

01

Whitepaper
Cybersicherheit & Regulierung

NIS2 im ersten Jahr: Umsetzen statt abwarten

Betroffenheit, Registrierung, Risikomanagement
und Meldewege – mit Fahrplan und Checkliste

Inhalt

01	Auf einen Blick	3
	Die wichtigsten Fakten, Fristen und ersten Schritte für eilige Leser.	
02	Die Lage	4
	Warum Cyberangriffe ein Thema für die Geschäftsleitung bleiben.	
03	Wer betroffen ist	5
	Direkt nach Sektor und Größe – oder indirekt über die Lieferkette.	
04	Registrierung	8
	Warum die Pflicht weiter gilt und wie die Registrierung abläuft.	
05	Pflichten, Haftung und Aufsicht	10
	Risikomanagement, Meldewege, Verantwortung der Leitung und die angekündigte Aufsicht.	
06	Fahrplan und Checkliste	14
	Eine Reihenfolge für die nächsten Monate, zum Abhaken.	
07	Wie Delta One unterstützt	15
	Bestandsaufnahme, Umsetzung und Betrieb aus einer Hand.	
	Quellen und Impressum	16

FÜR WEN

Geschäftsleitung und IT-Verantwortliche in Unternehmen mit 20 bis 150 Beschäftigten, in Kommunen und kommunalen Unternehmen

LESEZEIT

etwa 12 Minuten, Kapitel 01 in drei Minuten

STAND

15. Oktober 2026

Auf einen Blick

Das neue BSI-Gesetz gilt seit dem 06.12.2025^[1, 2]. Die Registrierungsfrist ist abgelaufen^[3], und das BSI hat angekündigt, die Pflichten durchzusetzen^[4]. Wer betroffen ist, braucht jetzt ein dokumentiertes Risikomanagement und einen geübten Meldeweg.

20.373

NIS2-Registrierungen beim BSI, Stand 30.09.2026, inklusive Nebenniederlassungen; BSI-Angabe laut Presse. Fast ein Drittel fehlt noch.^[4]

Quelle: ChannelPartner nach Tagesspiegel, 08.10.2026

58 %

der befragten Unternehmen hatten in den letzten zwölf Monaten einen Schaden durch Cyberangriffe.^[5]

Quelle: Bitkom, Wirtschaftsschutz 2026

24^h

Frist für die frühe Erstmeldung eines erheblichen Sicherheitsvorfalls, gerechnet ab Kenntnis.^[6]

Quelle: § 32 Abs. 1 BSIG



Gilt ohne allgemeine Übergangsfrist

Das Gesetz ist seit dem 06.12.2025 in Kraft^[1, 2]. Die Registrierungsfrist endete am 06.03.2026^[3], die Nachfrist des BSI am 31.07.2026^[7].



Das BSI kündigt Durchsetzung an

Laut Presseberichten hat das BSI für das vierte Quartal 2026 eine Durchsetzungsinitiative mit Anschreiben und Anhörung angekündigt. Ab dem ersten Quartal 2027 sollen Prüfungen folgen^[4].



Betroffenheit selbst prüfen

Sektor und Größe entscheiden. Das BSI prüft das nicht von sich aus^[3]. Halten Sie Ihr Ergebnis deshalb schriftlich fest.



Zehn Pflichtfelder umsetzen

§ 30 BSIG verlangt verhältnismäßige Maßnahmen von der Risikoanalyse bis zur Mehr-Faktor-Authentifizierung – und deren Dokumentation^[6].



Die Leitung bleibt verantwortlich

Die Geschäftsleitung muss die Maßnahmen umsetzen, ihre Umsetzung überwachen und regelmäßig an Schulungen teilnehmen^[6].



Die Lieferkette zieht mit

Auch wer nicht selbst betroffen ist, erhält Anforderungen über Fragebögen, Vertragsklauseln und Nachweispflichten seiner Kunden^[2].

Ihre ersten drei Schritte

1

Betroffenheit prüfen und das Ergebnis mit Datum dokumentieren.

2

Registrierung im BSI-Portal prüfen oder sofort nachholen.

3

Meldeweg für die 24-Stunden-Frist festlegen und einmal üben.

Cyberangriffe verursachen drei Viertel der Schäden

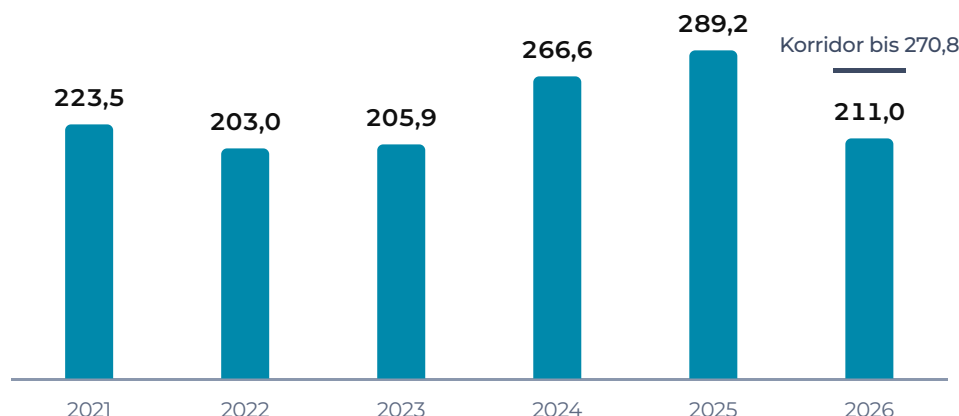
76%

Anteil der Cyberangriffe am Schaden durch Datendiebstahl, Spionage und Sabotage in Deutschland 2026. Insgesamt beziffert Bitkom diesen auf mindestens 211,0 Mrd. €^[5].

