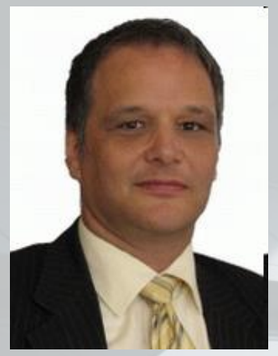
NIS2: Die neue Richtlinie für Cybersicherheit in Europa

Die NIS2-Richtlinie ist ein zentrales Regelwerk zur Stärkung der Cybersicherheit in der EU. Sie beseitigt Defizite der Vorgänger-Richtlinie NIS und erweitert ihren Geltungsbereich.



Ulrich Emmert

Rechtsanwalt
Lehrbeauftragter für Wettbewerbs-, Urheber- und Onlinerecht an der Hochschule für Wirtschaft und Umwelt in Nürtingen
Vorstand VOI e.V.

Informationssicherheit
Datenschutz
Haftungsrecht / AGB
Cloud Verträge
Mobile Device Management
Elektronischer Rechtsverkehr

esb Rechtsanwälte
Emmert Bücking Speichert
Matuszak-Lesny PartG mbB
Schockenriedstr. 8A
70565 Stuttgart
Tel. 0711/469058-0
Fax 0711/469058-99

ulrich.emmert@kanzlei.de
www.kanzlei.de
www.esb-rechtsanwaelte.de
www.emmert.de

Warum NIS2?

1 Verschärfte Bedrohungslage

Angetrieben durch Innovationen der Cyberkriminellen und KI-Tools nehmen komplexe Bedrohungen zu.

2 Globale Spannungen

Nationale Konflikte werden zunehmend im digitalen Raum ausgetragen, z.B. durch staatlich gefördertes Hacking.

3 Remote Work

Der starke Anstieg von Remote Work erhöht das Risiko durch ungeschützte private Endgeräte.

Ziele der NIS2-Richtlinie

Stärkung der Cybersicherheit

Verbesserung des Schutzes kritischer Infrastrukturen und Dienste.

Optimierte Zusammenarbeit

Förderung der Koordination zwischen Mitgliedstaaten bei Cyber-Vorfällen.

Sicherheitskultur

Sensibilisierung der Mitarbeitenden für sichere Verhaltensweisen.

Wichtigste Änderungen

Erweiterter Geltungsbereich

Mehr Sektoren und Einrichtungen fallen unter NIS2

Neue Verbindungsorganisation

EU-CyCLONe koordiniert das Management von Cyber-Krisen.

Strengere Meldepflichten

Sicherheitsvorfälle müssen innerhalb von 24 Stunden gemeldet werden.

Fokus auf Lieferkettensicherheit

Organisationen müssen Risiken durch Lieferanten bewerten. (“Lex Huawei”), wesentlich mehr betroffene Unternehmen in der Lieferkette

Cyberhygiene-Anforderungen

Grundlegende Sicherheitsmaßnahmen wie Software-Updates sind verpflichtend.

Persönliche Haftung

Leitungsorgane können für Verstöße persönlich haftbar gemacht werden.

Anwendungsbereich

1 Mehr Sektoren

NIS-2 gilt für deutlich mehr Sektoren als NIS-1, schätzungsweise 30.000 statt 2.000 Unternehmen.

2 Neue Adressaten

Qualifizierte Vertrauensanbieter, TLD-Registries, DNS-Anbieter, TK-Anbieter, kritische Anlagen und Verwaltung sind neu hinzugekommen.

3 Hohe Bußgelder

Verstöße können mit bis zu 10 Millionen Euro Bußgeld und persönlicher Haftung der Geschäftsleitung geahndet werden.

Betroffene Sektoren nach NIS 2 Anlage 1 und 2

Anlage 1

- Energie
- Verkehr
- Bankwesen
- Finanzmarktstrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastrukturen
- Verwaltung von IKT-Diensten
- Öffentliche Verwaltung
- Weltraum

Anlage 2

- Post- und Kurierdienste
- Abfall
- Chemikalien
- Lebensmittel
- Forschungseinrichtungen
- Verarbeitendes Gewerbe
- Digitale Dienste

Kritische Anlagen

Definition

Anlagen, deren Ausfall zu erheblichen Versorgungsengpässen oder Gefährdungen der öffentlichen Sicherheit führen würde.

