WHITEPAPER

NIS2

Der Weg zur neuen Cybersecurity Norm

rhöncloud

Inhaltsverzeichnis

NIS2 – das nächste Level der Cybersecurity

Die EU-Richtlinie NIS2 (The Network and Information Security Directive) ist eine EU-weite Regulierung für die Cyber- und Informationssicherheit. Sie enthält rechtliche Anforderungen zur IT-Sicherheit, um den aktuellen Mindestsicherheitsstandard auf eine neue Ebene zu bringen und bestehende Mängel zu beheben. Der enge Umsetzungszeitplan, die hohen Anforderungen und die strengen Aufsichts- und Sanktionierungsmaßnahmen setzen Unternehmen unter Druck. Bis zum **17. Oktober 2024** muss die Richtlinie in nationales Recht umgesetzt und Unternehmen bestimmter Definition, aktiv werden. Welche Unternehmen betroffen sind und welche Methoden zur KRITIS-Aktualisierung vorgeschrieben werden, führen wir in diesem Whitepaper auf.

NIS1 vs. NIS2: Was ist anders?

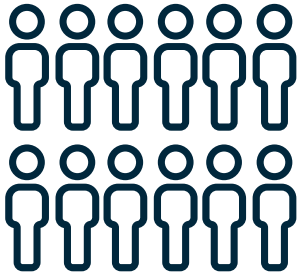
Bereits im Jahr 2016 wurde die NIS1-Richtlinie verabschiedet. Diese Richtlinie galt zumeist, neben vielen weiteren Cybersecurity-Vorgaben, für Einrichtungen und Unternehmen der kritischen Infrastruktur (KRITIS-Einrichtungen). In der neuen NIS2-Richtlinie wird der Anwendungsraum deutlich auf viele andere Bereiche ausgeweitet, sodass auch kleine und mittelständische Unternehmen von dieser einschlägigen Richtlinie betroffen sind und aufgrund der Verabschiedung der NIS2 erweiterbare Maßnahmen getroffen werden sollen.

Ziel ist es, das Cybersicherheitsniveau auf ein hohes Maß anzupassen und sicherzustellen.

Ist mein Unternehmen betroffen?

Ob Unternehmen von der NIS2-Richtlinie betroffen sind, hängt von dessen Tätigkeitsbereich sowie von der Unternehmensgröße ab. Dabei ist es wichtig, dass die NIS2-Richtlinie für deutlich mehr Bereiche relevant ist, als die erste NIS-Richtlinie. Unterschieden wird zwischen Sektoren mit hoher Kritikalität und sonstigen kritischen Sektoren. Zusätzlich zu dieser Unterscheidung gibt es die Kategorien wesentliche Einrichtungen und wichtige Einrichtungen.

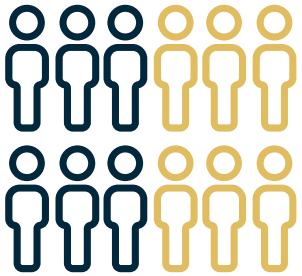
Die Durchsetzung von NIS2 ist abhängig von der Kategorie, in die eine Organisation eingestuft wird. Eine Organisation oder Institution kann als wesentlich **(Essential Entity)** oder als wichtig **(Important Entity)** klassifiziert werden. Die Abhängigkeit der Klassifizierung wird durch die Größe des Unternehmens bestimmt und ob es unter einen Sektor mit hoher Kritikalität oder in einen sonstigen kritischen Sektor fällt.



Große Unternehmen

mind. 250 Mitarbeiter

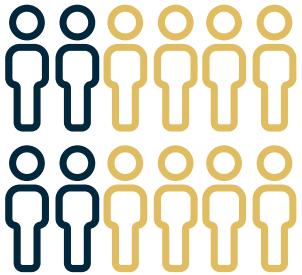
> 50 Mio. € Umsatz oder
> 43 Mio. € Bilanz



Mittlere Unternehmen

50 – 249 Mitarbeiter

max. 50 Mio. € Umsatz oder
10 – 43 Mio. € Bilanz



Kleine Unternehmen

< 50 Mitarbeiter

max. 10 Mio. € Umsatz oder
max. 10 Mio. € Bilanz

Separate Prüfung je nach Tätigkeitsfeld.

Bei kleinen Unternehmen ohne Einstufung entfällt die Anwendung der NIS2-Verordnung.

