NIS2 bringt die CyberSicherheits-Anforderungen der kritischen Infrastruktur in den Mittelstand

Teil 1 von 4: Die Grundlagen

1. Was ist NIS2?
2. Welche Ziele verfolgt NIS2?
3. Was genau bedeutet NIS2 für den Mittelstand?
4. Wie sehen die gesetzlichen Erwartungen aus?
5. Warum ist NIS2 für Geschäftsführer kritisch?

Christian Kreß

Externer Informationssicherheits-beauftragter (ISB) und CyberSicherheits Coach

INOVASEC GmbH
Christian Kreß
In den Obergärten 28
63329 Egelsbach

E-Mail: christian.kress@inovasec.de
Tel: +49 6103 8038055
Mobil: +49 1520 9276920
Web: www.inovasec.de

NIS2 ist ein Kooperations- und Kommunikationsprojekt

Begriffsabgrenzung

- **Datenschutz**
  schützt nicht die Daten, sondern die Betroffenenrechte. Der Daten-schutzbeauftragte (DSB) bringt oft einen juristischen Hintergrund mit.
- **IT-Sicherheit**
  Schützt die eigene IT-Infrastruktur, z.B. Windows durch Virenscanner und Patchmanagement oder das Netzwerk durch eine Firewall
- **Informationssicherheit**
  Schützt Unternehmensdaten und Geschäftsprozesse und hilft somit, die Lieferfähigkeit und die Digitalisierungsziele zu erfüllen
- **CyberSicherheit**
  Erweitert die **Informationssicherheit** um mobile Dienste, Cloud-Angebote und Vernetzungen mit Kunden und Lieferanten. Die Informationssicherheit wir auf den „CyberRaum“ ausgedehnt.

Was ist NIS2?

Die erste EU-Richtline aus einer ganzen Serie

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022

Über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union,
zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (Text von Bedeutung für den EWR)

NIS2 steht für Network and Information Security 2. Es handelt sich um eine neue Cybersicherheits-Richtlinie der EU.

… wie Datenschutz auf Extasy

Quelle: https://lexparency.de/eu/32022L2555/

Welche Ziele verfolgt NIS2?

Der Kern von NIS2

Das neue NIS2-Gesetz …

- ist für alle EU-Mitgliedstaaten verbindlich
- ist für Deutschland eine Konsolidierung der bestehenden KRITIS- und BSI-Gesetze
- ist eine systematische und umfangreiche Erweiterung der bestehenden KRITIS-Anforderungen auf weitere Zielgruppen und Unternehmen
- ist das erste Gesetz, das sehr konkrete Vorgaben auch für den Mittelstand definiert
- bedeutet eine massive Erweiterung der BSI-Kompetenzen
- ist am 16.01.2023 in der EU in Kraft getreten
- ist ab **Oktober 2024 als deutsches Gesetz verpflichtend**.

Kritische Infrastrukturen (**KRITIS**) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

BSI ist die Abkürzung vom Bundesamt für Sicherheit in der Informations-Technik.

NIS2UmsuCG NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz als 2. Referentenentwurf des **BMI** (Bundesministerium des Innern und für Heimat)

Erste Reaktionen auf das Gesetz

Handelsblatt 16.01.2023

IT-SICHERHEIT

„Kaum zu bewältigen“: Neue EU-Richtlinie für Cybersicherheit setzt Unternehmen unter Zeitdruck

Ob Energieversorger, Onlinemarktplätze, Konzerne oder Mittelständler: Unternehmen müssen auf Geheiß der EU mehr für Cybersicherheit tun. Die Frist ist knapp.

Was genau bedeutet NIS2 für den Mittelstand?

Welche Unternehmen sind „eingeladen“?

NIS2:
ANHANG II — **SONSTIGE KRITISCHE SEKTOREN**

>50 Mitarbeiter, >10 Mio. Euro Umsatz **(Artikel 2 des Anhangs der Empfehlung 2003/361/EG)**

Artikel 2

Mitarbeiterzahlen und finanzielle Schwellenwerte zur Definition der Unternehmensklassen

(1) Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.