Sektoren

Sektoren derzeit wie nach IT-Sicherheitsgesetz 2.0. Nach CER-Richtlinie und KRITIS Dachgesetz (ab 2026) stehen öffentliche Verwaltung sowie Medien und Kultur auf der Kippe.

KRITIS-Dachgesetz

Regelt zusätzliche Verpflichtungen für Betreiber kritischer Anlagen ab 2026.

Besonders wichtige Einrichtungen

Große Unternehmen

Aus den Sektoren Anlage 1
Mindestens 250 MA oder Umsatz/Bilanzsumme über 50/43 Mio. Euro.

Vertrauensdienste-anbieter

Qualifizierte Vertrauensdiensteanbieter sind besonders wichtige Einrichtungen.

TLD-Registries, DNS

Top-Level-Domain-Registries und DNS-Diensteanbieter sind einbezogen.

Telekommunikation

Anbieter von Telekommunikationsdiens ten und -netzen mit über 50 Mitarbeitern.

- **Einrichtungen, die von einem Mitgliedstaat als solches eingestuft sind**
- **Einrichtungen, die nach der CER-Richtlinie als kritisch eingestuft sind**
- **Einrichtungen, die nach der NIS aus 2016 von einem Mitgliedstaat als Betreiber wesentlicher Dienste eingestuft war**

Wichtige Einrichtungen

Große Unternehmen

- Aus den Sektoren Anlage 2
- Mindestens 250 MA oder Umsatz/ Bilanzsumme über 50/43 Mio. Euro.

Mittelgroße Unternehmen

- Aus den Sektoren Anlage 1 und 2
- Mindestens 50 MA oder Umsatz/ Bilanzsumme über 10 Mio. Euro.

Vertrauensdiensteanbieter

Nicht-qualifizierte Vertrauensdiensteanbieter gelten als wichtige Einrichtungen.

Einrichtungen, die von einem Mitgliedstaat als solches eingestuft sind

Ausnahmen

1 **Finanzunternehmen**

Unternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 sind ausgenommen; für diese gilt DORA

2 **Kreditwesen**

für diese gilt DORA

3 **Versicherungen**

für diese gilt DORA

Zeitplan zur Umsetzung

1

16. Januar 2023

NIS2 tritt offiziell in Kraft.

2

17. Oktober 2024

Frist für Mitgliedstaaten zur Umsetzung in nationales Recht.

3

17. April 2025

Mitgliedstaaten erstellen Liste betroffener Einrichtungen.

4

Oktober 2027

Überprüfung der NIS2-Richtlinie nach 3 Jahren.

NIS 2 Umsetzungsgesetz in Deutschland Zeitplan

1

April 2023

Referentenentwurf veröffentlicht.

2

Juli 2023

Aktualisierter Referentenentwurf.

3

September 2023

Diskussionspapier des BMI.

4

Mai 2024

Referentenentwurf veröffentlicht.

5

18. Oktober 2024

Geplantes Inkrafttreten von NIS-2.

NIS 2 Umsetzungsgesetz in Deutschland Fristen

Besonders wichtige Einrichtungen

- Registrierung innerhalb von drei Monaten nach Identifizierung **§33 (1)**
- Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten **§30 (7)**

Wichtige Einrichtungen

- Registrierung innerhalb von drei Monaten nach Identifizierung **§33 (1)**

Betreiber kritischer Anlagen

- Registrierung innerhalb von drei Monaten nach Identifizierung **§33 (1)** und **§33 (2)**
- Erstmaliger Nachweis über Maßnahmenumsetzung spätestens zu einem vom BSI und BBK bei der Registrierung festgelegten Zeitpunkt:

frühestens drei Jahre nach Inkrafttreten des Gesetzes **§39 (1)**, d.h. ab 2027.