Quelle: Bitkom e. V., Wirtschaftsschutz 2026, 26.08.2026, Folien 5 und 12

Abb. 1 Schaden 2026 unter Vorjahr, auf dem Niveau von 2021–2023

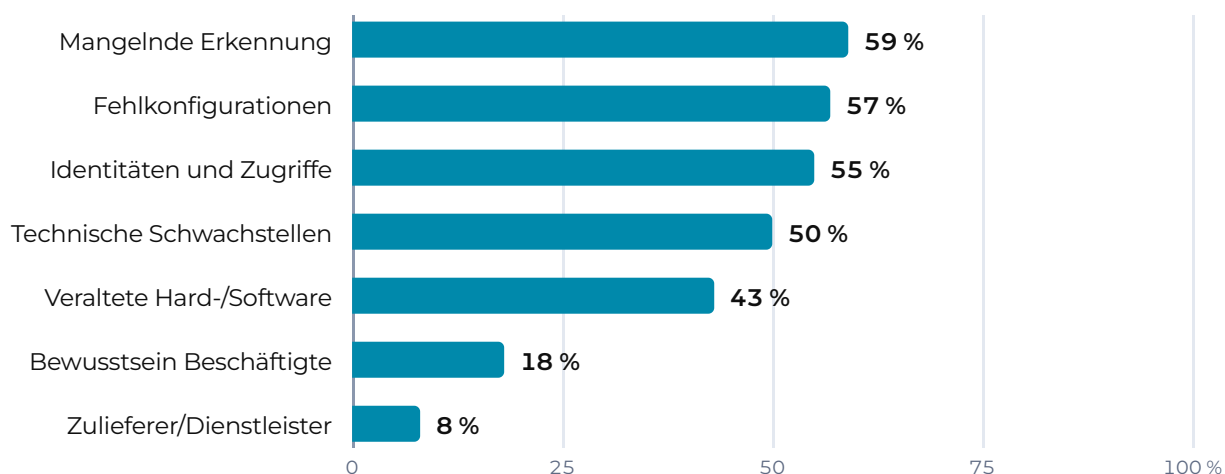
Schaden durch Datendiebstahl, Spionage und Sabotage in Deutschland, in Mrd. €; 2026 Mindestwert



Quelle: Bitkom e. V., Wirtschaftsschutz 2026, 26.08.2026, Folien 4 und 5; eigene Darstellung.

Abb. 2 Erkennung, Konfiguration und Zugriffe als häufigste Ursachen

Maßgebliche Faktoren erfolgreicher Angriffe; Anteil der Geschädigten in %, Mehrfachnennungen, n = 580



Quelle: Bitkom e. V., Wirtschaftsschutz 2026, 26.08.2026, Folie 15, n = 580; eigene Darstellung.

Zwei Fragen klären die Betroffenheit

Ob Ihr Unternehmen unter das BSI-Gesetz (BSIG) in der Fassung des NIS2-Umsetzungsgesetzes fällt, hängt von zwei Fragen ab: Ist es in einem Sektor der Anlage 1 oder 2 tätig? Und erreicht es die Größenschwelle^[6]?

Für die Region besonders wichtig ist Anlage 2 Nr. 5, das verarbeitende Gewerbe: unter anderem Maschinenbau, Kraftwagen und Kraftwagenteile, elektrische Ausrüstungen, elektronische Erzeugnisse und Medizinprodukte. Dazu kommen etwa Post- und Kurierdienste, Abfallbewirtschaftung, Chemie und Lebensmittel^[6]. Anlage 1 nennt ausdrücklich auch Managed Service Provider^[6].

Gezählt wird nach der KMU-Empfehlung der EU. Daten von Partner- und verbundenen Unternehmen werden nicht hinzugerechnet, wenn Ihr Unternehmen bei IT-Systemen und Prozessen unabhängig ist^[6]. Hier entstehen leicht Fehleinschätzungen.



