

HERAUSFORDERUNGEN, FALLSTRICKE UND
LÖSUNGSWEGE FÜR UNTERNEHMEN

DIE NIS-2-RICHTLINIE UND IHRE UMSETZUNG IN DEUTSCHLAND

AUTOREN PROTIVITI: ANDREJ GREINDL, CHRISTOPHER CHASSÉE
AUTOR ROBERT HALF: PHILIPP WEINGART

INHALT

1	EINLEITUNG	03
2	FÜR WELCHE UNTERNEHMEN GILT DIE NIS-2-RICHTLINIE?	04
3	WAS BEDEUTET DIE NIS-2-RICHTLINIE FÜR UNTERNEHMEN?	05
4	PRAXISPERSPEKTIVE: TYPISCHE HERAUSFORDERUNGEN BEI DER UMSETZUNG VON NIS-2	08
5	SANKTIONEN UND ERWEITERTE AUFSICHTSBEFUGNISSE UNTER NIS-2	14
6	UMSETZUNGSSTAND DER NIS-2-RICHTLINIE IN DEUTSCHLAND	14
7	FAZIT UND AUSBLICK	15
8	QUELLEN	15
9	ÜBER PROTIVITI	16
10	KONTAKTE	17

BILDVERZEICHNIS

ABBILDUNG 1: SEKTORENÜBERSICHT GEM. BSIG	04
ABBILDUNG 2: MINDESTANFORDERUNGEN DES § 30 BSIG	06

1. EINLEITUNG

Im Bestreben, einen sicheren europäischen Wirtschaftsraum zu gewährleisten, definiert die Europäische Union verbindliche Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus, die von den Mitgliedstaaten in nationales Recht zu überführen und durch zuständige Behörden durchzusetzen sind.

Treiber dieser Entwicklung sind die in den vergangenen Jahren stark zunehmenden Angriffe auf Netz- und Informationssysteme, die die EU als grenzüberschreitende Cyberbedrohungen einstuft und als erhebliches Risiko für Wirtschaft und Gesellschaft bewertet. Als „Cyberbedrohung“ gelten dabei alle Umstände, Ereignisse oder Handlungen, die Systeme, Daten oder deren Nutzer beeinträchtigen oder schädigen können. Vor dem Hintergrund einer zunehmend vernetzten und digitalisierten Wirtschaft entfalten solche Bedrohungen häufig schnell grenzüberschreitende Wirkung, wodurch Cybersicherheit zu einem zentralen Stabilitäts- und Wettbewerbsfaktor innerhalb der Europäischen Union geworden ist.

Bereits im Jahr 2016 trat die erste NIS-Richtlinie (Richtlinie (EU) 2016/1148) in Kraft. Ende 2022 wurde sie durch die „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)“ abgelöst. Ziel der neuen Richtlinie ist ein deutlich erweiterter und stärker harmonisierter Rechtsrahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Europäischen Union – insbesondere durch klar definierte Pflichten, risikobasierte Sicherheitsmaßnahmen sowie erweiterte Melde- und Aufsichtspflichten. [1]

Die Mitgliedstaaten sind verpflichtet, die NIS-2-Richtlinie in nationales Recht zu überführen. In Deutschland erfolgte dies durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“, das am 6. Dezember 2025 in Kraft trat. Bei diesem Gesetz handelt es sich um ein Artikelgesetz, das kein vollständig neues Cybersicherheitsregime schafft,

sondern bestehende Rechtsvorschriften – insbesondere das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)“ – umfassend an die Vorgaben der NIS-2-Richtlinie anpasst und erweitert. Das BSIG bleibt somit die zentrale gesetzliche Grundlage der Cybersicherheit in Deutschland. Das BSI fungiert als zentrale Stelle und maßgeblicher Adressat für Registrierung und Meldungen nach dem BSIG. Ergänzend dazu erkennt das BSIG, abhängig vom jeweiligen Sektor, weitere zuständige Aufsichtsbehörden des Bundes und der Länder an, die im jeweiligen Kontext einzubeziehen sind. [1,2]

Mit der Umsetzung der NIS-2-Richtlinie wurde der Anwendungsbereich erheblich ausgeweitet. Insgesamt betrifft sie nun nach Schätzungen des BSI rund 29.500 „wichtige“ oder „besonders wichtige Einrichtungen“.

» Nur etwa 18.000 Registrierungen bei ca. 29.500 von NIS-2 betroffenen Unternehmen verdeutlichen den kritischen Rückstand bei der Umsetzung regulatorischer Anforderungen. «

ANDREJ GREINDL, MANAGING DIRECTOR,
PROTIVITI DEUTSCHLAND



Für betroffene Unternehmen bedeutet dies, dass Anforderungen an Risikomanagement, technische und organisatorische Maßnahmen sowie Melde- und Registrierungspflichten nicht mehr nur als „Best Practice“ gelten, sondern verbindlich einzuhalten sind. Für die Erstregistrierung gilt eine gesetzliche Frist, die auf den 6. März 2026 festgelegt wurde [2,3,9].

Viele Unternehmen stehen vor der zentralen Herausforderung, regulatorische Anforderungen in konkrete, wirksame und nachhaltig verankerte Maßnahmen zu überführen.

Im Mittelpunkt dieses Whitepapers steht daher die Fragestellung, wie Unternehmen die Anforderungen der NIS-2-Richtlinie in der Praxis wirksam umsetzen können. Es beleuchtet die typischen Problemfelder, die sich bei der Überführung regulatorischer Vorgaben in operative Realität ergeben, und zeigt auf, warum viele Organisationen trotz technischer Investitionen, vorhandener Sicherheitsstrukturen und etablierter Prozesse an Grenzen stoßen. Anhand zentraler Herausforderungen und Fallstricke – von fehlender Regulierungserfahrung über projektgetriebene Umsetzungsansätze bis hin zu übermäßiger Technikorientierung, unterschätzten Lieferkettenrisiken und strukturellem Fachkräftemangel – bietet das Whitepaper eine praxisnahe Orientierung. Ziel ist es, Unternehmen dabei zu unterstützen, NIS-2 nicht nur formal zu erfüllen, sondern als strategischen Hebel für nachhaltige Cyberresilienz zu nutzen.

2. FÜR WELCHE UNTERNEHMEN GILT DIE NIS-2-RICHTLINIE?

Die NIS-2-Richtlinie definiert verbindliche Kriterien zur Einordnung betroffener Organisationen. Gemäß § 28 BSIG werden Einrichtungen anhand dieser Kriterien klassifiziert und dabei in „**besonders wichtigen Einrichtungen**“ (zu denen auch KRITIS-Betreiber gehören) und „**wichtigen Einrichtungen**“ unterteilt.

Zusätzlich wurde die Zahl der relevanten Sektoren erweitert. Das BSIG definiert, wie in Abbildung 1 dargestellt, 14 Sektoren, die in **Anlage 1 BSIG** „Sektoren besonders wichtiger und wichtiger Einrichtungen“ und **Anlage 2 BSIG** „Sektoren wichtiger Einrichtungen“ aufgeführt werden.



