Datenschutz und Informationssicherheit in der Lieferkette

(unter Einbeziehung von NIS2)

II | 2025

Wichtige Datenschutzinformationen für Ihr Unternehmen

CompuSaar

Inhalte | Datenschutzinformationen

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

Christoph Hildmann

eine zunehmende Digitalisierung und Vernetzung führt dazu, dass Unternehmen heute mehr denn je auf komplexe Lieferketten und externe Dienstleister angewiesen sind. Gleichzeitig wachsen die Herausforderungen im Datenschutz und in der Informationssicherheit stetig – nicht zuletzt durch strenger werdende Anforderungen auf europäischer Ebene.

Vor allem mit der NIS2-Richtlinie, die in Deutschland durch das NIS2UmsuCG in nationales Gesetz überführt wird, hat die Europäische Union die Weichen für ein höheres gemeinsames Sicherheitsniveau im Bereich kritischer Infrastrukturen und wesentlicher Dienste gestellt. Aber auch darüber hinaus wird ein ganzheitlicher Schutz sensibler Informationen entlang der gesamten Lieferkette zur unternehmerischen Herausforderung, Verpflichtung und zum Erfolgsfaktor. Verstöße gegen Datenschutz und mangelhafte Sicherheit können gravierende rechtliche und wirtschaftliche Folgen nach sich ziehen – insbesondere für Unternehmen in Leitungs- und Führungsfunktionen.

Wir möchten Ihnen mit der neuesten Ausgabe unserer Datenschutzzeitung einen praxisnahen Überblick über die wichtigsten Aspekte geben, wenn es um den Datenschutz und die Informationssicherheit in der Lieferkette unter Einbeziehung von NIS2 geht: Von rechtlichen Grundlagen über konkrete Anforderungen bis hin zu Maßnahmen im eigenen Unternehmen und gegenüber externen Partnern.

Wir zeigen Ihnen, wie Sie Risiken erkennen und minimieren, Pflichten umsetzen und so das Vertrauen Ihrer Kunden und Geschäftspartner stärken.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung zu diesem oder anderen Datenschutz und IT-Sicherheitsthemen in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer (06894) 38797-0 oder per E-Mail an info@compusaar.de.

Mit besten Grüßen

Christoph Hildmann

Externer Datenschutzbeauftragter

NIS2: Grundlagen und Zielsetzung

Relevanz für Unternehmen und betroffene Sektoren

NIS2 (Network and Information Security Directive) markiert einen entscheidenden Schritt der Europäischen Union, um die Sicherheit und Resilienz der digitalen Infrastruktur und der Lieferketten europaweit zu stärken. Sie betrifft deutlich mehr Unternehmen als ihr Vorgänger – darunter nicht mehr nur klassische Betreiber kritischer Infrastrukturen, sondern auch zahlreiche mittelständische und große Unternehmen verschiedener Branchen.

Wer ist betroffen?

- Unternehmen und öffentliche Einrichtungen ab 50 Beschäftigten oder mit einem Jahresumsatz von mindestens 10 Millionen Euro.
- Insgesamt 18 Sektoren, darunter Energie, Transport, Bankwesen, Gesundheitswesen, digitale Infrastrukturen, Wasser, Lebensmittel, Abfallwirtschaft und weitere.
- Firmen entlang der Lieferkette, die Dienstleistungen oder Produkte für diese Sektoren bereitstellen, müssen oftmals auch die Anforderungen umsetzen, auch wenn sie primär Zulieferer oder Dienstleister sind.

Für betroffene Unternehmen bedeutet die NIS2-Richtlinie:

- Strengere Sicherheitsanforderungen
- Verstärkte Prüf- und Dokumentationspflichten
- Höhere Haftungsrisiken und Transparenzanforderungen im Umgang mit Cyberrisiken

Ziele und Vorgaben von NIS2 für die Lieferkette

NIS2 zielt darauf ab, ein höheres und einheitlicheres Sicherheitsniveau bei der Nutzung von Informationssystemen und Netzwerken zu schaffen – einschließlich aller relevanten Unternehmen innerhalb der Lieferkette.

Wesentliche Ziele:

- Stärkung des EU-weiten Cyber-Resilienz-Niveaus
  Die Sicherheit bei allen kritischen und wichtigen digitalen Dienstleistungen und Waren soll verbessert werden.
- Verpflichtende Maßnahmen für die Lieferkette
  Unternehmen sind explizit verpflichtet, auch die Cybersicherheit von Zulieferern und Dienstleistern aktiv mit einzubeziehen.
- Risikomanagement
  Unternehmen müssen regelmäßige Risikoanalysen durchführen und technische und organisatorische Schutzmaßnahmen implementieren.

- Meldepflichten
  Sicherheitsvorfälle, die erhebliche Auswirkungen haben können, müssen unverzüglich gemeldet werden.

Konkret für die Lieferkette bedeutet das:

- Vertragsbedingungen und Prüfprozesse zur Cybersicherheit werden zur Normalität.
- Unternehmen müssen sich vergewissern, dass ihre externen Partner ebenfalls angemessene Sicherheitsmaßnahmen implementieren.

