NIS 2

Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union

Whitepaper

Wie müssen sich Unternehmen auf die neue Cybersicherheits-Richtlinie der EU vorbereiten

Abstract

Die NIS 2-Richtlinie der Europäischen Union (EU) ist ein Regulierungsrahmen, der darauf abzielt, die Cybersicherheits-Niveau von Betreibern kritischer Infrastrukturen und Anbietern digitaler Dienste zu stärken. Aufbauend auf den Erkenntnissen der Umsetzung der Vorgänger-Richtlinie NIS 1, zielt NIS 2 darauf ab, eine stärkere Harmonisierung der Anforderungen und Prozesse über die Mitgliedsstaaten hinweg zu erreichen. Das vorliegende Whitepaper bietet eine umfassende Analyse der NIS 2 Richtlinie und hebt deren Hauptziele, Umfang, Anforderungen und potenzielle Auswirkungen auf Organisationen innerhalb und außerhalb der EU hervor. Dieses Whitepaper soll das nötige Verständnis vermitteln, um aus Unternehmenssicht die Betroffenheit zu verstehen und die Einhaltung der Richtlinie zu erreichen.

Einleitung

1.1 Hintergrund

Die Europäische Union hat die zunehmende Bedeutung der Cybersicherheit im digitalen Zeitalter und die entscheidende Rolle erkannt, die sie beim Schutz lebenswichtiger Infrastruktur und der Gewährleistung des reibungslosen Funktionierens digitaler Dienste spielt. Ziel der Richtlinie (EU) 2016/1148 (NIS 1) war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen. Die Überprüfung von NIS 1 hat jedoch gezeigt, dass die Mitgliedstaaten die Richtlinie sehr unterschiedlich umgesetzt haben, unter anderem in Bezug auf ihren Anwendungsbereich, dessen Abgrenzung weitgehend im Ermessen der Mitgliedstaaten lag. Weiters wurde den Mitgliedstaaten auch ein sehr großer Ermessensspielraum bei der Umsetzung der in der Richtlinie festgelegten Verpflichtungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen eingeräumt. Diese Verpflichtungen wurden daher auf nationaler Ebene auf sehr unterschiedliche Weise umgesetzt, was zu einer Fragmentierung des Binnenmarkts führen und sich nachteilig auf dessen Funktionieren auswirken kann, insbesondere bei der grenzüberschreitenden Erbringung von Diensten.

1.2 Ziele der EU-NIS 2-Richtlinie

Ziel von NIS 2 ist, die großen Unterschiede in der Auslegung von NIS 1 zwischen den Mitgliedstaaten zu beseitigen, indem Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden. Die betrifft vor allem die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, sowie die Harmonisierung der Vorschriften hinsichtlich Mindestsicherheitsstandards und Meldepflichten. Weiters soll auch der behördliche Rahmen zu Überwachungs- und Durchsetzungsmaßnahmen vereinheitlicht werden. Als Konsequenz soll sichergestellt

werden, dass alle Mitgliedsstaaten ein vergleichbares Niveau and Resilienz gegenüber Cyberbedrohungen entwickeln und umsetzen.