Direktive betroffene Sektoren

Je nach Unternehmenssektor und -größe lassen sich Unternehmen entsprechend in wesentliche und wichtige Einrichtungen definieren.

Wesentliche Einrichtungen[1]

(Essential Entities)
Sektoren mit hoher Kritikalität

+ Energie
+ Verkehr und Transport
+ Bankwesen
+ Finanzmarktinfrastrukturen
+ Gesundheitswesen
+ Trinkwasser
+ Abwasser
+ Digitale Infrastruktur
+ Verwaltung von ITK-Diensten
+ Öffentliche Verwaltung
+ Weltraum

Wichtige Einrichtungen[2]

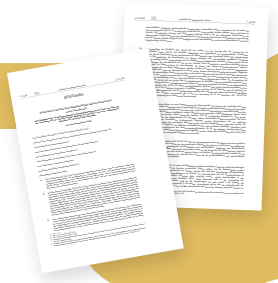
(Important Entities)
Sonstige kritische Sektoren

+ 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

Ausnahmen[3]

(Unterliegen der NIS2 unabhängig der Unternehmensgröße)

+ Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten
+ Vertrauensdiensteanbieter
+ Domain-Name-Systemanbieter oberster Stufe sowie Registrierungsstellen für Domains
+ Handelt es sich um einen einzigen Diensteanbieter, der für wichtige gesellschaftliche oder wirtschaftliche Aktivitäten unverzichtbar ist
+ Unternehmen, dessen Service gestört wird und es dadurch zu erheblichen Auswirkungen der öffentlichen Ordnung, der Sicherheit und Gesundheit kommen kann
+ Bei Unternehmen, dessen Störungen über die Landesgrenzen hinweg ein erhebliches Ausmaß annehmen würde
+ Die öffentliche Verwaltung



Download der Richtlinie NIS2

[1] Vgl. Richtlinie (EU), 2022/2555, Anhang I, S. 64 ff.
[2] Vgl. Richtlinie (EU), 2022/2555, Anhang II, S. 69 ff.
[3] Vgl. Richtlinie (EU), 2022/2555, Artikel 2, S. 29 ff.

Welche Pflichten erwarten Unternehmen und Kommunen?

Was müssen Unternehmen und Kommunen unternehmen, um NIS2-konform zu werden? Prinzipiell gibt die Europäische Union Unternehmen und Kommunen zwei große Pflichten auf. Erstens wird verlangt, dass Risikomanagementmaßnahmen getroffen werden, um die kritische Dienstleistung zu schützen. Zweitens wird verlangt, dass Sicherheitsvorfälle an die zuständigen staatlichen Einrichtungen gemeldet werden. Der Umfang und Aufwand richtet sich an die bereits umgesetzten Maßnahmen, welche im Unternehmen oder der Kommune umgesetzt wurden. Laut aktuellen Schätzungen müssen Unternehmen, welche in diesem Bereich noch keinerlei Vorkehrungen getroffen haben, 20 % mehr Budget für Schutz- und Vorbeugungsmaßnahmen bereitstellen. Die Unternehmen, welche bereits tätig geworden sind, müssen ungefähr 12 % mehr einplanen.

Risikomanagement[4]

Die NIS2 verpflichtet Unternehmen dazu, ihre IT-Landschaft einer regelmäßigen Evaluierung zu unterziehen, um Sicherheitslücken zu erkennen und entsprechende Maßnahmen zum Schutz und zur Prävention von potenziellen Cyberangriffen einsetzen zu können.
Zu diesen Maßnahmen gehören: Risikomanagement, Sicherheit der Lieferkette, verbesserte Netzsicherheit, bessere Zugangskontrolle und Verschlüsselung.

Geschäftskontinuität[5]

Die NIS2 setzt für den Fall eines größeren Cyberangriffs voraus, dass Unternehmen ihre Geschäftskontinuität sicherstellen. Dies sollte Maßnahmen über vollständige Backups bis hin zu Notfallverfahren und dem Einrichten eines Incident Response Teams beinhalten, um potenzielle Schäden zu minimieren.

