PDVSYSTEME
Industrial IT

PDV Factsheet

Navigieren Sie sicher durch die NIS 2-Welt.

Worum geht es?

NIS 2 steht für die EU-Richtlinie zur **N**etzwerk- und **I**nformations**S**icherheit (**N**etwork and **I**nformation **S**ecurity). Das **Ziel** von NIS 2 ist es, ein **hohes Cybersicherheitsniveau innerhalb der Europäischen Union sicherzustellen** und damit das **Funktionieren des europäischen Binnenmarktes zu verbessern.** Alle EU-Mitgliedstaaten müssen NIS 2 bis zum 17. Oktober 2024 in nationales Recht überführen. Dabei ist der **in der Richtlinie vorgegebene Rahmen die Mindestanforderung**, die jeder Mitgliedstaat umsetzen muss. **Höhere Anforderungen können im nationalen Recht umgesetzt werden.**

In **Deutschland** wird NIS 2 durch das **„NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz" (NIS2UmsuCG)** umgesetzt. Stand heute (30.07.2024) ist das Gesetz noch nicht verabschiedet, der aktuelle Regierungsentwurf ist vom 24.07.2024.

Alle folgenden Informationen basieren auf diesem Entwurf.

Ihr Ansprechpartner
Hagen Gerlach
Product Manager Services

+49 5321 3703-69
hagen.gerlach@pdv-systeme.de

1. Wen betrifft es?

Im Entwurf des NIS2UmsuCG finden sich die beschriebenen Regelungen in den § 28 und § 29

Deutschlandweit betrifft es schätzungsweise zwischen ~ 24.000 und 40.000 Unternehmen. Das Gesetz unterteilt die betroffenen Betriebe in „besonders wichtige und wichtige Einrichtungen“. Die folgende Tabelle zeigt welche Einrichtungen vom NIS2UmsuCG betroffen sind und ob sie als wichtig oder besonders wichtig eingestuft werden:

Tabelle 1 - Besonders wichtige und wichtige Einrichtungen

Besonders wichtige Einrichtungen sind	Wichtige Einrichtungen sind
alle **Betreiber kritischer Anlagen (KRITIS)**, die bisher unter die KRITIS Regulation gefallen sind	
qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter	**Vertrauensdiensteanbieter**
Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze mit	
mindestens 50 Beschäftigten oder einem **Jahresumsatz und** einer **Jahresbilanzsumme von mindestens 10 Millionen €.**	weniger als **50 Beschäftigten** und einem **Jahresumsatz und** einer **Jahresbilanzsumme** von **jeweils 10 Millionen € oder weniger.**
Bundesverwaltungseinrichtungen, konkret: **Bundesbehörden, öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung, weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Ihre Vereinigungen auf Bundesebene**, soweit durch das Bundesamt im Einvernehmen mit dem zuständigen Ressort angeordnet.	
Einrichtungen, die **in Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen** zum NIS2UmsuCG aufgeführt sind und	
und **mindestens 250 Beschäftigte** oder **einen Jahresumsatz von über 50 Millionen € und eine Jahresbilanzsumme von über43 Millionen € haben (ausgenommen Einrichtungen der Bundesverwaltung)**	und **50 bis 249 Beschäftigte** oder **einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen € haben (ausgenommen Einrichtungen der Bundesverwaltung)**
	Einrichtungen, die **in Anlage 2 Sektoren wichtiger Einrichtungen** zum NIS2UmsuCG aufgeführt sind und mindestens **50 Beschäftigte oder eine Jahresumsatz- und Jahresbilanzsumme > 10 Millionen € haben**

Die Anlagen 1 und 2 enthalten zusammen 13 Sektoren, welche teilweise weiter in Branchen und Einrichtungsarten aufgeschlüsselt sind.
Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in Anlage 1 und Anlage 2