Schnittstelle zu Datenschutz und DSGVO

NIS2 ergänzt die Datenschutzgrundverordnung (DSGVO), ohne sie zu ersetzen. Während die DSGVO den Schutz personenbezogener Daten regelt, befasst sich NIS2 mit der allgemeinen Sicherheit von Netzwerken und Informationssystemen, die auch nicht-personenbezogene Daten betreffen können.

Wichtige Überschneidungen und Abgrenzungen:

- Synergien
  Beide Regelwerke verlangen Risikomanagement, Präventions- und Schutzmaßnahmen sowie Meldepflichten bei Sicherheitsvorfällen.
- Trennschärfe
  Die DSGVO legt den Schwerpunkt auf personenbezogene Daten und die Rechte von Betroffenen, wohingegen NIS2 die Geschäfts- und Prozesskontinuität sowie die technische und organisatorische Sicherheit adressiert.
- Konkreter Bezug für die Compliance-Praxis
  Die Einhaltung der NIS2-Anforderungen trägt zur ganzheitlichen Compliance bei – Datenschutz- und IT-Sicherheitsmanagement greifen ineinander und stärken so den Schutz sensibler wie auch geschäftskritischer Informationen.

Fazit

NIS2 erweitert die rechtlichen Anforderungen für Unternehmen entlang der gesamten Lieferkette erheblich. Indem sie Lieferanten und Dienstleister einbezieht, erhöht sie die Sicherheit auf allen Ebenen und setzt neue Standards für das Zusammenspiel von Datenschutz und Informationssicherheit.

Risikomanagement in der Lieferkette

Identifikation und Bewertung von Risiken

Ein wirksames Risikomanagement beginnt mit der systematischen Identifikation und Bewertung von Risiken innerhalb der gesamten Lieferkette. NIS2 verpflichtet Unternehmen dazu, nicht nur ihre eigenen Prozesse, sondern insbesondere auch die ihrer Lieferanten und Dienstleister auf potenzielle Sicherheitslücken und Gefahrenquellen hin zu prüfen. Typische Risiken sind Datenabfluss, Kompromittierung von IT-Systemen oder Betriebsunterbrechungen.

Vorgehen:

- Durchführung regelmäßiger Risikoanalysen aller Schnittstellen zur Lieferkette.
- Einsatz von standardisierten Fragebögen, Auditverfahren oder Zertifizierungen zur Einstufung der Cyber-Resilienz der Lieferanten.
- Dokumentation und Bewertung aller erkannten Risiken hinsichtlich Eintrittswahrscheinlichkeit und möglicher Auswirkungen.

Ein strukturierter Bewertungsprozess schafft Transparenz und ermöglicht es, risikobehaftete Lieferanten frühzeitig zu identifizieren und gezielt Gegenmaßnahmen zu ergreifen.

Umgang mit Schwachstellen bei Lieferanten

Die Behebung und Prävention von Schwachstellen in der Lieferkette ist ein zentrales Element der NIS2-konformen Cybersicherheit. Cyberangriffe nutzen bevorzugt die Angriffsfläche externer Partner – insbesondere, wenn dort unzureichende Sicherheitsmaßnahmen bestehen.

Empfohlene Maßnahmen:

- Aufnahme verbindlicher Sicherheitsanforderungen und -standards in Verträge mit allen Lieferanten und Dienstleistern.
- Verpflichtende Sicherheitsüberprüfungen vor Vertragsschluss und regelmäßige Re-Audits während der Vertragslaufzeit.
- Zusammenarbeit und offene Kommunikation mit Lieferanten zur zeitnahen Identifikation und Behebung von Schwachstellen, etwa durch gemeinsame Sicherheitsprojekte oder Notfallübungen.
- Etablierung eines kontinuierlichen Monitorings der Lieferantenlandschaft mittels technischer und organisatorischer Maßnahmen.

Die Einbindung der Lieferanten in Cybersicherheitsprozesse ist für die ganzheitliche Risikosteuerung unerlässlich.

Risikomanagement in der Lieferkette

Stand der Technik berücksichtigen

NIS2 (Network and Information Security Directive) fordert explizit, dass Unternehmen beim Risikomanagement den Stand der Technik berücksichtigen und ihre technischen und organisatorischen Schutzmaßnahmen fortlaufend an aktuelle Bedrohungen und Entwicklungen anpassen.

Die folgenden Informationen verdeutlichen die Pflichten und Chancen des Risikomanagements in der modernen Lieferkette und geben konkrete Handlungsempfehlungen für eine rechtssichere und gesetzeskonforme Umsetzung.

Handlungsempfehlungen:

- Regelmäßige Aktualisierung der eingesetzten Technologien und Sicherheitsprozesse, um Sicherheitslücken zu vermeiden.
- Nutzung aktueller IT-Sicherheitsstandards und Zertifizierungen wie ISO 27001 oder branchenspezifischer Vorgaben.
- Berücksichtigung neuer gesetzlicher Anforderungen, wie etwa des Cyber Resilience Act, bei der Auswahl von Produkten und IT-Dienstleistungen.
- Fortlaufende Schulungen und Sensibilisierung der Mitarbeitenden und Lieferanten werden empfohlen, um das Sicherheitsniveau dauerhaft hoch zu halten.