Abbildung 1: Sektorenübersicht gem. BSIG

Als „**besonders wichtige Einrichtung**“ gilt eine Organisation, wenn mindestens eines der folgenden Kriterien erfüllt ist:

1. Es handelt sich um einen Betreiber kritischer Anlagen.
2. Es handelt sich bei der Einrichtung um einen qualifizierten Vertrauensdiensteanbieter, eine Top-Level-Domain-Namenregistrierungsstelle oder einen DNS-Diensteanbieter.
3. Es handelt sich um Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder Betreiber von öffentlichen Telekommunikationsnetzen, die
 - a) mindestens 50 Mitarbeiter beschäftigen oder
 - b) deren Jahresumsatz und Jahresbilanzsumme jeweils > 10 Millionen Euro aufweisen.
4. Es werden Dienstleistungen oder Waren entgeltlich angeboten und das Unternehmen ist einem der in Anlage 1 BSIG aufgeführten Sektoren zuzuordnen (siehe Abbildung 1). Zusätzlich muss das Unternehmen

- a) mindestens 250 Mitarbeiter beschäftigen oder
- b) einen Jahresumsatz von über 50 Millionen Euro sowie eine Bilanzsumme von über 43 Millionen Euro erzielen.

Von den genannten Kriterien zur Einstufung als „besonders wichtige Einrichtung“ ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.

Als „wichtige Einrichtung“ werden Organisationen eingestuft, die die oben genannten Kriterien nicht erfüllen, jedoch mindestens eines der folgenden Merkmale aufweisen:

1. Es handelt sich um einen Vertrauensdienstanbieter.
2. Es handelt sich um Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder Betreiber von öffentlichen Telekommunikationsnetzen, die
 - a) weniger als 50 Mitarbeiter beschäftigen und
 - b) deren Jahresumsatz oder Jahresbilanzsumme jeweils ≤ 10 Millionen Euro betragen.
3. Es werden Dienstleistungen oder Waren entgeltlich angeboten und das Unternehmen ist einem der in Anlage 1 oder Anlage 2 BSIG aufgeführten Sektoren zuzuordnen (siehe Abbildung 1). Zusätzlich muss die Organisation
 - a) mindestens 50 Mitarbeiter beschäftigen oder
 - b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

Von den genannten Kriterien zur Einstufung als „wichtige Einrichtung“ ausgenommen sind auch hier Einrichtungen der Bundesverwaltung. [1,3]

Abgrenzung der NIS-2-Richtlinie von bereits bestehenden Regulatoriken

Gemäß § 28 BSIG sind die Anforderungen der NIS-2-Richtlinie gegenüber anderen sektorenspezifischen Regelungen abzugrenzen. Für Finanzunternehmen, die in den Anwendungsbereich des § 28 Abs. 6 BSIG fallen, gelten die Anforderungen der §§ 30 bis 32 sowie §§ 35, 36, 38 und 39 BSIG nicht, da insoweit die sektorspezifischen Vorgaben der DORA maßgeblich sind. Die Registrierungspflicht nach § 33 BSIG bleibt grundsätzlich bestehen.

Für Betreiber Kritischer Anlagen ergibt sich ebenfalls keine Ablösung, sondern eine Ergänzung bestehender Vorgaben. KRITIS-Betreiber sind eine Teilmenge der „besonders wichtigen Einrichtungen“, wodurch die Vorgaben, die sich aus der NIS-2-Richtlinie ergeben, parallel zum „Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG)“ einzuhalten sind. Dies hat zur Folge, dass Betreiber Kritischer Anlagen zum einen gemäß § 33 Abs. 1 BSIG eine Registrierung als „besonders wichtige Einrichtung“ im BSI-Portal vornehmen müssen und zum anderen gemäß § 33 Abs. 2 BSIG in Verbindung mit § 8 KRITISDachG verpflichtet sind, sich als Betreiber kritischer Anlagen zu registrieren.

Die Möglichkeit, eine gemeinsame übergeordnete Ansprechstelle (GÜAS) zu benennen, entfällt und der Nachweiszyklus von Betreiber kritischer Anlagen verlängert sich von zwei auf drei Jahre. [6,7,8]

Unabhängig von den genannten Abgrenzungen bleiben zentrale Anforderungen der NIS-2-Richtlinie bestehen, insbesondere im Bereich Risikomanagement und Governance. Für betroffene Einrichtungen ist es daher entscheidend, die jeweiligen Anforderungen systematisch zu prüfen, Überschneidungen zu identifizieren und konsistent umzusetzen.

3. WAS BEDEUTET DIE NIS-2-RICHTLINIE FÜR UNTERNEHMEN?

Die NIS-2-Richtlinie konkretisiert die Anforderungen an die organisatorische und technische Ausgestaltung der Cybersicherheit und überführt diese in verbindliche unternehmerische Pflichten.

Im Fokus stehen Vorgaben zur systematischen Risikosteuerung, zur Absicherung informationstechnischer Systeme sowie zur Sicherstellung der Resilienz geschäftskritischer Prozesse. Die einschlägigen Regelungen des deutschen Umsetzungsgesetzes, insbesondere die §§ 30 ff. BSIG, strukturieren diese Anforderungen und definieren neben materiellen Pflichten auch Vorgaben zu Nachweis-, Melde- und Aufsichtspflichten.

Risikomanagement & Sicherheitsmaßnahmen

Den materiellen Kern der Cybersicherheitsanforderungen bildet § 30 BSIG. Dieser verpflichtet Unternehmen zur Umsetzung geeigneter und ver-

hältnismäßiger technischer und organisatorischer Maßnahmen, mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Netz- und Informationssystemen sicherzustellen und Sicherheitsvorfälle zu minimieren. Die konkrete Ausgestaltung orientiert sich an Faktoren wie Risikoexposition, Unternehmensgröße, Kosten sowie potenziellen Schadensauswirkungen.

Im Zentrum des **§ 30 BSIG** steht die Einführung eines strukturierten IKT-Risikomanagements, das die Identifikation, Bewertung und Behandlung von Risiken umfasst und als Grundlage für die Auswahl geeigneter Sicherheitsmaßnahmen dient. Diese müssen sich am Stand der Technik orientieren, einschlägige Normen berücksichtigen und einem ganzheitlichen Ansatz folgen.

Konkretisiert wird dies durch einen Katalog von zehn Mindestanforderungen. Hierzu zählen insbesondere die Etablierung von Prozessen zur Erkennung, Behandlung und Nachverfolgung von Sicherheitsvorfällen sowie die Sicherstellung der Betriebsfähigkeit durch ein wirksames Business-Continuity- und Notfallmanagement einschließlich Wiederherstellungs- und Wiederanlaufkonzepten. Darüber hinaus sind Risiken entlang der Lieferkette zu berücksichtigen, insbesondere im Zusammenhang mit IKT-Drittparteien, sowie Maßnahmen zur sicheren Beschaffung, Entwicklung und Wartung von IT-Systemen umzusetzen. Ergänzend erfordert die Vorschrift die Einführung eines wirksamen Schwachstellenmanagements sowie geeignete Maßnahmen zur Sensibilisierung und Schulung von Mitarbeitenden.