Sektoren in Anlagen 1 und 2

Anlage 1 - 1 Sektoren besonders wichtiger und wichtiger Einrichtungen

Besonders wichtig, wenn:
mindestens 250 Beschäftigte oder **ein Jahresumsatz von über 50 Millionen € und eine Jahresbilanzsumme von über 43 Millionen €**

Wichtig, wenn:
50 bis 249 Beschäftigte oder **ein Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen €**

ENERGIE
- Stromversorgung
- Fernwärme und -kälteversorgung
- Kraftstoff- und Heizölversorgung
- Gasversorgung

TRANSPORT UND VERKEHR
- Luftverkehr
- Schienenverkehr
- Schifffahrt
- Straßenverkehr

FINANZ- UND VERSICHERUNGSWESEN
- Bankwesen
- Finanzmarktinfrastrukturen

GESUNDHEIT
- Erbringer von Gesundheitsdienstleistungen
- EU-Referenzlaboratorien
- Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel ausüben
- Unternehmen, die pharmazeutische Erzeugnisse herstellen
- Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden

WASSER
- Trinkwasserversorgung
- Abwasserbeseitigung

WELTRAUM
- Betreiber von Bodeninfrastrukturen

INFORMATIONSTECHNIK UND TELEKOMMUNIKATION
- Betreiber von Internet Exchange Points
- DNS-Dienstanbieter, ausgenommen Betreiber von Root-Nameservern
- Top Level Domain Name Registry
- Anbieter von Cloud-Computing-Diensten
- Anbieter von Rechenzentrumsdiensten
- Betreiber von Content Delivery Networks
- Vertrauensdienstanbieter
- Anbieter öffentlicher elektronischer Kommunikationsnetze
- Anbieter öffentlich zugänglicher elektronsicher Kommunikationsdienste
- Managed Services Provider
- Managed Security Services Provider

Anlage 2 - Sektoren wichtiger Einrichtungen

Wichtig, wenn:
mindestens **50 Beschäftigte oder eine Jahresumsatz- und Jahresbilanzsumme > 10 Millionen € haben**

TRANSPORT UND VERKEHR
- Post und Kurierdienste

ABFALLBEWIRTSCHAFTUNG
- Unternehmen der Abfallbewirtschaftung

PRODUKTION, HERSTELLUNG UND HANDEL MIT CHEMISCHEN STOFFEN

VERARBEITENDES GEWERBE/ HERSTELLUNG VON WAREN
- Herstellung von Medizinprodukten und In-vitro-Diagnostika
- Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
- Maschinenbau
- Herstellung von Kraftwagen und Kraftwagenteilen
- Sonstiger Fahrzeugbau

PRODUKTION, VERARBEITUNG UND VERTRIEB VON LEBENSMITTELN

FORSCHUNG

ANBIETER DIGITALER DIENSTE
- Anbieter von Online-Marktplätzen
- Anbieter von Online-Suchmaschinen
- Anbieter von Plattformen für Dienste sozialer Netzwerke

Die **Unterteilung** hat **keine** direkten **Auswirkungen auf** die **Anforderungen** an die Einrichtungen. Dies **bedeutet**, dass **grundsätzlich alle Betriebe** die **gleichen Anforderungen erfüllen** müssen.

Ausnahmen gibt es auch, insbesondere für (§ 29):

- Einrichtungen der Bundesverwaltung
- Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz

und z.B. für folgende Einrichtungen (§ 28)

- Telekommunikationsanbieter, die den Regelungen des Telekommunikationsgesetzes unterliegen
- Betreiber von Energieversorgungsnetzen oder Energieanlagen, die den Regelungen des §5c des Energiewirtschaftsgesetzes unterliegen
- bestimmte Finanzunternehmen
- die Gesellschaft für Telematik
- Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Vertrauensdienstean-bieter, Managed Service Provider und Managed Security Services Provider

