EU-Richtlinie NIS-2 zur Cyber-Resilienz: Überblick – Betroffene Unternehmen – Pflichten und Lösungsweg(e)

Inhaltsverzeichnis

Einleitung

Erschreckende Meldungen zu erfolgten Cyberattacken sind inzwischen leider an der Tagesordnung. Als Führungskraft eines deutschen Unternehmens oder einer deutschen Institution ist deshalb das Thema Netzwerk- und Informationssicherheit allein schon aus eigenem Interesse ernst zu nehmen und sich mit entsprechenden Maßnahmen zur Cybersicherheit in der eigenen Organisation intensiv zu befassen.
Um dieses Thema auch auf gesamteuropäischer Ebene zu stärken, wurde bereits 2016 die NIS-1-Richtlinie veröffentlicht, die seitdem als eine der bedeutendsten europäischen Rechtsvorschriften im Bereich der Cybersicherheit gilt.
Inzwischen ist die NIS-2-Richtlinie in Kraft getreten, die NIS-1 um noch strengere Anforderungen für verschiedene Sektoren erweitert und sogar Sanktionen für den Fall enthält, dass NIS-2 in den betroffenen Unternehmen und Institutionen nicht oder nicht anforderungsgemäß umgesetzt wird. Der folgende Überblick dient dazu, dieses Thema zunächst insgesamt transparent zu machen.

Überblick zur EU-Richtlinie NIS-2 – Cyber-Resilienz per Gesetz

Die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) wurde am 27.12.2022 im Amtsblatt L333 als Richtlinie (EU) 2022/2555 der Europäischen Union veröffentlicht und trat ab dem 16.01.2023 in Kraft. Das Ziel dieser in Kurzform bekannten NIS-2-Richtlinie ist, in der Europäischen Union ein hohes gemeinsames Niveau der Cybersicherheit zu erreichen. Sie ersetzt damit die vorige NIS-1-Richtlinie, um den bisherigen Kritikpunkten der Gesetzgebung entgegenzuwirken. Dazu gehören auf EU-Ebene sowohl eine fehlende gemeinsame Krisenreaktion als auch ein unzureichendes gemeinsames Verständnis der wichtigsten Bedrohungen und Herausforderungen für die EU-Mitgliedstaaten. Um das übergreifende Ziel des hohen gemeinsamen Cybersicherheitsniveaus zu erreichen, soll die neue Richtlinie die Basis dafür legen, die Cyber-Resilienz von Unternehmen und eine konsistente Widerstandfähigkeit zwischen den Mitgliedstaaten und den Sektoren ermöglichen. Somit werden die Mitgliedstaaten grundsätzlich auf die Verabschiedung einer nationalen Cybersicherheitsstrategie verpflichtet.

Was bedeutet das für uns in Deutschland?

Die NIS-2-Richtlinie definiert ein Mindestmaß an erforderlichen Umsetzungen für viele Unternehmen und Institutionen: Mit NIS-2 werden auf Basis einer nationalen Cybersicherheitsstrategie strengere Aufsichtsmaßnahmen für Behörden sowie strengere Durchsetzungsanforderungen und eine Harmonisierung der Sanktionsregelungen für Unternehmen und Institutionen in allen Mitgliedstaaten eingeführt. Über angepasste oder erweiterte Möglichkeiten der Umsetzung entscheiden letztendlich die deutschen Behörden.
Anzuwenden ist diese europäische NIS-2-Richtlinie auf nationaler Ebene ab dem 18. Oktober 2024. Bis zu diesem Termin sind folglich alle notwendigen Maßnahmen in Bezug auf die IT-Sicherheit der unternehmensseitigen/institutionseigenen Anlagen, Netzwerke und IT-Systeme verbindlich umzusetzen. Dies wird aktuellen Schätzungen zufolge mindestens 30.000 Unternehmen und Institutionen in Deutschland betreffen. Somit gilt diese Richtlinie unabhängig von dem kommenden Gesetz zur Umsetzung von EU NIS-2 und der Stärkung der Cybersicherheit (NIS2UmsuCG), das die NIS-2-Vorgaben in die deutsche Regulierung überführen soll.
Unter der Leitung des Bundesministeriums des Innern und für Heimat (BMI) sind als Geschäftsbereiche das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) an der Überführung beteiligt. Es liegen mittlerweile mehrere Referentenentwürfe für das NIS2UmsuCG vor, das bis zum Oktober 2024 verabschiedet werden soll.
Neben der NIS-2 reguliert in Deutschland seit 2024 das KRITIS-Dachgesetz die Resilienz und physische Sicherheit Kritischer Infrastrukturen weiter. Zudem wird die EU CER-Richtlinie (EU 2022/2557) zusätzliche Pflichten für Betreiber kritischer Anlagen definieren. Für Finanzunternehmen und kritische IKT-Drittdienstleister (z. B. Cloud Provider) schreibt die EU-Verordnung Digital Operational Resilience Act (DORA), EU 2022/255, Maßnahmen für Risiko-Management und Sicherheit vor.
Wer also zu einem Finanzunternehmen gehört, kritischer IKT-Drittdienstleister oder ein KRITIS-Betreiber ist, für den gilt, dass ein Blick in die hier genannten, weiteren Regelungen, zwingend erforderlich ist. In den vorliegenden Ausführungen wird allerdings diesbezüglich nicht auf weitere Details dazu eingegangen – der Fokus liegt hier auf der NIS-2-Richtlinie.