- Fortlaufende Nachweise über Maßnahmenumsetzung anschließend alle drei Jahre **§39 (1)**
- Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten **§30 (7)**

NIS 2 Umsetzungsgesetz in Deutschland
Zahl der betroffenen Unternehmen

In Deutschland geht der Gesetzgeber von etwa 30.000 betroffenen Unternehmen in den verschiedenen Gruppen aus, von denen erst 17 Prozent (vorige Schätzung 40) im Grundsatz ausreichende Maßnahmen ergriffen haben. Abzüglich der bestehenden Betreiber haben laut Prognose **über 20.000 Unternehmen damit (neuen) Handlungsbedarf**.

Der Gesetzesentwurf prognostiziert betroffene Unternehmen:

- Besonders wichtige Einrichtungen: 8.100 Unternehmen
  - davon 4.693 digitale Dienste und Betreiber Kritischer Infrastrukturen (KRITIS)
  - davon rund 3.400 neue besonders wichtige Einrichtungen
  - davon rund 2.950 mit Nachholaufwand (83% von 3.550 neuen Einrichtungen)
- Wichtige Einrichtungen: 20.900 Unternehmen
  - davon rund 20.900 neue wichtige Einrichtungen
  - davon rund 17.900 mit Nachholaufwand (83% von 21.600 neuen Einrichtungen)

NIS 2 Umsetzungsgesetz in Deutschland Geschätzte Kosten

Einrichtungen	Aufwand	Rechnung	Summe
Besonders wichtig (neue)	Personalkosten jährlich	2.000 Unternehmen × 143.929 EUR	288 Mio. EUR
Besonders wichtig (neue)	Sachkosten jährlich	2.000 Unternehmen × 52 Tsd. EUR	104 Mio. EUR
Besonders wichtig	Nachweispflichten jährlich	3.550 Unternehmen × 35.211 EUR	125 Mio. EUR
Wichtig	Personalkosten jährlich	12.500 Unternehmen × 57.582 EUR	720 Mio. EUR
Wichtig	Sachkosten jährlich	12.500 Unternehmen × 21 Tsd. EUR	263 Mio. EUR
alle (neue)	Meldepflichten jährlich	25.157 Unternehmen × 2.400 Vorfälle	946 Tsd. EUR
alle	Schulungen jährlich	29.850 Unternehmen × 5.326 EUR	159 Mio. EUR
alle	Registrierungspflichten	diverse	diverse
alle	Einmaliger Aufwand	*freie Annahme*	2 Mrd. EUR

Quelle: openkritis.de

Sicherheitsverpflichtungen nach § 30 NIS 2-UmsG

- **Einrichtung eines Informationssicherheitsmanagementsystems (ISMS**): Unternehmen müssen ein ISMS nach ISO/IEC 27001 oder vergleichbaren Standards etablieren und betreiben. Dies umfasst die Festlegung von Richtlinien, Zielen und Prozessen zur Sicherstellung der Informationssicherheit.

- **Risikomanagement:** Unternehmen müssen regelmäßig Risikoanalysen durchführen, um Schwachstellen und Bedrohungen zu identifizieren und geeignete Maßnahmen zur Risikominimierung zu ergreifen. Dabei müssen sie auch die Auswirkungen von Sicherheitsvorfällen auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit berücksichtigen.

- **Sicherheitsvorfallmanagement:** Unternehmen müssen einen Prozess für das Management von Sicherheitsvorfällen einrichten. Dazu gehört die Überwachung, Erkennung und Reaktion auf Sicherheitsvorfälle sowie die Wiederherstellung des normalen Betriebs nach einem Vorfall.

- **Schutz vor Malware und Sicherheitslücken:** Unternehmen müssen angemessene technische und organisatorische Maßnahmen ergreifen, um ihre IT-Systeme vor Malware und Sicherheitslücken zu schützen. Dazu gehören regelmäßige Updates, die Implementierung von Firewalls und Virenschutzprogrammen sowie die Schulung der Mitarbeiter zur sicheren Nutzung von IT-Systemen.

- **Zugangs- und Berechtigungsmanagement:** Unternehmen müssen sicherstellen, dass nur autorisierte Personen Zugriff auf ihre IT-Systeme haben. Dazu gehören die Vergabe und Verwaltung von Zugangsrechten sowie die Überwachung und Protokollierung von Zugriffsaktivitäten.