Vorfallmanagement[6]

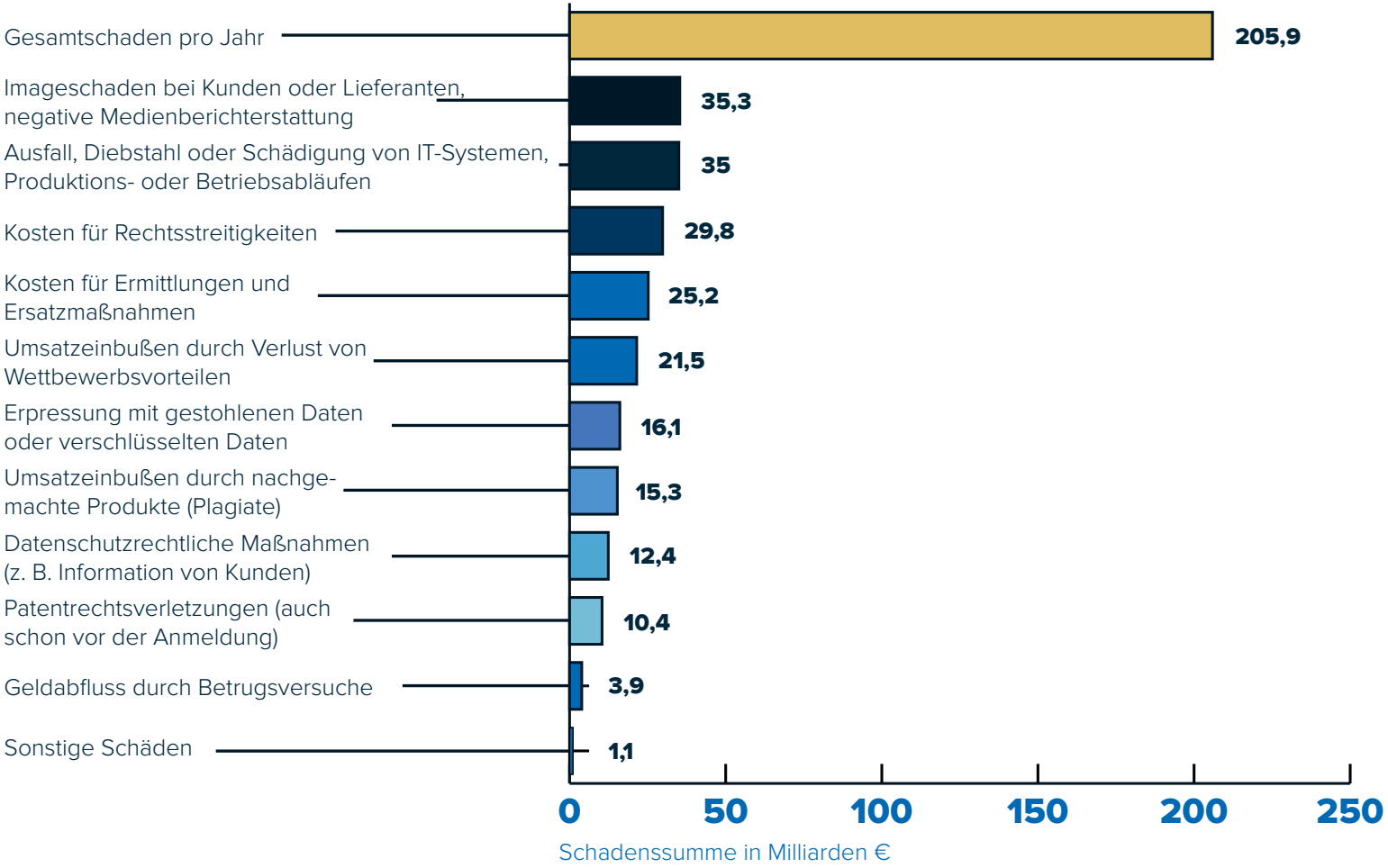
Die NIS2 fordert, dass Führungskräfte die Verantwortung zur Überwachung der Cybersicherheitsmaßnahmen ihres Unternehmens übernehmen und sich mit den NIS2-Richtlinien vertraut machen.
Bei Verstößen der Anforderungen können schwere Sanktionen gegen die Führungskräfte erfolgen.

Reporting[7]

Für den Fall eines Cyberangriffs, müssen Unternehmen aus kritischen und sehr kritischen Sektoren über Meldeverfahren von Cybersicherheitsvorfällen verfügen.
Die NIS2-Richtlinie schreibt unter anderem vor, dass Cybervorfälle innerhalb von 24 Stunden gemeldet werden müssen.

