TECHCARE RESEARCH · WHITEPAPER NR. 03

KOSTENFREI · PDF

NIS2 & Hardwarewartung — *was Auditoren prüfen.*

Wartungsverträge im Spannungsfeld der NIS2-Richtlinie: welche der zehn Pflicht-Maßnahmen aus Art. 21 den Hardware-Betrieb treffen, was Prüfer an Nachweisen sehen wollen — und wie SLA, Lieferkette und Verantwortlichkeiten im Vertrag so dokumentiert werden, dass sie im Audit standhalten.

10

Pflicht-Maßnahmen in Art. 21 — vier greifen direkt in den Hardware-Betrieb

~30.000

deutsche Einrichtungen im NIS2-Scope (BSIG, in Kraft seit Dez. 2025)

24h / 72h

Frühwarnung / Vorfallsmeldung — der Wartungspartner muss zuliefern

September 2026 · TechCare Research

TechCare Solutions GmbH · Hahnstätten · techcaresolutions.de

Inhalt

Hervorgehobene Kapitel enthalten die Arbeitshilfen: die Prüf-Matrix (Kap. 5), die SLA-Bausteine (Kap. 7) und die 12-Punkte-Klausel-Checkliste (Kap. 12).

KAPITEL 01

Management Summary

Die Kernthese dieses Whitepapers lautet: **Hardwarewartung ist unter NIS2 kein Beschaffungsthema mehr, sondern ein Prüfgegenstand.** Wer Server, Storage und Netzwerk betreibt, die in den Anwendungsbereich der Richtlinie fallen, muss dem Auditor nachweisen können, dass diese Systeme verfügbar gehalten, gegen Schwachstellen behandelt und über eine gesicherte Lieferkette gewartet werden — und dass die Geschäftsleitung genau das billigt und überwacht.

Der Grund liegt im Aufbau der Richtlinie. Art. 21 der NIS2-Richtlinie (EU) 2022/2555 verlangt von betroffenen Einrichtungen einen Mindestkatalog aus zehn technischen und organisatorischen Maßnahmen [1]. Mindestens vier davon greifen unmittelbar in den Hardware-Betrieb: Business-Continuity und Backup (lit. c), Sicherheit der Lieferkette einschließlich der Beziehungen zu Dienstleistern (lit. d), Sicherheit bei Erwerb, Entwicklung *und Wartung* von Systemen einschließlich der Behandlung von Schwachstellen (lit. e) sowie Zugriffskontrolle und Anlagenmanagement (lit. i). Deutschland hat diesen Katalog mit dem NIS2-Umsetzungsgesetz im Dezember 2025 in § 30 BSIG übernommen; rund 30.000 Unternehmen aus 18 Sektoren sind betroffen [3][4].

Für den Wartungsvertrag bedeutet das eine Verschiebung des Maßstabs. Bislang wurde ein SLA nach Reaktionszeit und Preis bewertet. Unter NIS2 muss er zusätzlich drei Fragen beantworten, die ein Prüfer stellt:

- **Verfügbarkeit als Sicherheitsziel:** Ist die Wiederherstellzeit kritischer Systeme vertraglich zugesichert, mit Ersatzteil-Vorhaltung hinterlegt und in Reports belegt (Art. 21 Abs. 2 lit. c)?
- **Der Dienstleister als Lieferkette:** Ist der Wartungspartner als Lieferant bewertet — Zertifizierungen, Sub-Unternehmer, Herkunft der Ersatzteile, Personal- und Zugriffsregeln (lit. d, lit. i)?
- **Schwachstellen und Support-Ende:** Ist dokumentiert, wie Firmware gepatcht wird, welche Systeme jenseits des Hersteller-Supports laufen und welche kompensierenden Maßnahmen die Geschäftsleitung dafür akzeptiert hat (lit. e, § 38 BSIG)?

Hinzu kommt die Meldekaskade: Frühwarnung binnen 24 Stunden, Vorfallsmeldung binnen 72 Stunden, Abschlussbericht binnen eines Monats [1][3]. Diese Fristen lassen sich nur halten, wenn Inventar, Patch-Stand und Ansprechpartner des Wartungspartners *vor* dem Vorfall dokumentiert vorliegen. Ein Wartungsvertrag, der keine Mitwirkung an der Meldung regelt, wird im Audit zur offenen Flanke.

Was das für den Betreiber bedeutet

Dieses Whitepaper übersetzt die Richtlinie in prüfbare Punkte. Kapitel 4 ordnet die zehn Maßnahmen dem Hardware-Betrieb zu. Kapitel 5 liefert die Prüf-Matrix — zehn Prüffelder mit den Nachweisen, die Auditoren typischerweise anfordern. Kapitel 6 bis 10 vertiefen Lieferkette, SLA, Schwachstellen, Meldewesen und physische Kontrollen. Kapitel 11 behandelt die Verantwortung der Geschäftsleitung nach § 38 BSIG, Kapitel 12 fasst alles in einer 12-Punkte-Klausel-Checkliste für den Wartungsvertrag zusammen.

> **KERNAUSSAGE**
>
> NIS2 macht den Wartungsvertrag zum Nachweisdokument. Wer SLA, Lieferkette, Patch-Prozess und Verantwortlichkeiten heute sauber dokumentiert, hat im Audit kein Hardware-Problem — sondern eine Akte, die für ihn spricht.

KAPITEL 02

NIS2 in zehn Minuten: Wer, was, ab wann

Die Richtlinie (EU) 2022/2555 — kurz NIS2 — ist am 16. Januar 2023 in Kraft getreten und war von den Mitgliedstaaten bis zum 17. Oktober 2024 in nationales Recht umzusetzen [1][2]. Sie ersetzt die erste NIS-Richtlinie von 2016 und weitet deren Anwendungsbereich erheblich aus: von einer Handvoll Betreiber kritischer Infrastrukturen auf einen breiten Kreis mittlerer und großer Unternehmen in 18 Sektoren.

Wer betroffen ist

NIS2 unterscheidet zwei Kategorien von Einrichtungen. **Wesentliche Einrichtungen** (im deutschen Recht: „besonders wichtige Einrichtungen") sind in der Regel Großunternehmen ab 250 Beschäftigten oder ab 50 Mio. EUR Umsatz in den Sektoren mit hoher Kritikalität nach Anhang I — Energie, Verkehr, Bankwesen, Finanzmarkt, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, IKT-Dienstleistungsmanagement, öffentliche Verwaltung, Weltraum. **Wichtige Einrichtungen** sind mittlere Unternehmen ab 50 Beschäftigten oder ab 10 Mio. EUR Umsatz in diesen sowie in den sieben weiteren Sektoren nach Anhang II — unter anderem Post, Abfall, Chemie, Lebensmittel, verarbeitendes Gewerbe (darunter Medizinprodukte, Elektronik, Maschinenbau, Fahrzeugbau), digitale Dienste und Forschung [1].