Auch technische Schutzmaßnahmen sind integraler Bestandteil des Anforderungskatalogs. Dazu gehört insbesondere der Einsatz kryptografischer Verfahren, ein Identitäts- und Berechtigungsmanagement sowie die Absicherung von Netzwerken und Kommunikationssystemen, etwa durch Multi-Faktor-Authentifizierung. [5]

Die Abbildung 2 zeigt einen Überblick über die zehn Mindestanforderungen des **§ 30 BSIG**.



Abbildung 2: Mindestanforderungen des § 30 BSIG

Besondere Anforderungen für KRITIS-nahe Systeme

Für Betreiber kritischer Anlagen gelten entsprechend des **§ 31 BSIG** weitergehende Anforderungen. Kritische Systeme und unterstützende Prozesse unterliegen erhöhten Anforderungen an Ausgestaltung und Angemessenheit der Sicherheitsmaßnahmen. Zudem besteht die Verpflichtung zur Implementierung von Systemen zur Angriffserkennung, wie beispielsweise SIEM-Lösungen, um Sicherheitsvorfälle zu erkennen. [8]

Melde- & Informationspflichten bei Sicherheitsvorfällen

Neben den Sicherheitsanforderungen etabliert das Umsetzungsgesetz umfassende Melde- und Informationspflichten, die der frühzeitigen Erkennung, Bewertung und Eindämmung von Sicherheitsvorfällen dienen. Diese betreffen sowohl die Kommunikation mit Behörden als auch die Informationspflichten gegenüber Kunden und der Öffentlichkeit.

Besonders relevant ist **§ 32 BSIG**, der Unternehmen verpflichtet, erhebliche Sicherheitsvorfälle unverzüglich zu melden, sobald der entsprechende Meldeweg eingerichtet ist. Die Meldung erfolgt dabei gestuft: Innerhalb von 24 Stunden nach Kenntniserlangung ist eine Erstmeldung abzugeben, gefolgt von einer detaillierten Bewertung innerhalb von 72 Stunden. Spätestens einen Monat nach der detaillierten Übermittlung der Meldung des Sicherheitsvorfalls, ist eine Abschlussmeldung einzureichen. Sofern der Sicherheitsvorfall zu diesem Zeitpunkt noch andauert, ist anstelle der Abschlussmeldung ein Fortschrittsbericht einzureichen. Auf Anforderung der zuständigen Behörden sind darüber hinaus Zwischenmeldungen mit aktuellen Statusinformationen bereitzustellen. Betreiber kritischer Anlagen sind zusätzlich verpflichtet, Angaben zur Art der betroffenen Anlage und der kritischen Dienstleistung sowie zu den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung zu übermitteln, wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die von ihnen betriebene Kritische Anlage hat oder haben könnte.

Ergänzend regelt **§ 35 BSIG** die Informationspflichten gegenüber Empfängern von Diensten. Im Fall eines erheblichen Sicherheitsvorfalls kann das BSI gemäß **§ 35 Abs. 1 BSIG** anordnen, dass Empfänger der Dienste unverzüglich zu informieren sind. Unabhängig davon besteht gemäß **§ 35 Abs. 2**

BSIG für bestimmte Sektoren die Pflicht, Kunden über erhebliche Cyberbedrohungen zu unterrichten, auch wenn noch kein konkreter Sicherheitsvorfall eingetreten ist, sofern dies unter Berücksichtigung der Umstände angemessen und erforderlich ist.

§ 36 BSIG erweitert diese Anforderungen auf die Information der Öffentlichkeit, sofern dies zur Schadensbegrenzung oder Gefahrenabwehr erforderlich ist. Eine solche Öffentlichkeitsinformation kann vom BSI angeordnet werden, ist jedoch nicht zwingend vorgeschrieben, sondern abhängig von der konkreten Gefährdungslage und dem Erfordernismaßstab.

Insgesamt entsteht ein mehrstufiges, strukturiertes Kommunikationsregime, das eine zeitnahe und zielgerichtete Information aller relevanten Stakeholder sicherstellt.

Registrierungspflichten

Unternehmen im Anwendungsbereich der NIS-2-Richtlinie sind gemäß **§ 33 BSIG** verpflichtet, sich beim BSI zu registrieren. Das BSI sieht hierfür einen zweistufigen Registrierungsprozess vor. Im ersten Schritt muss eine Registrierung beim digitalen Dienst erfolgen. Im zweiten Schritt erfolgt die Registrierung im BSI-Portal.

Betreiber kritischer Anlagen unterliegen dabei ergänzenden Anforderungen im Rahmen der bestehenden KRITIS-Regulierung und haben insbesondere weitergehende Melde- und Nachweispflichten zu beachten.

Die Registrierung hat spätestens drei Monate nach erstmaliger bzw. erneuter Betroffenheit zu erfolgen. Für Einrichtungen, die bereits mit Inkrafttreten am 06.12.2025 erfasst waren, endete diese Frist am 06.03.2026. Unternehmen sind verpflichtet, Änderungen relevanter Daten unverzüglich, spätestens jedoch innerhalb von zwei Wochen nach Kenntniserlangung, zu melden und die jeweils geltenden Fristen aktiv zu überwachen.

Rolle und Verantwortung der Geschäftsleitung im Kontext der NIS-2-Compliance

Die Verantwortung für die Umsetzung der NIS-2-Richtlinie liegt gemäß **§ 38 BSIG** explizit bei der Geschäftsleitung. Diese ist verpflichtet, geeignete Risikomanagement- und Sicherheitsmaßnahmen zu implementieren und deren Wirksamkeit kontinuierlich zu überwachen.

Verstöße gegen diese Pflichten können zu aufsichtsrechtlichen Maßnahmen und Sanktionen führen. Geschäftsleitungen, die ihre Pflichten zur Umsetzung und Überwachung der Risikomanagementmaßnahmen schuldhaft verletzen, haften ihrer Einrichtung nach den auf die jeweilige Rechtsform anwendbaren gesellschaftsrechtlichen Regelungen. Enthalten diese keine entsprechende Haftungsregelung, kann sich die Haftung unmittelbar aus **§ 38 Abs. 2 BSIG** ergeben.