1.3 Geltungsbereich der EU-NIS 2-Richtlinie

Die Vereinheitlichung des Geltungsbereichs ist ein wesentlicher Bestandteil von NIS 2. Markantes Merkmal ist der Wegfall der Unterscheidung zwischen Betreibern wesentlicher Dienste und Digitalen Serviceprovidern, welche ersetzt wird durch eine Unterteilung in wesentliche und wichtige Einrichtungen, die wiederum Sektoren zugeordnet sind. **Anhang 1** listet die „Sektoren mit hoher Kritikalität" auf (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, IKT-Service Management, Weltraum) und **Anhang 2** die „sonstigen kritischen Sektoren" (Post- und Kurierdienste, Abfallbewirtschaftung, Lebensmittel, Verarbeitendes Gewerbes bzw. Herstellung von Waren, Anbieter digitaler Dienste, Forschung). Neben dem Sektor ist noch die Unternehmensgröße für die Einteilung in wesentliche und wichtige Einrichtungen relevant, wobei hierfür die Definition der Europäischen Kommission[1] herangezogen wird. Grundregel ist, dass Großunternehmen (>250 Mitarbeiter, Jahresumsatz >50 Mio. €), welche unter Sektoren des Anhang 1 fallen, als *wesentliche Einrichtungen* gelten, und mittlere Unternehmen (>50 Mitarbeiter, Jahresumsatz >10 Mio. €) dieser Sektoren als *wichtige Einrichtungen*. Unternehmen, die unter Sektoren des Anhang 2 fallen gelten generell als *wichtige Einrichtungen,* sofern sie der Kategorie mittlere oder große Unternehmen angehören. Kleinunternehmen (< 50 Mitarbeiter) sind normalerweise ausgenommen, es gibt jedoch einige **Sonderfälle**, in denen auch Klein- und sogar Kleinstunternehmen (ohne Größenbeschränkung) als wichtige oder sogar wesentliche Einrichtungen eingeordnet werden können:

- Bestimmte Arten von Einrichtungen im Sektor Digitale Infrastruktur (Anbieter öffentlicher elektronischer Kommunikationsdienste, DNS-Diensteanbieter, Top Level Domain Registrare und Vertrauensdiensteanbieter)
- Nach CER-Richtlinie[2] als kritische Einrichtung ermittelt Unternehmen
- Vom Staat als wichtig oder wesentlich eingestufte Unternehmen, wobei folgende Kriterien anzuwenden sind:
  - Wenn es sich um den einzigen Erbringer eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten wesentlich ist.
  - Wenn die Unterbrechung der Dienstleistung erhebliche Auswirkungen auf die öffentliche Sicherheit, die öffentliche Ordnung oder die öffentliche Gesundheit haben könnte.
  - Wenn die Unterbrechung der Dienstleistung ein erhebliches Systemrisiko mit sich bringen könnte (insbesondere grenzüberschreitende Auswirkungen).
  - Bei besonderer Bedeutung auf regionaler oder nationaler Ebene für den betreffenden Sektor oder die betreffende Art von Dienstleistung oder Kritikalität für andere voneinander abhängige Sektoren.

Für den Fall, dass es für bestimmte Sektoren sektorspezifische Rechtsakte gibt, die den in NIS 2 festgelegten Verpflichtungen in ihrer Wirkung als gleichwertig gelten (hinsichtlich Sicherheitsmaßnahmen und Meldepflichten), dann gelten diese sektorspezifische

[1] Empfehlung 2003/361/EG der Kommission; https://eur-lex.europa.eu/DE/legal-content/summary/micro-small-and-medium-sized-enterprises-definition-and-scope.html
[2] Richtlinie (EU) 2022/2557; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557

Rechtsakte statt NIS 2 (sogenannte „Lex specialis“). Für den Bankensektor ist DORA[3] ein solches „Lex specialis“.

Zentrale Anforderungen der EU-NIS 2-Richtlinie an Unternehmen

2.1 Risikomanagement und Governance

Risikomanagement und Governance stellen einen zentralen Teil der Anforderungen an von NIS 2 betroffene Unternehmen dar. Dabei haben die „Leitungsorgane“ (das heißt Vorstände, Geschäftsführer u.ä.) wesentlicher und wichtiger Einrichtungen die Risikomanagementmaßnahmen im Bereich der Cybersicherheit explizit zubilligen, ihre Umsetzung zu überwachen und können für Verstöße gegen diese auch verantwortlich gemacht werden. Um dies erreichen zu können, müssen die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an regelmäßigen einschlägigen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Grundsätzlich müssen wesentliche und wichtige Einrichtungen *geeignete* und *verhältnismäßige* technische, operative und organisatorische Maßnahmen *nach Stand der Technik* ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Unternehmen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Die *Verhältnismäßigkeit* ist hierbei maßgeblich und nicht die Zugehörigkeit zur Kategorie wesentlich oder wichtig. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen.