Entscheidend für den Mittelstand: Die Größenschwelle ist eine *Oder*-Regel. Ein Maschinenbauer mit 60 Beschäftigten fällt ebenso in den Anwendungsbereich wie ein Lebensmittelhersteller mit 12 Mio. EUR Umsatz. Ob das eigene Unternehmen betroffen ist, lässt sich mit der Betroffenheitsprüfung des BSI in wenigen Minuten klären [4].

Deutschland: NIS2UmsuCG und BSIG

Deutschland hat die Frist verfehlt und das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) im Dezember 2025 in Kraft gesetzt. Kern ist die Novelle des BSI-Gesetzes (BSIG). Nach Schätzung des Bundesinnenministeriums sind rund 30.000 Einrichtungen erfasst — etwa 8.250 besonders wichtige und rund 21.600 wichtige [3][16]. Die zentralen Paragraphen:

§ BSIG	Regelungsgegenstand	Bezug zur Hardwarewartung
§ 28	Anwendungsbereich	Klärt, ob die gewartete Infrastruktur überhaupt im NIS2-Scope liegt
§ 30	Risikomanagement-Maßnahmen	Pendant zu Art. 21 — Lieferkette, Wartung, Schwachstellen, BCM
§ 31	Besondere Anforderungen an Betreiber kritischer Anlagen	Systeme zur Angriffserkennung — betrifft auch Netzwerk- und Management-Hardware
§ 32	Meldepflichten	24h/72h/1-Monat-Kaskade — Wartungspartner muss zuliefern
§ 33	Registrierungspflicht	Registrierung beim BSI binnen drei Monaten nach Betroffenheit
§ 38	Pflichten der Geschäftsleitung	Billigung, Überwachung, Schulung — persönliche Verantwortung
§ 65	Bußgeldvorschriften	Bis 10 Mio. EUR / 2 % bzw. 7 Mio. EUR / 1,4 % des weltweiten Umsatzes

Ab wann geprüft wird

Anders als bei einer Zertifizierung gibt es unter NIS2 keinen festen Audit-Termin. Besonders wichtige Einrichtungen unterliegen der laufenden Aufsicht des BSI und müssen Nachweise auf Verlangen vorlegen; Betreiber kritischer Anlagen weisen ihre Maßnahmen regelmäßig nach. Wichtige Einrichtungen werden anlassbezogen geprüft — typischerweise nach einem Vorfall oder einem Hinweis [1][3]. In der Praxis kommen die Prüffragen aber schneller: über Kunden, die ihre eigene Lieferkette nach Art. 21 Abs. 2 lit. d bewerten müssen, über Versicherer und über Wirtschaftsprüfer, die die Geschäftsleitungspflichten nach § 38 BSIG in ihre Prüfung einbeziehen.

> **KERNAUSSAGE**
>
> Der Prüfer kommt selten mit Termin. Wer die Nachweise erst für den Audit zusammensucht, ist zu spät — der erste „Auditor" ist oft der eigene Großkunde mit einem Lieferanten-Fragebogen.

KAPITEL 03

Warum Hardwarewartung ein NIS2-Thema ist

Auf den ersten Blick handelt NIS2 von Cybersicherheit — von Angriffen, Schwachstellen und Meldewegen. Der Handlungsdruck ist real: Der Bitkom beziffert den jährlichen Schaden durch Cyberangriffe, Sabotage und Spionage für die deutsche Wirtschaft in seiner Studie Wirtschaftsschutz 2024 auf rund 266,6 Mrd. EUR [15]. Hardwarewartung klingt daneben nach Ersatzteilen und Reaktionszeiten. Der Zusammenhang wird klar, wenn man drei Schutzziele der Richtlinie auf den physischen Betrieb anwendet.

1. Verfügbarkeit ist ein Sicherheitsziel

Art. 21 Abs. 1 verpflichtet Einrichtungen, Maßnahmen zu treffen, um „die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder möglichst gering zu halten" [1]. „Sicherheitsvorfall" ist in Art. 6 weit definiert: jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der angebotenen Dienste beeinträchtigt. Ein ausgefallener Storage-Controller ohne verfügbares Ersatzteil ist damit kein reines Betriebsproblem, sondern kann ein meldepflichtiger Vorfall sein — unabhängig davon, ob ein Angreifer beteiligt war.

2. Der Wartungspartner ist Teil der Lieferkette

Art. 21 Abs. 2 lit. d verlangt Maßnahmen zur „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern". Abs. 3 präzisiert: Dabei sind die spezifischen Schwachstellen jedes Anbieters sowie die Gesamtqualität seiner Produkte und Cybersicherheitspraxis zu berücksichtigen [1]. Ein Wartungsdienstleister, dessen Techniker physischen und Remote-Zugriff auf Server erhalten und Ersatzteile in die Umgebung einbringen, ist ein unmittelbarer Diensteanbieter im Sinne dieser Vorschrift. Er muss bewertet, vertraglich eingebunden und überwacht werden.

3. Wartung ist ausdrücklich genannt

Lit. e verlangt „Sicherheit bei Erwerb, Entwicklung und **Wartung** von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen" [1]. Die Richtlinie nennt die Wartungsphase also nicht beiläufig, sondern als eigenen Regelungsgegenstand — und koppelt sie an die Behandlung von Schwachstellen. Für Hardware heißt das: Firmware-Stände, Management-Controller (BMC, iLO, iDRAC, CIMC), Netzwerk-Betriebssysteme und Storage-Microcode sind Teil des Schwachstellen-Managements, nicht nur der Applikations-Stack.

Was Auditoren daraus ableiten

Prüfer arbeiten selten mit dem Richtlinientext, sondern mit Prüfkatalogen, die daraus abgeleitet sind — in Deutschland vor allem mit dem IT-Grundschutz-Kompendium des BSI [5] und mit ISO/IEC 27001:2022 [8]. Beide kennen eigene Bausteine für genau diese Schnittstelle: OPS.2.3 „Nutzung von Outsourcing", OPS.1.1.3 „Patch- und Änderungsmanagement", CON.6 „Löschen und Vernichten", DER.2.1 „Behandlung von Sicherheitsvorfällen" auf BSI-Seite; die Controls 5.19 bis 5.22 (Lieferantenbeziehungen), 7.13 (Instandhaltung von Geräten), 7.14 (sichere Entsorgung oder Wiederverwendung) und 8.8 (Handhabung technischer Schwachstellen) im Anhang A der ISO 27001. Wer seinen Wartungsvertrag gegen diese Bausteine hält, weiß, was der Prüfer sehen will.

> **KERNAUSSAGE**
>
> Verfügbarkeit, Lieferkette, Wartung: drei Begriffe aus Art. 21, die zusammen genau die Leistung beschreiben, die ein Hardware-Wartungsvertrag erbringt. Deshalb steht er im Audit auf der Liste.