PRAXISTIPP

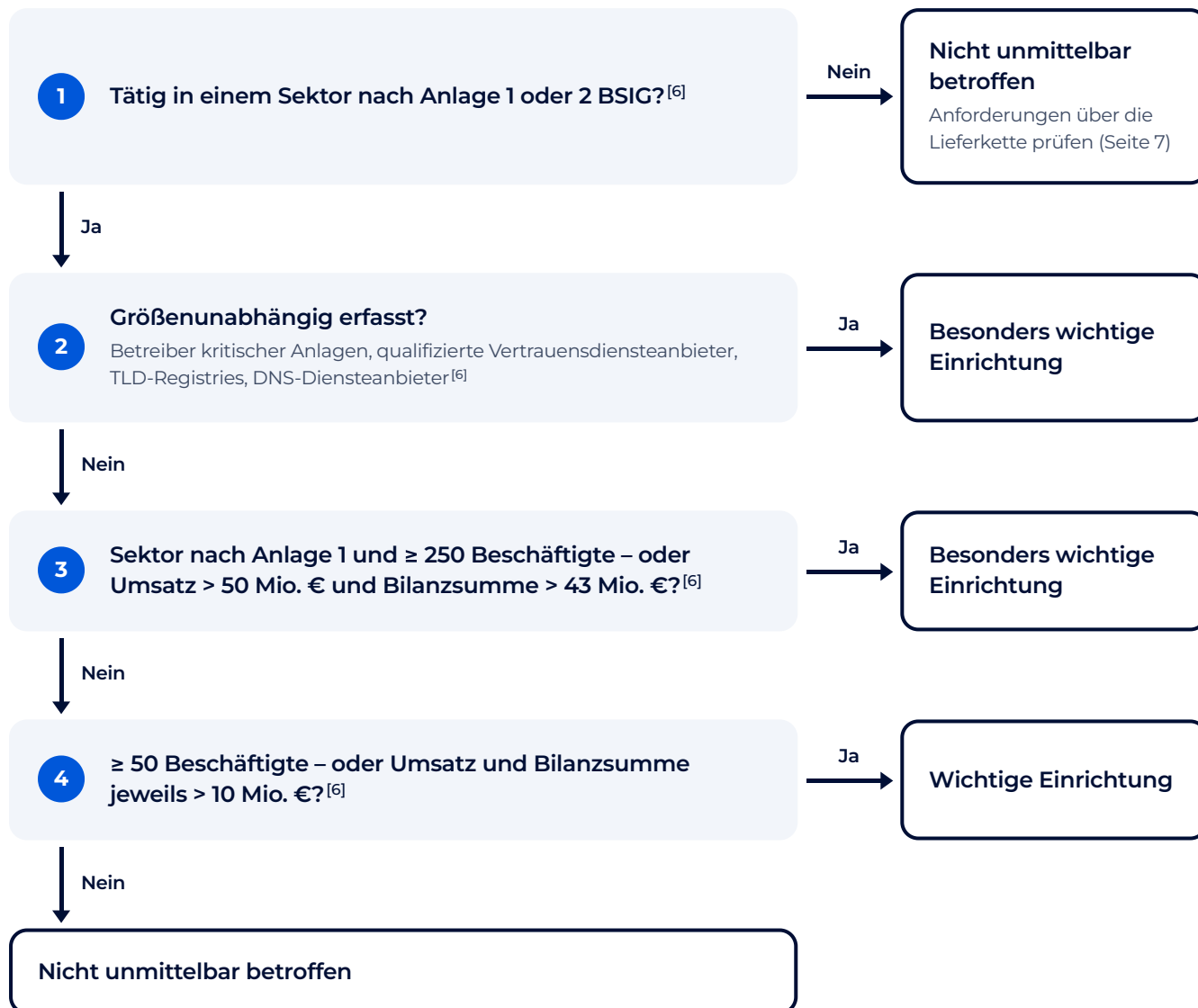
Das BSI prüft die Betroffenheit nicht von sich aus^[3]. Nutzen Sie die Online-Betroffenheitsprüfung des BSI^[8] und halten Sie Ihr Ergebnis mit Datum schriftlich fest.

KOMMUNEN

Kommunale Verwaltungen fallen in der Regel nicht unter das BSIG^[6]. In Bayern gelten die NIS2-Pflichten nach dem Bayerischen Digitalgesetz (Änderung vom 08.10.2024) nur für staatliche Behörden; Kommunen einschließlich der Landratsämter sind laut Gesetzesbegründung ausdrücklich nicht einbezogen^[9]. Sie sind damit nicht unmittelbar verpflichtet, aber von denselben Risiken betroffen. Kommunale Unternehmen wie Stadtwerke können dagegen erfasst sein.

Abb. 3 Sektor und Größe bestimmen die Einstufung

Vereinfachte Darstellung nach § 28 BSIG, ersetzt keine Einzelfallprüfung.



Zählung nach KMU-Empfehlung 2003/361/EG; Partner- und verbundene Unternehmen sowie vernachlässigbare Tätigkeiten: § 28 Abs. 3 und 4 BSIG^[6]. Kommunalverwaltungen in der Regel nicht erfasst (§ 28 Abs. 8 BSIG)^[6].

Quelle: § 28 Abs. 1–4 und 8 sowie Anlagen 1 und 2 BSIG; vereinfachte eigene Darstellung, ersetzt keine Einzelfallprüfung.

Die Anforderungen kommen über die Lieferkette

Wer selbst nicht unter das BSIG fällt, bekommt dessen Anforderungen oft über Kunden, die es tun. Ein vorbereitetes Nachweispaket macht Sie dafür auskunftsfähig.