Wer ist davon betroffen?

Die NIS-2 definiert grundsätzlich zwei Gruppen von betroffenen Unternehmen bzw. Organisationen (im Folgenden Einrichtungen genannt). Diese werden kurz dargestellt, um eine Übersicht zu ermöglichen. Dabei wird nicht im Detail auf die relevanten Sektoren bei den Einrichtungen eingegangen, da diese in den Anlagen 1 und 2 des NIS-2-Umsetzungsgesetzes konkret definiert werden, wobei die Zugehörigkeit als Einrichtung von der Unternehmensgröße, dem Teilsektor und der Art der jeweiligen Einrichtung abhängt.
Als erste Gruppe der besonders wichtigen Einrichtungen sind in NIS-2 **Großunternehmen aus den Sektoren in der NIS-2-Anlage 1** definiert sowie einige **größenunabhängige Unternehmen und KRITIS-Betreiber**. Entscheidende Faktoren sind die Mitarbeiterzahl (mindestens 250 FTE) oder ein jährlicher Umsatz von mehr als 50 Mio. € und eine Bilanzsumme von mehr als 43 Mio. €.
Die zweite Gruppe der wichtigen Einrichtungen sind in NIS-2 **Großunternehmen und mittlere Unternehmen aus den Sektoren in der NIS-2-Anlage 1 & 2**. Entscheidend sind hier ebenfalls die Mitarbeiterzahl (mindestens 50 FTE) oder ein jährlicher Umsatz von mehr als 10 Mio. € und eine Bilanzsumme von mehr als 10 Mio. €.
Die KRITIS-Sektoren der kritischen Anlagen bleiben bestehen: **KRITIS-Betreiber** zählen per se zu den besonders wichtigen Einrichtungen.
Im NIS-2-Umsetzungsgesetz sind im Sektor Staat **Einrichtungen der Bundesverwaltung** reguliert. Hier muss beachtet werden, dass das KRITIS-Dachgesetz ebenfalls Einrichtungen der Bundeverwaltung reguliert.
Darüber hinaus gibt es noch einige Sonderfälle und Ausnahmeregelungen, auf die in diesem Artikel nicht näher eingegangen wird. Durch diese Komplexität mit den unterschiedlichen Kategorien und Parametern zur Einstufung (siehe Anlagen der NIS-2) wird dringend empfohlen, im nicht eindeutigen Fall einen Juristen zu Rate zu ziehen und den zugrundeliegenden Sachverhalt umgehend als Organisation/Einrichtung bewerten zu lassen.
Was darüber hinaus noch wichtig ist: Selbst wer durch NIS-2 nicht direkt betroffen ist, kann als Dienstleister oder Lieferant für ein NIS-2 betroffenes Unternehmen indirekt wiederum dennoch betroffen sein: Die NIS-2-Richtlinie fordert, explizit die Sicherheit in der Lieferkette zu gewährleisten - und somit werden die Anforderungen Organisation der direkten Lieferanten und Dienstleister betreffen. Daher ist es für jedes Unternehmen angeraten, sofort in eine Prüfung zu gehen und notwendigen Handlungsbedarf umgehend zu bearbeiten.

Was ist durch die Unternehmen umzusetzen?