KAPITEL 04

Die zehn Maßnahmen aus Art. 21 — und ihr Hardware-Bezug

Art. 21 Abs. 2 zählt zehn Maßnahmenbereiche auf, die jede betroffene Einrichtung „zumindest" umsetzen muss. § 30 Abs. 2 BSIG übernimmt den Katalog nahezu wortgleich [1][3]. Die folgende Übersicht ordnet jedem Bereich zu, was er für den Betrieb und die Wartung physischer Infrastruktur bedeutet und welchen Nachweis ein Prüfer typischerweise sehen will.

Art. 21 (2)	Maßnahme	Hardware-/Wartungsbezug	Typischer Nachweis
a	Risikoanalyse und Sicherheitskonzepte	Hardware-Assets sind Teil der Risikoanalyse — inkl. Alter, Support-Status, Redundanz	Risikoregister mit Asset-Bezug
b	Bewältigung von Sicherheitsvorfällen	Hardware-Ausfall und Firmware-Kompromittierung als Vorfallstypen; Rolle des Wartungspartners	Incident-Prozess, Eskalationsmatrix
c	Business Continuity, Backup, Krisenmanagement	Wiederherstellzeiten, Ersatzteil-Vorhaltung, Redundanz — der SLA-Kern	BCM-Plan, SLA-Reports, Test-Protokolle
d	Sicherheit der Lieferkette	Wartungsdienstleister, Ersatzteil-Herkunft, Sub-Unternehmer	Lieferantenbewertung, Vertrag, Zertifikate
e	Sicherheit bei Erwerb, Entwicklung, Wartung; Schwachstellen	Firmware-Patching, EOSL-Umgang, Hersteller-Advisories	Patch-Log, Schwachstellen-Tracking
f	Bewertung der Wirksamkeit	Regelmäßige Prüfung, ob SLA und Patch-Prozess wirken	KPI-Review, interne Audits
g	Cyberhygiene und Schulung	Techniker-Verhalten vor Ort, Umgang mit Wechselmedien und Diagnosetools	Schulungsnachweise, Verhaltensregeln
h	Kryptografie und Verschlüsselung	Verschlüsselte Datenträger; Schlüsselhandling beim Tausch von Platten	Krypto-Konzept, Erase-Zertifikate
i	Personalsicherheit, Zugriffskontrolle, Anlagenmanagement	Asset-Inventar, Zutritt von Fremdpersonal, Remote-Zugriff	Inventar, Zutrittsprotokolle, Zugriffslogs
j	MFA, sichere Kommunikation, Notfallkommunikation	MFA für Remote-Wartungszugänge; Notfall-Erreichbarkeit des Service-Desks	MFA-Nachweis, Erreichbarkeits-Matrix

Vier Bereiche mit direktem Durchgriff

Die Bereiche c, d, e und i wirken unmittelbar auf den Wartungsvertrag. Sie beantworten in Summe die Frage, die der Prüfer stellt: *Wird diese Hardware verfügbar gehalten, von einem bewerteten Partner, mit aktueller Firmware, unter kontrolliertem Zugriff?* Die übrigen sechs Bereiche wirken mittelbar — sie setzen den organisatorischen Rahmen, in dem der Vertrag lebt.

Stand der Technik und Verhältnismäßigkeit

Art. 21 Abs. 1 verlangt, dass die Maßnahmen dem „Stand der Technik" entsprechen und verhältnismäßig sind — gemessen an Risikoexposition, Größe der Einrichtung, Eintrittswahrscheinlichkeit und Schwere möglicher Vorfälle [1]. Für den Mittelstand ist das eine Entlastung und eine Pflicht zugleich: Niemand verlangt vom 80-Personen-Zulieferer die Prozesse eines Netzbetreibers. Aber die Angemessenheit muss begründet und dokumentiert sein. Ein Wartungsvertrag mit 4-Stunden-Vor-Ort-Reaktion für das ERP-Cluster und Next-Business-Day für die Testumgebung ist genau so eine begründete Abstufung — sofern sie aus der Risikoanalyse (lit. a) folgt und nicht aus dem Budget.

> **KERNAUSSAGE**
>
> Zehn Maßnahmen, vier davon mit direktem Hardware-Durchgriff: BCM (c), Lieferkette (d), Wartung und Schwachstellen (e), Zugriff und Anlagen (i). Sie bilden das Raster, entlang dessen Kapitel 5 die Prüf-Matrix aufbaut.

KAPITEL 05

Was Auditoren prüfen: die Prüf-Matrix

Auditoren prüfen nicht, ob eine Einrichtung „NIS2-konform" ist — dieser Begriff existiert als Zertifikat nicht. Sie prüfen, ob die geforderten Maßnahmen *umgesetzt, dokumentiert und wirksam* sind. Für den Hardware-Betrieb hat sich ein Muster aus zehn Prüffeldern herausgebildet, das sich aus Art. 21, den BSI-Bausteinen und ISO 27001 ableiten lässt. Die folgende Matrix ist eine TechCare-Arbeitshilfe: Sie nennt je Prüffeld die Prüffrage, den Nachweis, den Prüfer typischerweise anfordern, und die Referenz, auf die sie sich stützen [1][5][8].