Darüber hinaus muss die Geschäftsleitung über ausreichende Kenntnisse und Kompetenzen verfügen, um Cybersicherheitsrisiken angemessen zu bewerten und entsprechende Maßnahmen strategisch zu steuern. **§ 38 BSIG** verpflichtet die Mitglieder der Geschäftsleitung daher ausdrücklich zur regelmäßigen Teilnahme an Schulungen zu Cybersicherheit und Risikomanagement, um ein angemessenes Verständnis der Anforderungen sicherzustellen und fundierte Entscheidungen treffen zu können. [3,5]

Nachweis- und Auditpflichten

Betreiber kritischer Anlagen sind gemäß **§ 39 BSIG** verpflichtet, die Umsetzung der für ihre kritischen Anlagen geltenden Sicherheitsmaßnahmen regelmäßig gegenüber dem BSI nachzuweisen. Der Nachweis ist grundsätzlich alle drei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen zu erbringen. Dabei sind dem BSI die Ergebnisse einschließlich der festgestellten Sicherheitsmängel zu übermitteln. Das BSI kann ergänzende Dokumentationen anfordern und bei festgestellten Mängeln die Vorlage eines geeigneten Mängelbeseitigungsplans, die Behebung der Mängel sowie einen entsprechenden Nachweis über deren Behebung verlangen. [3]

4. PRAXISPERSPEKTIVE: TYPISCHE HERAUSFORDERUNGEN BEI DER UMSETZUNG VON NIS-2

Die Umsetzung der Anforderungen der NIS-2-Richtlinie stellt Unternehmen vor wiederkehrende strukturelle und operative Problemfelder. Für dieses Whitepaper haben wir daher fünf typische Herausforderungen und Fallstricke identifiziert, die Erfahrungsgemäß einen wesentlichen Einfluss auf die erfolgreiche Umsetzung der Anforderungen haben. Sie führen nicht nur zu Verzögerungen, sondern bergen auch das Risiko, dass regulatorische An-

forderungen unvollständig umgesetzt werden, Sicherheitsmaßnahmen ihre beabsichtigte Wirksamkeit verfehlen und zusätzliche operative wie geschäftliche Risiken entstehen.

Die folgenden fünf Herausforderungen und Fallstricke stehen dabei im Fokus:

1. Unternehmen ohne Regulierungserfahrung stehen vor NIS-2-Unklarheiten
2. Behandlung von NIS-2 als einmaliges Projekt
3. Unterschätzung von Lieferketten- und Drittparteirisiken
4. Übermäßige Fokussierung auf technische Maßnahmen
5. Der Mangel an IT-Fachkräften zeigt keine Anzeichen einer Entlastung

Im weiteren Verlauf des Whitepapers werden diese zentralen Problemfelder näher beleuchtet. Dabei werden typische Schwachstellen herausgearbeitet, die in der Praxis regelmäßig auftreten, und durch konkrete, praxisorientierte Lösungsansätze ergänzt. Ziel ist es, ein klar strukturiertes Verständnis der wesentlichen Handlungsfelder zu vermitteln und Unternehmen eine fundierte Orientierung für eine wirksame und nachhaltige Umsetzung von NIS-2 zu geben.

1: Unternehmen ohne Regulierungserfahrung stehen vor NIS-2 Unklarheiten

Problemstellung

Mit NIS-2 sehen sich viele Unternehmen erstmals mit umfassenden, strukturierten und teilweise komplexen Anforderungen an die Informationssicherheit konfrontiert. Insbesondere Organisationen ohne bisherige Berührung mit regulatorischen Vorgaben stehen damit vor einer grundlegenden Herausforderung, da entsprechende Strukturen oft nicht oder nur in Ansätzen vorhanden sind und regulatorische Denkweisen erst aufgebaut werden müssen. Neben technischen Schutzmaßnahmen werden auch organisatorische und prozessuale Elemente gefordert, etwa ein umfassendes Risikomanagement, Meldeprozesse, Verantwortlichkeitsstrukturen und Nachweispflichten. [5]

Typische Symptome

In der Praxis zeigt sich häufig, dass das Thema zunächst primär aus einer technischen Perspektive betrachtet wird. Dadurch werden insbesondere organisatorische und prozessuale Anforderungen unterschätzt. Gleichzeitig besteht oft Unsicherheit darüber, welche Anforderungen konkret relevant

sind und wie diese zu interpretieren sind. Zuständigkeiten sind nicht klar definiert, ein strukturiertes Risikomanagement fehlt oder ist ausschließlich ansatzweise vorhanden. Darüber hinaus werden Maßnahmen eher punktuell umgesetzt. Dies führt in vielen Fällen zu fragmentierten Lösungsansätzen, ineffizientem Mitteleinsatz und einer insgesamt geringer Orientierung an den neuen Anforderungen.

Lösungsansatz

Der Lösungsansatz sollte sich auf einen klar strukturierten und pragmatischen Einstieg in die regulatorischen Anforderungen konzentrieren, um Orientierung zu schaffen und eine nachhaltige Umsetzung zu ermöglichen.

- **Strukturierter Einstieg:** Ein klarer und nachvollziehbarer Einstieg in die regulatorischen Anforderungen schafft Orientierung und reduziert anfängliche Unsicherheiten. Beispielsweise kann eine Gap-Analyse entlang der NIS-2-Anforderungsbereiche durchgeführt werden. Dabei wird geprüft, welche Vorgaben bereits erfüllt sind, wo bestehende Prozesse, Richtlinien oder Kontrollen genutzt werden können und an welchen Stellen konkreter Handlungsbedarf besteht.
- **Gemeinsames Verständnis:** Die Anforderungen müssen einheitlich verstanden und in einen klaren organisatorischen Kontext eingeordnet werden. Dazu gehört, gemeinsam zu klären, welche Anforderungen für das Unternehmen relevant sind, welche Bereiche betroffen sind und welche bestehenden Strukturen einbezogen werden müssen, um eine konsistente Umsetzung zu ermöglichen.
- **Ableitung von Handlungsfeldern:** Relevante Handlungsfelder sollten identifiziert und in konkrete, umsetzbare Maßnahmen überführt werden. Dazu können beispielsweise die Anpassung bestehender Richtlinien, die Einführung oder Erweiterung von Risiko- und Kontrollprozessen, die Definition von Meldewegen oder die Verbesserung der Nachweisfähigkeit gehören.
- **Priorisierung und pragmatisches Vorgehen:** Durch gezielte Priorisierung und ein verständliches Vorgehen kann die Komplexität reduziert und der Ressourceneinsatz effektiv gesteuert werden. Auf Basis der Gap-Analyse sollten Maßnahmen nach Risiko, regulatorischer Relevanz, Umsetzungsaufwand und Abhängigkeiten prio-

risiert werden. So können zunächst besonders kritische Lücken geschlossen werden, während weniger dringende Maßnahmen in eine realistische Umsetzungsplanung überführt werden.

- **Aufbau belastbarer Strukturen:** Ziel ist die schrittweise Etablierung tragfähiger organisatorischer und prozessualer Strukturen als Grundlage für eine nachhaltige Weiterentwicklung der Informationssicherheit. Die Ergebnisse der Gap-Analyse und der Umsetzungsplanung sollten daher in bestehende Governance-, Risiko- und Informationssicherheitsprozesse überführt werden. So entsteht eine belastbare Grundlage für die nachhaltige Weiterentwicklung der Informationssicherheit.

Ein strukturierter, praxisnaher und priorisierter Ansatz ermöglicht es, regulatorische Anforderungen effizient umzusetzen, Unsicherheiten zu minimieren und gleichzeitig eine nachhaltige sowie belastbare Organisationsstruktur im Bereich der Informationssicherheit aufzubauen.

2: Behandlung von NIS-2 als einmaliges Projekt

Problemstellung

Die Umsetzung regulatorischer Anforderungen wird in vielen Organisationen weiterhin als einmalige, projektgetriebene Aufgabe verstanden. Insbesondere bei Vorgaben wie NIS-2 zeigt sich häufig ein Fokus auf kurzfristige Zielerreichung, der der strukturellen Tragweite der Anforderungen nicht gerecht wird [4].