Die NIS-2-Richtlinie definiert ein Mindestmaß an Anforderungen, das NIS2UmsuCG konkretisiert und/oder verschärft diese Anforderungen sogar. Die Pflichten der KRITIS-Betreiber (BSI-Gesetz) werden teils präzisiert und teils sogar verschärft bzw. neu strukturiert. Die Anforderungen an Betreiber und Einrichtungen ändern sich mit der NIS-2-Umsetzung somit deutlich.
Folgende Pflichten sind für alle betroffenen Unternehmen nach NIS2UmsuCG relevant und werden hier kurz dargestellt (spezielle Anforderungen an KRITIS-Betreiber sind hier ausgenommen):

- Risikomanagementmaßnahmen, Business Continuity Management (§§ 30, 31)
- Meldepflichten (§ 32)
- Registrierungspflicht (§§ 33, 34)
- Unterrichtungspflichten gegenüber Kunden (§ 35)
- Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter (§ 38)

Die Pflicht zur Nachweisführung gemäß § 39 wird in diesem Artikel nicht weiter vertieft.

Gemäß § 30 und § 31 ist die Einführung eines systematischen **Risikomanagementsystems** Pflicht, das auf dem All-Gefahren-Ansatz basiert. Dabei umfasst diese Vorgabe sämtliche IT-Systeme, Komponenten und Prozesse, die für die Erbringung der Dienste genutzt werden (= sämtliche Aktivitäten, für die IT-Systeme eingesetzt werden) und fällt damit recht umfassend aus. Neben den im Folgenden detaillierter beschriebenen Präventionsmaßnahmen wird dabei auch Wert auf die Aufrechterhaltung des Geschäftes, also der reaktiven Geschäftskontinuität gelegt. All dies zielt primär auf die Erhöhung der Cyber-Resilienz des Unternehmens ab.
Präventionsmaßnahmen können sein:

- Konzepte in Bezug auf Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall sowie Krisenmanagement
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- 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 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

Um NIS-2 zu genügen, müssen somit grundlegende Anforderungen an die Cyber-Sicherheit erfüllt werden. Es gilt, mit angemessenen und verhältnismäßigen Maßnahmen auf technischer, betrieblicher und organisatorischer Ebene permanent die damit verbundenen Risiken zu kontrollieren, die die jeweiligen Informationssysteme betreffen. Bei alledem gilt im Idealfall der Grundsatz des „Zero Trust“: Keinem Nutzer, keinem Gerät, keinem Dienst sollte von vornherein Vertrauen geschenkt werden, da unbegründetes Vertrauen die IT-Risiken erheblich steigert. Hinzu kommt die Forderung nach geringstmöglichen Zugangsberechtigungen und Erlaubnis zum Zugriff nur dann, wenn es tatsächlich dringend erforderlich ist. Die Implementierung einer belastbaren Zero Trust-Initiative im Vorfeld von NIS-2 ist demnach definitiv zielführend. Bestehende Insellösungen, die über die gesamte Organisation verteilt sind, sollten zudem schnellstens durch eine zentralisierte Lösung ersetzt werden.
Darüber hinaus werden die **Meldepflichten** in § 32 erweitert. Somit verpflichtet die NIS-2 dazu, bei erheblichen Störungen, Vorfällen oder Cyber-Attacken innerhalb von 24 Stunden nach Bekanntwerden eine Frühwarnung an die zuständige nationale Behörde zu übermitteln. Eine detailliertere Bewertung der Situation wird innerhalb von 72 Stunden erwartet, ein umfassender Abschlussbericht nach einem Monat. Das BSI meldet sich (nach Möglichkeit) innerhalb der ersten 24 Stunden nach Meldung bei der Einrichtung zurück, um mögliche Rückfragen zu stellen oder die meldende Einrichtung mit Informationen und Unterstützungsangeboten zu versorgen.
KRITIS-Betreiber kennen bereits die damit verbundene **Registrierungspflicht**, die nun auch für die betroffenen Unternehmen und Institutionen/Einrichtungen der NIS-2-Richtlinie