[4] Vgl. Richtlinie (EU), 2022/2555, Artikel 21, S. 48
[5] Vgl. Richtlinie (EU), 2022/2555, Artikel 21, S. 48
[6] Vgl. Richtlinie (EU), 2022/2555, Artikel 21, S. 48
[7] Vgl. Richtlinie (EU), 2022/2555, Artikel 23, S. 49 f.

Schäden durch Datendiebstahl, Industriespionage oder Sabotage in Deutschland im Jahr 2023 (in Mrd. €)



Weitere Informationen: Deutschland; Bitkom Research; KW16 bis KW23 2023; 1.002 Befragte; Computergestützte Telefoninterviews (CATI)

Quelle: Bitkom | © Statista 2024

Welche Strafe droht bei Nicht-einhaltung?

Hohe Bußgelder[8]
Sollten sich Unternehmen nicht an die neuen Maßnahmen der NIS2-Richtlinie halten, können je nach Sektor hohe Geldstrafen entstehen. Die Bußgelder reichen bei wesentlichen Einrichtungen von 10 Mio. Euro oder 2 % des vorangeganenen Jahresumsatzes. Für die wichtigen Einrichtungen können kosten von 7 Mio. Euro oder 1,4 % des Jahresumsatzes entstehen.

Drohende Sanktionen sollen wirksam, verhältnismäßig und abschreckend sein.

[8] Vgl. Richtlinie (EU), 2022/2555, Artikel 34, S. 60

Die Geschäftsführung kann persönlich haftbar gemacht werden!

NIS2 macht die Cybersicherheit zur Chefsache! Die neue Richtlinie nimmt die Geschäftsführung deutlich mehr in die Pflicht als noch ihr Vorgänger. So können bei Verstößen nicht nur hohe Bußgelder für das Unternehmen verhängt werden, sondern es kann auch die Geschäftsführung persönlich haftbar gemacht werden. Im Worstcase kann die zuständige Behörde die Geschäftsführung temporär außer Funktion setzen.

> **Bei Nichteinhaltung drohen hohe Bußgelder!**

Wie hilft Ihnen die rhöncloud bei der Umsetzung?

Als Cloud-Service-Provider bringen wir bereits eine wichtige Grundlage der neuen Richtlinie mit. Durch die Auslagerung Ihrer IT-Infrastruktur in das Rechenzentrum der rhöncloud setzen Sie bereits jetzt auf eine zertifizierte Grundlage im Bereich der IT-Sicherheit. Durch die hohen Ansprüche an den Schutz von Unternehmensinfrastrukturen in unseren Rechenzentren sorgen wir bereits durch technische Maßnahmen dafür, dass unsere Services bestmöglich gesichert sind.

Aus diesem Grund haben wir uns auch der internationalen Cybersicherheitsnorm ISO/IEC 27001 unterzogen, welche durch die Zertifizierungen ISO/IEC 27017 (Cloud-Sicherheit) und ISO/IEC 27018 (Cloud-Datenschutz) erweitert werden.

Allerdings bilden die Maßnahmen in der rhöncloud nur das Grundgerüst, sodass weitere Maßnahmen notwendig werden.

Beispiele weiterer Maßnahmen

Erhöhung der IT-Sicherheit durch technische Maßnahmen wie Multi-Faktor-Authentifizierung, der Einsatz von IT-Security-Software auf den einzelnen Servern und Clients, Remote-Monitoring und Patchmanagement und Implementierung einer funktionellen Backup- und Desaster-Recovery-Strategie.

Durchführung von regelmäßigen Penetrationstests und IT-Sicherheitschecks, um den aktuellen Stand der IT-Sicherheit stetig neu zu bewerten.

Regelmäßige Präventionsmaßnahmen der Mitarbeiterinnen und Mitarbeiter.

Einführung einer SIEM-Lösung (besonders bei KRITIS-Einrichtungen)

Erarbeitung einer verlässlichen IT-Sicherheitsstrategie als Ergänzung zur IT-Strategie.

TÜVRheinland® ZERTIFIZIERT
Management System ISO/IEC 27001:2013
www.tuv.com ID 9000017326

rhöncloud

Gerne unterstützen wir Sie in
unserem Leitthema IT-Sicherheit.

**Sprechen Sie uns an,
wir starten gemeinsam!**

Tel. 06682 212003-0
sales@rhoencloud.de

NIS2