Betroffene Einrichtungen müssen nach § 30 Abs. 2 Nr. 4 BSIG die Sicherheit ihrer Lieferkette gewährleisten, auch gegenüber unmittelbaren Anbietern und Diensteanbietern^[6]. Diesen Druck geben sie über Fragebögen, Vertragsklauseln und Nachweise an ihre Zulieferer weiter^[2]. Typisch sind Selbstauskünfte zu technischen und organisatorischen Maßnahmen (TOM), Audit- und Prüfrechte, Verweise auf ISO/IEC 27001 oder IT-Grundschutz und die Pflicht, Vorfälle unverzüglich zu melden^[2]. Denn der Kunde muss seine eigenen Meldefristen von 24 und 72 Stunden halten^[6].

21 %

der geschädigten Unternehmen berichten, dass ihr Schaden Folgen für andere Unternehmen hatte (Bitkom 2026, n = 671)^[5].

Das Risiko ist real: Bei jedem fünften erfolgreichen Angriff hatte der Schaden Folgen für andere Unternehmen^[5]. Laut Bitkom nennen 8 % der durch Cyberangriffe geschädigten Unternehmen die Kompromittierung über Zulieferer oder Dienstleister als maßgeblichen Faktor erfolgreicher Angriffe^[5].

DIGITALBONUS BAYERN

Zuschuss bis 7.500 € (Standard) oder 30.000 € (Plus), jeweils bis 50 %, Mindestausgaben 4.000 €^[10]. Antrag nur durch das Unternehmen selbst per ELSTER-Unternehmenskonto, Start erst nach Eingangsbestätigung^[10]. Laufzeit bis 31.12.2027^[10].

Was Zulieferer vorbereiten sollten

Empfehlenswert ist ein schlankes Nachweispaket: eine TOM-Übersicht entlang der zehn Pflichtfelder aus Kapitel 05, ein Nachweis zu Datensicherung und Wiederanlauf, die Abdeckung der Mehr-Faktor-Authentifizierung und ein benannter Ansprechpartner für Sicherheitsvorfälle. Einmal sauber erarbeitet, lässt sich dieses Paket für mehrere Kunden verwenden und bei Änderungen zentral aktualisieren.



FÖRDERHINWEIS

Kleine Unternehmen in Bayern mit weniger als 50 Beschäftigten können über den Digitalbonus Bayern Zuschüsse für IT-Sicherheit erhalten, etwa für Firewalls^[10]. Maßnahmen mit gesetzlicher Verpflichtung sind nicht förderfähig^[10] – der Bonus passt daher für Zulieferer, die selbst nicht NIS2-pflichtig sind.

Die Registrierungspflicht gilt unverändert

Besonders wichtige und wichtige Einrichtungen müssen sich spätestens drei Monate, nachdem sie erstmals oder erneut als solche gelten, beim BSI registrieren (§ 33 BSIG)^[6]. Für alle, die schon bei Inkrafttreten betroffen waren, endete diese Frist am 06.03.2026^[3]. Die Nachfrist bis 31.07.2026 war eine Kulanz des BSI, keine Gesetzesänderung^[7, 13].

NICHT VERWECHSELN

Mit einem Ende Juli 2026 verkündeten Gesetz (BGBl. 2026 I Nr. 221) wurde im KRITIS-Dachgesetz ein Stichtag gestrichen – der 17.07.2026 für die Registrierung kritischer Anlagen beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)^[11]. Die NIS2-Registrierung nach § 33 BSIG ist davon nicht berührt^[6, 8].

Registriert wird in zwei Schritten: zuerst ein ELSTER-Organisationszertifikat über „Mein Unternehmenskonto“ beantragen, dann mit diesem Konto im BSI-Portal registrieren^[8]. Über dasselbe Portal laufen später die Meldungen^[3, 6]. Änderungen, etwa von Kontaktdaten, sind binnen zwei Wochen mitzuteilen^[6]. Fehlt die Registrierung, kann das BSI selbst registrieren^[6]; außerdem droht ein Bußgeld bis 500.000 €^[6].

„Die gesetzliche Registrierungsfrist ist bereits abgelaufen.“

BSI, Themenseite NIS-2-regulierte Unternehmen, Stand 10.08.2026^[8]



PRAXISTIPP

Die Beantragung des ELSTER-Zertifikats braucht Zeit. Warten Sie damit nicht bis zum ersten Vorfall – ohne Zugang zum Portal lässt sich auch keine Meldung abgeben.

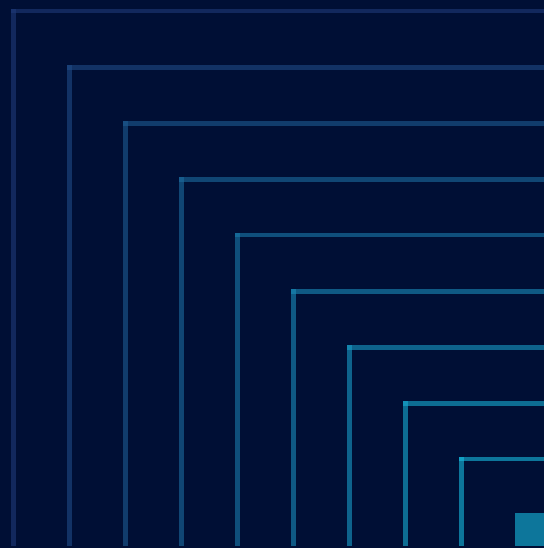
Abb. 4 Fristen abgelaufen, Durchsetzung angekündigt

Stationen der NIS2-Umsetzung in Deutschland; Quartalsangaben sind Ankündigungen des BSI laut Presse.