Ein effektives Risikomanagement in der Lieferkette erfordert ein ganzheitliches und dynamisches Vorgehen – nur die Unternehmen, die Risiken konsequent identifizieren, Schwachstellen proaktiv adressieren und dabei den Stand der Technik im Blick behalten, werden den gestiegenen Anforderungen von NIS2 gerecht und sichern nachhaltigen Unternehmenserfolg.

Organisation und Governance im Unternehmen

Aufgaben der Geschäftsleitung

Die Geschäftsleitung darf Sicherheitsaufgaben nicht mehr nur delegieren!

Sie muss nachweislich ein funktionierendes Sicherheitsniveau sicherstellen und im Notfall auch persönlich haften!

NIS2 rückt die Geschäftsleitung ins Zentrum der Informationssicherheitsstrategie. Sie ist nicht mehr nur indirekt verantwortlich, sondern wird explizit verpflichtet, sich aktiv mit der Informationssicherheit auseinanderzusetzen:

- Verantwortung übernehmen
  Die Geschäftsführung muss Strategien, Zielsetzungen und Rahmenbedingungen für Informationssicherheit festlegen und freigeben.
- Risikomanagement steuern
  Die Geschäftsleitung ist dafür verantwortlich, dass Risiken systematisch identifiziert, bewertet und durch angemessene Maßnahmen gemindert werden.
- Ressourcen sicherstellen
  Es müssen ausreichend finanzielle, personelle und technische Ressourcen zur Umsetzung der Sicherheitsstrategie bereitgestellt werden.
- Schulungspflicht
  NIS2 verlangt die regelmäßige Schulung der Geschäftsleitung zu aktuellen Bedrohungen und Pflichten.

Rollen und Verantwortlichkeiten

Eine wirksame Informationssicherheit basiert auf klar definierten Rollen und eindeutig zugewiesenen Verantwortlichkeiten:

- Verantwortlichkeiten festlegen
  Wer ist wofür zuständig? Ein organisationsweites Rollenkonzept mit eindeutigen Zuständigkeiten beugt Überschneidungen oder Lücken vor.
- Funktionstrennung
  Trennung von administrativen Aufgaben und Kontrolle (z. B. Vier-Augen-Prinzip beim Berechtigungsmanagement).
- Ernennung von Verantwortlichen
  Bestimmung von Informationssicherheitsbeauftragten oder -teams als zentrale Ansprechpartner für alle Belange der Cyber- und Informationssicherheit.
- Kontinuierliche Kommunikation
  Förderung einer offenen Datenschutz- und Sicherheitskultur durch regelmäßigen Austausch zwischen Geschäftsleitung, Datenschutz-Verantwortlichen, IT, Fachbereichen und externen Partnern.

Jede Rolle sollte über die notwendigen Kompetenzen und Entscheidungsspielräume verfügen, um die Vorgaben von NIS2 effizient und nachvollziehbar umzusetzen.

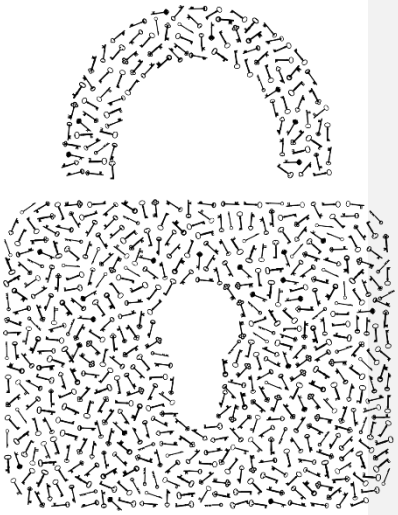
Etablierung eines Informationssicherheits-Managementsystems (ISMS)

Die Umsetzung der NIS2-Anforderungen erfordert ein systematisches Vorgehen, das durch ein Informationssicherheits-Managementsystem (ISMS) nach internationalen Standards wie z. B. der DIN EN ISO 27001 optimal unterstützt wird:

- ISMS als organisatorisches Rückgrat
  Ein ISMS definiert Prozesse, Richtlinien und Maßnahmen zur kontinuierlichen Sicherung der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.
- Zentrale Elemente eines ISMS
  - Regelmäßige Risikoanalysen und -bewertungen
  - Steuerung und Überwachung von TOM
  - Monitoring, Audit und ständige Verbesserung
  - Dokumentation aller Maßnahmen und Entscheidungen
- Verzahnung mit Datenschutz und Compliance
  Das ISMS fördert ein integriertes Management, das die Anforderungen aus Datenschutz, Business Continuity und weiteren regulatorischen Vorgaben miteinander verbindet.
- Nachweis der NIS2-Konformität
  Mit einem ISMS kann ein Unternehmen systematisch dokumentieren, dass die gesetzlichen Anforderungen umgesetzt werden – und somit mögliche Bußgelder und Haftungsrisiken minimieren.

