LINK11

WHITEPAPER

NIS-2: Haftung. Handlungsbedarf. Was jetzt zu tun ist.

www.link11.com

Liebe Leserinnen und Leser,

Lange war Cybersicherheit ein Thema, das im Maschinenraum blieb. In der IT-Abteilung, bei den Administratoren, bei den Spezialisten. Die Geschäftsleitung wurde informiert, wenn etwas schiefging, und vergaß das Thema wieder, wenn es ruhig war. Mit NIS-2 ist diese Ära vorbei. Das Gesetz ist seit dem 6. Dezember 2025 in Kraft und betrifft Sie persönlich als Geschäftsführer, als Vorstand oder als Leitungsperson. Die Pflicht zur Umsetzung und Überwachung von Cybersicherheitsmaßnahmen ist nicht delegierbar. Das ist keine Drohung, sondern eine überfällige Klarstellung.

Was ich in meiner täglichen Arbeit bei Link11 erlebe, deckt sich mit dem, was wir in Gesprächen mit Unternehmen aus ganz Europa hören. Die meisten Organisationen stehen nicht mehr am Anfang. Es gibt Firewalls, Backups und Sicherheitsrichtlinien. Was jedoch häufig fehlt, ist die Systematik dahinter, also ein kohärenter Ansatz, der Einzelmaßnahmen zu einem nachweisbaren Sicherheitskonzept zusammenfügt. Hier kommt NIS-2 ins Spiel und dazu informiert Sie dieses Whitepaper.

Wir haben diesen Leitfaden gemeinsam mit unseren Partnern der apro.gmbH und Nethinks entwickelt, weil wir überzeugt sind: NIS-2-Compliance ist kein Selbstzweck und kein bürokratisches Übel. Vielmehr bietet sie die Chance, Cybersicherheit endlich dort zu verankern, wo sie hingehört: auf der Agenda der Unternehmensführung. Dieser Leitfaden liefert Ihnen keine Theorie. Er zeigt Ihnen konkrete Schritte, praxiserprobte Checklisten und gibt Ihnen eine klare Orientierung.

Viel Freude mit der Lektüre!

Herzliche Grüße
Jens-Philipp Jung, CEO, Link11

Inhalt

Executive Summary

Am 6. Dezember 2025 trat das NIS-2-Umsetzungsgesetz in Kraft und damit eine neue Realität für rund 29.000 Unternehmen in Deutschland. Cybersicherheit ist kein IT-Thema mehr. Es ist eine persönliche Chefsache mit Haftungskonsequenzen.

Dieses Whitepaper übersetzt gesetzliche Anforderungen in klare Handlungsfelder.

Die 5 wichtigsten Erkenntnisse auf einen Blick

1. NIS-2 ist geltendes Recht. Kein Entwurf, keine Frist mehr. Handeln zählt ab sofort.
2. Geschäftsführer haften persönlich. § 38 BSIG macht die Leitungspflicht nicht delegierbar.
3. Es werden Bußgelder bis 10 Mio. Euro oder 2 % des Jahresumsatzes fällig. Der höhere Betrag zählt.
4. Die Registrierungspflicht greift nach 3 Monaten. Ab dem Moment, in dem Ihr Unternehmen die Kriterien erfüllt.
5. Die Umsetzung ist machbar. Dieser Leitfaden zeigt Ihnen genau, wo Sie ansetzen sollten.

NIS-2 – Warum Chefsache?

Viele Geschäftsführungen haben NIS-2 bisher als IT-Projekt behandelt. Das Gesetz ist jedoch unmissverständlich: Die Verantwortung liegt bei Ihnen.

Das Gesetz ist in Kraft

Die EU-Richtlinie NIS-2 (EU 2022/2555) wurde am 14. Dezember 2022 verabschiedet. Deutschland hat die Umsetzungsfrist zunächst verpasst, aber am 5. Dezember 2025 das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz im Bundesgesetzblatt verkündet (BGBl. 2025 I Nr. 301). Seit dem 6. Dezember 2025 gilt es.

Das Gesetz ersetzt das bisherige BSI-Gesetz vollständig und zieht Folgeänderungen in 28 weiteren Gesetzen und Verordnungen nach sich – vom Energiewirtschaftsgesetz bis zum Sozialgesetzbuch.

Persönliche Haftung der Geschäftsleitung

§ 38 Abs. 1 BSIG ist klar: Geschäftsleitungen müssen die Risikomanagementmaßnahmen nach § 30 umsetzen und deren Umsetzung überwachen. Diese Pflicht ist nicht delegierbar. Sie können operative Aufgaben beauftragen. Die Verantwortung bleibt bei Ihnen.

§ 38 Abs. 2 regelt die Haftungsfolgen: Wer diese Pflichten schuldhaft verletzt, haftet seiner Einrichtung für entstandene Schäden. Bei einer GmbH nach § 43 GmbHG, bei einer AG nach § 93 AktG – also mit dem Privatvermögen.