Quellen: Richtlinie (EU) 2022/2555; Scheja & Partner, 07.01.2026; Heuking, 19.02.2026; it-daily, 17.06.2026; zfk, 04.08.2026; ChannelPartner, 08.10.2026; eigene Darstellung.

05



Pflichten, Haftung und Aufsicht

Risikomanagement, Meldewege, Verantwortung der Leitung und die angekündigte Aufsicht.

IN DIESEM KAPITEL

5.1	Zehn Pflichtfelder, verhältnismäßig umgesetzt	11
5.2	Melden in drei Stufen: 24 Stunden, 72 Stunden, ein Monat	12
5.3	Verantwortung liegt bei der Geschäftsleitung	13

Zehn Pflichtfelder, verhältnismäßig umgesetzt

Kern des Gesetzes ist das Risikomanagement nach § 30 BSIG. Verlangt wird keine Maximallösung, sondern angemessene Maßnahmen – und der Nachweis, dass sie umgesetzt sind.

FUNDSTELLE

§ 30 Abs. 1 und 2 BSIG.
Fehlende Dokumentation ist ein eigener Bußgeldtatbestand (§ 65 Abs. 2 Nr. 3 BSIG)^[6].

Gefordert sind „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“. Maßstab sind Risikoexposition, Größe, Kosten sowie Wahrscheinlichkeit, Schwere und Auswirkungen möglicher Vorfälle; dazu soll der Stand der Technik eingehalten werden. Die Einhaltung ist zu dokumentieren. Mindestens diese zehn Felder sind abzudecken^[6], in Klammern Beispiele der Redaktion:

1 Risikoanalyse und Sicherheitskonzepte

(Inventar, Schutzbedarf, Risikoliste mit Verantwortlichen)

2 Bewältigung von Sicherheitsvorfällen

(Rollen, Erreichbarkeit, Meldewege)

3 Aufrechterhaltung des Betriebs

(Backup, Notfallwiederherstellung, Krisenmanagement; Wiederherstellung testen)

4 Sicherheit der Lieferkette

(Dienstleister und unmittelbare Anbieter)

5 Sicherheit bei Erwerb, Entwicklung und Wartung

(Patch-Prozess, Schwachstellenmanagement)

6 Bewertung der Wirksamkeit

(interne Prüfungen, Kennzahlen, Übungen)

7 Schulungen und Sensibilisierung

(für alle Beschäftigten, nicht nur die IT)

8 Kryptografie

(Verschlüsselung von Datenträgern, Backups und Übertragungen)

9 Personalsicherheit, Zugriffskontrolle, IT-Verwaltung

(Ein- und Austritt, Rechtekonzept)

10 Mehr-Faktor-Authentifizierung (MFA) und gesicherte Kommunikation

(Sprache, Video, Text, gegebenenfalls Notfall)

AUS DER LAGE

Mangelnde Erkennung (59 %), Fehlkonfigurationen (57 %) und schwaches Identitäts- und Zugriffsmanagement (55 %) begünstigten laut Bitkom erfolgreiche Angriffe – Felder 2, 5 und 9/10^[5].

Für einen Betrieb mit 20 bis 150 Beschäftigten heißt verhältnismäßig nach unserer Einschätzung meist: kein eigenes Sicherheitsteam, aber klare Zuständigkeiten, ein gepflegtes Inventar, getestete Backups und MFA überall dort, wo von außen zugegriffen wird. Entscheidend ist, dass jede Maßnahme begründet und dokumentiert ist.

ISO/IEC 27001 und der IT-Grundschutz des BSI sind ein geeigneter Rahmen, aber gesetzlich nicht vorgeschrieben^[6]. Orientierung bietet die NIS-2-Checkliste des BSI vom 13.03.2026^[8].

Melden in drei Stufen: 24 Stunden, 72 Stunden, ein Monat

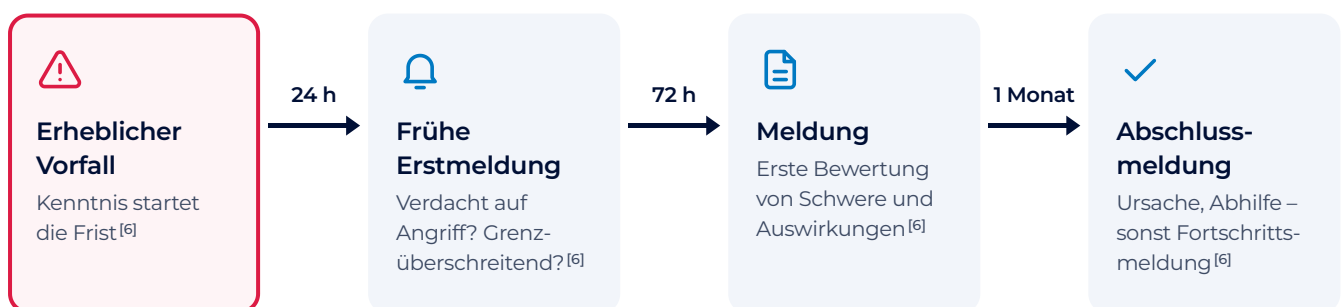
Meldepflichtig ist ein erheblicher Sicherheitsvorfall: Er hat schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht oder kann sie verursachen – oder er schädigt andere erheblich, materiell oder immateriell^[6]. Gemeldet wird an eine gemeinsame Meldestelle von BSI und BBK über das BSI-Portal^[3, 6].