- **Awareness- und Schulungsmaßnahmen:** Unternehmen müssen ihre Mitarbeiter regelmäßig über IT-Sicherheitsrichtlinien und -verfahren informieren und schulen. Dadurch soll das Bewusstsein für Sicherheitsrisiken geschärft und das richtige Verhalten der Mitarbeiter gefördert werden.

Sicherheitsverpflichtungen nach § 30 NIS 2-UmsG

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme (ISMS, z.B. ISO 27001)
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung des Betriebs, wie Back-up-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. **Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern** (hier gelten gem. § 30 Abs. 8 BSIG-E weitere spezifische Besonderheiten unter Einbeziehung der Entwicklungsprozesse)
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Sonderregeln für Bundeseinrichtungen §§ 43 ff.

1

Anforderungen

Risikomanagement, Meldepflichten, Registrierung, Nachweise, Unterrichtung.

2

Zusätzlich

Informationssicherheitsmanagement nach IT-Grundschutz.

3

Strukturen

Bundes-CISO, ISB in Einrichtungen und Ressorts.

Physische und technische Sicherheitskontrollen

1

Physische Sicherheit

Angemessene physische Schutzmaßnahmen sind unerlässlich, um Informationen und Systeme vor unbefugtem Zugriff, Schäden und Störungen zu schützen. Hierzu zählen Zugangskontrolle, Umweltschutz und Sicherung von Standorten.

2

Technische Sicherheit

Betriebssicherheit, Kommunikationssicherheit und Kontrollen bei der Systementwicklung stellen sicher, dass Informationen auch auf technischer Ebene vor Bedrohungen geschützt sind. Regelmäßige Backups und Notfallplanung erhöhen die Ausfallsicherheit.

3

Kontinuierliche Verbesserung

Das ISMS muss ständig überwacht und an neue Bedrohungen, Technologien und Geschäftsanforderungen angepasst werden. Regelmäßige Audits und Managementbewertungen bilden die Grundlage für kontinuierliche Verbesserungen.

Systementwicklung und -beschaffung

1

Sicherheitsanforderungen

Definition von Sicherheitsanforderungen bereits in der Konzeptionsphase.

2

Sichere Entwicklungsmethoden

Anwendung sicherer Programmier- und Entwicklungsmethoden.

3

Sicherheitsüberprüfungen

Durchführung von Tests und Code-Reviews zur Sicherstellung der Qualität.

Lieferantenbeziehungen

Auswahl vertrauenswürdiger Partner

Durchführung von Sicherheitsüberprüfungen potentieller Lieferanten.

Vertragliche Vereinbarungen

Festschreibung von Sicherheitsanforderungen in Lieferantenverträgen.

Überwachung und Audits

Regelmäßige Überprüfung der Lieferanten hinsichtlich Sicherheitskonformität.

Handhabung von Sicherheitsvorfällen

1

Meldeprozesse

Etablierung von Prozessen für die Meldung und Eskalation von Sicherheitsvorfällen.

2

Reaktionspläne

Vorbereitung und Bereitstellung von Reaktionsplänen für verschiedene Vorfallsszenarien.

3

Kontinuitätsplanung

Erstellung von Notfallplänen zur Gewährleistung der Geschäftskontinuität.

Risikomanagement

1

Risikoanalyse

Regelmäßige Risikoanalysen zur Identifizierung von Schwachstellen und Bedrohungen.

2

Risikominimierung

Ergreifen geeigneter Maßnahmen zur Minimierung von Risiken.