Die Etablierung eines ISMS nach dem aktuellen Stand der Technik ist ein wesentlicher Schritt zur Stärkung der Resilienz und des Vertrauens in die gesamte Lieferkette. Ein ganzheitlicher, von der Leitung getragener Sicherheitsmanagement-Ansatz wird damit zum Erfolgsfaktor für Unternehmen unter NIS2.

Technische und organisatorische Maßnahmen (TOM)



Der Schutz von Informationen und die Sicherstellung der Sicherheit digitaler Lieferketten sind zentrale Herausforderungen für Unternehmen – insbesondere aus der Sicht der aktuellen NIS2-Anforderungen. Unternehmen werden verpflichtet, nicht nur ihre eigenen Systeme, sondern auch die ihrer Lieferanten und Dienstleister in die Sicherheitsstrategie einzubeziehen. Eine entscheidende Rolle spielen dabei technische und organisatorische Maßnahmen, die im Folgenden unter drei Aspekten betrachtet werden.

IT-Sicherheitsanforderungen (z.B. Verschlüsselung, Zutrittskontrolle)

Um Angriffe und Datenschutzverletzungen innerhalb der Lieferkette zu verhindern, verlangt NIS2, dass Unternehmen wirksame und angemessene IT-Sicherheitsmaßnahmen umsetzen. Zu den wichtigsten zählen:

- Verschlüsselung sensibler Daten
  Sowohl bei der Übertragung als auch bei der Speicherung sind geeignete Verschlüsselungsverfahren Pflicht, um unbefugten Zugriff abzuwehren.
- Zutrittskontrollen
  Physischer Zugang zu besonders schützenswerten IT-Bereichen sowie technischer Zugang zu Daten und Systemen sind eindeutig zu regeln und auf das Notwendige zu beschränken. Personalisierte Zugangsdaten, Mehr-Faktor-Authentifizierung und regelmäßige Überprüfung von Berechtigungen sind etablierte Maßnahmen.
- Monitoring und Reaktion
  Laufende Überwachung von Zugriffsversuchen und automatisierte Alarmierung bei verdächtigen Aktivitäten helfen, Angriffe frühzeitig zu erkennen und einzudämmen.

NIS2 fordert, dass diese Maßnahmen auch auf die unmittelbaren Anbieter und deren Dienstleistungen ausgedehnt werden. Risiken, die durch diese Partner entstehen, müssen explizit regelmäßig bewertet und adressiert werden.

Sicherheitsbewertung von Produkten und Dienstleistungen

Mit der neuen EU-Verordnung zur Produktsicherheit und durch NIS2 sind Unternehmen verpflichtet, die Sicherheitsstandards von Produkten und Dienstleistungen systematisch zu bewerten. Wesentliche Bausteine dabei sind:

- Risikobewertung jedes Produkts vor Inverkehrbringen und während des gesamten Lebenszyklus.
- Technische Unterlagen müssen erstellt und mindestens zehn Jahre aktuell gehalten werden.

- Sicherheits- und Cybersicherheitsmerkmale überprüfen: Dazu zählen nicht nur technische Eigenschaften wie Hard- und Software, sondern auch Wechselwirkungen mit anderen Produkten sowie die Ausgestaltung von Benutzeroberflächen und Warnhinweisen.
- Nachweisführung der Sicherheit: Über Zertifizierungen (z. B. nach ISO/IEC 27001, IEC 62443 für Lieferketten), Lieferanten-Audits und Cyber-Risk-Ratings können Unternehmen und Partner die Umsetzung der Anforderungen nachweisen und dokumentieren.

Für Dienstleistungen gilt gleiches Recht: Die Cybersicherheits-Praxis der Dienstleister, insbesondere ihre Entwicklungsprozesse und Supportleistungen (u. a. Sicherheitsupdates), wird Teil der Gesamtbewertung und vertraglich abgesichert.

Umsetzung der „Security by Design"-Prinzipien

Security by Design bedeutet, dass Sicherheit bereits in der Entwicklung von Produkten, Dienstleistungen und Geschäftsprozessen mitgedacht und systematisch integriert wird. NIS2 und flankierende Gesetze wie der EU Cyber Resilience Act machen dies zur Pflicht:

- Von Anfang an Sicherheitsanforderungen definieren: Bereits bei der Planung sind Risiken zu identifizieren und Schutzmaßnahmen zu berücksichtigen – dies betrifft Software ebenso wie Hardware und organisatorische Abläufe.
- Cybersicherheitsupdates müssen einfach und zuverlässig über die gesamte Nutzungsdauer bereitgestellt werden, um neu entdeckte Schwachstellen schnell zu beheben.
- Dokumentation und Überprüfung: Entwicklungs- und Änderungsprozesse sind so zu gestalten, dass sie nachvollziehbar bleiben und systematische Schwachstellenanalysen und regelmäßige Überprüfungen (z. B. Penetrationstests) ermöglichen.