Typische Symptome

In der Praxis zeigt sich dieser Fallstrick insbesondere durch eine starke Fokussierung auf kurzfristige Auditfähigkeit. Nach Projektabschluss nimmt die Umsetzungsintensität häufig ab, da klare Verantwortlichkeiten für Betrieb und Weiterentwicklung fehlen.

Sicherheitsmaßnahmen bleiben dadurch oft isoliert und sind nicht ausreichend in operative Abläufe integriert, was ihre Wirksamkeit deutlich einschränkt.

Lösungsansatz

NIS-2 erfordert einen klaren Wechsel hin zu einer nachhaltigen und integrierten Umsetzung regulatorischer Anforderungen. Daraus ergeben sich zentrale Handlungsfelder, die systematisch adressiert werden sollten, um eine langfristig wirksame Umsetzung sicherzustellen.

- **Perspektivwechsel zum Managementansatz:** Regulatorische Anforderungen sind nicht als einmalige Aufgabe, sondern als dauerhafter Bestandteil der Unternehmenssteuerung zu verstehen. Eine reine projektbezogene Umsetzung, bei der einmalig Richtlinien, Konzepte oder Nachweisdokumente erstellt werden, reicht nicht aus. Werden diese Inhalte nach Projektabschluss nicht regelmäßig überprüft und aktualisiert, verlieren sie schnell an Relevanz und verfehlen die gewünschte Wirkung.

» Ein Bericht der ENISA zeigt, dass 47 % der Unternehmen Lieferkettenangriffe als größte Bedrohung einstufen, während nur 59 % ihre Lieferanten-Kontrollen als ausreichend bewertet sehen. Dies ist ein deutlicher Hinweis darauf, dass Resilienz nur entsteht, wenn externe Abhängigkeiten konsequent gesteuert werden. «

CHRISTOPHER CHASSÉE, DIRECTOR,
PROTIVITI DEUTSCHLAND



- **Integration in bestehende Strukturen:** Anforderungen müssen systematisch in Governance-, Risiko- und Kontrollstrukturen eingebettet werden, um ihre Wirksamkeit sicherzustellen. Beispielsweise sollten NIS-2-Anforderungen nicht isoliert behandelt werden, sondern in bestehende Risikomanagementprozesse, Kontrollhandlungen und Entscheidungsprozesse integriert werden.
- **Klare Verantwortlichkeiten:** Zuständigkeiten für Betrieb, Steuerung und Weiterentwicklung sind eindeutig zu definieren und organisatorisch zu verankern. Andernfalls besteht das Risiko, dass Maßnahmen nach Projektabschluss nicht weiterverfolgt werden. Verantwortlichkeiten sollten daher sowohl fachlich als auch auf Managementebene klar zugeordnet sein.
- **Kontinuierliche Weiterentwicklung:** Regelmäßige Überprüfung, Bewertung und Anpassung der Maßnahmen sind notwendig, um auf regulatorische Veränderungen und neue Risikolagen reagieren zu können. Beispielsweise können organisatorische Veränderungen, neue IT-Systeme, veränderte Bedrohungslagen oder neue regulatorische Anforderungen dazu führen, dass bestehende Dokumente, Kontrollen und Prozesse nicht mehr ausreichend greifen und angepasst werden müssen.

Eine konsequente Verankerung im Management, klare Verantwortlichkeiten und eine kontinuierliche Weiterentwicklung stellen sicher, dass regulatorische Anforderungen nicht nur formal erfüllt, sondern dauerhaft und wirksam in der Organisation umgesetzt werden.

3: Unterschätzung von Lieferketten- und Drittparteirisiken

Problemstellung

Viele Organisationen konzentrieren sich bei der Umsetzung von Sicherheitsanforderungen zunächst auf ihre internen Systeme und Prozesse. Risiken, die aus der Einbindung externer Dienstleister entstehen, werden dabei häufig nur eingeschränkt betrachtet. Diese einseitige Perspektive steht im Widerspruch zu den Anforderungen von NIS-2, die ein systematisches Management von IKT-Drittparteien verlangen. Fehlende Transparenz über Dienstleister, unzureichende vertragliche Regelungen und nicht etablierte Prüfprozesse führen dazu, dass externe Risiken unbemerkt auf die eigene

Organisation übergreifen können. Die zunehmende Verflechtung digitaler Lieferketten verstärkt diese Problematik und macht deutlich, dass ein rein interner Sicherheitsfokus nicht ausreicht, um regulatorische Vorgaben zu erfüllen oder die operative Resilienz sicherzustellen [4].

Typische Symptome

In der Praxis zeigt sich dieses Problem durch ein uneinheitliches und fragmentiertes Bild der Drittparteienlandschaft. Es existiert häufig kein konsolidiertes Register aller relevanten Dienstleister, Bewertungen erfolgen dezentral und nach unterschiedlichen Kriterien und Verträge enthalten meist nur allgemeine Sicherheitsformulierungen ohne verbindliche Prüf- und Meldeprozesse. Veränderungen bei Dienstleistern wie Subunternehmerwechsel, Standortverlagerungen oder Sicherheitsvorfälle bleiben oft unentdeckt, weil regelmäßige Überprüfungen fehlen. Parallel dazu werden technische Maßnahmen punktuell umgesetzt, ohne in ein übergreifendes Governance-Modell eingebettet zu sein, sodass die Wirksamkeit einzelner Lösungen begrenzt bleibt und die Anforderungen von NIS-2 nicht vollständig erfüllt werden.

Lösungsansatz

Ein wirksamer Lösungsansatz beginnt mit der Einsicht, dass Drittparteienmanagement kein nachgelagerter Administrationsakt, sondern ein integraler Bestandteil der Sicherheits- und Risikosteuerung ist. Bevor konkrete Maßnahmen umgesetzt werden, ist es notwendig, die organisatorischen Grundlagen zu schaffen, die technische Maßnahmen erst wirksam machen. Auf dieser Basis lassen sich die folgenden Handlungsfelder systematisch angehen.

- **Transparenz schaffen durch ein vollständiges Drittparteienregister:** Zunächst ist ein reichsübergreifend gepflegtes, digitales Register aller Drittparteien aufzubauen. Dieses Register muss nicht nur Hauptdienstleister, sondern auch Subunternehmer und indirekte IT-Leistungen erfassen. Nur mit einer vollständigen Übersicht lassen sich Abhängigkeiten identifizieren und Prioritäten für weitergehende Maßnahmen ableiten.
- **Risikobasierte Bewertung und Kritikalitätsbestimmung:** Auf Grundlage des Registers ist ein standardisiertes Bewertungsmodell zu etablieren, das Geschäftsrelevanz, Datensensibilität, regu-

latorische Anforderungen und Austauschbarkeit berücksichtigt. Die resultierende Kritikalitätsklassifikation ermöglicht eine nachvollziehbare Priorisierung und legt fest, welche Dienstleister intensiver überwacht oder vertraglich strenger geregelt werden müssen.