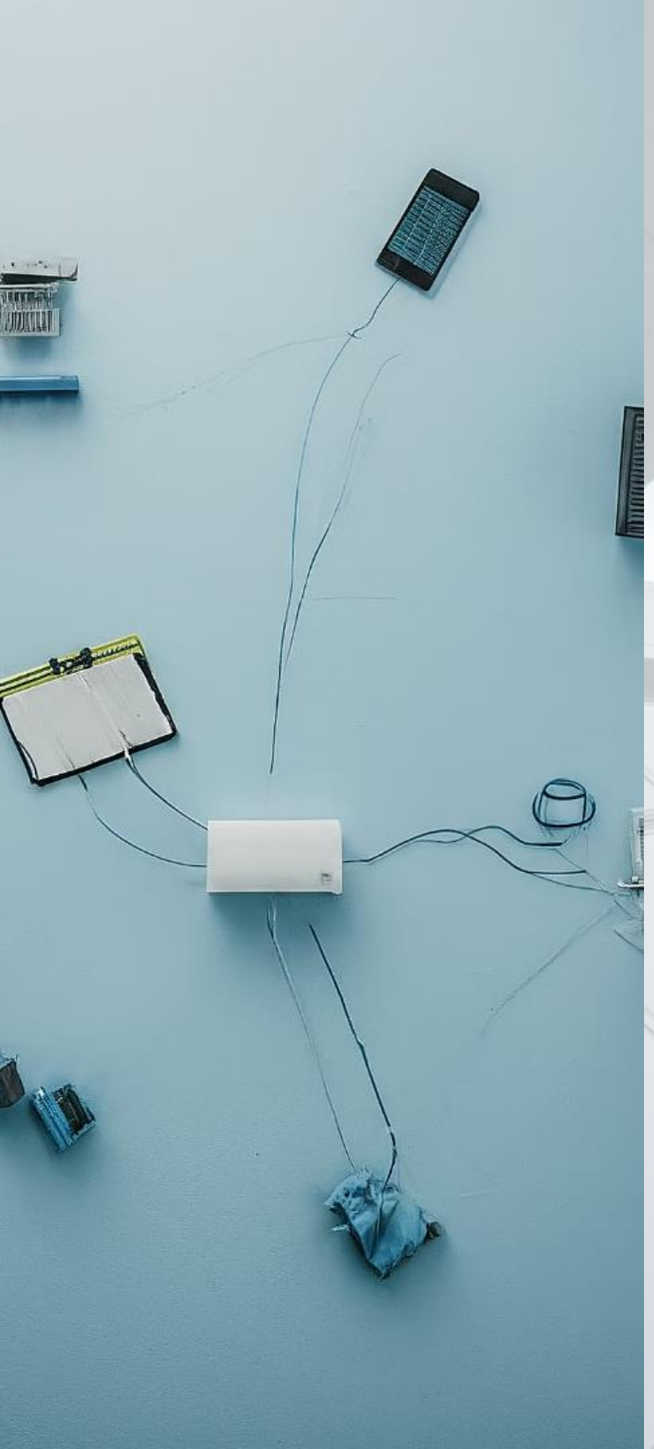
3

Auswirkungen

Berücksichtigung der Auswirkungen von Sicherheitsvorfällen auf Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit.

Risikomanagement und Informationssicherheit

Risikoanalyse	Konzepte für Risikoanalyse und Sicherheit von Informationssystemen
Sicherheitsvorfälle	Bewältigung von Sicherheitsvorfällen
Betriebsaufrechterhaltung	Back-up-Management, Wiederherstellung, Krisenmanagement
Lieferkette	Sicherheit der Lieferkette und Beziehungen zu Anbietern



Protokollierung

1

Zentrale Protokollsammlung

Das BSI empfiehlt eine zentrale Sammlung von Protokolldaten mit Agenten auf allen Geräten.

2

Normalisierung & Zeitsynchronisation

Die Protokolldaten sollten normalisiert und zeitsynchronisiert werden, um Angriffe zu erkennen.

3

Security Information and Event Management (SIEM)

SIEM-Systeme können zur Visualisierung und Auswertung der Protokolldaten eingesetzt werden.

Detektion

1

Erkennung von Angriffen

Die Protokolldaten müssen systematisch ausgewertet werden, um Angriffe frühzeitig zu erkennen.

2

Schadensreduktion & -vermeidung

Eine effektive Angriffserkennung hilft, Schäden zu reduzieren und zu vermeiden.

Reaktion

1

Erkennung

Angriffe müssen zunächst erkannt werden.

2

Analyse

Die Bedrohung muss analysiert und bewertet werden.

3

Gegenmaßnahmen

Angemessene Gegenmaßnahmen müssen ergriffen werden.