innerhalb von drei Monaten verpflichtend wird. Wesentliche Informationen dazu finden sich auf der Webseite des BSI wieder. Für bestimmte Unternehmen gelten darüber hinaus spezielle Registrierungsregeln, die es zu beachten gilt.
Die **Unterrichtungspflichten** ergänzen die o. a. Meldepflichten gegenüber den Kunden. So kann das BSI bei erheblichen Sicherheitsvorfällen „besonders wichtige“ und „wichtige“ Einrichtungen anweisen, ihre Kunden von diesem Sicherheitsvorfall zu unterrichten. So müssen Einrichtungen aus einigen Sektoren die potenziell betroffenen Kunden unverzüglich über mögliche zu ergreifende Gegenmaßnahmen auf der Kundenseite informieren. Ist aufgrund eines Sicherheitsvorfalls z. B. die Sensibilisierung der Öffentlichkeit erforderlich, kann das BSI diese informieren oder Einrichtungen dazu auffordern. Dies sei hier als Beispiel dafür angeführt, dass die NIS-2-Richtlinie neben den Pflichten für die betroffenen Unternehmen ebenso die Befugnisse der Behörden teils deutlich erweitert hat.
Die **Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen** besagt, dass die Geschäftsleitungen von Einrichtungen die Cybersecurity-Maßnahmen aus dem Risikomanagement billigen und die Umsetzung in ihrem Unternehmen/ihrer Einrichtung überwachen müssen. Ergänzend müssen Geschäftsleitungen regelmäßig an Schulungen teilnehmen, um diesen Pflichten nachkommen zu können. Hierzu müssen nachweislich ausreichende Kenntnisse und Fähigkeiten zur Bewertung von Risiken und Maßnahmen erworben werden.

Sanktionierbarkeit von Unternehmen

Zuletzt noch ein wesentlicher **Haftungsaspekt**: Wird die NIS-2-Richtlinie nicht eingehalten, drohen einem Unternehmen/einer Einrichtung Strafen bis zu 10 Millionen Euro (je nach Bußgeldtatbestand). Zudem ist vorgesehen, dass Geschäftsführungen und Vorstände bei nachweislichen Fehlern in der Umsetzung und Verstößen gegen die Cybersecurity-Pflichten sogar zivilrechtlich mit ihrem Privatvermögen haftbar gemacht werden können (Binnenhaftung gegenüber der Unternehmung/Einrichtung). Somit gibt es für die in den Unternehmen/Einrichtungen Verantwortlichen keine Chance, die hier dargestellte Thematik einfach zu ignorieren oder deren Bearbeitung zu verzögern - denn der Countdown läuft.

Ein möglicher Lösungsweg

Cyberattacken sind schon lange nicht mehr nur auf öffentliche Verwaltungen, große Konzerne und kritische Infrastrukturen beschränkt. Vielmehr müssen sich vermehrt auch kleine und mittelständische Unternehmen (KMU) mit dieser Problematik beschäftigen und ihre Widerstandsfähigkeit aufrechterhalten. Zumal Angreifer gerade im KMU-Umfeld immer noch sehr selten auf entsprechende Sicherheitsmaßnahmen stoßen. Denn dieses Umfeld steht in Zeiten der digitalen Transformation, des Einsatzes von künstlicher Intelligenz (KI) und weiteren Themen rund um die Automatisierung unter Innovationsdruck.
Da die technische Infrastruktur in der Regel sehr komplex, qualifizierte Fachkräfte aber in vielen Branchen und Sektoren kaum noch vorhanden sowie die Gehälter für eigene Security-Spezialisten sehr hoch sind und zudem immer mehr vermeintliche technische Security-Lösungen angeboten werden, bleibt die Frage, wie sich die Geschäftsbereiche der zur NIS-2-Umsetzung verpflichteten Unternehmen/Einrichtungen optimal und abgestimmt auf deren Umsetzung vorbereiten können. Professionelle externe Dienstleistungsunternehmen bieten hier im anspruchsvollen Umfeld von integrierten Managementsystemen, physischer Sicherheit, technischen Umsetzungen und Awareness-Kampagnen für die Mitarbeitenden ganzheitliche Ansätze und Lösungswege bei überschaubaren finanziellen Aufwendungen.
Wenngleich das NIS2UmsuCG zwar konkretere Vorgaben zur Erfüllung der Anforderungen als die NIS-2-Richtlinie macht, so bleiben aktuell immer noch viele Fragen offen. Unter diesen