Dazu kommt § 38 Abs. 3: Die Geschäftsleitung muss regelmäßig an NIS-2-Schulungen teilnehmen. Wer sich weigert, riskiert nach § 61 Abs. 9 BSIG sogar eine vorübergehende Untersagung der Leitungstätigkeit.

Hinweis zur Haftung

Die Geschäftsleitung kann Cybersicherheit nicht vollständig an die IT-Abteilung übergeben. Überwachungspflicht und Schulungspflicht sind gesetzlich verankert und nicht ausführbar.

Bußgelder und Durchsetzung

Das Bußgeldregime ist gestaffelt und orientiert sich am Schweregrad des Verstoßes sowie der Kategorie der Einrichtung:

Wen betrifft es? Besonders wichtige vs. wichtige Einrichtungen

Das Gesetz unterscheidet in § 28 BSIG zwei Kategorien. Die Zuordnung bestimmt die Intensität der Aufsicht, nicht die inhaltlichen Pflichten – die Risikomanagementmaßnahmen nach § 30 gelten für beide.

Verstoß	Besonders wichtige Einrichtung	Wichtige Einrichtung
Risikomanagement- und Meldepflichten (§ 30, § 32)	Bis 10 Mio. EUR	Bis 7 Mio. EUR
Bei Jahresumsatz > 500 Mio. EUR	Bis 2 % des Jahresumsatzes	Bis 1,4 % des Jahresumsatzes
Registrierungspflicht (§ 33)	Bis 500.000 EUR	Bis 500.000 EUR
Auskunftsverlangen (§ 14)	Bis 100.000 EUR	Bis 100.000 EUR

Als Ultima Ratio kann das BSI über die zuständige Aufsichtsbehörde gemäß § 61 Abs. 9 sogar die Genehmigung einer Einrichtung vorübergehend aussetzen oder der Geschäftsleitung die Ausübung ihrer Leitungstätigkeit untersagen.

Kategorie	Kriterien	Sektoren (Auswahl)
Besonders wichtige Einrichtung (§ 28 Abs. 1)	≥ 250 MA oder Umsatz > 50 Mio. + Bilanzsumme > 43 Mio. EUR	Energie, Transport, Finanzen, Gesundheit, Wasser, Digitale Infrastruktur, Weltraum
Wichtige Einrichtung (§ 28 Abs. 2)	≥ 50 MA oder Umsatz + Bilanzsumme jeweils > 10 Mio. EUR	Alle Anlage-1-Sektoren + Post, Chemie, Lebensmittel, Maschinenbau, Automotive, Forschung

Konzernstrukturen beachten

Die Bestimmung von Mitarbeiterzahl, Umsatz und Bilanzsumme richtet sich nach der EU-KMU-Empfehlung 2003/361/EG. Verbundene und Partnerunternehmen werden grundsätzlich einbezogen – es sei denn, die IT-Systeme werden nachweislich unabhängig betrieben (§ 28 Abs. 4 BSIG). Ausgegliederte Rechenzentren innerhalb eines Konzerns fallen nicht unter die Ausnahmeregelung.

Kernbereiche im Praxis-Check

§ 30 Abs. 1 BSIG verpflichtet alle betroffenen Einrichtungen zu geeigneten, verhältnismäßigen und wirksamen Maßnahmen. § 30 Abs. 2 konkretisiert zehn Mindestbereiche. Wir fassen die wichtigsten für den Praxiseinstieg in sechs Kernbereiche zusammen.

Das Verhältnismäßigkeitsprinzip gilt: Größe, Risikoexposition, Umsetzungskosten und Schadenswahrscheinlichkeit bestimmen den konkreten Aufwand. Kein Unternehmen muss von null auf perfekt – aber alle müssen anfangen.

Risikobewertung

Was fordert NIS-2?

Einrichtungen müssen Konzepte zur Risikoanalyse erstellen und umsetzen. Der Ansatz muss gefahrenübergreifend sein und den Stand der Technik einhalten (§ 30 Abs. 2 Nr. 1 BSIG). Das bedeutet: keine Insellösung für einzelne Bedrohungen, sondern ein systematischer Prozess.

Was bedeutet das in der Praxis?

Ein dokumentierter Risikomanagementprozess, der alle relevanten Bedrohungen erfasst – Cyberangriffe, technische Ausfälle, physische Gefahren. Zentrale Elemente sind die Identifikation und Bewertung von IT-Assets, regelmäßige Risikobeurteilungen, die Ableitung von Behandlungsmaßnahmen und deren Dokumentation im Sicherheitskonzept. ISO/IEC 27001:2022 fordert dazu einen dokumentierten Prozess (Abschnitt 6.1.2). BSI-Standard 200-3 beschreibt die Risikoanalyse in vier Schritten: Gefährdungsübersicht, Risikoeinstufung, Risikobehandlung und Konsolidierung des Sicherheitskonzepts.

