advisio
CORPORATE CONSULTING

Die neue EU-Richtlinie für Netz- und Informationssicherheit

NIS2 (Network and Information Security 2)

Fakten • Hinweise • Meinungen

NIS2, eine Richtlinie der europäischen Union gibt einen neuen Takt im Umgang mit Cybersecurity vor.

Am 16. Januar 2023 ist die EU-Richtlinie (EU) 2022/2555 für Netz- und Informationssicherheit NIS2 in Kraft getreten. Diese schreibt strenge Standards in der Bekämpfung von Cyberattacken vor und wird bis Oktober 2024 in Deutschland rechtsverbindlich.

Wie ist der Stand der Dinge, wie geht es weiter, was kommt auf uns zu?

Ein Bericht von Martin Zeyer, Senior Consultant für Informationssicherheit bei der advisio GmbH.

Inhaltsübersicht

1. Einleitung

Die Cyberkriminalität nimmt zu und die Schäden durch Störungen der Informations- und Kommunikationstechnik für Wirtschaft und Gesellschaft werden immer bedrohlicher. Das findet auch in der EU immer mehr Beachtung.
Nicht nur kriegerische Auseinandersetzungen haben uns verdeutlicht, dass annähernd alle Institutionen und das Funktionieren von Arbeitsmärkten, Finanzmärkten, Wirtschaft und Gesellschaft von der Funktionalität der digitalen Versorgung komplett abhängig sind. Ein großflächiger Ausfall hätte katastrophale Auswirkungen.

Um diesen Gefahren zu begegnen, erließ die EU im Dezember die Richtlinie 2022/2555 (NIS2 – Network and Information Security 2), die die bisherigen Richtlinien zur Erhöhung der Cybersicherheit ersetzte und verschärfte, insbesondere die Richtlinie 2016/1148.

Diese Richtlinie trat im Januar 2023 in Kraft und muss laut EU-Gesetzgebung bis Oktober 2024 in nationales Gesetz umgesetzt werden.

2. Stand der Dinge

Die Umsetzung der EU-Direktive ist in Deutschland noch nicht erfolgt. Sie wird vermutlich über die Änderung oder Erweiterung des bisherigen IT-Sicherheitsgesetz (IT-SiG 2.0) bzw. des BSI-Gesetzes (BSIG) erfolgen.

Dazu wurden Referenten-Entwürfe eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und eines KRITIS-Dachgesetz (KRITIS-DachG) vorgestellt. Zweiteres bezieht sich vor allem auf die kritischen Infrastrukturen. Beide Entwürfe stammen vom Juli 2023.

Die Umsetzung der Maßnahmen, die Implementierung der zugehörigem Melde- und Nachweisverfahren und die drohenden drastischen Strafen weckten Widerstand in den Reihen der betroffenen Unternehmen. Daraufhin veröffentlichte das Bundesministerium des Inneren und für die Heimat ein Diskussionspapier, das die vorgesehenen gesetzlichen Regelungen bedeutend entschärft. So sind Prüfungen nur alle 3 Jahre, statt 2 Jahre vorgesehen. Ebenso müssen Nachweise nicht mehr erbracht werden, sie „können" vom BSI angefordert werden. Weiterhin wird beschwichtigend angekündigt, dass das BSI nach Inkrafttreten nicht flächendeckend Prüfungen und Strafen verhängen wird.

Fakt ist jedoch, dass die Umsetzung der EU-Richtlinie in deutschen Gesetzen bis zum Oktober 2024 erfolgen muss.

3. Eckpunkte der EU-Richtlinie

Die Vorgaben der EU lassen sich wie folgt in Eckpunkte einteilen.

I. Ausweitung der Geltungspflicht auf 18 Sektoren, Kommunen und Mittelstand Registrierungspflicht
II. Pflicht zur Durchführung von Risikoanalysen (All-Gefahren-Ansatz)
III. Pflicht zur Umsetzung von Maßnahmen aus der Risikoanalyse
IV. Nachweispflicht
V. Pflicht zur Meldung von Sicherheitsvorfällen
VI. Strafen bei Verstößen gegen Vorgaben oder gegen die Meldepflicht

3.1 Ausweitung des Geltungsbereiches auf 18 Sektoren, Kommunen und Mittelstand

Der bisherige Geltungsbereich bezog sich vor allem auf die elementare Grundversorgung, wie Energie, Gesundheit, Transport, Kommunikation, Wasser, Finanzen, Ernährung, Entsorgung.

Zum einen erweitert sich der Geltungsbereich auf mehr Sektoren und zum anderen sinken die Schwellenwerte für die Unternehmensgrößen deutlich.