Die frühe Erstmeldung muss unverzüglich, spätestens 24 Stunden nach Kenntnis eingehen. Sie sagt, ob ein rechtswidriger oder böswilliger Hintergrund vermutet wird und ob grenzüberschreitende Auswirkungen möglich sind. Spätestens nach 72 Stunden folgt die Meldung mit einer ersten Bewertung von Schweregrad und Auswirkungen. Auf Anforderung des BSI kommt eine Zwischenmeldung hinzu. Spätestens einen Monat nach der Meldung folgt die Abschlussmeldung mit Ursache und Abhilfemaßnahmen – oder eine Fortschrittsmeldung, falls der Vorfall andauert^[6].

Die 24-Stunden-Frist beginnt mit der Kenntnis, nicht mit der Aufklärung^[6]. Erreichbarkeit am Wochenende, eine Meldevorlage und die Entscheidung, wer meldet, gehören deshalb vorab ins Notfallhandbuch. Sind personenbezogene Daten betroffen, gilt zusätzlich die Meldepflicht an die Datenschutzaufsicht nach Art. 33 DSGVO^[14]. Verstöße gegen die Meldepflichten sind bußgeldbewehrt^[6].

Abb. 5 Die Uhr läuft ab Kenntnis des Vorfalls

Meldestufen nach § 32 BSIG: 24 h und 72 h ab Kenntnis, Abschluss einen Monat nach der Meldung.



Quelle: § 32 Abs. 1 und 2 BSIG; eigene Darstellung.

Verantwortung liegt bei der Geschäftsleitung

Das BSIG nimmt die Leitung ausdrücklich in die Pflicht. Gleichzeitig bereitet das BSI die Durchsetzung vor – nach eigener Ankündigung in Stufen und mit Anhörung.

10 Mio. €

Bußgeldrahmen für besonders wichtige Einrichtungen bei Verstößen gegen Risikomanagement-, Dokumentations- und Meldepflichten; für wichtige Einrichtungen 7 Mio. €^[6].

Die Geschäftsleitung ist verpflichtet, die Maßnahmen nach § 30 „umzusetzen und ihre Umsetzung zu überwachen“ (§ 38 Abs. 1 BSIG)^[6]. Aufgaben kann sie an die IT oder an Dienstleister übertragen, die Verantwortung bleibt bei ihr. Verletzt sie diese Pflichten, haftet sie der eigenen Einrichtung für schuldhaft verursachte Schäden nach den Regeln des Gesellschaftsrechts (§ 38 Abs. 2)^[6]. Das ist eine Haftung gegenüber dem eigenen Unternehmen, keine unmittelbare Haftung gegenüber Dritten. Außerdem müssen Geschäftsleitungen regelmäßig an Schulungen teilnehmen (§ 38 Abs. 3)^[6].

In der Praxis heißt das: Die Leitung gibt das Risikomanagement schriftlich frei, lässt sich mindestens quartalsweise berichten und legt ihren Schulungsnachweis ab.

2 % / 1,4 %

des weltweiten Jahresumsatzes – nur bei mehr als 500 Mio. € Umsatz, für Unternehmen mit 20 bis 150 Beschäftigten in aller Regel nicht relevant^[6].

Was das BSI angekündigt hat

Nach Angaben des BSI, über die der Tagesspiegel und ChannelPartner berichteten, beginnt im vierten Quartal 2026 eine Durchsetzungsinitiative. Zuerst werden Einrichtungen angeschrieben, die sich offensichtlich hätten registrieren müssen. Es folgt eine Anhörung; dabei werde es „nicht sofort ein Bußgeld geben“. Ab dem ersten Quartal 2027 sollen Prüfungen mit Themenschwerpunkt angeordnet werden, zuerst bei besonders wichtigen Einrichtungen^[4].

500.000 €

Bußgeldrahmen bei Verstößen gegen die Registrierungspflichten nach § 33 BSIG^[6].

Auf EU-Ebene hat die Kommission am 20.01.2026 gezielte Änderungen der NIS2-Richtlinie vorgeschlagen, etwa eine Kategorie „kleine Midcaps“ unter 750 Beschäftigten^[15]. Ob und wann die Änderungen kommen, ist offen. Für heutige Entscheidungen ist der Vorschlag nicht maßgeblich.

Schritt für Schritt zu prüfbaren Nachweisen

Links die Reihenfolge, rechts die Punkte zum Abhaken. Die Zeitangaben sind eine Empfehlung der Redaktion, keine gesetzlichen Fristen.

Delta One begleitet die Schritte auf Wunsch.

Fahrplan

Sofort

- **Betroffenheit klären**
Sektor, Größe und Konzernverbund prüfen, Ergebnis mit Datum ablegen.