#	Prüffeld	Prüffrage	Erwarteter Nachweis	Referenz
1	**Asset-Inventar**	Ist jedes Hardware-System mit Modell, Standort, Verantwortlichem, Support-Status und Kritikalität erfasst?	Aktuelle Inventarliste, Abgleich mit CMDB, letzte Aktualisierung	Art. 21 (2) i · ISO 5.9 · DVO 2024/2690 Abschn. 12
2	**Kritikalität & Risiko**	Ist je System die Ausfallwirkung bewertet und die Schutzmaßnahme daraus abgeleitet?	Risikoregister, Schutzbedarfsfeststellung, SLA-Zuordnung	Art. 21 (2) a · BSI Standard 200-3
3	**Verfügbarkeit & SLA**	Sind Reaktions- und Wiederherstellzeiten vertraglich fixiert und mit Ersatzteil-Vorhaltung hinterlegt? Werden sie eingehalten?	Wartungsvertrag, SLA-Performance-Reports, Ticket-Auswertung	Art. 21 (2) c · ISO 5.30 · BSI OPS.2.3
4	**Lieferanten-Bewertung**	Ist der Wartungspartner als Lieferant bewertet — Zertifikate, Sub-Unternehmer, Standorte, Sicherheitspraxis?	Lieferantenbewertung, ISO-27001-Zertifikat, Sub-Outsourcing-Liste	Art. 21 (2) d, (3) · ISO 5.19–5.22
5	**Vertrag & Klauseln**	Enthält der Vertrag Sicherheitsanforderungen, Melde-Mitwirkung, Audit-Rechte, Exit-Regeln?	Vertragstext mit Sicherheitsanhang	Art. 21 (2) d · ISO 5.20 · DORA Art. 30 (Blaupause)
6	**Firmware & Patches**	Werden Hersteller-Advisories verfolgt und Firmware-Updates dokumentiert eingespielt?	Patch-Log je System, Advisory-Abgleich, Ausnahmen mit Begründung	Art. 21 (2) e · BSI OPS.1.1.3 · ISO 8.8
7	**Support-Ende (EOSL)**	Welche Systeme laufen jenseits des Hersteller-Supports — und mit welcher dokumentierten Risiko-Akzeptanz?	EOSL-Liste, Risiko-Akzeptanz der Leitung, kompensierende Maßnahmen	BSI OPS.1.1.3 (MUSS) · § 38 BSIG
8	**Vorfälle & Meldung**	Ist geregelt, wie Hardware-Vorfälle erkannt, eskaliert und in die 24h/72h-Kaskade eingespeist werden?	Incident-Prozess, Eskalationsmatrix mit Wartungspartner, Übungsprotokoll	Art. 23 · § 32 BSIG · BSI DER.2.1
9	**Datenträger & Ersatzteile**	Werden getauschte Datenträger nachweislich gelöscht oder vernichtet? Ist die Herkunft von Ersatzteilen belegt?	Erase-/Vernichtungszertifikate, Chain-of-Custody, Seriennummern-Protokoll	BSI CON.6 · ISO 7.10, 7.14 · NIST SP 800-88
10	**Zugriff Externer**	Sind physischer Zutritt und Remote-Zugriff von Technikern kontrolliert, protokolliert und mit MFA gesichert?	Zutrittsprotokolle, Zugriffslogs, MFA-Nachweis, Begleitregelung	Art. 21 (2) i, j · BSI ORP.4, INF.2

Wie Prüfer vorgehen

Die Reihenfolge der Matrix entspricht dem typischen Prüfablauf: Der Auditor beginnt beim Inventar, leitet über die Kritikalität zu SLA und Lieferant über und endet bei den physischen Kontrollen. Stichproben sind üblich: „Zeigen Sie mir für dieses Storage-System den Support-Status, das letzte Firmware-Update, den zuständigen Ansprechpartner beim Wartungspartner und den letzten Ersatzteil-Tausch mit Datenträger-Nachweis."

Die häufigsten Lücken

Drei Lücken sind in der Prüfpraxis typisch: erstens ein Inventar, das Hardware jenseits des Hersteller-Supports nicht kennzeichnet; zweitens Wartungsverträge ohne Sicherheitsanhang — Reaktionszeit ja, Melde-Mitwirkung, Sub-Unternehmer und Datenträger-Regeln nein; drittens fehlende Nachweise für getauschte Datenträger.

> **KERNAUSSAGE**
>
> Zehn Prüffelder, vier Belege pro Stichprobe: Support-Status, Patch-Stand, Ansprechpartner, Datenträger-Nachweis. Wer das für jedes System liefern kann, führt das Audit — nicht der Auditor.

KAPITEL 06

Lieferketten-Sicherheit: der Wartungsdienstleister als Lieferant

Lieferketten-Angriffe gehören laut ENISA seit Jahren zu den prägenden Bedrohungen der europäischen Cybersicherheitslage; die Behörde widmet ihnen in der Threat-Landscape-Reihe eigene Kapitel [14]. NIS2 reagiert darauf mit Art. 21 Abs. 2 lit. d und Abs. 3 sowie mit den koordinierten Risikobewertungen kritischer Lieferketten nach Art. 22 [1]. Für den Betreiber heißt das: Jeder unmittelbare Dienstleister mit Zugriff auf Netz- und Informationssysteme muss bewertet werden — und der Hardware-Wartungspartner gehört zu den Dienstleistern mit dem tiefsten Zugriff überhaupt.

Was „bewerten" bedeutet

Art. 21 Abs. 3 nennt drei Dimensionen: die spezifischen Schwachstellen des Anbieters, die Gesamtqualität seiner Produkte und Cybersicherheitspraxis sowie seine sicheren Entwicklungsverfahren [1]. Übertragen auf Wartungsdienstleister ergibt sich ein Prüfraster, das ISO/IEC 27001:2022 in den Controls 5.19 bis 5.22 konkretisiert [8]:

- **5.19 Informationssicherheit in Lieferantenbeziehungen** — Gibt es eine Richtlinie, welche Anforderungen an Dienstleister mit Systemzugriff gelten?
- **5.20 Behandlung in Lieferantenvereinbarungen** — Stehen diese Anforderungen im Vertrag (Kapitel 12)?
- **5.21 Sicherheit in der IKT-Lieferkette** — Ist bekannt, woher Ersatzteile stammen und welche Sub-Unternehmer der Dienstleister einsetzt?
- **5.22 Überwachung und Änderungsmanagement** — Werden SLA-Reports geprüft, Zertifikate nachgehalten, Änderungen (neue Sub-Unternehmer, neue Standorte) gemeldet?

Der BSI-Blick: OPS.2.3

Der Baustein OPS.2.3 „Nutzung von Outsourcing" des IT-Grundschutz-Kompendiums (Edition 2023) ist die deutsche Konkretisierung [5]. Er verlangt unter anderem eine Outsourcing-Strategie, eine Sicherheitsanforderungs-Spezifikation für den Dienstleister, vertragliche Regelungen zu Sicherheit und Kontrolle, eine geregelte Beendigung sowie die laufende Überwachung. Übertragen auf Hardwarewartung sind vier Punkte prüfungsrelevant: Wer darf wann mit welcher Berechtigung an welches System? Welche Sub-Unternehmer sind mit welchem Zugriff beteiligt? Wo lagern Ersatzteile und wie ist die Herkunft belegt? Wie endet die Zusammenarbeit — Rückgabe von Zugängen, Dokumentation, Übergabe?

DORA als Blaupause

Für Finanzunternehmen regelt die DORA-Verordnung (EU) 2022/2554 seit Januar 2025 in Art. 28 bis 30 sehr konkret, was in Verträgen mit IKT-Drittdienstleistern stehen muss: Leistungsbeschreibung, Standorte der Leistungserbringung, Verfügbarkeits- und Integritätszusagen, Unterstützung bei Vorfällen, Zusammenarbeit mit Behörden, Kündigungsrechte, Exit-Strategien [9]. NIS2 ist weniger detailliert, doch Prüfer nutzen DORA zunehmend als Maßstab dafür, was ein „angemessener" Dienstleistervertrag enthält.

Sub-Outsourcing: die unsichtbare zweite Reihe

Der häufigste Befund in Lieferantenprüfungen betrifft die zweite Reihe: Der Vertragspartner ist bekannt und bewertet, seine Sub-Unternehmer — Ersatzteil-Logistiker, regionale Techniker-Partner, Remote-Support-Zentren — nicht. Praktisch heißt das: Der Wartungsvertrag sollte eine Liste der eingesetzten Sub-Unternehmer mit Rolle und Standort enthalten und eine Meldepflicht bei Änderungen vorsehen.