- **Verträge stärken mit konkreten Sicherheitsanforderungen und Kontrollrechten:** Verträge sind das zentrale Steuerungsinstrument gegenüber Drittparteien. Sie müssen verbindliche Meldepflichten bei Sicherheitsvorfällen, Audit- und Kontrollrechte, Vorgaben zur Nutzung von Subunternehmern sowie Exit- und Übergangsregelungen enthalten. Nur so lassen sich Nachweispflichten erfüllen und Handlungsoptionen im Krisenfall sicherstellen.
- **Kontinuierliche Prüf- und Bewertungsprozesse etablieren:** Einmalige Assessments genügen nicht. Es sind regelmäßige Reviews und automatisierte Monitoring-Mechanismen einzuführen, die Veränderungen bei Dienstleistern frühzeitig erkennen. Diese Prozesse müssen in die operative Steuerung integriert werden, damit Bewertungen aktualisiert und Maßnahmen zeitnah angepasst werden können.
- **Governance und Integration technischer Maßnahmen:** Technische Investitionen entfalten ihre Wirkung nur, wenn sie in ein klares Governance- und Entscheidungsmodell eingebettet sind. Zuständigkeiten, Eskalationswege und Verantwortlichkeiten sind zu definieren; technische Kontrollen sind entlang dieser Steuerungsmechanismen zu koordinieren. So entsteht ein integriertes Gesamtgerüst, in dem organisatorische und technische Elemente ineinandergreifen und die NIS-2-Anforderungen nachweisbar erfüllt werden.

Abschließend ist zu betonen, dass die Kombination aus vollständiger Transparenz, risikobasierter Priorisierung, robusten vertraglichen Regelungen, kontinuierlichen Prüfprozessen und einer klaren Governance die Voraussetzung dafür bildet, dass Drittparteirisiken nicht nur identifiziert, sondern auch nachhaltig gesteuert werden können. Nur so wird Drittparteienmanagement zum integralen Bestandteil der Sicherheits- und Risikosteuerung und erfüllt die Erwartungen moderner Regulierung.

4: Übermäßige Fokussierung auf technische Maßnahmen

Problemstellung

In der Praxis zeigt sich im Kontext von NIS-2 häufig eine starke Fokussierung auf technische Maßnahmen. Investitionen in Sicherheitswerkzeuge, Systemhärtung und technische Schutzmechanismen stehen im Vordergrund, während organisatorische und steuernde Elemente weniger Beachtung finden.

Diese einseitige Ausrichtung greift jedoch zu kurz, da NIS-2 ausdrücklich ein Zusammenspiel aus technischen und organisatorischen Anforderungen fordert. Ein übermäßiger Fokus auf Technologien führt dazu, dass notwendige Governance-Strukturen nicht im gleichen Maße entwickelt werden. In der Folge fehlt es an klaren Zuständigkeiten, verbindlichen Entscheidungsprozessen und übergreifenden Steuerungsmechanismen. Technische Lösungen bleiben dadurch oft punktuell wirksam, entfalten jedoch nicht ihr volles Potenzial zur nachhaltigen Risikoreduktion. [4]

Typische Symptome

Organisationen implementieren eine Vielzahl technischer Maßnahmen, ohne diese in ein konsistentes Gesamtmodell einzubetten. Verantwortlichkeiten sind nicht eindeutig geregelt, wodurch Entscheidungen verzögert oder uneinheitlich getroffen werden. Zudem fehlen strukturierte Prozesse zur Überprüfung und Weiterentwicklung, wodurch eine fragmentierte Sicherheitslandschaft entsteht, in der einzelne Lösungen nebeneinander bestehen, aber nicht integriert wirken.

Lösungsansatz

Der Lösungsansatz zielt darauf ab, technische und organisatorische Maßnahmen konsequent miteinander zu kombinieren, um eine wirksame und ganzheitliche Umsetzung zu erreichen. Hieraus lassen sich zentrale Ansatzpunkte ableiten, die eine abgestimmte und strukturierte Umsetzung unterstützen.

- **Verknüpfung von Technik und Organisation:** Technische Maßnahmen sind systematisch mit den organisatorischen Strukturen zu verzahnen, damit ihre volle, nachhaltige und konsistent abgesicherte Wirksamkeit erreicht wird.
- **Etablierung klarer Governance-Strukturen:** Es sind verbindliche Modelle zu definieren, die Rollen, Verantwortlichkeiten sowie die Prozesse

für Planung, Umsetzung, Überwachung und kontinuierliche Weiterentwicklung eindeutig festlegen.

- **Einbettung technischer Maßnahmen:** Technische Lösungen müssen in übergeordnete Steuerungsmechanismen integriert und entlang klar definierter Verantwortlichkeiten koordiniert werden, um Konsistenz und Steuerbarkeit sicherzustellen.

» Der ENISA-Report zeigt, dass 76 % der befragten Organisationen Schwierigkeiten bei der Gewinnung von Cyber-Fachkräften haben und 71 % bestehende Experten nicht halten können. Ein strukturelles Defizit, das ohne klares Operating-Model und gezielte Entlastungsmaßnahmen jede NIS-2-Umsetzung ausbremst. «

PHILIPP WEINGART, MANAGING DIRECTOR,
ROBERT HALF



- **Aufbau eines integrierten Gesamtansatzes:** Ziel ist ein abgestimmtes Zusammenspiel von technischen und organisatorischen Elementen, das eine nachhaltige und effektive Risikoreduktion ermöglicht.

Erst durch die enge Verzahnung technischer und organisatorischer Maßnahmen sowie klare Governance-Strukturen entsteht ein ganzheitlicher Ansatz, der Risiken wirksam reduziert und eine nachhaltige Umsetzung sicherstellt.

5: Fachkräftemangel als struktureller Umsetzungsblocker

Problemstellung

Der Mangel an qualifizierten IT- und Cybersecurity-Fachkräften entwickelt sich zunehmend zu einem der zentralen strukturellen Blocker für die Umsetzung von NIS-2. Während die regulatorischen Anforderungen steigen, bleibt der Arbeitsmarkt angespannt. Viele Organisationen kämpfen damit, geeignete Expertinnen und Experten zu gewinnen oder langfristig zu halten. Die Folge ist eine Überlastung bestehender Teams, die ohnehin schon mit steigender Komplexität, wachsender Bedrohungslage und zusätzlichen Dokumentations- und Nachweispflichten konfrontiert sind. NIS-2 verlangt jedoch nicht nur technische Maßnahmen, sondern auch klare Verantwortlichkeiten, definierte Prozesse und kontinuierliche Überwachung, Anforderungen, die ohne ausreichende personelle Ressourcen kaum erfüllbar sind. [4]

Typische Symptome

In der Praxis zeigt sich der Fachkräftemangel in Form überlasteter Security-Teams, die zentrale Aufgaben wie Patch-Management, Monitoring oder Incident Response nur verzögert oder unvollständig umsetzen können. Lange Reaktionszeiten, fehlende Priorisierung und eine starke Abhängigkeit von einzelnen Schlüsselpersonen sind häufige Begleiterscheinungen. Gleichzeitig fehlt es an strukturierten Weiterbildungsprogrammen, wodurch bestehende Mitarbeitende nicht ausreichend auf neue Technologien oder regulatorische Anforderungen vorbereitet sind. Die hohe Fluktuation verstärkt diese Probleme zusätzlich. Wissen geht verloren, Projekte verzögern sich und die Umsetzung von NIS-2-Pflichten bleibt fragmentiert. Besonders kleinere Organisationen geraten hier schnell an ihre Grenzen, da sie weder die finanziellen Mittel noch die organisatorischen Strukturen haben, um spezialisierte Rollen aufzubauen.