Security by Design trägt dazu bei, dass Produkte und Dienstleistungen widerstandsfähig gegen aktuelle und zukünftige Bedrohungen sind und langfristig den gesetzlichen und vertraglichen Anforderungen entsprechen.

Fazit

Die Umsetzung technischer und organisatorischer Maßnahmen in Übereinstimmung mit NIS2 ist keine einmalige Aufgabe, sondern ein fortlaufender Prozess. Sie verlangt eine enge Zusammenarbeit mit allen Partnern in der Lieferkette, transparente Nachweise und eine konsequente Integration von Sicherheitsmaßnahmen bereits ab den ersten Schritten der Produktentwicklung.

Zusammenarbeit mit Lieferanten und Dienstleistern

Die Sicherung der Lieferkette ist mit Einführung von NIS2 zu einem zentralen Bestandteil des betrieblichen Informationssicherheitsmanagements geworden. Unternehmen müssen gewährleisten, dass auch ihre Lieferanten und Dienstleister angemessene Datenschutz- und IT-Sicherheitsstandards einhalten. Entscheidend hierfür sind gezielte Maßnahmen zur vertraglichen Absicherung, konkrete Anforderungen an die Cybersecurity bei Anbietern und ein konsequentes Monitoring inkl. Audits von Lieferanten.

Vertragliche Absicherung

NIS2 verpflichtet Unternehmen, die Zusammenarbeit mit Lieferanten und Dienstleistern durch klare vertragliche Regelungen abzusichern. Vertragsinhalte sollten explizit Anforderungen an die Informationssicherheit, Datenschutz, Meldepflichten bei Sicherheitsvorfällen sowie Kontrollrechte umfassen.

Wichtig sind hierbei:

- Definition von Mindestsicherheitsstandards und deren kontinuierliche Erfüllung durch den Partner.
- Verpflichtung zu Zertifizierungen (z. B. ISO 27001, TISAX) als Nachweis eines etablierten Sicherheitsmanagementsystems.
- Transparente Prozesse für den Informationsaustausch im Falle von Vorfällen und Änderungen bei den Sicherheitsmaßnahmen.

Auf diese Weise schafft die vertragliche Gestaltung die notwendige Grundlage für eine vertrauensvolle, rechtssichere und überprüfbare Lieferkettensicherheit.

Anforderungen an Cybersecurity bei Anbietern

NIS2 schreibt vor, dass Unternehmen bei der Auswahl und Steuerung ihrer Lieferanten deren Cybersicherheitspraktiken umfassend prüfen und berücksichtigen müssen. Dazu gehören:

- Sicherheitsüberprüfung von IT-Produkten und -Dienstleistungen
  Bereits bei der Auswahl der Lieferanten muss deren Cybersicherheitsniveau bewertet und dokumentiert werden – beispielsweise durch Zertifikate oder unabhängige Nachweise.
- Berücksichtigung der Entwicklungspraxis
  Qualität und Sicherheit bei der Entwicklung und Wartung von Produkten und Systemen müssen nachweisbar sein (z. B. sichere Softwareentwicklung, regelmäßige Updates).

- Reduzierung der Abhängigkeit von Einzelanbietern (Vendor Lock-in)
  Wo sinnvoll, empfiehlt NIS2 eine Diversifizierung der Zulieferer, um Risiken durch Ausfälle oder Schwachstellen zu streuen.
- Kontinuierliche Qualifizierung
  Auch Dienstleister und externe Mitarbeitende müssen regelmäßig zu Sicherheitsanforderungen geschult werden.

Die Erfüllung dieser Anforderungen sollte fester Bestandteil des Auswahlprozesses und der laufenden Zusammenarbeit sein.

Monitoring und Audits der Lieferanten

Zur Sicherstellung der laufenden Einhaltung der vereinbarten Sicherheitsstandards gehört ein konsequentes Lieferantenmonitoring.

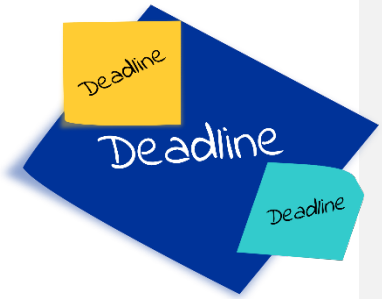
Unternehmen sind gefordert:

- Verzeichnis relevanter Lieferanten und Dienstleister
  Es sollte ein Verzeichnis aller relevanten Lieferanten und Dienstleister gepflegt werden, welches regelmäßig aktualisiert und bewertet wird.
- Kontinuierliches Monitoring der Sicherheitslage
  Die Wirksamkeit technischer und organisatorischer Maßnahmen der Lieferanten muss kontinuierlich überwacht werden, etwa durch Security Assessments, Zertifikatsprüfungen oder Überwachung von Sicherheitsupdates.
- Regelmäßige Audits und Überprüfungen
  Unternehmen sollten Kontrollrechte im Vertrag verankern und nutzen, um stichprobenartig oder anlassbezogen Audits durchzuführen. Ziel ist es, kritische Schwachstellen frühzeitig zu erkennen und sofortige Gegenmaßnahmen einzuleiten.