> **KERNAUSSAGE**
>
> Der Wartungspartner hat physischen Zugriff, Remote-Zugriff und bringt Teile in die Umgebung — kein anderer Lieferant kommt der Infrastruktur näher. Entsprechend tief muss die Bewertung reichen: bis zu Sub-Unternehmern, Ersatzteil-Herkunft und Exit-Regelung.

KAPITEL 07

SLA-Anforderungen unter NIS2: Verfügbarkeit ist Sicherheitsziel

Ein Service Level Agreement war lange ein kaufmännisches Instrument: Reaktionszeit gegen Preis. Unter NIS2 wird es zum Sicherheitsnachweis für Art. 21 Abs. 2 lit. c — Aufrechterhaltung des Betriebs, Backup-Management, Wiederherstellung nach Notfällen [1]. Der Auditor liest den SLA-Abschnitt deshalb mit einer anderen Frage: Nicht „Ist das günstig?", sondern „Ist die Wiederherstellzeit kritischer Systeme zugesichert, belegbar und getestet?"

Warum Ausfälle Sicherheitsvorfälle sind

Das Uptime Institute weist in seiner Annual Outage Analysis 2024 aus, dass gut die Hälfte der befragten Betreiber in den vorangegangenen drei Jahren mindestens einen bedeutenden Ausfall hatte; mehr als die Hälfte der gravierenden Ausfälle kostete über 100.000 US-Dollar, rund jeder sechste über eine Million [13]. Hardware- und Stromversorgungsprobleme bleiben unter den führenden Ursachen. Für NIS2 zählt weniger der Kostenschaden als die Dienstbeeinträchtigung: Sobald ein wesentlicher Dienst erheblich gestört ist, greift die Meldepflicht nach Art. 23 — auch bei rein technischer Ursache.

Die vier SLA-Bausteine, die Prüfer erwarten

Baustein	Was vereinbart sein sollte	Nachweis im Audit
Reaktions- und Wiederherstellzeit	Abgestuft nach Kritikalität (z. B. 4h Vor-Ort für Tier-1, NBD für Tier-3), je System zugeordnet; Wiederherstellzeit als Ziel, nicht nur Reaktion	SLA-Matrix mit Asset-Bezug, monatlicher Performance-Report
Ersatzteil-Vorhaltung	Regionale Depots, kritische Komponenten vorab bevorratet, Lieferzeit zugesichert, Herkunft dokumentiert	Depot-Liste, Ersatzteil-Reservierung, Chain-of-Custody
Eskalation und Erreichbarkeit	24/7-Service-Desk, benannte Eskalationsstufen, Notfallkontakt außerhalb der Ticket-Kette (Art. 21 (2) j)	Eskalationsmatrix, Erreichbarkeitstest
Reporting und Review	Regelmäßige SLA-Reports, Ticket-Auswertung, jährliches Service-Review mit Maßnahmen	Reports, Review-Protokoll (Art. 21 (2) f)

Reaktion ist nicht Wiederherstellung

Viele SLAs sichern eine Reaktionszeit zu — den Zeitpunkt, an dem ein Techniker den Fall annimmt. Für Art. 21 Abs. 2 lit. c zählt die Wiederherstellung des Dienstes. Der Unterschied ist im Audit entscheidend: Ein SLA mit „Reaktion binnen 4 Stunden" sagt nichts über die Verfügbarkeit, wenn das Ersatzteil drei Tage unterwegs ist. Prüfer erwarten daher entweder eine zugesicherte Wiederherstellzeit oder — realistischer bei Hardware — eine Reaktionszeit *plus* nachweisbare Ersatzteil-Vorhaltung, aus der sich die tatsächliche Wiederherstellzeit ableiten lässt. Die Ticket-Historie der letzten zwölf Monate ist dabei der überzeugendste Beleg.

Testen statt vertrauen

ISO 27001:2022 verlangt in Control 5.30 „IKT-Bereitschaft für Business Continuity", dass Wiederherstellungsfähigkeiten geplant, umgesetzt und *getestet* werden [8]. Für die Hardwarewartung bedeutet das mindestens: einmal jährlich den Ausfall eines kritischen Systems durchspielen — inklusive Anruf beim Service-Desk, Ersatzteil-Abruf und Protokoll der tatsächlichen Zeiten. Ein solches Übungsprotokoll ist im Audit mehr wert als jede Vertragsklausel.

> **KERNAUSSAGE**
>
> Unter NIS2 beantwortet der SLA die Frage nach der Wiederherstellzeit, nicht nach der Reaktionszeit. Zugesicherte Zeiten, hinterlegte Ersatzteile, gemessene Reports und ein jährlicher Test — das ist der Nachweis für Art. 21 Abs. 2 lit. c.

KAPITEL 08

Firmware, Patches, Schwachstellen: OPS.1.1.3 und EOSL-Hardware

Das BSI registrierte im Berichtszeitraum seines Lageberichts 2024 durchschnittlich 78 neue Schwachstellen in Softwareprodukten pro Tag — ein Anstieg gegenüber dem Vorjahr [6]. Ein wachsender Anteil betrifft Firmware — Server, Management-Controller, Storage, Netzwerk. Genau diese Schicht adressiert Art. 21 Abs. 2 lit. e mit der Formel „Sicherheit bei Wartung … einschließlich Management und Offenlegung von Schwachstellen" [1].

Warum Firmware im Audit auffällt

Management-Controller (iLO, iDRAC, CIMC, BMC) laufen unterhalb des Betriebssystems, sind oft dauerhaft am Netz und werden in vielen Umgebungen seltener aktualisiert als der Applikations-Stack. Hersteller-Advisories [17] und der CISA-Katalog bekannter ausgenutzter Schwachstellen (KEV) [11] führen wiederholt Einträge zu Management- und Netzwerkkomponenten. Für den Prüfer ist die Frage einfach: „Wann wurde die Firmware dieses Systems zuletzt aktualisiert, und wer hat die Hersteller-Advisories abgeglichen?"

Der BSI-Baustein OPS.1.1.3

OPS.1.1.3 „Patch- und Änderungsmanagement" (Edition 2023) verlangt einen dokumentierten Prozess für Patches und Änderungen — Verantwortlichkeiten, Test, Freigabe, Einspielen, Nachweis [5]. Zwei Anforderungen sind für die Hardwarewartung zentral. Erstens: Patches müssen zeitnah bewertet und eingespielt werden, und zwar auch für Firmware. Zweitens, als MUSS-Anforderung formuliert: Werden Produkte eingesetzt, die vom Hersteller nicht mehr unterstützt werden, MUSS geprüft werden, ob sie noch sicher betrieben werden können; ist das nicht der Fall, DÜRFEN sie nicht weiterverwendet werden.