Es wird erwartet, dass in Deutschland rund 30.000 bis 40.000 Unternehmen und Institutionen von der neuen Regelung betroffen sind. Da Unternehmen auch Lieferketten schützen müssen (Lieferkettenschutzgesetz, LkSG), kann es durchaus sein, dass Lieferanten ebenfalls gewisse Vorgaben dieser Unternehmen erfüllen müssen, wenn sie selber auch keinen direkten Nachweis für NIS2 bringen müssen.

Der Zusammenhang zwischen den Sektoren (Wirtschafts-Bereiche, Kommunen und anderen Einrichtungen) und den tatsächlich betroffenen Unternehmen, Einrichtungen und Institutionen ist also nicht ganz unerheblich.

3.1.1 Sektoren mit hoher und sonstiger Kritikalität

Die EU-Kommission definiert in zwei Anhängen zwei unterschiedlich kritische Bereiche – die typischen KRITIS Unternehmen und die etwas weiter gefasste kritische Infrastruktur.

A) Sektoren mit hoher Kritikalität

Energie	Elektrizität, Fernwärme (kalt, warm), Erdöl, Erdgas, Wasserstoff	Betreiber von Anlagen, Netzen, Stützpunkten, Anbieter, Versorger, Ladestationen, …
Verkehr	Luft, Schiene, Schiff, Straße	Unternehmen, Infrastrukturbetreiber, Organe, Behörden, …
Banken		Kreditinstitute
Finanzmarkt		Betreiber und zentrale Gegenparteien
Gesundheitswesen		Dienstleister, Labore, Einrichtungen, Pharmaunternehmen, Forschung, …
Trinkwasser		Lieferanten, Versorger, …
Abwasser		Kommunen, Unternehmen, industrielle Entsorger
Digitale Infrastruktur		Anbieter von: Internet-Infrastruktur, DNS, Namensregister, Cloud-Diensten, RZ-Diensten, Netzen, Kommunikationsdiensten, Authentifizierungs-, Zertifikats- oder Identifizierungsdiensten
IKT-Dienste		B2B Anbieter
Öffentliche Verwaltung		Regionale und zentrale Verwaltung

Weltraum		Betreiber von Infrastrukturen, weltraumgestützten Diensten und elektronischer Netze

B) Sonstige kritische Sektoren

Transport und Verkehr	Post- und Kurierdienste	
Abfallbewirtschaftung		
Chemische Erzeugnisse		Produktion, Herstellung und Handel
Lebensmittel		Industrielle Produktion und Verarbeitung, Großhandel
Herstellung und Verarbeitung	Medizinprodukte, Diagnostika, Datenverarbeitungsgeräte, elektronische und optische Geräte, Maschinenbau, Kfz und deren Teile,	
Anbieter digitaler Dienste		Online-Marktplätze, Online-Suchmaschinen, soziale Netzwerke
Forschung		

Unabhängig davon besitzen die digitalen Dienste, insbesondere DNS (Domain-Name Systems), Anbieter von Vertrauensdiensten (trust services) und Telekommunikation, sowie öffentliche Verwaltung als Teil der Regierung oder Regionalverwaltung einen höheren Stellenwert. Diese Bereiche gelten als besonders schützenswert.

3.1.2 Betriebsgrößen – mittlere Unternehmen und Groß-Unternehmen

Als mittlere Unternehmen werden Einrichtungen definiert, die mehr als 50 Mitarbeiter*innen beschäftigen oder mehr als 10 Mio. Euro Jahresumsatz haben.

Groß-Unternehmen sind Einrichtungen mit mehr als 250 Mitarbeiter*innen oder mehr als 50 Mio. Euro Jahresumsatz.

3.1.3 Besonders wichtige, wichtige und kritische Einrichtungen

Die eigentliche Zuordnung von Regelungen, Sektoren und Betriebsgrößen erfolgt über die Definition der Wichtigkeit von Einrichtungen.

A) Besonders wichtige Einrichtungen
- Alle qualifizierten Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter
- Alle Betreiber kritischer Anlagen (KRITIS)
- Alle Einrichtungen öffentlicher Verwaltung der Regierung
- Großunternehmen, die den Sektoren mit hoher Kritikalität angehören
- Mittlere Unternehmen, die TK-Netze oder -Dienste anbieten

B) Wichtige Einrichtungen
- Alle Anbieter von Vertrauensdiensten (Trust Services)
- Alle Mittleren und Groß-Unternehmen, die irgendeinem der genannten Sektoren angehören.