2.2 Sicherheitsanforderungen und Sicherheitsmaßnahmen

Die dabei umzusetzenden Maßnahmen müssen auf einem *gefahrenübergreifenden Ansatz* („*all hazards approach*“) beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen. NIS 2 listet hierbei eine Reihe von Maßnahmen auf, die zumindest davon umfasst sein müssen:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- Prozesse zur Bewältigung von Sicherheitsvorfällen;
- Maßnahmen zur Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
- Maßnahmen zur Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den Unternehmen und ihren Dienstleistern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

[3] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Im Gegensatz zu NIS 1 ist hiermit NIS 2 deutlich konkreter in ihren Anforderungen. Zusätzlich erlässt die Kommission bis zum 17. Oktober 2024 Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen an die genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter. Weitere Durchführungsrechtsakte, in denen die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen detailliert oder erweitert werden, können folgen.

2.3 Sicherheit in der Lieferkette

Bezüglich der Sicherheit der Lieferkette wird speziell hervorgehoben, dass bei der Risikobewertung die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Dienstleister sowie die Gesamtqualität ihrer Produkte und ihrer Cybersicherheitspraxis, einschließlich der Sicherheit ihrer Entwicklungsprozesse, zu berücksichtigen sind.

Das Thema Cybersicherheit in der Lieferkette findest sich auch im Artikel 7 wieder, bei dem es um die nationale Cybersicherheitsstrategie geht. Dort ist die Forderung vermerkt, dass die nationale Cybersicherheitsstrategie folgendes umfassen muss:

- Konzepte für die Cybersicherheit in der Lieferkette für IKT-Produkte und IKT-Dienste, die von Einrichtungen für die Erbringung ihrer Dienste genutzt werden;
- Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und IKT-Dienste bei der Vergabe öffentlicher Aufträge, einschließlich hinsichtlich der Zertifizierung der Cybersicherheit, der Verschlüsselung und der Nutzung quelloffener Cybersicherheitsprodukte;
- Konzepte zur Stärkung des Grundniveaus für Cyberresilienz und Cyberhygiene kleiner und mittlerer Unternehmen, insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU, durch Bereitstellung leicht zugänglicher Orientierungshilfen und Unterstützung für ihre spezifischen Bedürfnisse;

Die starke Betonung der Lieferkettensicherheit und zugehöriger Sicherheitsmaßnahmen auch in der Lieferkette, dehnt den Kreis der von NIS 2 betroffenen Unternehmen bis weit in den Mittelstand aus. Im Prinzip ist jedes Unternehmen - zumindest indirekt - betroffen, das Zulieferer von wesentlichen oder wichtigen Einrichtungen ist. Aufgrund der Tatsache, dass

von NIS 2 betroffene Unternehmen zukünftig die Sicherheit in ihrer Lieferkette sicherstellen müssen, folgt daraus die Überbindung der Basis-Sicherheitsanforderungen an ihre Lieferanten, welche das auch entsprechend nachweisen müssen. Das Cyber Trust Label ist dafür ein anerkannter Nachweis.

2.4 Meldung von Vorfällen und Zusammenarbeit mit Behörden

Wesentliche und wichtige Einrichtungen sind verpflichtet, ihrem CSIRT/CERT oder gegebenenfalls ihre zuständigen Behörde unverzüglich über jeden Sicherheitsvorfall unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat (erheblicher Sicherheitsvorfall). Ein Sicherheitsvorfall gilt als ***erheblich***, wenn er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann und/oder wenn er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann. Weiters müssen Unternehmen, wenn erforderlich, auch potenziell von einer erheblichen Cyberbedrohung betroffene Empfänger ihrer Dienste unverzüglich über die gegenständliche Cyberbedrohung informieren sowie über alle Maßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Erstmeldung hat dabei innerhalb von 24 Stunden zu erfolgen, nach spätestens 72 Stunden muss zudem bereits eine erste Bewertung des Sicherheitsvorfalls nachgeliefert werden, einschließlich einer Einschätzung seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren. Spätestens nach einem Monat muss dann ein Abschlussbericht vorliegen, der eine ausführliche Beschreibung des Sicherheitsvorfalls umfasst, einschließlich seines Schweregrads und seiner Auswirkungen, Angaben zur Art der Bedrohung bzw. der zugrunde liegenden Ursache, sowie Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.