EOSL-Hardware unter NIS2

Damit ist EOSL-Hardware ein eigenes Prüffeld (Kapitel 5, Feld 7). Verboten ist der Weiterbetrieb nicht — verlangt wird eine dokumentierte Prüfung der sicheren Betreibbarkeit. Im Audit standhaltend ist der Weiterbetrieb, wenn vier Bedingungen erfüllt sind:

- **Kennzeichnung im Inventar:** Das System ist als EOSL markiert, mit Datum des Hersteller-Support-Endes.
- **Schwachstellen-Status:** Es ist geprüft, ob offene, ausgenutzte Schwachstellen (KEV) für Modell und Firmware-Stand bekannt sind.
- **Kompensierende Maßnahmen:** Netzsegmentierung, gehärtete Management-Zugänge, erhöhtes Monitoring, ggf. Abschaltung nicht benötigter Dienste — dokumentiert und umgesetzt.
- **Risiko-Akzeptanz der Leitung:** Der Weiterbetrieb ist als bewusste Entscheidung mit Wiedervorlage dokumentiert und von der Geschäftsleitung gebilligt (§ 38 BSIG).

Herstellerunabhängige Wartung liefert den operativen Teil, ersetzt aber nicht die Sicherheitsbewertung. Diese Trennung sollte im Vertrag klar sein: Der Wartungspartner sichert Verfügbarkeit zu und liefert Firmware-Stände und Advisories zu; die Entscheidung über den Weiterbetrieb trifft der Betreiber. Vertiefend behandelt das Whitepaper Nr. 02 „EOSL-Strategie" den Bewertungsprozess mit einem Sechs-Dimensionen-Risiko-Score.

Der Cyber Resilience Act als Ausblick

Die Verordnung (EU) 2024/2847 (Cyber Resilience Act) verpflichtet Hersteller vernetzter Produkte künftig zu Sicherheitsupdates über einen Unterstützungszeitraum von mindestens fünf Jahren sowie zur Meldung aktiv ausgenutzter Schwachstellen; die Meldepflichten gelten ab September 2026, die vollständige Anwendung ab Dezember 2027 [10]. Für Neubeschaffungen wird der Support-Zeitraum damit zum vertraglich fassbaren Lifecycle-Kriterium.

> **KERNAUSSAGE**
>
> Firmware ist Teil des Schwachstellen-Managements, und Support-Ende ist ein Prüffeld: Weiterbetrieb ist zulässig, wenn Inventar, Schwachstellen-Status, kompensierende Maßnahmen und Risiko-Akzeptanz der Leitung dokumentiert sind — nicht, weil das Gerät noch läuft.

KAPITEL 09

Die Meldekaskade 24h / 72h / 1 Monat: was der Wartungspartner liefern muss

Art. 23 NIS2 und § 32 BSIG verpflichten betroffene Einrichtungen, erhebliche Sicherheitsvorfälle in drei Stufen zu melden: eine **Frühwarnung binnen 24 Stunden** nach Kenntnis, eine **Vorfallsmeldung binnen 72 Stunden** mit erster Bewertung von Schwere, Auswirkungen und Kompromittierungsindikatoren sowie einen **Abschlussbericht binnen eines Monats** mit Ursache, Maßnahmen und grenzüberschreitenden Auswirkungen [1][3]. Ein Vorfall ist „erheblich", wenn er schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht oder verursachen kann, oder andere Personen erheblich beeinträchtigt.

Wo Hardware in die Kaskade fällt

Drei Szenarien machen die Hardwarewartung zum Teil des Meldeprozesses. Erstens der *Ausfall mit Dienstbeeinträchtigung*: Ein Storage-Cluster verliert Redundanz und ein wesentlicher Dienst steht — technische Ursache, aber erhebliche Betriebsstörung. Zweitens die *Firmware-Kompromittierung*: Ein Management-Controller zeigt Anzeichen unautorisierten Zugriffs. Drittens der *Vorfall beim Dienstleister*: Der Wartungspartner selbst wird kompromittiert, und seine Remote-Zugänge oder Ersatzteil-Logistik sind betroffen. In allen drei Fällen braucht der Betreiber binnen 24 Stunden Informationen, die nur der Wartungspartner hat.

Was der Vertrag regeln muss

Stufe	Frist	Zulieferung des Wartungspartners
Frühwarnung	24 h	Sofortige Meldung von Hardware-Vorfällen mit Dienstbezug; Erstinformation, ob ein Sicherheitsbezug vermutet wird; benannter Ansprechpartner rund um die Uhr
Vorfallsmeldung	72 h	Technische Einordnung (betroffene Komponenten, Firmware-Stände, Zugriffslogs des Wartungszugangs), Unterstützung bei der Bewertung der Schwere, Sicherung von Beweismitteln
Abschlussbericht	1 Monat	Ursachenanalyse aus Sicht der Hardware, Ersatzteil- und Tausch-Protokoll, umgesetzte Maßnahmen, Lessons Learned

Der Vorfall beim Dienstleister

Besonders prüfungsrelevant ist die dritte Konstellation. Wird der Wartungspartner selbst Ziel eines Angriffs, muss der Betreiber das erfahren — schnell genug, um seine eigene 24-Stunden-Frist zu halten. Eine vertragliche Meldepflicht des Dienstleisters bei eigenen Sicherheitsvorfällen mit möglichem Kundenbezug ist deshalb unter NIS2 kein Nice-to-have, sondern die Voraussetzung dafür, dass die eigene Meldekette überhaupt funktioniert. ISO 27001 Control 5.20 und DORA Art. 30 Abs. 2 nennen genau diese Klausel [8][9].

Der BSI-Baustein DER.2.1

DER.2.1 „Behandlung von Sicherheitsvorfällen" verlangt definierte Meldewege, Verantwortlichkeiten, eine Eskalationsstrategie und die Einbindung externer Stellen [5]. Übertragen auf die Wartung: Der Service-Desk des Partners muss in der Eskalationsmatrix des Betreibers stehen — mit Namen, Nummer und Vertretungsregel. Ein Prüfer, der die Matrix sieht und dort keinen Hardware-Partner findet, wird nachfragen, wie ein Storage-Ausfall um drei Uhr morgens in die 24-Stunden-Frist passt.

> **KERNAUSSAGE**
> Die Meldefristen sind die des Betreibers, aber die Fakten liegen oft beim Wartungspartner. Ohne vertragliche Mitwirkungs- und Meldepflicht des Dienstleisters ist die 24-Stunden-Frist im Hardware-Fall nicht zu halten.

KAPITEL 10

Datenträger, Ersatzteile, Zugriff: die physischen Kontrollen

NIS2 wird als Cyber-Richtlinie gelesen, doch ein erheblicher Teil der Prüfpunkte im Hardware-Betrieb ist physisch: Was passiert mit einer getauschten Festplatte? Woher kommt der Ersatz-Controller? Wer war wann im Serverraum? Drei Kontrollbereiche stehen im Fokus.