Typische Pain Points

- Keine systematische Asset-Inventur vorhanden
- Risikoanalysen werden einmalig durchgeführt, aber nicht aktualisiert
- IT-Risiken werden nicht als Unternehmensrisiken betrachtet und berichtet
- Fehlende Verknüpfung zwischen Risikoanalyse und konkreten Schutzmaßnahmen

Checkliste

- ✓ **Asset-Inventar erstellt** (IT-Systeme, Daten, Prozesse)
- ✓ **Kritische Geschäftsprozesse** und deren IT-Abhängigkeiten identifiziert
- ✓ **Bedrohungsanalyse durchgeführt** (All-Hazard-Ansatz)
- ✓ **Risikobewertung dokumentiert** (Eintrittswahrscheinlichkeit × Schadenshöhe)
- ✓ **Behandlungsmaßnahmen** abgeleitet und priorisiert
- ✓ **Jährliche Überprüfung** und Aktualisierung geplant

Praxisbeispiel: DDoS-Angriff auf einen Logistikdienstleister

Ein mittelständischer Logistikdienstleister führt seine erste strukturierte Risikoanalyse durch. Ergebnis: Die Auftragsmanagement-Plattform ist ein geschäftskritisches Asset mit hohem DDoS-Risiko, da sie öffentlich erreichbare Schnittstellen hat.

Behandlungsmaßnahmen: (1) Cloud-basierter DDoS-Schutz wie von Link11 implementiert, (2) Geo-Blocking für nicht benötigte Regionen aktiviert, (3) Notfallprozess für manuellen Betrieb dokumentiert.

Das Risiko wurde auf ein akzeptables Niveau reduziert und der Prozess ist nachweislich dokumentiert.

Sicherheitsrichtlinien & Dokumentation

Was fordert NIS-2?

§ 30 Abs. 1 S. 3 BSIG verlangt ausdrücklich den Nachweis der ergriffenen Maßnahmen. Die bloße Existenz von Sicherheitslösungen reicht nicht. Wer nicht dokumentiert, kann nicht nachweisen und haftet im Zweifelsfall.

Was bedeutet das in der Praxis?

Sicherheitsrichtlinien müssen schriftlich fixiert, regelmäßig überprüft und allen relevanten Mitarbeitern zugänglich sein. Das betrifft Passwortrichtlinien, Zugriffskontrolle, Umgang mit mobilen Geräten, Patch-Management und viele weitere operative Bereiche. Ergänzt wird dies durch ein zentrales Dokumentenmanagementsystem, das Versionshistorie und Gültigkeitsdaten pflegt.

Typische Pain Points

- Richtlinien existieren, sind aber nicht aktuell, nicht kommuniziert oder nicht gelebt
- Keine klare Dokumentationsstruktur – im Ernstfall fehlt der Nachweis
- Zuständigkeiten sind unklar: Wer ist Eigentümer welcher Richtlinie?

Checkliste

- ✓ **Informationssicherheitsleitlinie vorhanden** und von Geschäftsleitung unterzeichnet
- ✓ Alle **Sicherheitsmaßnahmen** nach § 30 Abs. 2 **dokumentiert**
- ✓ **Richtlinien regelmäßig überprüft** (mindestens jährlich)
- ✓ **Mitarbeiter** nachweislich über Richtlinien **informiert**
- ✓ **Dokumentenmanagement** mit Versionshistorie **implementiert**
- ✓ **Verantwortlichkeiten** für jede Richtlinie klar benannt

Praxisbeispiel: Fehlende Dokumentation als Haftungsrisiko

Ein Fertigungsunternehmen wird nach einem Sicherheitsvorfall vom BSI geprüft. Die Maßnahmen waren technisch gut umgesetzt, aber nicht dokumentiert. Der CISO kann nicht nachweisen, wann Patches eingespielt wurden und wer Zugriff auf welche Systeme hatte.

Ergebnis: Die Behörde verhängt ein Bußgeld nicht wegen des Vorfalls selbst, sondern wegen fehlender Nachweise. Lesson learned: Sicherheit und Dokumentation sind zwei Seiten derselben Medaille.

> *„Mit NIS-2 wird Cybersicherheit zur Führungsaufgabe. Wer das versteht, hat nicht nur das Gesetz auf seiner Seite, sondern auch einen echten Wettbewerbsvorteil.“*

Jens-Philipp Jung, CEO, Link11

Incident Management & Meldefristen

Was fordert NIS-2?

§ 30 Abs. 2 Nr. 2 BSIG verpflichtet zur Etablierung von Prozessen zur Bewältigung von Sicherheitsvorfällen. Eng verbunden damit sind die strikten Meldepflichten nach § 32 BSIG.

Was bedeutet das in der Praxis?

Sicherheitsrichtlinien müssen schriftlich fixiert, regelmäßig überprüft und allen relevanten Mitarbeitern zugänglich sein. Das betrifft Passwortrichtlinien, Zugriffskontrolle, Umgang mit mobilen Geräten, Patch-Management und viele weitere operative Bereiche. Ergänzt wird dies durch ein zentrales Dokumentenmanagementsystem, das Versionshistorie und Gültigkeitsdaten pflegt.