Damit wird die Lieferkettensicherheit zu einem fortlaufenden Steuerungs- und Verbesserungsprozess, statt zu einer einmaligen Aktivität.

Mit diesen Maßnahmen können Unternehmen alle Datenschutzvorgaben und alle Vorgaben von NIS2 zur Zusammenarbeit mit Lieferanten und Dienstleistern erfüllen und so die Informationssicherheit und den Datenschutz in der Lieferkette wirksam stärken.

Meldepflichten und Vorfallmanagement



Die Umsetzung von NIS2 stellt Unternehmen in der Lieferkette vor neue Herausforderungen im Bereich Datenschutz und Informationssicherheit. Zentrale Anforderungen sind die Einhaltung klarer Meldepflichten bei Sicherheitsvorfällen, ein strukturierter Umgang mit Datenschutzverletzungen sowie die enge Zusammenarbeit mit Behörden und spezialisierten Incident-Response-Teams (CSIRT).

Meldewege und Fristen bei Sicherheitsvorfällen

NIS2 verpflichtet betroffene Unternehmen, erhebliche IT-Sicherheitsvorfälle innerhalb definierter Fristen an die zuständigen Behörden und CSIRTs zu melden. Ziel ist es, Cyber-Bedrohungen schnell zu erkennen, darauf zu reagieren und die Auswirkungen auf Unternehmen, Kunden und Gesellschaft zu begrenzen.

Meldefristen im Überblick:

- Frühwarnung (Initialmeldung)
  Spätestens 24 Stunden nach Kenntnis eines erheblichen Vorfalls muss eine Erstmeldung mit Verdacht und grundlegenden Informationen erfolgen.
- Detaillierte Analyse (Folgemeldung)
  Innerhalb von 72 Stunden folgt eine vertiefte Bewertung inklusive Ausmaß des Vorfalls, betroffener Systeme und eingeleiteter Maßnahmen.
- Abschlussbericht
  Spätestens einen Monat nach der Erstmeldung ist ein detaillierter Bericht einzureichen, der Ursachen, Bewältigungsschritte und eventuelle grenzüberschreitende Auswirkungen dokumentiert.

Die Verantwortung für die rechtzeitige und vollständige Meldung liegt bei Informationssicherheitsbeauftragten, Compliance-Teams und der Geschäftsführung. Verstöße gegen die Meldepflichten können mit Bußgeldern bis zu 10 Millionen Euro oder 2 % des Jahresumsatzes geahndet werden.

Umgang mit Datenschutzverletzungen

Datenschutzverletzungen sind immer dann relevant, wenn bei einem Sicherheitsvorfall personenbezogene Daten betroffen sind. In solchen Fällen greifen neben NIS2 auch die direkten Vorgaben der DSGVO:

- Die Datenschutzverletzung muss unverzüglich – spätestens binnen 72 Stunden – an die zuständige Datenschutzbehörde gemeldet werden, sofern ein Risiko für die Rechte und Freiheiten der Betroffenen besteht.

- Betroffene Personen müssen ebenfalls zeitnah und transparent informiert werden, vor allem, wenn ein hohes Risiko für deren Privatsphäre besteht.

Wesentliche Maßnahmen im Fall einer Datenschutzverletzung:

- Sofortige Eindämmung und Sicherung der IT-Systeme
- Interne Untersuchung und transparente Dokumentation des Vorfalls
- Einschätzung und Minimierung von Risiken für Betroffene
- Einleitung technischer und organisatorischer Abhilfemaßnahmen

Ein durchdachtes Vorfallmanagement sowie eine klare Rollenverteilung im Unternehmen (z. B. Notfallteam, Datenschutzbeauftragte) sind essenziell, um strukturiert und regelkonform handeln zu können.

Zusammenarbeit mit Behörden und CSIRT

Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die jeweiligen CSIRTs (Computer Security Incident Response Teams) sind zentrale Ansprechpartner und Koordinatoren für Unternehmen bei Sicherheitsvorfällen.

- Meldungen erfolgen an das nationale CSIRT oder die von den Mitgliedstaaten benannte Aufsichtsbehörde – häufig online über spezielle Meldeformulare.
- Die Zusammenarbeit dient nicht nur der gesetzlichen Pflichterfüllung, sondern auch dem schnelleren Austausch von Bedrohungsinformationen, Analysen und bewährten Gegenmaßnahmen.
- Behörden und CSIRTs können proaktiv bei der Analyse, Bewertung und Eindämmung von Vorfällen unterstützen und bieten Unternehmen aktuelle Lagebilder sowie technische Hilfestellungen.

Die Rolle der geschäftsführenden Leitung wird durch NIS2 weiter gestärkt: Sie trägt die Verantwortung für die Umsetzung und Überwachung der Meldeprozesse im Unternehmen sowie für deren kontinuierliche Verbesserung.