1. Datenträger: Löschen und Vernichten

Jeder Festplatten- oder SSD-Tausch bewegt einen Datenträger mit potenziell vertraulichen Daten aus der kontrollierten Umgebung. Der BSI-Baustein CON.6 „Löschen und Vernichten" verlangt ein Löschkonzept mit Verfahren je Datenträgertyp und Schutzbedarf sowie den Nachweis der Durchführung [5]. ISO 27001 Control 7.14 fordert, dass Geräte mit Speichermedien vor Entsorgung oder Wiederverwendung geprüft und Daten sicher entfernt werden; Control 7.10 regelt den Umgang mit Speichermedien über den gesamten Lebenszyklus [8]. Als technischer Maßstab hat sich NIST SP 800-88 „Guidelines for Media Sanitization" etabliert, das die Stufen Clear, Purge und Destroy definiert [12].

Für den Wartungsvertrag folgen daraus drei Regeln: Defekte Datenträger verbleiben beim Kunden oder werden vor Ort vernichtet; jeder Tausch wird mit Seriennummer protokolliert; für jeden Datenträger, der die Umgebung verlässt, existiert ein Lösch- oder Vernichtungszertifikat. Prüfer fragen gezielt nach dem letzten Tausch und dem zugehörigen Zertifikat — Prüffeld 9 der Matrix.

2. Ersatzteile: Herkunft und Chain-of-Custody

Art. 21 Abs. 2 lit. d und ISO 5.21 verlangen Transparenz über die IKT-Lieferkette — dazu gehört die Herkunft von Ersatzteilen [1][8]. Gefälschte oder manipulierte Komponenten sind ein bekanntes Risiko in Sekundärmärkten; Hersteller warnen regelmäßig vor nicht autorisierten Teilen [17]. Der Nachweis, den Prüfer erwarten, ist eine lückenlose Chain-of-Custody: Bezugsquelle, Eingangsprüfung, Lagerort, Seriennummer, Einbaudatum, Techniker. Ein Wartungspartner mit eigenen Depots und dokumentierter Eingangsprüfung kann das liefern; ein Vertrag sollte es verlangen.

3. Zugriff Externer: Zutritt und Remote

Lit. i verlangt Zugriffskontrolle und Anlagenmanagement, lit. j Multi-Faktor-Authentifizierung [1]. Für Wartungstechniker bedeutet das zweierlei. **Physisch:** Zutritt zum Serverraum nur angemeldet, begleitet oder mit personalisiertem Ausweis, protokolliert (BSI INF.2 „Rechenzentrum sowie Serverraum") [5]. **Remote:** Wartungszugänge nur über MFA-gesicherte, personalisierte Konten, zeitlich begrenzt, protokolliert, ohne dauerhafte Standing-Access-Verbindungen; Prüfer sehen sich Zutrittsprotokolle und Zugriffslogs stichprobenartig an und vergleichen sie mit den Wartungstickets: Jeder Zugriff braucht ein Ticket, jedes Ticket einen Zugriff.

Personalsicherheit

Lit. i nennt ausdrücklich die Sicherheit des Personals. Für Fremdtechniker heißt das: Vertraulichkeitsverpflichtung, dokumentierte Qualifikation (Hersteller-Zertifizierungen), bei Bedarf Zuverlässigkeitsüberprüfung — und eine namentliche Liste der Personen, die Zugriff erhalten dürfen.

> **KERNAUSSAGE**
>
> Drei physische Fragen entscheiden Prüffelder 9 und 10: Wo ist die getauschte Platte und wer hat sie gelöscht? Woher stammt das Ersatzteil? Wer war mit welchem Ticket wann am System? Jede braucht einen Beleg — nicht eine Zusicherung.

KAPITEL 11

Dokumentierte Verantwortlichkeiten: § 38 BSIG und die Geschäftsleitung

Die größte Veränderung, die NIS2 in den Unternehmensalltag trägt, ist nicht technisch. Art. 20 der Richtlinie und § 38 BSIG verpflichten die **Geschäftsleitung** persönlich, die Risikomanagement-Maßnahmen zu billigen, ihre Umsetzung zu überwachen und sich regelmäßig schulen zu lassen [1][3]. Wer diese Pflichten verletzt, haftet der Einrichtung gegenüber nach den Regeln des Gesellschaftsrechts. Cybersicherheit — und damit der sichere Betrieb der Hardware — ist damit Leitungsaufgabe, nicht mehr delegierbare IT-Aufgabe.

Was „billigen und überwachen" für die Hardwarewartung heißt

Die Geschäftsleitung muss nicht jeden Wartungsvertrag lesen. Sie muss aber nachweisen können, dass sie die Grundsatzentscheidungen kennt und getragen hat: Welche Systeme sind kritisch, welche Verfügbarkeit ist für sie zugesichert, welcher Partner wartet sie, welche Systeme laufen jenseits des Hersteller-Supports und mit welcher Begründung. Im Audit wird diese Frage typischerweise über Protokolle geprüft: Gibt es einen Beschluss oder eine Kenntnisnahme der Leitung zur Risikoanalyse, zur Lieferantenstrategie, zur EOSL-Liste?

Die Verantwortungsmatrix

Prüfer erwarten, dass Verantwortlichkeiten nicht nur intern, sondern auch gegenüber dem Wartungspartner eindeutig sind. Eine einfache Zuordnung nach dem RACI-Muster — wer entscheidet, wer führt aus, wer wird konsultiert, wer informiert — schafft die Klarheit, die Art. 21 Abs. 2 lit. a und lit. i verlangen:

Aufgabe	Betreiber (Leitung)	Betreiber (IT / CISO)	Wartungspartner
Kritikalität und Schutzbedarf festlegen	Billigt	Erarbeitet	Wird informiert
SLA-Stufen je System zuordnen	Billigt	Entscheidet	Setzt um, berichtet
Firmware-Advisories bewerten	—	Entscheidet	Liefert zu, spielt ein
Weiterbetrieb von EOSL-Systemen	Billigt Risiko-Akzeptanz	Bewertet, beantragt	Sichert Betrieb, liefert Fakten
Sicherheitsvorfall Hardware melden (24h/72h)	Verantwortet Meldung	Meldet an BSI	Meldet an Betreiber, liefert Analyse
Datenträger löschen / vernichten	—	Kontrolliert Nachweise	Führt aus, zertifiziert
Lieferantenbewertung jährlich	Nimmt zur Kenntnis	Führt durch	Liefert Nachweise (Zertifikate, Sub-Liste)

Dokumentation als Entlastung

§ 38 BSIG ist für die Leitung zunächst ein Haftungsrisiko. Richtig gelesen ist die Vorschrift aber auch eine Entlastung: Wer Risikoanalyse, Lieferantenwahl und EOSL-Entscheidungen nachweislich gebilligt und überwacht hat, hat seine Pflicht erfüllt — auch wenn ein Vorfall eintritt. Die Akte schützt. Umgekehrt ist ein Vorfall an einem nicht inventarisierten, nicht bewerteten System ohne dokumentierten Beschluss genau die Konstellation, in der die persönliche Verantwortung greift.

