Ihrer IT-Compliance auf dem Weg zur Erfüllung Ihrer NIS-2 Anforderung.

Göken, Pollak, Partner Treuhandgesellschaft mbH

Schwachhauser Heerstraße 67
28211 Bremen
Tel. 0421 35048-200
bremen@gpp-treuhand.de

Beyerstraße 25
09113 Chemnitz
Tel. 0371 43100-0
chemnitz@gpp-treuhand.de

Lütticher Straße 132
40547 Düsseldorf
Tel 0211 5381993-0
duesseldorf@gpp-treuhand.de

Hansestraße 37
20144 Hamburg
Tel. 0421 35048-200
hamburg@gpp-treuhand.de

Alte Gärtnerei 1
55128 Mainz
Tel. 06131 231832
mainz@gpp-treuhand.de

Maxfeldstraße 9
90409 Nürnberg
Tel. 0911 217959-70
nuernberg@gpp-treuhand.de

Humboldtstraße 2
14467 Potsdam
Tel. 0331 743826-0
potsdam@gpp-treuhand.de

Keesburgstraße 36a
97074 Würzburg
Tel. 0931 99161-997
wuerzburg@gpp-treuhand.de