Fazit

Konsequentes Vorfallmanagement nach NIS2 stärkt die Position von Unternehmen beim Datenschutz in der Lieferkette und erhöht das Vertrauen von Kunden und Geschäftspartnern. Eine klare Strategie, definierte Meldewege und die enge Anbindung an Behörden und CSIRTs sind für rechtssichere und effiziente Reaktionen auf Sicherheitsvorfälle unerlässlich.

Schulungen, Awareness und Unternehmenskultur

Mit Inkrafttreten der NIS2-Richtlinie und der Überführung in nationales Gesetz stehen Unternehmen in der Lieferkette vor der Aufgabe, Datenschutz und Informationssicherheit strukturell neu zu denken. Dabei sind die Sensibilisierung der Belegschaft, die gezielte Schulung von Führungskräften und der Aufbau einer nachhaltigen Sicherheitskultur zentrale Erfolgsfaktoren, um die gestiegenen Anforderungen rechtskonform und wirksam umzusetzen.

Sensibilisierung der Belegschaft

Empfehlung

Beachten Sie hierzu unsere Datenschutzzeitung zum Thema: *„Mitarbeiter-Awareness“*

Ein funktionierender Datenschutz lebt von aufgeklärten und aufmerksamen Mitarbeitenden. NIS2 fordert die Einführung eines effektiven Managementsystems zur Steuerung und Dokumentation aller datenschutz- und sicherheitsrelevanten Vorgänge. Dies erfordert regelmäßige Awareness-Maßnahmen, die praxisnah auf Risiken im Arbeitsalltag eingehen: Phishing, Social Engineering oder der sichere Umgang mit sensiblen Daten müssen für jeden verständlich und relevant vermittelt werden. Nur so können Fehlverhalten und unbewusste Verstöße minimiert und die betriebliche Resilienz gegenüber Cyber-Bedrohungen gestärkt werden.

- Interaktive E-Learnings, kurze Lernimpulse und realitätsnahe Szenarien erreichen die Belegschaft besser als reine Theorie.
- Ein Hinweisgebersystem und offene Kommunikationskanäle bestärken Mitarbeitende, Verdachtsfälle oder Datenschutzverstöße vertrauensvoll zu melden.

Schulung von Führungskräften

Führungskräfte stehen in besonderer Verantwortung, denn NIS2 verpflichtet sie explizit zur regelmäßigen Teilnahme an Schulungen zu Cybersicherheitsrisiken und -maßnahmen. Sie müssen aktuelle Gesetze, Pflichten und interne Prozesse nicht nur kennen, sondern aktiv vorleben und die Einhaltung im Team sicherstellen:

- Fachseminare liefern Know-how zu Meldepflichten, Risikoanalysen und organisatorischen Maßnahmen, mit praktischem Bezug zum Unternehmensalltag.
- Führungskräfte lernen, wie sie Risiken bewerten, Prioritäten setzen und Compliance-Lücken schnell beheben.
- Schulungsprogramme sollen individuell auf die jeweilige Verantwortungsebene abgestimmt sein, um gezielt auf Herausforderungen im Management und in den Fachabteilungen einzugehen.

Diese Qualifizierung schafft Verantwortungsbewusstsein und hilft, potenzielle Haftungsrisiken zu minimieren.

Schulungen, Awareness und Unternehmenskultur

Entwicklung einer Sicherheitskultur

Der grundlegende Wandel in Richtung einer starken Sicherheitskultur ist kein kurzfristiges Compliance-Projekt, sondern eine dauerhafte Führungs- und Kommunikationsaufgabe.

Datenschutz und Informationssicherheit müssen im Unternehmen Wertecharakter erlangen – von der obersten Leitung bis zum einzelnen Mitarbeitenden.

- Eine offene, transparente Fehlerkultur fördert aktives Melden und schnelles Lernen aus Zwischenfällen.
- Die Unterstützung durch Geschäftsführung und Management, etwa durch klare Vorbildfunktion und regelmäßige interne Kommunikation, verankert das Thema als festen Bestandteil der Unternehmenskultur.
- Auch kleine und mittlere Unternehmen sind gefordert, eine Sicherheitskultur zu etablieren, die technische Maßnahmen, organisatorische Abläufe und menschliches Verhalten miteinander verzahnt. Die Praxis zeigt: Unternehmen mit hoher Awareness sind widerstandsfähiger gegen Datenschutzvorfälle und Cyberangriffe.

Die Integration von Datenschutz und Informationssicherheit in alltägliche Prozesse – auch in der Lieferkette – sowie die Förderung einer offenen Lernkultur leisten einen entscheidenden Beitrag, um gesetzlichen Verpflichtungen wie NIS2 und DSGVO nachzukommen und das Vertrauen von Kunden und Partnern zu sichern.

Sanktionen, Haftung und Ausblick

Mit Inkrafttreten von NIS2 und den weiterentwickelten Anforderungen der DSGVO verschärft sich das regulatorische Umfeld für Datenschutz und Informationssicherheit in der Lieferkette erheblich. Unternehmen müssen jetzt nicht nur technische, sondern auch organisatorische Maßnahmen klar nachweisen – Fehler, Versäumnisse oder unzureichende Compliance können zu empfindlichen Sanktionen und persönlichen Haftungsrisiken führen.