3. Was ist zu tun?

3.1. Identifizieren & Registrieren

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 33

Vom NIS2UmsuCG betroffene Einrichtungen müssen sich selbst als solche identifizieren und sich dann innerhalb von drei Monaten bei einer noch nicht festgelegten Registrierungsstelle des Bundesamtes für Sicherheit in der Informationstechnik (BSI) registrieren und folgende Angaben machen:

- Name, Rechtsform und Handelsregisternummer
- Anschrift, aktuelle Kontaktdaten, öffentliche IP-Adressbereiche
- Relevanter Sektor oder einschlägige Branche (aus Anlage 1 oder 2)
- Auflistung der EU-Staaten, in denen die Einrichtung entsprechende Dienste erbringt
- Die für die Tätigkeiten zuständigen Aufsichtsbehörden des Bundes und der Länder

Betreiber kritischer Anlagen müssen zusätzlich folgende **Angaben** machen:

- Kritische Dienstleistung
- Öffentliche IP-Adressbereiche der Anlagen
- Anlagenkategorie
- Ermittelte Versorgungskennzahlen
- Standorte der Anlagen
- Eine Kontaktstelle

und **außerdem sicherstellen, dass sie über die genannte Kontaktstelle jederzeit erreichbar sind.**

Das BSI kann wichtige und besonders wichtige Einrichtungen auch selbst registrieren, wobei die Einrichtungen dann verpflichtet sind, die erforderlichen Angaben zu machen.

Änderungen der Angaben müssen spätestens zwei Wochen nach Bekanntwerden der Änderungen übermittelt werden. Änderungen der Versorgungskennzahlen müssen nur einmal jährlich gemeldet werden.

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 34 und § 60

Bestimmte Einrichtungen (DNS-Diensteanbieter, Top Level Domain Name Registries, Domain Name Registry Anbieter, Anbieter von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke) **die Ihre Dienste in der EU anbieten und ihre Hauptniederlassung in der Bundesrepublik Deutschland haben müssen dem BSI innerhalb von drei Monaten**, nachdem Sie als eine dieser Einrichtungen gelten, **die entsprechenden Angaben und die Anschrift der Hauptniederlassung in der EU, oder eines benannten Vertreters mitteilen.**

3.2. Risikomanagementmaßnahmen umsetzen

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 30 und § 31

Besonders wichtige und wichtige Einrichtungen müssen angemessene, verhältnismäßige und wirksame Risikomanagementmaßnahmen ergreifen, um IT-Störungen zu verhindern und die Auswirkungen von Sicherheitsvorfällen zu minimieren. Dabei sind das Risiko, die Größe der Einrichtung, die Kosten der Maßnahmen sowie die Wahrscheinlichkeit und Schwere von Vorfällen und deren gesellschaftliche und wirtschaftliche Folgen zu berücksichtigen.

Die Maßnahmen sollen dem **Stand der Technik** entsprechen und **einschlägige Normen** berücksichtigen und auf einem **gefahrenübergreifenden Ansatz** beruhen.

Das **NIS2UmsuCG verpflichtet** dazu **mindestens folgende Maßnahmen umzusetzen:**

- ☑ Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
- ☑ Bewältigung von Sicherheitsvorfällen
- ☑ Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und 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 informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- ☑ Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- ☑ grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
- ☑ Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- ☑ Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das 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.

Die Einrichtungen müssen die Einhaltung der Verpflichtung dokumentieren. Mögliche Arten der Dokumentation sind:

- Interne Richtlinien,
- Handlungsanweisungen,
- Checklisten,
- Mitarbeiterschulungen,
- Vereinbarungen,
- Merkblätter o.ä.,
- aber auch Auditberichte, Zertifizierungen oder Prüfungen.