Stufe	Frist	Inhalt
Erstmeldung	24 Stunden	Verdachtseinschätzung: rechtswidrige Handlung? Grenzüberschreitende Auswirkungen?
Bewertungsmeldung	72 Stunden	Bestätigung, Schweregrad, Auswirkungen, Kompromittierungsindikatoren
Zwischenmeldung	Auf Ersuchen des BSI	Statusaktualisierungen zum laufenden Vorfall
Abschlussmeldung	1 Monat	Vollständige Beschreibung, Ursache, Abhilfemaßnahmen, grenzüberschreitende Auswirkungen

Ein erheblicher Sicherheitsvorfall liegt gemäß § 2 Nr. 11 BSIG vor, wenn er schwerwiegende Betriebsstörungen, finanzielle Verluste oder erhebliche Schäden bei Dritten verursacht hat oder verursachen kann. Im Zweifelsfall: lieber zu früh melden als zu spät.

Was bedeutet das in der Praxis?

24 Stunden sind wenig. Wer im Ernstfall erst nach einem Schuldigen sucht oder interne Abstimmungsschleifen dreht, verpasst die Frist. Ein funktionierender Incident-Response-Prozess muss vor dem ersten Vorfall stehen – mit klaren Rollen, Eskalationswegen und vorbereiteten Meldetexten.

Typische Pain Points

- Kein dediziertes Incident-Response-Team oder klar benannter Notfallkoordinator
- Meldeprozess zum BSI nicht bekannt oder nicht geübt
- Keine Klassifikationskriterien: Was ist ein „erheblicher Sicherheitsvorfall“?
- Interne Kommunikationswege im Krisenfall nicht definiert

Checkliste

- ✓ **Incident-Response-Plan** dokumentiert und kommuniziert
- ✓ **Incident-Response-Team** benannt (intern oder extern)
- ✓ **Klassifikationskriterien** für erhebliche Sicherheitsvorfälle definiert
- ✓ **Meldeprozess** zum BSI (24h/72h/Abschluss) implementiert und geübt
- ✓ **Interne Eskalationskette** und Kommunikationskanäle festgelegt
- ✓ Mindestens jährlich **eine Incident-Response-Übung** durchgeführt
- ✓ **Nachbereitung** (Lessons Learned) als fester Prozessbestandteil

Praxisbeispiel: Ransomware-Angriff auf einen Gesundheitsdienstleister

Freitagabend, 22 Uhr: Ein Krankenhausbetreiber stellt fest, dass mehrere Server verschlüsselt sind. Ohne vorbereiteten Incident-Response-Plan beginnt eine mehrstündige Orientierungsphase. Die BSI-Erstmeldung erfolgt erst nach 31 Stunden. Das ist zu spät.

Mit einem vorbereiteten Plan sieht es anders aus: Vorfallklassifikation in 15 Minuten, BSI-Erstmeldung nach 4 Stunden, parallele Forensik und Eindämmungsmaßnahmen. Die Differenz: ein Bußgeldverfahren auf der einen, ein ordnungsgemäß abgewickelter Vorfall auf der anderen Seite.

> *„Die NIS2 bestätigt, es kann keine Digitalisierung ohne IT-Sicherheit erfolgen.“*

Tobias Apel, Geschäftsführer Apro GmbH

Kontinuitätsplanung (Business Continuity Management & Disaster Recovery)

Was fordert NIS-2?

§ 30 Abs. 2 Nr. 3 BSIG fordert Maßnahmen zur Aufrechterhaltung des Betriebs: Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement. Der Referenzstandard ist ISO 22301, in Deutschland ergänzt durch BSI-Standard 200-4.

Was bedeutet das in der Praxis?

Business Continuity Management ist mehr als Backups. Es geht darum, geschäftskritische Prozesse zu identifizieren, Wiederherstellungsziele zu definieren (RTO/RPO) und dokumentierte Notfall- sowie Wiederanlaufpläne vorzuhalten. Entscheidend: Diese Pläne müssen regelmäßig getestet werden. Ein ungetestetes Backup ist kein Backup.

RTO steht für „**Recovery Time Objective**" und bezeichnet die maximale Zeitspanne, die ein System oder ein Prozess ausfallen darf, bevor der Schaden für das Unternehmen untragbar wird. Vereinfacht ausgedrückt stellt sich die Frage: Wie lange darf es dauern, bis alles wieder läuft?

RPO steht für „**Recovery Point Objective**" und bezeichnet den maximalen Zeitraum, für den Datenverlust noch akzeptabel ist. Vereinfacht gefragt: Wie alt darf das letzte Backup sein, auf das ich im Notfall zurückgreife?