Qualifizierung von Ereignissen

Filterung

Sicherheitsrelevante Ereignisse müssen gefiltert werden.

Überprüfung

Die Ereignisse müssen auf Hinweise für Sicherheitsvorfälle überprüft werden.

Nachjustierung

Basierend auf den Erkenntnissen müssen die Detektionsmechanismen angepasst werden.

Managed Detection and Response

Das Managed Detection and Response System muss die genannten Anforderungen durch Livenetzwerkanalyse, automatisierte Erkennung und Unterstützung durch Fachleute erfüllen. Es ermöglicht schnelle Reaktionen auf Bedrohungen unter Einhaltung des EU-Datenschutzrechts.

Meldepflichten

1

Innerhalb 24 Stunden (!)

Initiale Meldung eines Sicherheitsvorfalls.

2

Innerhalb 72 Stunden

Details und erste Bewertung des Vorfalls.

3

Innerhalb 1 Monats

Abschlussbericht mit Ursachen und Gegenmaßnahmen.

Meldepflichten nach NIS 2

1

Erstmeldung

Innerhalb von 24 Stunden nach Kenntniserlangung eines Vorfalls.

2

Detailmeldung

Innerhalb von 72 Stunden mit erster Bewertung und Indikatoren.

3

Zwischenmeldungen

Auf Ersuchen des Bundesamts mit Statusaktualisierungen.

4

Abschlussmeldung

Spätestens einen Monat nach Detailmeldung mit Beschreibung und Maßnahmen.

Einhalten kurzer Reaktionszeiten

Klare Ziele

Realistische Ziele und Prioritäten für Reaktionszeiten festlegen. bei 24 Stunden Meldepflicht müssen intern zuständige Personen in weniger als 8 Stunden von dem Vorfall unterrichtet werden

Kommunikationskanäle

Geeignete Kanäle für Meldungen identifizieren und bekannt machen (Telefon, Mail, Whatsapp, interner Messenger etc).

Teamorganisation

Team und Zuständigkeiten für effiziente Bearbeitung organisieren.

Optimierte Workflows

Arbeitsabläufe optimieren, z.B. durch Automatisierung.

Protokollierung nach TKG

1

Erheben nur für bestimmte Zwecke

Verkehrsdaten dürfen nur für gesetzlich definierte Zwecke erhoben werden.

2

Unverzügliche Löschung

Nach Verbindungsende müssen Verkehrsdaten i.d.R. unverzüglich gelöscht warden, Ausnahme IT-Sicherheitsprüfungen, Verpflichtung zur Angriffserkennung bei KRITIS.

3

Leitfaden beachten

Es gibt einen Leitfaden für datenschutzgerechte Speicherung von Verkehrsdaten.

Vorratsdatenspeicherung bei TK- und Video-Daten

BGH-Urteil

Verkehrsdaten dürfen für 7 Tage aufbewahrt werden, unabhängig von Verdacht. Urteil vom 13.01.2011, auf Basis anderer Gesetzesregelungen in TKG und TMG gefällt, heute angesichts der Bedrohungslage meiner Ansicht nach überholt und nicht mehr vertretbar

BVerwG-Entscheidung / Europäischer Gerichtshof

Vorratsdatenspeicherung verstößt gegen Grundrechte und ist nicht anwendbar. Neue Entscheidung des EuGH lockert das Verbot, Urt. v. 30.04.2024, Az. C-470/21

BAG-Entscheidung vom 23.08.2018

Videodaten dürfen bis zum Ende der regulären Verjährungsfrist aufbewahrt warden, dies ist weniger eingriffsintensiv als komplette Kontrolle innerhalb von 7 Tagen

Sofortige Löschpflicht

1 Grundregel

Protokolldaten müssen bei Behörden pseudonymisiert werden und nach 18 Monaten ohne Verdacht gelöscht warden.
Bei Unternehmen keine Frist mehr im TTDSG für Sicherheitsuntersuchungen, altes BGH Urteil 7 Tage.
Empfehlung ohne Pseudonymisierung 6 Monate, mit Pseudonymisierung 18 Monate (Bundesarbeitsgericht sagt bis max. 36)
Protokolldaten müssen unverzüglich nach Auswertung gelöscht werden, soweit sich kein Verdacht ergibt.