Generell gelten die meisten gesetzlichen Vorgaben für alle wichtigen und besonders wichtigen Einrichtungen. Innerhalb des Gesetzes gibt es jedoch an der einen oder anderen Stelle unterschiedliche Regelungen und Vorgaben für diese beide Sparten. Insbesondere gibt es bei den möglichen Bußgeldern durchaus Unterschiede.

Unabhängig davon gilt die KRITIS-Verordnung für kritische Einrichtungen, die im BSI-Gesetz verankert sind und deren dort festgelegten Schwellenwerte. Dieses wird durch das KRITIS-Dachgesetz entsprechend erweitert.

Für strafverfolgende Behörden und die Justiz gelten diese Einordnungen nicht.

In den Entwürfen des Bundesministeriums finden sich teilweise Abweichungen von der EU-Regelung. D.h. die nationale endgültige gesetzliche Umsetzung birgt vielleicht die eine oder andere Überraschung. Letztendlich muss jedoch davon ausgegangen werden, dass die EU-Richtlinie als Mindeststandard durchgesetzt wird.

3.2 Registrierungspflicht

Betroffene Einrichtungen, Unternehmen und Institutionen müssen sich selbst registrieren, wenn NIS2-Regelungen auf sie zutreffen. Dazu müssen unter anderem Kontaktdaten genannt werden, über diese die Einrichtung jederzeit erreichbar ist. Die Registrierung muss bis Januar 2025 erfolgen.

3.3 Durchführen von Risikoanalysen

All-Gefahren-Ansatz: Gefährdungen können technisch bedingt sein, aber auch durch menschliches Versagen, durch Naturkatastrophen oder gar durch vorsätzliche Handlungen herbeigeführt werden.

Einrichtungen müssen eine Risikoanalyse ihrer Institution durchführen. Diese muss die Auswirkungen jeglicher Gefahren auf die Erbringung der Leistungen bewerten. Dabei sollen folgende Parameter berücksichtigt werden:

- Größe der Einrichtung
- Risikoexposition der Einrichtung
- Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen
- Schwere von Sicherheitsvorfällen
- Gesellschaftliche und wirtschaftliche Auswirkungen

Anhand der Risikoanalysen müssen geeignete technische, operative und organisatorische Maßnahmen ergriffen werden, die den bestehenden Risiken angemessen sind.

3.4 Umsetzung von Maßnahmen aus der Risikoanalyse und den allgemeinen Standards

Maßnahmen, die auf Basis der Risikoanalyse beschlossen worden sind, müssen umgesetzt werden. Weiterhin müssen Mindest-Standards umgesetzt werden. Diese umfassen:

- Konzepte zur Risikoanalyse

- Konzepte zur Sicherheit der Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Backup-Management
- Wiederherstellung nach einem Notfall
- Krisenmanagement
- Sicherheit der Lieferketten
- Erwerb, Entwicklung und Wartung von Informations- Systemen und -Infrastruktur
- Management und Offenlegung von Schwachstellen
- Bewertung von Risikomanagementmaßnahmen zur Cybersicherheit
- Cyberhygiene
- Schulungen zur Cybersicherheit
- Kryptografie, gesicherte Übertragung
- Personal
- Zugriffskontrolle
- MFA

In allen Fällen muss der Stand der Technik umgesetzt werden. Sämtliche Aufwendungen müssen im Verhältnis zu den Folgen eines Ausfalls stehen.

3.5 Nachweispflicht

Alle diese Institutionen müssen alle 3 Jahre nach Inkrafttreten des Gesetzes einen Nachweis erbringen, wie sie der Umsetzung der gesetzlichen Pflichten nachkommen (Risikoanalysen und Maßnahmenpläne).

Der Nachweis kann durch Audits, Zertifizierungen oder Prüfungen erfolgen. Die Ergebnisse müssen gemeldet werden. Dabei sind auch Sicherheitsmängel oder noch nicht umgesetzte Maßnahmen zu dokumentieren. Eine Spezifikation, wie ein solcher Nachweis aussehen kann, erfolgt außerhalb der gesetzlichen Grundlage durch das BMI. Im Diskussionspapier wird abweichend von der EU-Regelung nicht von einem MUSS gesprochen, sondern davon, dass die verantwortliche Stelle (BSI) einen Nachweis einfordern KANN. Hier wird es sicherlich noch Anpassungen geben.

Dabei behält sich das BMI vor, für besonders wichtige Unternehmen ein unabhängiges Prüfverfahren in Kraft zu setzen (entsprechend den Hinweisen aus NIS2) oder eigene Kontrollen durchzuführen.