Typische Pain Points

- Backups existieren, werden aber nie auf Wiederherstellbarkeit getestet
- RTO und RPO sind nicht definiert. Niemand weiß, wie lange ein Ausfall tolerierbar ist
- BCM-Pläne existieren auf Papier, sind aber nicht geübt oder veraltet
- Keine Krisenorganisation: Im Ernstfall fehlt Führung und klare Zuständigkeit

Checkliste

- ✓ **Business-Impact-Analyse durchgeführt:** kritische Prozesse identifiziert
- ✓ **RTO und RPO** für alle kritischen Systeme **definiert**
- ✓ **Backup-Konzept nach 3-2-1-Regel implementiert** (3 Kopien, 2 Medien, 1 off-site)
- ✓ **Backup-Wiederherstellung** mindestens jährlich getestet
- ✓ **Notfall- und Wiederanlaufpläne** dokumentiert und zugänglich
- ✓ **Krisenorganisation** mit Rollen und Stellvertretungen definiert
- ✓ **Regelmäßige BCM-Übungen** durchgeführt (mindestens jährlich)

Praxisbeispiel: Das ungetestete Backup

Ein produzierendes Unternehmen hat seit Jahren täglich Backups eingespielt. Nach einem Ransomware-Angriff stellt sich heraus: Die Backups sind korrumpiert, weil eine Konfigurationsänderung vor Monaten unbemerkt den Backup-Prozess unterbrochen hat. RTO: theoretisch 4 Stunden. Realität: 3 Wochen Produktionsausfall.

Die Lösung wäre einfach gewesen: Quartalsweise Wiederherstellungstests mit Protokoll. Kosten: wenige Stunden IT-Zeit. Ersparnis: Millionenschäden und ein Bußgeldverfahren.

Lieferkettensicherheit

Was fordert NIS-2?

§ 30 Abs. 2 Nr. 4 BSIG verpflichtet zur Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern und Diensteanbietern. ISO/IEC 27002:2022 widmet Maßnahmen 5.19 bis 5.22 eigens diesem Bereich.

Was bedeutet das in der Praxis?

Mehr als die Hälfte aller Unternehmen gibt an, bei der Lieferkettensicherheit Nachholbedarf zu haben. Kein Wunder: Die Anforderungen sind komplex. Es geht um Sicherheitsanforderungen in Verträgen, die regelmäßige Bewertung kritischer Lieferanten, Monitoring, Audit-Rechte und die Berücksichtigung von Konzentrationsrisiken.

Wichtig: Eine einfache Klausel im Vertrag, die den Lieferanten zur Einhaltung von Sicherheitsstandards verpflichtet, reicht nicht aus. Ohne tatsächliche Überprüfung und Überwachung ist die vertragliche Regelung wertlos und schützt nicht vor Haftung.

Typische Pain Points

- Kein strukturiertes Lieferantenverzeichnis mit Kritikalitätsbewertung
- Sicherheitsanforderungen in Verträgen zu allgemein oder nicht überprüft
- Keine Prozesse für das Monitoring von Lieferantensicherheit
- Konzentrationsrisiken (Abhängigkeit von wenigen kritischen Dienstleistern) nicht bewertet

Checkliste

- ✓ **Verzeichnis aller kritischen IT-Dienstleister** und Lieferanten erstellt
- ✓ **Kritikalitätsbewertung** für jeden Lieferanten durchgeführt
- ✓ **Sicherheitsanforderungen vertraglich verankert** (Patch-Management, BCM, Incident Management)
- ✓ **Nachweise von kritischen Lieferanten eingeholt** (Zertifikate, Audit-Berichte)
- ✓ **Notfall- und Wiederanlaufpläne** dokumentiert und zugänglich
- ✓ **Monitoring-Prozess** für laufende Lieferantenbewertung etabliert
- ✓ **Konzentrationsrisiken bewertet** und Alternativoptionen geprüft

Praxisbeispiel: Der kompromittierte Dienstleister

Ein IT-Dienstleister, der für mehrere mittelständische Unternehmen das Remote-Monitoring betreibt, wird Opfer eines Angriffs. Über die kompromittierten Zugangsdaten des Dienstleisters dringen Angreifer in die Netzwerke von sechs Kundenunternehmen ein.

Zwei dieser Unternehmen hatten den Dienstleister vertraglich zu Sicherheitsmaßnahmen verpflichtet und Nachweis-Audits durchgeführt. Sie erkennen den Angriff früh und begrenzen den Schaden. Die vier anderen werden wochenlang kompromittiert, bevor der Angriff auffällt.

Security Awareness & Schulungen

Was fordert NIS-2?

§ 30 Abs. 2 Nr. 7 BSIG fordert grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Informationssicherheit. § 38 Abs. 3 macht diese Pflicht explizit auch für die Geschäftsleitung verbindlich.

Was bedeutet das in der Praxis?