2 Ausnahme

Nur bei konkreten Anhaltspunkten für Missbrauch dürfen Daten länger gespeichert werden.
Löschung aller Daten auch bei Verdacht nach spätestens 10 Jahren.

Empfehlungen

1

Pseudonymisierung

Protokolldaten sollten pseudonymisiert werden, soweit möglich.

2

Verdächtige Daten aussortieren

Nur verdächtige Daten sollten gespeichert werden, nicht der gesamte Datenverkehr.

SIEM-Lösung als Software (2) oder Managed Service (3)

1

Protokollierung

Protokollierung von Logdaten.

2

Zeitversetzte Auswertung

Protokolldaten können zeitversetzt ausgewertet werden.

3

Just-In-Time-Verarbeitung

Verdächtige Daten werden innerhalb von 15 Minuten durch Experten untersucht.

Angriffserkennung in Echtzeit

Erkennen

Systeme zur Angriffserkennung ermöglichen Echtzeitanalyse.

Eingrenzen

Nur verdächtige Logdaten werden langfristig gespeichert.

Beseitigen

Bedrohungen können schnell beseitigt werden.

Gesetzliche Vorgaben NIS 2, BSIG, TKG, EnWG

Systeme zur Angriffserkennung

Kontinuierliche Erfassung und Auswertung

Identifizierung und Vermeidung von Bedrohungen

Pflicht ab 1. Mai 2023 für KRITIS, schon vorher für TK-Netze und Energieanlagen

Geeignete Parameter und Merkmale

Beseitigungsmaßnahmen vorsehen

Orientierungshilfe

Zentralisierte Protokollierung

Protokolldaten müssen zentral gespeichert werden.

Bereitstellung für Auswertung

Protokolldaten müssen für Auswertung verfügbar gemacht werden.

Befristete Speicherung

Temporäre Speicherung von Rohdaten kann Detektion unterstützen.

Pseudonymisierung

1

Interne Daten

Pseudonymisierung von Mitarbeiterdaten wie IP-Adressen ist oft ausreichend.

2

Externe Daten

Vollständige Anonymisierung vor Untersuchung ist aufwändiger.

Lieferkettensicherheit

Kritische Anlagen

Müssen Maßnahmen nach § 9b BSIG ergreifen.

Wichtige Unternehmen

Müssen zertifizierte IKT-Produkte nach NIS 2 verwenden.

Vermeidung

Von Produkten aus Risikostaaten zur Spionageabwehr.

Lieferkettensicherheit

1

Risikobewertung

Untersuchung der Cybersicherheit von Lieferanten.

2

Vertragsklauseln

Festlegung von Sicherheitsanforderungen in Lieferantenverträgen.

3

Kontinuierliches Monitoring

Laufende Überwachung der Lieferkettensicherheit.

Sanktionen für Unternehmen

Hohe Bußgelder

Bußgelder bis zu 10 Millionen Euro als Abschreckung.

Untersuchung

Bußgelder nach Untersuchung und Bewertung des Verstoßes.

Anreiz

Anreiz, in Cybersicherheit zu investieren.

Haftung der Geschäftsführung

1

Persönliche Haftung

Geschäftsleiter haften persönlich für Fehler im Risikomanagement.

2

Schulungen

Regelmäßige Schulungen zu Risikomanagementthemen sind Pflicht.

3

Unabhängig von Rechtsform

Haftung gilt unabhängig von der Rechtsform des Unternehmens.

Fazit

Frühzeitig handeln

Unternehmen sollten frühzeitig Sicherheitskonzepte implementieren.

Hersteller aus EU

Empfehlenswert, einen EU-Hersteller zu wählen (Datenschutzgründe).

Hohe Strafen

Hohe Bußgelder und persönliche Haftung als Anreiz.

Dokumentation

KRITIS-Betreiber und besonders wichtige Unternehmen müssen die ergriffenen Maßnahmen umfangreich dokumentieren und nachweisen.

Withsecure Whitepaper zu NIS 2