Durch die neue **Rechtslage ergeben sich** für die bisherigen **Betreiber kritischer Anlagen zusätzliche Pflichten.** Während sie bisher „nur" für die für die Erbringung der kritischen Dienste notwendige IT-Infrastruktur besonderen Regelungen unterlagen, erweitert sich der **Anwendungsbereich** nun auf die **gesamte IT-Infrastruktur der Einrichtung.**

Für den Betrieb der kritischen Anlage gelten trotzdem weiter erhöhte Anforderungen, **Betreiber kritischer Anlagen müssen zusätzlich**

- **besondere Maßnahmen** ergreifen, um IT-Systeme, Komponenten und Prozesse, die für den Betrieb ihrer Anlagen entscheidend sind, zu schützen. Diese Maßnahmen gehen über das Schutzniveau der gesamten Einrichtung hinaus. Diese zusätzlichen Maßnahmen sind angemessen, solange die Kosten für diese Maßnahmen nicht unverhältnismäßig hoch im Vergleich zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Anlage sind.
- Systeme zur Angriffserkennung einsetzen, die Bedrohungen im laufenden Betrieb identifizieren, vermeiden und nach Eintritt von Störungen Beseitigungsmaßnahmen vorsehen.

3.3. Geschäftsleitung schulen

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 38

Die **Geschäftsleitung** von wichtigen und besonders wichtigen Einrichtungen ist **verpflichtet regelmäßig (mindestens alle drei Jahre) an Schulungen, zur Vermittlung der notwendigen Kenntnisse zu Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik teilzunehmen.** Hintergrund ist die Verantwortung der Geschäftsleitung. Mehr dazu folgt im Abschnitt: Wer ist verantwortlich?.

3.4. Sicherheitsvorfälle melden

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 32

Besonders wichtige und wichtige Einrichtungen müssen **spätestens innerhalb von 24 Stunden nachdem** ein **erheblicher Sicherheitsvorfall erkannt** wurde, eine **Erstmeldung** an eine noch einzurichtende Meldestelle übermitteln. Aus der Meldung muss hervorgehen, **ob** der **Verdacht** besteht, dass der Sicherheitsvorfall durch eine **rechtswidrige oder böswillige Handlung verursacht** wurde oder **grenzüberschreitende Auswirkungen** haben könnte.

Spätestens 72 Stunden nach Bekanntwerden des Sicherheitsvorfalls sind die Informationen aus der Erstmeldung **zu korrigieren oder zu bestätigen und** eine erste **Bewertung mit Schweregrad, Auswirkungen und ggf. den Kompromittierungsindikatoren** anzugeben.

Sofern das BSI Zwischenmeldungen über relevante Statusaktualisierungen anfordert, sind diese zu liefern.

Spätestens nach einem Monat ist eine **Abschlussmeldung** abzugeben, mit

- ausführlicher Beschreibung des Sicherheitsvorfalls mit Schweregrad und Auswirkungen
- Angaben zur Bedrohungsart und der wahrscheinlichen Ursache
- Angaben zu den ergriffenen Abhilfemaßnahmen.

Betreiber kritischer Anlagen müssen **zusätzlich** die **Art der betroffenen Anlage und kritischen Dienstleistung melden.**

3.5. Umsetzung nachweisen / prüfen

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 39 , § 61 und § 62

Bei der Nachweispflicht spielt nun die Einordnung der Einrichtung als besonders wichtiges oder wichtiges Unternehmen eine Rolle:

Besonders wichtige Einrichtungen können vom BSI oder durch vom BSI beauftragte Dritte **stichprobenartig** auf die Einhaltung der Anforderungen aus dem NIS2UmsuCG **geprüft** werden. Das BSI kann Audits, Prüfungen und Zertifizierungen durch unabhängige Stellen anordnen.

Wichtige Einrichtungen werden **nur** dann **Anlass bezogen geprüft**, wenn eine gerechtfertigte Annahme besteht, dass sie die Gesetzesanforderungen nicht oder nicht richtig umsetzen.

Der Prüfumfang betrifft in beiden Fällen die gesamte Einrichtung.