Sanktionen bei Verstößen gegen NIS2 und DSGVO

NIS2 bringt ab 2025 deutlich härtere Sanktionen: Bei Verstößen gegen Sicherheitsanforderungen, Meldepflichten oder Managementvorgaben drohen Bußgelder von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes, je nachdem, welcher Wert höher ist. Für Unternehmen, die als „wichtige Einrichtungen“ eingestuft sind, liegt die maximale Sanktion immerhin noch bei 7 Millionen Euro oder 1,4 % des Umsatzes. Diese Beträge ergänzen die bereits hohen Geldbußen der DSGVO, die bei Datenschutzverletzungen fällig werden können.

Die Behörden haben ausdrücklich die Möglichkeit, auch wiederholte oder vorsätzliche Verstöße härter zu ahnden. Verstöße gegen die NIS2-Bestimmungen – etwa verspätete Meldungen von Vorfällen, fehlende Risikoanalysen oder mangelhafte Schutzmaßnahmen – stehen damit im Zentrum einer neuen behördlichen Prüfdichte. Besonders gravierend: Unternehmen riskieren nicht nur Bußgelder, sondern auch den temporären oder dauerhaften Entzug von Betriebserlaubnissen und Ausschluss von öffentlichen Vergaben.

Haftungsrisiken für Führungskräfte

Eine der wichtigsten Neuerungen unter NIS2: Führungskräfte und Mitglieder der Geschäftsleitung haften persönlich für die Einhaltung der gesetzlichen Vorgaben. Bei Verstößen gegen Sicherheitsanforderungen, unterlassener Umsetzung von Schutzmaßnahmen oder mangelhaften Schulungen der Belegschaft kann die persönliche Haftung der Leitungsgremien greifen. Konkret bedeutet dies: Geschäftsführer und Vorstände müssen nachweisen können, dass sie Risiken frühzeitig erkannt, geeignete Maßnahmen eingeleitet und die Compliance kontinuierlich überwacht haben.

Nachlässigkeit oder Untätigkeit können schwerwiegende Folgen für die persönliche Reputation und das Vermögen von Führungskräften haben, etwa durch Schadenersatzansprüche von Gesellschaftern oder Dritten. Die verpflichtende Cybersicherheitsschulung für das Management ist daher kein „Nice to have“, sondern ein zentraler Baustein rechtssicherer Unternehmensführung.

Sanktionen, Haftung und Ausblick

Weiterentwicklung und Trends in der EU-Rechtslage

Datenschutz und Cybersicherheit entwickeln sich in der EU dynamisch weiter. Nach NIS2 sind zusätzliche Verschärfungen und Weiterentwicklungen zu erwarten:

- Cyber Resilience Act
  Die EU arbeitet an weiteren Regelwerken, um Sicherheitsanforderungen für Produkte und Dienstleistungen zu ergänzen und neue Haftungs- sowie Meldepflichten für Hersteller und Anbieter einzuführen.
- KI-Regulierung
  Mit dem Vormarsch von Künstlicher Intelligenz werden zusätzliche Datenschutzanforderungen und Prüfpflichten eingeführt, vor allem beim Umgang mit Trainingsdaten und Transparenz im Datenumgang.
- Angleichung der Meldewege
  Die Datenschutzaufsichten verlangen EU-weit einheitliche und digitalisierte Prozesse zur Meldung von Sicherheitsvorfällen, um Transparenz und Effizienz zu steigern.

Fazit

Unternehmen sollten nicht nur kurzfristig auf die verschärfte Rechtslage reagieren, sondern Compliance, Datenschutz und Cybersicherheit als dauerhaften Führungsauftrag verstehen – auch um die eigene Marktposition und das Vertrauen in der Lieferkette zu sichern.

Wer frühzeitig investiert und tragfähige Führungsstrukturen aufbaut, schafft nicht nur im Datenschutz und in der Informationssicherheit Rechtssicherheit, sondern gewinnt im Wettbewerb nachhaltig an Widerstandsfähigkeit.

Impressum

CS Hard- & Software Consulting GmbH
Saarbrücker Straße 72
66386 St. Ingbert
Tel.: 06894 38797 – 0
Fax: 06894 38797 – 99
Web: www.compusaar.de
E-Mail: info@compusaar.de

Amtsgericht St. Ingbert, HRB 13312
Ust-IdNr.: DE813536236
Geschäftsführer/in: Ursula Doll

Redaktion
Alexander Eich

Bildnachweise
Diese Unterlage wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, in 97491 Aidhausen erstellt. Alle verwendeten Bilder sind von https://pixabay.com/de/ einer Plattform für lizenzfreie Bilder.

Nutzung von künstlicher Intelligenz
Bei der Recherche und zur Kontrolle der Richtigkeit der Aussagen, wurde bei der Erstellung dieser Unterlage zum Teil auf KI zurückgegriffen.