Technik allein schützt nicht. Der Mensch bleibt das häufigste Einfallstor. Ein wirksames Awareness-Programm umfasst zielgruppenspezifische Schulungen, Phishing-Simulationen, anlassbezogene Trainings und zwingend dokumentierte Teilnahmenachweise. Für die Geschäftsleitung bedeutet das: nicht nur eine Einmalteilnahme, sondern regelmäßige Aktualisierung.

Typische Pain Points

- Schulungen sind Pflichtprogramm ohne erkennbare Wirkung
- Phishing-Simulationen fehlen: Mitarbeiter werden nie auf Social Engineering-Angriffe getestet
- Keine Differenzierung nach Zielgruppen: IT-Admins, Management und Sachbearbeiter haben verschiedene Bedrohungsprofile
- Teilnahmenachweise werden nicht systematisch erfasst

Checkliste

- ✓ **Jährliches Awareness-Training** für alle Mitarbeiter implementiert
- ✓ **Phishing-Simulationen** regelmäßig durchgeführt und ausgewertet
- ✓ **Zielgruppenspezifische Schulungen** für Management, IT und Fachabteilungen
- ✓ **NIS-2-Schulung** für alle Mitglieder der Geschäftsleitung dokumentiert
- ✓ **Anlassbezogene Schulungen** bei neuen Bedrohungen oder Vorfällen
- ✓ **Teilnahmenachweise** systematisch erfasst und archiviert

Praxisbeispiel: Phishing-Mail trifft Finanzabteilung

Eine täuschend echte E-Mail, angeblich vom CEO, fordert die Buchhaltung auf, dringend eine Zahlung auszuführen. CEO-Fraud gehört zu den üblichen Angriffsszenarien. In Unternehmen ohne Awareness-Training landet solche Post oft beim Ziel.

Unternehmen, die regelmäßig Phishing-Simulationen durchführen, zeigen statistisch deutlich niedrigere Klickraten auf echte Angriffe. Awareness-Training ist keine Soft-Maßnahme – es ist messbare Risikoreduktion.

In 4 Schritten zur Compliance

NIS-2-Compliance ist kein Sprint, sondern ein strukturiertes Projekt. Die folgende Roadmap ist typischerweise in 12 bis 18 Monaten durchführbar und orientiert sich am PDCA-Zyklus. Der PDCA-Zyklus ist ein iteratives Managementmodell zur kontinuierlichen Verbesserung von Prozessen. Er besteht aus vier Phasen:

Entscheidend: Starten Sie jetzt. Jeder Tag ohne Handeln erhöht das Haftungsrisiko.

Schritt 1

Gap-Analyse

Betroffenheit nach § 28 BSIG prüfen. Registrierung beim BSI (§ 33 BSIG). Inventur vorhandener Sicherheitsmaßnahmen, Dokumentation und Prozesse. Identifikation kritischer Geschäftsprozesse.

Schritt 2

Bestandsaufnahme

Systematischer Abgleich des Ist-Zustands mit § 30 Abs. 2 BSIG. Lücken identifizieren. Risikobewertung der Lücken. Priorisierten Maßnahmenplan mit Budget und Zeitplan erstellen.

Schritt 3

Maßnahmen umsetzen

Priorisierte Maßnahmen umsetzen. Meldeprozesse nach § 32 aufbauen. Incident-Response-Organisation etablieren. Geschäftsleitungsschulungen nach § 38 Abs. 3 durchführen. Alle Maßnahmen gemäß § 30 Abs. 1 S. 3 dokumentieren.

Schritt 4

Nachweis & kontinuierliche Verbesserung

Interne Audits zur Wirksamkeitsprüfung. Für Betreiber kritischer Anlagen: Vorbereitung der Nachweispflicht nach § 39 BSIG (alle drei Jahre). PDCA-Zyklus etablieren. Regelmäßige Managementbewertung.

Zeitrahmen beachten

Die Registrierungspflicht greift drei Monate nach erstmaliger Betroffenheit. Für besonders wichtige Einrichtungen kann das BSI frühestens drei Jahre nach Inkrafttreten (also ab Dezember 2028) Nachweise anordnen. Für Krankenhäuser nach § 108 SGB V erst nach fünf Jahren. Das bedeutet aber nicht, dass bis dahin nichts zu tun ist, die Pflichten gelten ab sofort.

Schritt 1

Bestandsaufnahme
(Monate 1 bis 3)

Klären Sie zuerst die Grundfragen: Ist Ihr Unternehmen betroffen? In welche Kategorie fällt es? Welche Sektorzugehörigkeit liegt vor? Verbundene Unternehmen einberechnet? Erfüllen Sie die Registrierungspflicht innerhalb von drei Monaten nach Betroffenheit.
Gleichzeitig erheben Sie den Status quo: Welche Sicherheitsmaßnahmen, Richtlinien und Prozesse existieren bereits? Was ist dokumentiert? Was fehlt? Diese Bestandsaufnahme ist die Grundlage für alles Folgende.