(2) Innerhalb der Kategorie der KMU wird ein kleines Unternehmen als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.

(3) Innerhalb der Kategorie der KMU wird ein Kleinstunternehmen als ein Unternehmen definiert, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet.

Wichtige und besonders wichtige Einrichtungen

Das **NIS2UmsuCG** spricht überwiegend von **wichtigen Einrichtungen** und von **besonders wichtigen Einrichtungen**.

Unternehmen	Mitarbeiter		Umsatz		Bilanz
Mittlere Unternehmen	50-249	**und**	< 50 Mio. EUR	oder	< 43 Mio. EUR
Großunternehmen	≥ 250	**oder**	≥ 50 Mio. EUR	oder	≥ 43 Mio. EUR

Quellen: NIS2UmsuCG/www.openkritis.de

Wie genau ist der Mittelstand betroffen?

Quelle: NIS 2, Anhang II, z.B. Absatz 5

Verarbeitendes Gewerbe/Herstellung von Waren

a) Herstellung von Medizinprodukten und In-vitro-Diagnostika
b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
c) Herstellung von elektrischen Ausrüstungen
d) Maschinenbau
e) Herstellung von Kraftwagen und Kraftwagenteilen
f) sonstiger Fahrzeugbau

ca. 29.000 zusätzliche Unternehmen alleine in Deutschland!
NIS2 ist ein Kooperations- und Kommunikationsprojekt!

Wie sehen die gesetzlichen Erwartungen aus?

Was bedeutet NIS2 für die Unternehmen?

Mittelstand

Pflicht	KRITIS-Betreiber	Betreiber kritischer Anlagen	Besonders wichtige Einrichtung	Wichtige Einrichtung
Geltungsbereich		Anlage(n)	Unternehmen	Unternehmen
Maßnahmen (Risikomanagement) §30		✓	✓	✓
Höhere Maßstäbe §30 (3)		✓		
Besondere Maßnahmen (SzA) §39		✓		
Registrierung §32 §33		✓	✓	✓
Meldepflichten §31		✓	✓	✓
Nachweise §34		*	✓	
Informationsaustausch §35 §36		*	✓	✓
Governance Leitungsorgane §38		*	✓	✓

* - implizit, da Betreiber kritischer Anlagen auch besonders wichtige Einrichtungen sind

Quelle: NIS2UmsuCG/www.openkritis.de

§ 30 Risikomanagementmaßnahmen (Auszug)

(1) Besonders wichtige Einrichtungen und **wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu verhindern oder möglichst gering zu halten.**

Oder kürzer: „ISMS einführen!“
(kommt in Teil 3)

(2) Maßnahmen nach Absatz 1 sollen den **Stand der Technik** einhalten und unter Berücksichtigung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe der Einrichtung oder des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen.

Quelle: NIS2UmsuCG

https://www.teletrust.de/publikationen/broschueren/stand-der-technik/
Aktuell von 05/2023

§30, Abs. 4 Risikomanagementmaßnahmen

Was sind die Erwartungen an die Unternehmen?

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
2. **Bewältigung von Sicherheitsvorfällen**
3. Aufrechterhaltung des Betriebs, wie Backup-Management und **Wiederherstellung nach einem Notfall**, und Krisenmanagement
4. **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Quelle: NIS2UmsuCG

Wie formuliert das aktuelle BSI-Gesetz die Kernbereiche der CyberSicherheit?