Sofort

- **Registrierung sichern**
ELSTER-Zertifikat beantragen, im BSI-Portal registrieren, Daten aktuell halten.

Kurzfristig

- **Bestand aufnehmen**
Systeme, Daten, externe Zugänge und Dienstleister erfassen, Risiken bewerten.

Kurzfristig

- **Lücken schließen**
MFA, Backups und Patch-Prozess zuerst, nach Risiko priorisiert.

Mittelfristig

- **Meldeweg üben**
Planspiel mit der Geschäftsleitung, etwa ein Ransomware-Fall am Freitagabend.

Laufend

- **Wirksamkeit prüfen**
Kennzahlen erheben, quartalsweise berichten, Dokumentation fortschreiben.

Checkliste

- ☐ **Betroffenheitsprüfung ist dokumentiert**
Sektor, Größe nach KMU-Empfehlung und Verbund mit Datum abgelegt.
- ☐ **Registrierung im BSI-Portal ist abgeschlossen**
Änderungen werden binnen zwei Wochen gemeldet.^[6]
- ☐ **Leitung hat das Risikomanagement freigegeben**
Schriftliche Freigabe, Ansprechperson benannt, Schulungsnachweis der Leitung abgelegt.
- ☐ **Inventar und Risikoanalyse liegen vor**
Systeme, Dienste, Dienstleister; Maßnahmen mit Frist und Verantwortlichen.
- ☐ **MFA schützt Fernzugänge, E-Mail und Administratorkonten**
Danach schrittweise auf alle Konten ausweiten.
- ☐ **Wiederherstellung aus dem Backup ist getestet**
Offline- oder unveränderliche Kopie vorhanden, Test dokumentiert.
- ☐ **Meldeprozess für 24 und 72 Stunden steht**
Vorlage, Erreichbarkeit rund um die Uhr, Abgleich mit DSGVO-Meldung.
- ☐ **Lieferkette und Schulungen sind geregelt**
Anforderungen in Verträgen, Beschäftigte geschult, eigenes Nachweispaket bereit.



FRIST

Die gesetzliche Registrierungsfrist ist abgelaufen^[8]. Wer betroffen und nicht registriert ist, riskiert ein Bußgeld bis 500.000 €^[6] und sollte die Registrierung sofort nachholen.

Wie Delta One unterstützt

Delta One ist ein inhabergeführtes IT-Systemhaus aus Schnaittach im Nürnberger Land. Wir unterstützen Unternehmen, Kommunen und Handwerksbetriebe bei der technischen und organisatorischen Umsetzung – von der Bestandsaufnahme bis zum laufenden Betrieb.



IT-Beratung & Strategie

Bestandsaufnahme, Risikoanalyse und Maßnahmenplanung entlang der zehn Pflichtfelder nach § 30 BSIG – als technische Grundlage Ihrer Entscheidungen.



Cyber Security

Mehr-Faktor-Authentifizierung, Härtung, Schwachstellen- und Patchmanagement, Firewall und Netzwerksegmentierung mit UniFi, sichere Konfiguration von Microsoft 365.



Backup und Notfallvorsorge

Backup-Konzepte mit Veeam, Offline- oder unveränderliche Sicherungen, Wiederherstellungstests und Mitarbeit an Notfallhandbuch und Übungen.



Managed Services

Laufender Betrieb, Monitoring und Patchmanagement mit NinjaOne – dokumentiert als Grundlage für Ihre Nachweise.

So gehen wir vor



Technologiepartner in diesem Thema: Microsoft, Ubiquiti/UniFi, Veeam und NinjaOne. Delta One leistet keine Rechtsberatung; die rechtliche Einordnung bleibt Sache Ihres Unternehmens und seiner Rechtsberatung.

Sprechen Sie mit uns über Ihre Ausgangslage.

Delta One GmbH, Kirschenleite 15, 91220 Schnaittach

+49 911 477 193 80
info@delta-one.net

delta-one.net

Quellen

Nummeriert in der Reihenfolge der ersten Nennung. Online-Quellen abgerufen am 15.10.2026.