3.6 Meldung von Sicherheitsvorfällen

Alle von NIS2 betroffen Institutionen müssen erhebliche Sicherheitsvorfälle melden. Die Gesetzesentwürfe sehen eine Meldung an das BSI vor, das wiederum die Vorfälle an die entsprechende EU-Organisation melden muss.

Eine Meldung erfolgt in mehreren Stufen.

- Innerhalb von 24 Stunden nach Detektion müssen erhebliche Sicherheitsvorfälle gemeldet werden
- Spätestens nach 72 Stunden muss die Meldung aktualisiert werden
- Spätestens nach 1 Monat muss eine Abschlussmeldung erfolgen
- Sollte ein Vorfall noch nicht abgeschlossen sein, ist so lange monatlich eine Folgemeldung abzugeben, bis der Abschluss erfolgt ist. Danach muss eine Abschlussmeldung abgegeben werden

Erhebliche Sicherheitsvorfälle sind

a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung
b) erhebliche materielle oder immaterielle Schäden von anderen natürlichen oder juristischen Personen

Zu beachten ist hierbei, dass nicht nur dann eine Meldung zu erfolgen hat, wenn ein Schaden entsteht, sondern auch, wenn einer entstehen könnte.

3.7 Drastische Strafen bei Verstößen gegen Vorgaben oder gegen die Meldepflicht

NIS 2 gibt bereits einen Rahmen vor, wie Verstöße zu ahnden sind. Dabei geht es vor allem um die Umsetzung der Risikomaßnahmen und die Meldepflicht bei erheblichen Sicherheitsvorfälle.

Weiterhin wird unterschieden, ob eine besonders wichtige oder eine wichtige Einrichtung einen Verstoß begangen hat und ob ein Verstoß schwerwiegend ist.

Schwerwiegende Verstöße sind:

- wiederholte Verstöße
- eine unterlassene Meldung
- eine unterlassene Behebung von erheblichen Sicherheitsvorfällen
- eine Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden
- die Behinderung von Prüfungen oder Überwachungstätigkeiten
- Übermittlung falscher oder grob verfälschender Informationen

Verstöße können je nach Schwere mit drastischen Geldstrafen geahndet werden.

Bei besonders wichtigen Unternehmen kann die Strafe bis zu 10 Mio. Euro oder 2% des Jahresumsatzes betragen. Bei wichtigen Einrichtungen liegt die Höchstgrenze immerhin noch bei 7 Mio. Euro oder 1,4% des Jahresumsatzes. Es gilt der jeweils höhere Betrag.

3.8 Zusammenarbeit der nationalen und internationalen Cyber-Einrichtungen wird gestärkt

Letztendlich sieht die EU-Richtlinie eine stärkere Zusammenarbeit der Cyber-Einrichtungen der nationalen und internationalen Behörden vor. Ein Informationsaustausch, die länderübergreifenden Meldungen und gemeinsame Vereinbarungen und Orientierungshilfen werden explizit gefördert.

4. Fristen, Termine

Die Termine, Fristen und andere Daten finden Sie hier nochmals in tabellarischer Form.

14.12.2022	Veröffentlichung der EU-Richtlinie NIS2
16.01.2023	Inkrafttreten der Richtlinie NIS2 und Ablösung der bisherigen Regelungen
01.03.2024	Bekanntgeben der nationalen Gesetzesänderungen durch die Bundesregierung, damit die Unternehmen noch 6 Monate Zeit für die Umsetzung haben
01.10.2023	Ziel-Datum des KRITIS-DachG und der daraus resultierenden Gesetzes-Änderung in Deutschland
18.10.2024	Späteste Umsetzungspflicht von NIS2 durch die nationalen Gesetzgebungen in allen Mitgliedsstaaten
18.10.2024	Start der Meldepflicht für Informationssicherheitsvorfälle für alle betroffenen Unternehmen
18.01.2025	Abschluss der Registrierung – bis dahin müssen sich alle betroffenen Unternehmen beim BSI registriert haben
17.04.2025	Zieldatum bis zu dem alle Nationen alle betroffenen Unternehmen zentral melden müssen
Frühestens Oktober 2026	Bzw. 3 Jahre nach Inkrafttreten des deutschen Gesetzes bzw. danach alle 3 Jahre: Nachweis der Betreiber kritischer Anlagen über Gesetzes-Konformität
Noch zu definierender Zeitpunkt	Und danach alle 2 Jahre: Nachweis aller Betreiber über Gesetzes-Konformität

5. Meinung

Analog der DSGVO und der KRITIS-Verordnung (NIS) setzt die EU mit NIS2 neue Maßstäbe bei der Abwehr von Cyber-Bedrohungen und der Festigung der Informationssicherheit. Immer mehr wird klar, dass die Welt von der gelegten digitalen Basis mehr und mehr abhängig ist. Eine Erschütterung der Grundfesten unserer Gesellschaft mit katastrophalen Auswirkungen auf unser Leben sowohl in wirtschaftlicher als auch in sozialer und ökologischer Hinsicht kann durch erhebliche Störungen der Informations-Infrastrukturen erfolgen.