Lösungsansatz

Ein wirksamer Lösungsansatz beginnt mit der Erkenntnis, dass der Fachkräftemangel nicht allein durch zusätzliche Rekrutierung gelöst werden kann. Stattdessen braucht es ein integriertes Vorgehen, das interne Kompetenzen stärkt, externe Ressourcen gezielt einbindet und klare Governance-Strukturen schafft. Erst wenn organisatorische und technische Maßnahmen miteinander verzahnt werden, entsteht ein belastbares Fundament für die Umsetzung von NIS-2.

- **Aufbau eines klaren Operating Models für Cybersecurity:** Im Zentrum steht die Etablierung eines strukturierten Operating Models, das Rollen, Verantwortlichkeiten und Entscheidungswege eindeutig definiert. Dies schafft Klarheit darüber, welche Aufgaben intern wahrgenommen werden müssen und wo externe Unterstützung sinnvoll ist. Ein solches Modell bildet die Grundlage für effiziente Zusammenarbeit, reduziert Abhängigkeiten von Einzelpersonen und stellt sicher, dass NIS-2-relevante Aufgaben dauerhaft verankert sind.
- **Make-or-Buy-Strategie zur gezielten Entlastung:** Da nicht alle Kompetenzen intern aufgebaut werden können, ist eine strategische Make-or-Buy-Entscheidung notwendig. Externe Partner, etwa Managed Security Service Provider, können operative Aufgaben wie Monitoring, Incident Detection oder Vulnerability Management übernehmen. Dadurch gewinnen interne Teams Zeit für strategische Aufgaben, Governance und die Umsetzung regulatorischer Anforderungen. Eine solche Strategie erhöht die Resilienz und reduziert gleichzeitig die Abhängigkeit vom angespannten Arbeitsmarkt.
- **Systematische Upskilling- und Weiterbildungsprogramme:** Parallel dazu müssen bestehende Mitarbeitende gezielt weitergebildet werden. Strukturierte Trainingsprogramme, Zertifizierungen und praxisnahe Schulungen stärken interne Kompetenzen und ermöglichen es Teams, neue Technologien und regulatorische Anforderungen souverän zu bewältigen. Dies erhöht nicht nur die Qualität der Sicherheitsmaßnahmen, sondern wirkt auch dem Risiko von Fluktuation entgegen, da Mitarbeitende Entwicklungsperspektiven erhalten.

- **Automatisierung und Tooling zur Entlastung der Teams:** Automatisierungslösungen, etwa im Patch-Management, in der Log-Analyse oder im Incident-Handling, können operative Lasten erheblich reduzieren. Moderne Tools unterstützen Teams dabei, repetitive Aufgaben effizienter zu bewältigen und sich auf komplexere Tätigkeiten zu konzentrieren. Dadurch steigt die Wirksamkeit der Sicherheitsmaßnahmen, selbst wenn personelle Ressourcen begrenzt bleiben.
- **Governance und Priorisierung entlang der NIS-2-Pflichten:** Abschließend ist sicherzustellen, dass alle Maßnahmen in ein übergreifendes Governance-Modell eingebettet sind. Klare Prioritäten, definierte Eskalationswege und regelmäßige Reviews ermöglichen es, Ressourcen gezielt dort einzusetzen, wo sie den größten Beitrag zur NIS-2-Compliance leisten. So entsteht ein integriertes Gesamtgerüst, das technische, organisatorische und personelle Aspekte miteinander verbindet.

Ein solcher Ansatz macht das Personalrisiko steuerbar und stellt sicher, dass die Umsetzung von NIS-2 nicht an fehlenden Kapazitäten scheitert, sondern auf einer stabilen, zukunftsfähigen Struktur aufbaut.

5. SANKTIONEN UND ERWEITERTE AUFSICHTS-BEFUGNISSE UNTER NIS-2

Die Anpassung eines bestehenden Managementsystems für Informationssicherheit (ISMS) an die neuen Anforderungen sollte zeitnah und strukturiert erfolgen. Unternehmen, die die Vorgaben nicht einhalten, müssen mit erheblichen Bußgeldern sowie einer erweiterten Verantwortlichkeit auf Leitungsebene rechnen.

Für „wichtige Einrichtungen“ sind Bußgelder von bis zu **7 Mio. €** vorgesehen. Für „besonders wichtige Einrichtungen“ kann der Bußgeldrahmen bis zu **10 Mio. €** betragen (§ 65 Abs. 5 BSIG). Für Unternehmen mit einem Gesamtumsatz von mehr als 500 Millionen Euro können die Bußgelder darüber hinaus umsatzbasiert festgelegt werden und bis zu **1,4 % (wichtige Einrichtungen)** beziehungsweise **2 % (besonders wichtige Einrichtungen)** des weltweiten Jahresumsatzes betragen (§ 65 Abs. 6 und 7 BSIG).

Parallel dazu wurden die Befugnisse der Aufsichtsbehörden deutlich ausgeweitet. Dazu zählen insbesondere Vor-Ort-Inspektionen, die Anordnung bzw. Durchführung regelmäßiger Sicherheitsaudits, anlassbezogene Überprüfungen im Ereignisfall sowie Sicherheitsscans.

Zudem ist eine grenzüberschreitende Zusammenarbeit und Durchsetzung in Abstimmung mit anderen nationalen Aufsichtsbehörden vorgesehen.

Für Unternehmen bedeutet dies, dass Sicherheitsmaßnahmen nicht nur implementiert, sondern kontinuierlich überwacht, bewertet und weiterentwickelt werden müssen, um sowohl mit dynamischen Bedrohungslagen als auch mit regulatorischen Entwicklungen Schritt zu halten. Ein proaktives Vorgehen ist daher empfehlenswert, einschließlich eines strukturierten Austauschs mit den zuständigen Aufsichtsbehörden sowie eines regelmäßigen Monitorings relevanter Informationen, etwa von der ENISA und einschlägigen Fach- und Branchenverbänden.

Unternehmen, die bislang nur geringe Berührungspunkte mit dem BSI oder anderen Institutionen der Informationssicherheit hatten, sollten den Aufbau belastbarer Kommunikations- und Meldewege als festen Bestandteil ihres ISMS priorisieren und systematisch etablieren. [3]

6. UMSETZUNGSSTAND DER NIS-2-RICHTLINIE IN DEUTSCHLAND

Die NIS-2-Richtlinie erweitert den Kreis der betroffenen Unternehmen erheblich und erhöht die Anzahl der regulierten Organisationen in Deutschland nach Schätzungen des BSI auf rund 29.500.