-
- [1] Scheja & Partner Rechtsanwälte: NIS2 Implementation Act – new cybersecurity obligations since 5 December 2025. Blogbeitrag, 07.01.2026. <https://scheja-partners.de/en/2026/01/07/nis2-implementation-act-new-cybersecurity-obligations-since-5-december-2025>
 - [2] RAK LAW für Bayerischer Industrie- und Handelskammertag (BIHK): NIS2 & Lieferkettensicherheit. Webinar-Vortrag, April 2026. https://www.bihk.de/fileadmin/BIHK.de_Dateien/Webinare/IT-Sicherheit/20260428-NIS2_Lieferkettensicherheit_RAK_LAW.pdf
 - [3] Heuking: NIS-2-Registrierungspflicht bis zum 6. März 2026 – jetzt handeln. Newsletter-Fachbeitrag, 19.02.2026. <https://www.heuking.de/de/news-events/newsletter-fachbeitraege/artikel/nis-2-registrierungspflicht-bis-zum-6-maerz-2026-jetzt-handeln.html>
 - [4] ChannelPartner (Peter Marwan): BSI will bei NIS2 ernst machen. 08.10.2026, nach einem Bericht des Tagesspiegels. <https://www.channelpartner.de/article/4232480/bsi-will-bei-nis2-ernst-machen.html>
 - [5] Bitkom e. V.: Wirtschaftsschutz 2026. Präsentation, Berlin, 26.08.2026. <https://www.bitkom.org/sites/main/files/2026-08/bitkom-praesentation-wirtschaftsschutz-2026.pdf>
 - [6] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in der Fassung des NIS2-Umsetzungsgesetzes, BGBl. 2025 I Nr. 301, verkündet am 05.12.2025; zitiert: § 2 Nr. 11, § 28, § 30, § 32, § 33, § 38, § 65, Anlagen 1 und 2. https://www.gesetze-im-internet.de/bsig_2025/ (Wortlaut geprüft über <https://lexmea.de/de/gesetz/bsig-2025>)
 - [7] Zeitung für kommunale Wirtschaft (zfk), Julian Korb: NIS2-Nachfrist abgelaufen – BSI behält sich Bußgelder vor. 04.08.2026. <https://www.zfk.de/digitalisierung/it/nis2-bsi-registrierung-nachfrist-stadtwerke-bussgelder>
 - [8] Bundesamt für Sicherheit in der Informationstechnik (BSI): NIS-2-regulierte Unternehmen. Themenseite mit Links zur NIS-2-Betroffenheitsprüfung und zur NIS-2-Checkliste (13.03.2026), zuletzt aktualisiert 10.08.2026. https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html
 - [9] Gesetz zur Änderung des Bayerischen Digitalgesetzes vom 08.10.2024, GVBl. 2024 S. 474, in Kraft seit 18.10.2024; Begründung: Bayerischer Landtag, Drucksache 19/2591 (Gesetzentwurf der Staatsregierung), 25.06.2024. <https://www.verkuendung-bayern.de/files/gvbl/2024/19/gvbl-2024-19.pdf>; https://www.bayern.landtag.de/www/ElanTextAblage_WP19/Drucksachen/Basisdrucksachen/0000002000/0000002129.pdf
 - [10] Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi): Digitalbonus Bayern – Förderprogramm; Antragstellung. <https://www.digitalbonus.bayern/foerderprogramm/>; <https://www.digitalbonus.bayern/antragstellung/>
 - [11] borncity.com: Doch keine NIS2-Registrierungslücke; Kuriose Änderung am KRITIS-Dachgesetz. Blogbeitrag, 24.08.2026. <https://borncity.com/blog/2026/08/24/doch-keine-nis2-registrierungsluecke-kuriose-aenderung-am-kritis-dachgesetz/>
 - [12] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates (NIS-2-Richtlinie), ABl. L 333 vom 27.12.2022; zitiert: Art. 41. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Quellen

Fortsetzung

-
- [13] it-daily.net: BSI setzt Nachfrist: NIS2-Registrierung bis Ende Juli. Kurzmeldung (nach Tagesspiegel), 17.06.2026. <https://www.it-daily.net/shortnews/bsi-nis2-registrierung-bis-ende-juli>
 - [14] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung), ABl. L 119 vom 04.05.2016; zitiert: Art. 33. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
 - [15] Freshfields: EU cybersecurity package: Commission proposes targeted NIS2 amendments and a revised Cybersecurity Act. Blog „Technology Quotient“, 27.01.2026. <https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/eu-cybersecurity-package-commission-proposes-targeted-nis2-amendments-and-a-revi-102me35>

Impressum

HERAUSGEBER

Delta One GmbH
Kirschenleite 15
91220 Schnaittach

KONTAKT

+49 911 477 193 80
info@delta-one.net
delta-one.net

STAND

15. Oktober 2026.
Rechtslage,
Herstellerangaben und
Zahlen nach dem Stand
der genannten Quellen.

HINWEIS

Dieses Whitepaper dient der allgemeinen Information und stellt **keine Rechtsberatung** dar. Es ersetzt nicht die Prüfung des Einzelfalls durch eine Rechtsanwältin oder einen Rechtsanwalt. Ob und in welchem Umfang Ihr Unternehmen den Pflichten des BSI-Gesetzes unterliegt, ist im Einzelfall zu prüfen. Trotz sorgfältiger Recherche übernimmt Delta One keine Gewähr für Vollständigkeit und Aktualität. Genannte Produkt- und Firmennamen sind Marken ihrer jeweiligen Inhaber.

Alle Grafiken: Delta One GmbH, eigene Darstellung auf Grundlage der angegebenen Quellen.

Ihr Partner im IT Sektor

Delta One ist ein inhabergeführtes IT-Systemhaus und Managed Service Provider aus Schnaittach im Nürnberger Land.

Die Whitepaper-Reihe

01 **NIS2 im ersten Jahr: Umsetzen statt abwarten**

02 KI im Unternehmen: erst Regeln, dann Copilot

03 Raus aus VMware? Erst prüfen, dann planen

Adresse

Delta One GmbH
Kirschenleite 15
91220 Schnaittach

Kontakt

+49 911 477 193 80
info@delta-one.net

Web

delta-one.net