Es ist dringend notwendig, für ein Umdenken zu sorgen. Vergleichbar mit der Einführung der Helmpflicht beim Motorradfahren und der Gurtpflicht beim Autofahren werden viele Unternehmungen umdenken müssen. Die Risiken und Gefahren betreffen nicht nur die Unternehmen selber, sondern auch die Strukturen in deren Umfeld, z.B. Geschäftspartner, Zulieferer, Leistungsempfänger. Und hier ist die Gesellschaft verwundbar.

Deutschland versucht, zusammen mit den Wirtschaftsvertretern eine gesetzliche Regelung zu finden, die NIS2 im Kern abdeckt. Bei den ersten Entwürfen fällt aber auf, dass man versucht die Umsetzung möglichst abzufedern. Zum einen bekommen die Unternehmen für die Umsetzung sehr viel Zeit, zum anderen sind Kontrollen für Registrierungen und Meldepflichten nicht konkret vorgesehen. Das birgt generell die Gefahr, dass die gesetzlichen Regelungen nicht ernst genommen oder gar nicht wirklich wahrgenommen werden. Andererseits besteht das Risiko, dass analog dem Inkrafttreten der DSGVO Abmahnvereine wie Geier ihre Kreise ziehen. Dies dient nicht der Sache und stärkt die Argumente der Sicherheits-Gegner.

NIS2 enthält viele gute Ansätze, ist jedoch in Teilen sehr schwammig formuliert und zumindest für die deutsche Rechtsprechung oft nicht konkret genug. Viele Artikel und Absätze sind mit einem „kann“ formuliert. Das ermöglicht in manchem Falle eine besondere Handlungsfähigkeit, ist aber dadurch auch strittig.
Eine zu lasche Umsetzungs-Politik der Länder wird aber als mangelhafte Handlungskompetenz anzusehen sein und damit mittelfristig zu einer Verschärfung der Regelungen (NIS3) führen.

Vielleicht gilt hier auch die alte Wahrheit, dass man nur warten muss, bis etwas Schwerwiegendes passiert und dann die Rufe kommen „warum hat man hier nicht mehr gemacht“.

Über advisio

Das Team der advisio GmbH besteht aus kompetenten Mitarbeitern, die langjährige Erfahrung im Informationssicherheits-Umfeld, im Datenschutz, bei Digitalisierung und weiteren Betriebsprozessen haben.

Der Aufbau eines Informationssicherheitsmanagement-Systems (ISMS), wie auch durch NIS2 gefordert, gehört zu unseren Kernkompetenzen. Business Impact Analysen, Risikoanalysen, Erstellung von Maßnahmenplänen, Schulungen und Notfallplanung werden auf Wunsch durch unsere Fach-Spezialisten durchgeführt. Dies nicht nur im Aufbau, sondern auch im Betrieb eines ISMS. Durch entsprechende Zertifizierungen können wir Sie bei Bedarf bis zur ISO-Zertifizierung nach 27001:2022 oder anderen Standards führen.

Wenn Sie nicht sicher sind, ob Sie von NIS2 betroffen sind, unterstützt die advisio Sie bei der Feststellung. Vereinbaren Sie gerne einen unverbindlichen Beratungstermin.

Über den Autor

Martin Zeyer ist Diplom Informatiker und Spezialist für Informationssicherheit und IT-Service Management.
Seit Anfang der 1990 Jahre beschäftigt Herr Zeyer sich mit Themen der Informationssicherheit und dem IT-Servicemanagement und begleitet namhafte Unternehmen verschiedener Branchen – u.a. Mercedes Benz, T-Systems International GmbH, SPIRIT/21 AG.
Den defacto Standard ITIL begleitet Martin Zeyer als Experte bereits seit frühen Versionen. Bereits frühzeitig spezialisierte sich Herr Zeyer zudem auf Managementsysteme für Informationssicherheit nach verschiedenen Standards wie der internationalen Norm ISO/IEC 27001 und dem BSI-Grundschutz.
Über Jahre dozierte Herr Zeyer an der Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen (HfWU) zur Wirtschaftsinformatik.