Betreiber kritischer Anlagen unterliegen zusätzlichen Prüfpflichten. Sie müssen **alle drei Jahre** in Form eines Sicherheitsaudits, einer Prüfung oder Zertifizierung die **Umsetzung der Anforderungen des NIS2UmsuCG beim BSI nachweisen.**

4. Wer ist verantwortlich?

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 38

Die **Geschäftsleitung** ist verantwortlich und verpflichtet die oben beschriebenen Risikomanagementmaßnahmen umzusetzen und zu überwachen. Das Gesetz besagt zusätzlich, dass die Geschäftsleitungsorgane für Schäden, die den Einrichtungen entstehen, weil Sie Ihren Pflichten nicht nachkommen, persönlich haftbar sind.

5. Was passiert, wenn man sich nicht kümmert?

Eine fehlende Umsetzung der Regulatorien kann verschiedene Folgen haben:

Im Entwurf des NIS2UmsuCG finden sich die detaillierten Informationen in § 65 und § 61

Mögliche Folgen sind:

- Die **Verhängung von Bußgeldern** (eine Aufstellung enthält untenstehende Tabelle)
- Und als **letztes Mittel, wenn Anordnungen** des BSIs im Rahmen von Durchsetzungsmaßnahmen nicht Folge geleistet wird:
  - Der **Entzug von Genehmigungen durch zuständige Aufsichtsbehörden**
  - die **vorübergehende Untersagung der Ausübung der Tätigkeit als Geschäftsleitung**

bis den Anordnungen nachgekommen wurde.

Zusätzlich zu den Sanktionen und Bußgeldern kann die mangelnde Beschäftigung mit der Informationssicherheit natürlich auch ganz konkrete Folgen für die Einrichtung haben, z.B.:

- Einschränkung der Produktion / des Betriebs
- Negative Folgen auf Wirtschaft und Bevölkerung
- Verlust / Diebstahl von Daten
- Rufschädigung
- Finanzielle Verluste

Bußgeldhöhe bis zu	Betreiber kritischer Anlagen	besonders wichtige Einrichtungen	wichtige Einrichtungen
€ 10 Millionen oder bei Umsatz > 500 Millionen € 2% des Jahresumsatzes	• Missachtung der Unterrichtungspflichten (aus § 35) • Maßnahmen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ergreift (aus § 30) • Fehlende Dokumentation (aus § 30) • Meldungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt (aus § 32) • eine Abschlussmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht (aus § 32)		
€ 7 Millionen oder bei Umsatz > 500 Millionen € 1,4 % des Jahresumsatzes			• Missachtung der Unterrichtungspflichten (aus § 35) • Maßnahmen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ergreift (aus § 30) • Fehlende Dokumentation (aus § 30) • Meldungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt (aus § 32) • eine Abschlussmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht (aus § 32)
€ 2 Millionen – und Anwendung des Gesetzes über Ordnungswidrigkeiten (OWiG § 30(2) 3)	• Falsche oder unvollständige Vorlage eines Nachweises über eine erfolgte Mängelbeseitigung (§39)	• Nur **Hersteller von ITK-Systemen:** Verweigerung der Mitwirkung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit (§ 11) • Nur **Anbieter von Telekommunikationsdiensten** und **Anbieter von Telemediendiensten:** Verweigerung der Mitwirkung bei der Abwehr erheblicher Gefahren (§16 und § 17)	
€ 1 Million – und Anwendung des Gesetzes über Ordnungswidrigkeiten (OWiG § 30(2) 3)	• Fehlende oder falsche Vorlage der Nachweise über Erfüllung der Anordnungen (§39)		