1. Information Security Management System (ISMS)
2. Asset Management
3. Continuity- und Notfallmanagement
4. Technische Informationssicherheit
5. Personelle und organisatorische Sicherheit
6. Bauliche/physische Sicherheit
7. Vorfalls Erkennung und -bearbeitung
8. Überprüfung im laufenden Betrieb
9. Lieferanten, Dienstleister und Dritte
10. Branchenspezifische Technik und (Kern-)Komponenten

Risiko Management

IT-Sicherheit

Betrifft auch IT-Partner und Cloud-Anbieter

B3S Branchenspezifische Sicherheitsstandards

Quelle:
Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG, Anhang E

§ 31 Meldepflichten

(1) Besonders wichtige Einrichtungen und **wichtige Einrichtungen** übermitteln dem Bundesamt über eine vom Bundesamt im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Meldemöglichkeit:

1. unverzüglich, spätestens jedoch innerhalb von **24 Stunden** nach Kenntniserlangung von einem **erheblichen Sicherheitsvorfall**, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

2. unverzüglich, spätestens jedoch innerhalb von **72 Stunden** nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über den Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

4. spätestens **einen Monat** nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung

Quelle: NIS2UmsuCG

§ 32 Registrierungspflicht

(1) Besonders wichtige Einrichtungen und **wichtige Einrichtungen** sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, spätestens drei Monate nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten, dem Bundesamt die folgenden Angaben zu übermitteln:

1. der **Name der Einrichtung**, einschließlich der **Rechtsform** und soweit einschlägig der **Handelsregisternummer**,
2. die Anschrift und **aktuellen Kontaktdaten**, einschließlich **E-Mail-Adresse**, **IP-Adressbereiche** und **Telefonnummern**,
3. der relevante in der Rechtsverordnung nach § 57 Absatz 1 genannte Sektor oder soweit einschlägig Teilsektor,
4. eine **Auflistung der Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste erbringt**, die die in der in der Rechtsverordnung nach § 57 Absatz 1 genannten Einrichtungsarten erbringen.

Quelle: NIS2UmsuCG

Hier beginnt der Übergang zu §38 …

Warum ist NIS2 für Geschäftsführer kritisch?

§38 – Die Haftungsregelung für Geschäftsführer

§ 38
Billigungs- und Überwachungspflicht für Leitungsorgane von Wesentlichen Einrichtungen und Wichtigen Einrichtungen; Schulungen

(1) **Geschäftsleiter** besonders wichtiger Einrichtungen und **wichtiger Einrichtungen sind verpflichtet**, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen **Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen. Die Beauftragung eines Dritten zu Erfüllung der Verpflichtungen nach Satz 1 ist nicht zulässig.**

(2) **Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden.** Die Amtshaftung bleibt unberührt.

(3) **Ein Verzicht der Einrichtung auf Ersatzansprüche nach Absatz 2 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam.** Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

(4) Die **Geschäftsleiter von** Wesentlichen Einrichtungen und **Wichtigen Einrichtungen müssen** und deren Mitarbeiter sollen **regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.**

Quelle: NIS2UmsuCG

§ 59 Sanktionsvorschriften

(6) Handelt es sich bei dem Betroffenen um eine **wichtige Einrichtung** kann die Ordnungswidrigkeit in den Fällen der Absätze 2 Nummern 2 und 8 mit einer Geldbuße **bis zu 7 Millionen Euro** oder mit einem Höchstbetrag von **mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes** des Unternehmens, dem der Betroffene angehört, in den Fällen des Absatzes 2 Nummern 3, 5 und 9 mit einer **Geldbuße bis zu fünfhunderttausend Euro** und in dem Fall des Absatzes 2 Nummern 7, 14 und 15 mit einer **Geldbuße bis zu einhunderttausend Euro** geahndet werden.

Quelle: NIS2UmsuCG

Hinweis: Die Sanktionsvorschriften im kommenden Cyber Resilience Act (CRA) liegen aktuell noch darüber.

NIS2 ist ein Kooperations- und Kommunikationsprojekt

- **Teil 1 von 4: Die Grundlagen** 
- Teil 2 von 4: Die Hintergründe (persönliche Einschätzung)
- Teil 3 von 4: Die allgemeine Lösung für NIS2
- Teil 4 von 4: Eine konkrete Lösung für den Mittelstand