Schritt 2

Gap-Analyse
(Monate 3 bis 6)

Gleichen Sie den Ist-Zustand systematisch mit den zehn Maßnahmenbereichen des § 30 Abs. 2 BSIG ab. Identifizieren Sie Lücken, bewerten Sie deren Risiko und erstellen Sie einen priorisierten Maßnahmenplan mit klaren Verantwortlichkeiten, Budget und Zeitplan.
Tipp: Holen Sie sich externe Expertise. Ein unabhängiger Blick deckt blinde Flecken auf und externe Auditoren haben im Zweifelsfall Bedeutung vor Behörden.

Schritt 3

Maßnahmenumsetzung
(Monate 6 bis 15)

Setzen Sie die priorisierten Maßnahmen um, von der dringendsten Lücke zur langfristigen Optimierung. Parallel dazu: Meldeprozesse aufbauen, Incident-Response-Organisation etablieren, Geschäftsleitungsschulungen durchführen und alle Maßnahmen dokumentieren. § 30 Abs. 1 S. 3 BSIG fordert den Nachweis ausdrücklich.

Schritt 4

Nachweis & kontinuierliche Verbesserung
(ab Monat 15)

Compliance ist kein Endzustand. Die Bedrohungslage verändert sich, neue Technologien kommen, Lieferanten wechseln. Etablieren Sie einen PDCA-Zyklus mit regelmäßigen internen Audits, Penetrationstests und Managementbewertungen.

Für Betreiber kritischer Anlagen gilt zusätzlich die Nachweispflicht nach § 39 BSIG alle drei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen.

> *„Wer als Geschäftsführer nachweisen kann, dass er sich aktiv mit dem Thema Informationssicherheit auseinandergesetzt hat, steht in einem ganz anderen Licht – gegenüber Behörden, Kunden und sich selbst. Der erste Schritt ist der wichtigste.“*

Uwe Bergmann, Geschäftsführer Nethinks

10 Sofortmaßnahmen für Geschäftsführer

Diese zehn Maßnahmen können Sie unmittelbar einleiten. Priorisiert nach Dringlichkeit und Wirkung.
Dafür ist kein langer Vorlauf, keine aufwändige Vorbereitung notwendig.

	Sofortmaßnahme	Rechtsgrundlage
1	Betroffenheit prüfen: Mitarbeiterzahl, Umsatz und Sektorzugehörigkeit verbindlich feststellen. Verbundene Unternehmen einberechnen.	§ 28 BSIG
2	Registrierung beim BSI: Pflichtangaben innerhalb von drei Monaten über die gemeinsame Registrierungsstelle von BSI und BBK übermitteln.	§ 33 BSIG
3	Verantwortlichkeiten benennen: Informationssicherheitsbeauftragten bestimmen und direkten Berichtsweg an die Geschäftsleitung sicherstellen.	§ 30, § 38 BSIG
4	Geschäftsleitungsschulung: Qualifizierte NIS-2-Schulung für alle Mitglieder der Geschäftsleitung planen und dokumentiert durchführen.	§ 38 Abs. 3 BSIG
5	Incident-Response-Prozess: Meldeverfahren aufbauen, das die 24h/72h-Fristen des § 32 einhalten kann. Incident-Response-Team benennen.	§ 32, § 30 Abs. 2 Nr. 2
6	Risikoinventar erstellen: Kritische IT-Assets identifizieren, geschäftskritische Prozesse benennen und erste Risikobeurteilung durchführen.	§ 30 Abs. 2 Nr. 1
7	Backup-Strategie validieren: Backups auf Aktualität, Testbarkeit und Wiederherstellbarkeit prüfen. RTO und RPO für kritische Systeme definieren.	§ 30 Abs. 2 Nr. 3
8	MFA aktivieren: Multi-Faktor-Authentifizierung für alle administrativen und fernzugangsfähigen Zugänge einführen.	§ 30 Abs. 2 Nr. 10
9	Lieferanten bewerten: Verzeichnis kritischer IT-Dienstleister erstellen, Kritikalität bewerten und Sicherheitsnachweise einfordern.	§ 30 Abs. 2 Nr. 4
10	Dokumentation starten: Alle Sicherheitsmaßnahmen systematisch dokumentieren. § 30 Abs. 1 S. 3 fordert den Nachweis ausdrücklich.	§ 30 Abs. 1 S. 3

Compliance ist eine Haltung

NIS-2 ist kein bürokratisches Übel. Es ist der überfällige Schritt, Cybersicherheit dort zu verankern, wo sie hingehört: in der Unternehmensführung. Wer jetzt handelt, schützt nicht nur sein Unternehmen vor Bußgeldern und Haftungsrisiken, sondern baut Vertrauen auf. Bei Kunden, Lieferanten und Partnern.

Die Realität ist: Die meisten Unternehmen sind nicht bei null. Sie haben Firewalls, Backup-Systeme, vielleicht sogar ein anfängliches ISMS. Was fehlt, ist meistens die Systematik bzw. ein strukturierter Ansatz, der Einzelmaßnahmen zu einem kohärenten Sicherheitskonzept zusammenfügt und dieses nachvollziehbar dokumentiert.