Sofern die Offenlegung des erheblichen Sicherheitsvorfalls im öffentlichen Interesse liegt, kann die zuständige Behörde nach Konsultation der betreffenden Einrichtung die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun. NIS 2 hält darüber hinaus fest, dass mit der bloßen Meldung keine höhere Haftung der meldenden Einrichtung begründet wird.

Überwachung und Durchsetzung

3.1 Aufsichtsmaßnahmen

Der Aufsichtsrahmen ist der größte Unterschied zwischen Einrichtungen wesentlicher und wichtiger Dienste. Grundsätzlich erfolgt bei wesentlichen Einrichtungen eine Ex-ante Beaufsichtigung und bei wichtigen Einrichtungen eine Ex-post Beaufsichtigung. Das bedeutet, dass bei wichtigen Einrichtungen eine behördliche Überprüfung nur erfolgt, wenn Nachweise, Hinweise oder Informationen vorliegen, wonach eine wichtige Einrichtung mutmaßlich den Anforderungen von NIS 2, insbesondere bezüglich Sicherheitsmaßnahmen oder Meldepflichten nicht nachkommt. Bei wesentlichen Einrichtungen erfolgt hingegen die Überprüfung der Einhaltung regelmäßig im Rahmen von Sicherheitsüberprüfungen. Dabei sind die Behörden befugt, mindestens folgende Aktivitäten vorzunehmen:

- Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich von geschulten Fachleuten durchgeführten Stichprobenkontrollen;
- regelmäßige und gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

- Ad-hoc-Prüfungen, einschließlich solcher, die aufgrund eines erheblichen Sicherheitsvorfalls oder Verstoßes gegen diese Richtlinie der wesentlichen Einrichtung gerechtfertigt sind;
- Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung;
- Anforderung von Informationen, die für die Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte;
- Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind;
- Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise.

3.2 Durchsetzungs- und Strafmaßnahmen

Wenn die Behörde feststellt, dass eine Einrichtung den genannten Maßnahmen und Anforderungen nicht nachkommt, ist sie befugt, unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen zu ergreifen. Dazu zählen:

- Das Aussprechen von Warnungen über Verstöße
- Das Erlassen verbindlicher Anweisungen bezüglich Maßnahmen zur Mängelbehebung, inklusive Fristen für die Durchführung dieser Maßnahmen und für die Berichterstattung über ihre Durchführung;
- Anweisungen zur Information natürlicher oder juristischer Personen über erhebliche Cyberbedrohung und mögliche Abwehr- oder Abhilfemaßnahmen;
- Ernennung eines Überwachungsbeauftragten, um die Einhaltung der Sicherheitsanforderungen und Meldepflichten für einen bestimmten Zeitraum zu überwachen;
- Anweisungen, Aspekte der Verstöße gegen NIS 2 öffentlich bekannt zu machen;
- Die Verhängung von Geldbußen.

Für den Fall, dass die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen werden, sind die zuständigen Behörden überdies befugt, die Zertifizierung oder Genehmigung für einen Teil oder alle von der wesentlichen Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten vorübergehend auszusetzen sowie natürlichen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene in dieser wesentlichen Einrichtung zuständig sind, vorübergehend zu untersagen, Leitungsaufgaben in dieser Einrichtung wahrzunehmen. NIS 2 hält weiters fest, dass diese natürlichen Personen für Verstöße gegen NIS 2 auch **persönlich haftbar** gemacht werden können.

Die Geldbußen umfassen einen Höchstbetrag von mindestens 10 Mio. EUR oder einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens. Bei wichtigen Einrichtungen verringert sich dieser Höchstbetrag auf 7 Mio. EUR bzw. einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten Umsatzes.