Nach Ablauf der ersten Registrierungsfrist am 6. März 2026 zeigt sich jedoch eine signifikante Umsetzungslücke. Lediglich knapp 14.000 der betroffenen Organisationen haben sich bis eine Woche nach Ablauf der Registrierungspflicht beim BSI-Portal angemeldet. Demnach sind knapp die Hälfte der von NIS-2 betroffenen Unternehmen ihren Registrierungspflichten nicht fristgerecht nachgekommen. [9]

Bis zum 30.06.2026 ist diese Zahl auf rund 18.000 gestiegen. Für diese Unternehmen wird das Risiko zunehmend konkret und kurzfristig wirksam. Das BSI ist gemäß § 65 BSIG befugt, Verwaltungsverfahren einzuleiten und bereits für die versäumte Registrierung Bußgelder von bis zu 500.000 Euro zu verhängen. [3]

Vor diesem Hintergrund wird deutlich, dass viele Organisationen vor der Herausforderung stehen, regulatorische Anforderungen schnell und strukturiert in konkrete Maßnahmen zu überführen. Die zeitnahe Schließung bestehender Compliance-Lücken sowie die Etablierung belastbarer Sicherheits- und Governance-Strukturen sind entscheidend, um regulatorische Risiken zu minimieren und die Konformität nachhaltig sicherzustellen.

7. FAZIT UND AUSBLICK

NIS-2 erhöht die Anforderungen an Unternehmen signifikant. Entscheidend ist dabei weniger die isolierte Verbesserung einzelner Sicherheitsmaßnahmen, sondern die Schaffung eines konsistenten, wirksamen Gesamtsystems, das im operativen Alltag funktioniert und gegenüber internen sowie externen Stakeholdern nachvollziehbar und belastbar ist.

Gefordert sind klare Verantwortlichkeiten, eine risikobasierte Priorisierung von Maßnahmen sowie eine konsequent auf Wirksamkeit ausgerichtete Umsetzung.

Für viele Organisationen besteht die zentrale Herausforderung darin, regulatorische Anforderungen in konkrete, umsetzbare Arbeitspakete zu übersetzen. Dabei stellen sich insbesondere folgende Fragen: Welche Pflichten gelten konkret? Wo bestehen die größten Handlungsbedarfe? Welche Maßnahmen leisten den größten Beitrag zur Risikoreduktion?

In der Praxis zeigt sich, dass insbesondere Transparenz über den eigenen Reifegrad sowie eine strukturierte Priorisierung der Maßnahmen entscheidend sind. Unternehmen, die frühzeitig Klarheit über ihre Betroffenheit und den konkreten Handlungsbedarf schaffen, können Umsetzungsaufwände gezielt steuern und regulatorische Risiken deutlich reduzieren.

NIS-2 ist dabei nicht als einmaliges Compliance-Projekt zu verstehen, sondern als kontinuierlicher Managementprozess zur nachhaltigen Stärkung der Cybersicherheit. Die Anforderungen wirken dauerhaft auf Organisation, Prozesse und Technologie und erfordern eine regelmäßige Überprüfung sowie kontinuierliche Weiterentwicklung der implementierten Maßnahmen.

Gleichzeitig bietet die Umsetzung von NIS-2 strategische Chancen. Unternehmen, die ihre Strukturen systematisch weiterentwickeln, stärken nicht nur ihre Resilienz gegenüber Cyberbedrohungen, sondern erhöhen auch das Vertrauen von Kunden, Partnern und Aufsichtsbehörden.

8. QUELLEN

[1] Europäisches Parlament und Rat der Europäischen Union (Hrsg.) (2022). 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). Amtsblatt der Europäischen Union, L 333, 27.12.2022, S. 80.

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555>. (Zugriff 03/2026)

[2] Bundesministerium der Justiz (Hrsg.) (2025). Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2. Dezember 2025. Bundesgesetzblatt Teil I 2025, Nr. 301.

<https://www.recht.bund.de/bgbl/1/2025/301/V0.html>. (Zugriff 03/2026)

[3] Bundesministerium der Justiz und für Verbraucherschutz; Bundesamt für Justiz (Hrsg.) (2026). Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG).

https://www.gesetze-im-internet.de/bsig_2025/. (Zugriff 03/2026)

[4] European Union Agency for Cybersecurity (ENISA) (Hrsg.) (2025). NIS Investments 2025.

NIS Investments 2025 - Main report.pdf. (Zugriff 04/2026)

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2025). nis2know: NIS-2-Risikomanagementmaßnahmen.

<https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Risikomanagementmassnahmen/NIS-2-Risikomanagementmassnahmen.html>. (Zugriff 04/2026)

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2025). nis2know: DORA und NIS-2.

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-DORA/NIS-2-DORA_node.html. (Zugriff 04/2026)

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2026). ISO/IEC 27001 im Kontext NIS-2/BSIG.

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-iso-27000-onepager.pdf>. (Zugriff 04/2026)

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2026). Kritische Infrastrukturen (KRITIS).

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-kritis-onepager.pdf>. (Zugriff 03/2026)

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2026). Verpflichtung für Unternehmen: NIS-2.

https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/Newsletter-Einfach-Cybersicher/Einfach-Cybersicher_260401/_documents/Basics_2_NIS-2.html. (Zugriff 03/2026)

9. ÜBER PROTIVITI

Protiviti (www.protiviti.com) ist ein weltweit tätiges Beratungsunternehmen, das fundiertes Fachwissen, objektive Erkenntnisse, einen maßgeschneiderten Ansatz und beispiellose Zusammenarbeit bietet, um Führungskräfte selbstbewusst in die Zukunft blicken zu lassen. Protiviti und seine unabhängigen und regional ansässigen Mitgliedsfirmen unterstützen Kunden mit Beratungsleistungen und Managed Solutions in Bezug auf Finanzen, Technologien, Operatives, Digitales, HR, Risiko und Interne Revision – mithilfe eines Netzwerks von mehr als 90 Niederlassungen in über 25 Ländern.

Protiviti wurde zum zehnten Mal in Folge in die Liste der **Fortune 100 Best Companies to Work For®** aufgenommen und hat mehr als 80 Prozent der Fortune-100- und fast 80 Prozent der Fortune-500-Unternehmen betreut. Protiviti arbeitet ebenfalls mit Regierungsbehörden sowie kleineren und wachsenden Unternehmen zusammen, einschließlich solchen, die den Börsengang planen. Protiviti ist darüber hinaus eine hundertprozentige Tochter der **Robert Half Inc.** (NYSE: RHI).

© Protiviti Inc. Protiviti ist nicht als Wirtschaftsprüfungsgesellschaft zugelassen oder registriert und gibt keine Einschätzung zu Finanzberichten oder anderen Bestätigungsleistungen ab.

www.protiviti.de



© Protiviti GmbH

10. KONTAKTE



ANDREJ GREINDL

Managing Director
Protiviti Deutschland
+49 172 698 30 53
andrej.greindl@protiviti.com



CHRISTOPHER CHASSÉE

Director
Protiviti Deutschland
+49 172 621 73 01
christopher.chassee@protiviti.com



PHILIPP WEINGART

Managing Director
Robert Half
+49 711 120 91 306
philipp.weingart@roberthalf.de