Bußgeldhöhe bis zu	Betreiber kritischer Anlagen	besonders wichtige Einrichtungen	wichtige Einrichtungen
€ 500.000	• Verweigerung der Herausgabe der zur Bewältigung der Störung notwendigen Informationen (§ 40) • Mangelnde Sicherstellung der Erreichbarkeit über die Kontaktstelle (§ 33)	• Verweigerung der Vorlage von Nachweisen (§ 63, § 64) • Verweigerung der Umsetzung angeordneter Maßnahmen (§ 63, § 64) • Verweigerung der Veröffentlichung von Informationen (§ 63, § 64)	
	• Nur **Hersteller von IKT-Produkten:** Verweigerung der Mitwirkung bei der Beseitigung oder Vermeidung erheblicher Sicherheitsvorfälle ($ 18) • Missachtung der Registrierungspflichten oder Übermittlung von falschen oder unvollständigen Daten (§ 34) • Nur **Domain Name Registries:** Fehlende Vorhaltung einer Vorgabe oder eines Verfahrens im Rahmen der Pflicht zum Führen einer Datenbank (§ 51) • Nur **Domain Name Registries:** einen Zugang nicht rechtzeitig gewährt (§ 52) • Unberechtigt ein Zertifikat für Produkte Leistungen oder Personen verwendet (§ 54) • Unberechtigt eine Konformitätserklärung verwendet (§ 55) • Unberechtigt als Konformitätsbewertungsstelle tätig wird (§ 55 und § 56) • Unberechtigt ein Cybersicherheitszertifikat oder eine Konformitätserklärung verwendet (§ 56) • Unberechtigt das IT-Sicherheitskennzeichen verwendet		
€ 100.000	• Mangelnde Erreichbarkeit der Kontaktstelle (§ 33)		
	• Behinderung der Prüfung auf Einhaltung der Anforderungen, indem Dokumente nicht oder nicht rechtzeitig bereitgestellt werden, oder der Zugang zu Räumlichkeiten nicht gewährt wird (§ 63) • Falsche oder unvollständige Vorlage eines Nachweises über eine erfolgte Mängelbeseitigung (§39)		

6. Wie geht es weiter?

Der Regierungsentwurf befindet sich derzeit im Gesetzgebungsverfahren, einen konkreten Termin steht noch nicht fest. Zweifellos wird das Gesetz aber in dieser oder ähnlicher Form kommen, die Grundanforderungen sind durch die NIS 2 Richtlinie der EU vorgegeben, der Gesetzgeber kann diese nur verschärfen.
PDV-Systeme empfiehlt, sich bereits heute mit den Anforderungen zu beschäftigen, sofern dies noch nicht geschehen ist.

1. Prüfen Sie, ob Ihr Unternehmen betroffen ist. Für eine erste Einschätzung können Sie den PDV-Quick-Check oder die „NIS-2 Betroffenheitsprüfung“ des BSI nutzen. Wenn Ihre Organisation nicht direkt betroffen ist, klären Sie ob ggf. Kunden oder Partner betroffen sind, und diese planen Anforderungen an Sie „durchzureichen“
2. Wenn Sie betroffen sind, informieren Sie Ihre Geschäftsleitung und weisen Sie sie daraufhin, dass sie für die Umsetzung und Überwachung der Risikomanagementmaßnahmen verantwortlich ist. (§ 38) und die Pflicht hat sich regelmäßig entsprechend Schulen lassen muss.
3. Bestimmen Sie zuständige Personen für die Koordinierung der Informationssicherheit in Ihrer Organisation.
4. Prüfen Sie den aktuellen Stand Ihrer Informationssicherheitsmaßnahmen dokumentieren sie diesen (falls sie das nicht sowieso schon getan haben) und gleichen Sie diesen mit den Anforderungen ab, die in NIS 2 definiert sind.
5. Beginnen Sie mit der Umsetzung von Risikomanagementmaßnahmen, die sie bisher nicht implementiert haben und dokumentieren sie dies.
6. Verfolgen Sie den Gesetzgebungsprozess informiert und berücksichtigen Sie gegebenenfalls neue Erkenntnisse. Informationen dazu finden sich auf der Website des BSI.