Drei Grundprinzipien gelten für jeden, der jetzt anfangen will: Erstens, Betroffenheit klären und registrieren. Zweitens, die größten Risiken zuerst angehen. Perfektionismus ist der Feind des Fortschritts. Drittens, alles dokumentieren. Was nicht nachgewiesen werden kann, zählt vor Behörden nicht.

Cybersicherheit ist keine einmalige Investition. Die Bedrohungslage verändert sich täglich, neue Angriffsmöglichkeiten entstehen durch KI-gestützte Angriffswerkzeuge, wachsende Lieferketten und zunehmende Vernetzung. Wer heute compliant ist, muss morgen weiter lernen. NIS-2 gibt dafür den rechtlichen Rahmen, die innere Haltung muss jedes Unternehmen selbst entwickeln.

NIS-2-Compliance gelingt am schnellsten mit erfahrenen Partnern an Ihrer Seite. Kontaktieren Sie uns für ein unverbindliches Erstgespräch. Wir helfen Ihnen, den nächsten konkreten Schritt zu machen.

apro.gmbh – IT-Sicherheit & Compliance

Die apro.gmbh begleitet Unternehmen bei der strukturierten NIS-2-Umsetzung: von der Gap-Analyse über den Aufbau eines ISMS bis zur Prüfungsvorbereitung. Mit klarem Fokus auf mittelständische Realitäten.

apro.gmbh/

Link11 – DDoS-Schutz & Cloud-Security

Link11 schützt Unternehmen und kritische Infrastrukturen vor DDoS-Angriffen und weiteren Cyberbedrohungen, mit KI-gestützter Echtzeiterkennung und höchster Verfügbarkeit rund um die Uhr.

www.link11.com

Nethinks – Managed Security & Infrastruktur

Nethinks liefert die technische Infrastruktur für sichere IT-Betriebsumgebungen und unterstützt Unternehmen beim Aufbau NIS-2-konformer Systeme, von Netzwerksicherheit bis Managed Services.

www.nethinks.com

Glossar

Begriff	Erläuterung
Besonders wichtige Einrichtung	Einrichtung nach § 28 Abs. 1 BSIG – unterliegt der proaktiven Aufsicht des BSI (§ 61 BSIG)
Wichtige Einrichtung	Einrichtung nach § 28 Abs. 2 BSIG – unterliegt der reaktiven Aufsicht bei begründetem Verdacht (§ 62 BSIG)
Erheblicher Sicherheitsvorfall	Vorfall, der schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht oder Dritte erheblich schädigt (§ 2 Nr. 11 BSIG)
Kritische Anlage	Anlage von erheblicher Bedeutung für eine kritische Dienstleistung (§ 2 Nr. 22 BSIG)
Geschäftsleitung	Natürliche Person zur Führung und Vertretung berufen (§ 2 Nr. 13 BSIG) – Haftungsadressat nach § 38
BSIG	Gesetz über das BSI und über die Sicherheit in der IT von Einrichtungen (Artikel 1 des NIS-2-Umsetzungsgesetzes)
ISMS	Informationssicherheitsmanagementsystem nach ISO/IEC 27001
BCM / BCMS	Business Continuity Management (System) nach ISO 22301
RTO / RPO	Recovery Time Objective / Recovery Point Objective: maximale Ausfallzeit / maximaler Datenverlust
All-Hazard-Ansatz	Gefahrenübergreifender Ansatz: Berücksichtigung aller Bedrohungsarten (Cyber, physisch, organisatorisch)
DDoS	Distributed Denial of Service: Angriff zur Überlastung von IT-Systemen oder Netzwerken
PDCA-Zyklus	Plan-Do-Check-Act: Qualitätsmanagementkreislauf für kontinuierliche Verbesserung

Weiterführende Quellen

Gesetzestexte und Regulierung

- NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (BGBl. 2025 I Nr. 301)
- EU-Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)
- BSI-Kritisverordnung (BSI-KritisVO) in der jeweils geltenden Fassung

Standards und Normen

- ISO/IEC 27001:2022 – Informationssicherheitsmanagementsysteme
- ISO/IEC 27002:2022 – Informationssicherheitsmaßnahmen
- ISO/IEC 27005:2022 – Informationssicherheitsrisikomanagement
- ISO 22301:2019 – Business Continuity Management
- BSI-Standard 200-1: Managementsysteme für Informationssicherheit
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 200-4: Business Continuity Management
- BSI IT-Grundschutz-Kompendium (aktuellste Fassung)

BSI und ENISA

BSI – Registrierung, Meldestelle, IT-Grundschutz: www.bsi.bund.de

ENISA – Europäische Agentur für Cybersicherheit: www.enisa.europa.eu

NIS-2-Betroffenheitsprüfung des BSI: www.bsi.bund.de/NIS-2


LINK11