Gesichtspunkten bleibt die Frage, was der kleinste gemeinsame Nenner sein wird und worüber in Expertenkreisen diskutiert wird. Ein klares Votum lässt sich definitiv nicht geben.
Es ist daher unbedingt empfehlenswert, im Idealfall als Unternehmen/Einrichtung ein bereits **etabliertes, prozessorientiertes integriertes Managementsystem** zu nutzen. Hier lassen sich weitere branchenübergreifende und sektorspezifische Disziplinen einbringen, um die Resilienz eines Unternehmen/einer Einrichtung gezielt auszubauen. Allen voran sollen hier die international anerkannten Normen zur Informationssicherheit (ISO 2700x) sowie zur Geschäftskontinuität (ISO 22301) als kleinster gemeinsamer Nenner genannt werden. Diese Basis sollte integriert werden und weitere sektorspezifische Anforderungen zur Erhöhung der Sicherheit (z. B. C5-Standard bei Cloudanbietern) oder die branchenspezifischen Sicherheitsstandards (B3S) beachtet werden, die auch schon KRITIS-Betreibern überwiegend hilfreiche Dienste erwiesen haben. Gerade auch die Webseite des BSI bietet eine Fülle von Informationen zu einer möglichen Implementierung. Was für ein Unternehmen/eine Einrichtung sinnvoll und damit vor allem praktikabel ist, kann mit einem professionellen externen Dienstleister abgestimmt werden. Dieser bietet in der Regel abgestimmte und mit Juristen und Experten ausgearbeitete Schulungen speziell für Geschäftsleitungen an.
Darüber hinaus bietet es sich an, sich mit weiteren Betroffenen und Experten z. B. in einer dafür ausgelegten Community of Practice (CoP), regelmäßig auszutauschen und darüber praxisorientierte Lösungswege zu diskutieren. Vor allem können so die aktuellsten Entwicklungen rund um die NIS-2-Richtlinie und dem NIS2UmsuCG verfolgt werden.

Fazit

Dass eine gute Cybersicherheit nicht per Gesetz verordnet werden kann, wird oft kritisiert. Dennoch sind aus der Erfahrung heraus die geforderten Maßnahmen zur Erhöhung der eigenen Widerstandsfähigkeit nicht neu und jedes Unternehmen tut gut daran, diese in einer individuellen und angemessenen Art und Weise zu etablieren. Die weltpolitischen Veränderungen der letzten Jahre und die nahezu täglichen Pressemeldungen zu Cyberattacken zeigen doch mehr als deutlich, dass eine gute Cyber-Resilienz ein entscheidender Faktor zur Aufrechterhaltung des eigenen Geschäftsbetriebes oder der Versorgung der Allgemeinheit darstellt.
Was aber auch in der Kritik steckt, zeigt der erhobene Zeigefinger gegen noch mehr Formalismus und Bürokratie. Dies ist wiederum sehr gut nachvollziehbar, denn auch hier zeigt die Erfahrung eine nicht abgestimmte Priorisierung zwischen den deutschen Aufsichtsbehörden in einigen Sektoren und damit geforderten zahnlosen Papiertigern. Dies lähmt dann eher die betroffenen Unternehmen durch Unsicherheiten und überbordenden Arbeitsaufwand, der sinnvoller in die Gewährleistung einer nachhaltigen Cybersicherheit investiert wäre.
Dem will die NIS-2-Richtlinie mit einer höheren Harmonisierung von Schnittstellen zwischen diversen Beteiligten entgegentreten. Jedes Unternehmen kann also bereits jetzt mit einem systematisch funktionierenden Risikomanagement die Angemessenheit und Wirksamkeit von individuell definierten Maßnahmen zur eigenen Cyber-Resilienz nachhaltig stärken.

Quellen

- https://www.NIS-2-directive.com
  (Die Seite der EU zur NIS-2-Direktive, 19.06.2024, 09:48 Uhr)
- https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html
  (Webseite des BMI zum Umsetzungsgesetz, 07.06.2024, 18:10 Uhr)
- https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html
  (Informationsplattform OpenKRITIS, 08.06.2024, 10:46 Uhr)
- https://cop.sollence-academy.de
  (Community of Practice für digitale Transformation, 12.06.2024, 11:01 Uhr)

Über den Autor

Andreas Altena, ist Geschäftsführer der Sollence® GmbH aus Krefeld, einem Dienstleistungsunternehmen im Bereich Organisationsentwicklung, das sich unter anderem auch sehr intensiv mit dem Thema „Cyber Security & Resilience“ beschäftigt und einen Security-Standard entwickelt hat.
Seit über 22 Jahren setzt sich der gelernte Betriebswirt u. a. mit Themen zur Informationssicherheit, zum Risikomanagement und zu integrierten Managementsystemen auseinander - zunächst in seiner Funktion als IT-Manager und mittlerweile breitgefächert als anerkannter Berater, Trainer und Auditor.
Über diese Tätigkeiten hinaus fördert er als Vorstand des Bundesverbands für Informationsschutz (BVFIS e. V.) das Bewusstsein für die Sicherheit von Informationen sowie für die INSTICERT® - Institut für nachhaltige Zertifizierung GmbH als Senior-Lead-Auditor die nachhaltige Qualität von Zertifizierungen und Prüfungen.