Schulungspflicht

Die Leitung muss an Schulungen teilnehmen, die ausreichen, um Risiken und Managementpraktiken zu bewerten [1][3]. Für den Hardware-Betrieb bietet sich ein jährliches Briefing an, das die EOSL-Liste, die SLA-Performance und den Status der Lieferantenbewertung zusammenfasst — kurz, dokumentiert, mit Unterschrift. Es erfüllt die Schulungspflicht und erzeugt zugleich den Nachweis der Kenntnisnahme.

> **KERNAUSSAGE**
>
> § 38 BSIG hebt den Wartungsvertrag auf die Leitungsebene: Kritikalität, Lieferant und EOSL-Weiterbetrieb brauchen einen dokumentierten Beschluss. Die Akte ist der Nachweis — für den Prüfer und für die Leitung selbst.

KAPITEL 12

Der Wartungsvertrag im Audit: 12-Punkte-Klausel-Checkliste

Diese Checkliste fasst die Anforderungen der Kapitel 4 bis 11 in zwölf prüfbare Vertragspunkte. Sie ist als Arbeitsvorlage gedacht: für die Prüfung eines bestehenden Wartungsvertrags ebenso wie für die Ausschreibung eines neuen. Jeder Punkt nennt die Referenz, auf die sich ein Prüfer stützen würde [1][3][5][8][9].

- ☐ **1 · Leistungsgegenstand mit Asset-Bezug.** Der Vertrag listet die gewarteten Systeme (Modell, Seriennummer, Standort) und ordnet jedem eine SLA-Stufe zu.
  Art. 21 (2) i · ISO 5.9

- ☐ **2 · Reaktions- und Wiederherstellzeiten.** Zeiten je Stufe fixiert; Wiederherstellung als Ziel benannt; Ersatzteil-Vorhaltung und Depot-Standorte beschrieben.
  Art. 21 (2) c · ISO 5.30

- ☐ **3 · SLA-Reporting und Review.** Monatliche Performance-Reports, jährliches Service-Review mit Maßnahmen-Protokoll.
  Art. 21 (2) f · ISO 5.22

- ☐ **4 · Sicherheitsanhang.** Verbindliche Sicherheitsanforderungen an den Dienstleister (Zertifizierung, Personal, Zugriff, Datenträger) als Vertragsbestandteil.
  Art. 21 (2) d · ISO 5.20 · BSI OPS.2.3

- ☐ **5 · Sub-Unternehmer-Transparenz.** Liste der Sub-Unternehmer mit Rolle und Standort; Meldepflicht bei Änderung; Zustimmungsvorbehalt für sicherheitsrelevante Sub-Vergaben.
  ISO 5.21 · DORA Art. 30 (2)

- ☐ **6 · Firmware und Advisories.** Zulieferung von Hersteller-Advisories und Firmware-Ständen; Einspielen nach Freigabe des Betreibers; Dokumentation je System.
  Art. 21 (2) e · BSI OPS.1.1.3 · ISO 8.8

- ☐ **7 · Umgang mit Support-Ende.** Kennzeichnung von EOSL-Systemen; Zulieferung von Fakten für die Risiko-Akzeptanz; klare Trennung: Betriebssicherung durch Partner, Weiterbetriebs-Entscheidung durch Betreiber.
  BSI OPS.1.1.3 · § 38 BSIG

- ☐ **8 · Melde-Mitwirkung.** Sofortmeldung von Hardware-Vorfällen mit Dienstbezug; Meldung eigener Sicherheitsvorfälle des Dienstleisters; Zulieferung für 24h/72h/1-Monat-Kaskade; Eskalationskontakt 24/7.
  Art. 23 · § 32 BSIG · BSI DER.2.1

- ☐ **9 · Datenträger.** Verbleib defekter Datenträger beim Kunden oder Vor-Ort-Vernichtung; Seriennummern-Protokoll; Lösch-/Vernichtungszertifikat je Datenträger.
  BSI CON.6 · ISO 7.10, 7.14 · NIST SP 800-88

- ☐ **10 · Ersatzteil-Herkunft.** Bezugsquellen, Eingangsprüfung und Chain-of-Custody dokumentiert; keine nicht autorisierten Teile.
  Art. 21 (2) d · ISO 5.21

- ☐ **11 · Zugriff und Personal.** Namentliche Technikerliste, Vertraulichkeit, Qualifikationsnachweis; Zutritt begleitet und protokolliert; Remote nur mit MFA, personalisiert, zeitlich begrenzt, protokolliert.
  Art. 21 (2) i, j · BSI ORP.4, INF.2

☐ **12 · Audit-Rechte und Exit.** Prüfrecht des Betreibers und seiner Aufsicht; Mitwirkung bei Audits; geregelte Beendigung mit Rückgabe von Zugängen, Dokumentation und Übergabe.

ISO 5.22 · BSI OPS.2.3 · DORA Art. 30 (2)

Anwendung

Für einen Bestandsvertrag genügt oft ein Sicherheitsanhang als Nachtrag, der die Punkte 4 bis 12 ergänzt — die kaufmännischen Punkte 1 bis 3 sind meist vorhanden. Für eine Neuvergabe sollte die Checkliste Teil der Anforderungsspezifikation sein; Anbieter, die einzelne Punkte nicht erfüllen können, scheiden aus der Lieferantenbewertung aus, bevor der Preis verglichen wird.

> **KERNAUSSAGE**
>
> Zwölf Klauseln, drei davon kaufmännisch, neun sicherheitsbezogen. Ein Wartungsvertrag, der alle zwölf abdeckt, ist im NIS2-Audit kein Risiko, sondern ein Nachweis — für Art. 21, § 32 und § 38 zugleich.

KAPITEL 13

Fazit

NIS2 verändert, was ein Wartungsvertrag ist. Aus einem kaufmännischen Dokument über Reaktionszeiten wird ein Nachweisdokument für vier der zehn Pflicht-Maßnahmen aus Art. 21: Business Continuity, Lieferkette, Wartung und Schwachstellen, Zugriff und Anlagen. Der Auditor liest ihn entsprechend — und stellt Fragen, die ein klassischer SLA nicht beantwortet.

Die gute Nachricht: Keine dieser Fragen erfordert neue Hardware oder grundlegend andere Prozesse. Sie erfordern Dokumentation. Ein vollständiges Inventar mit Support-Status, eine Lieferantenbewertung, die bis zu Sub-Unternehmern und Ersatzteil-Herkunft reicht, ein Firmware-Prozess mit Nachweis, eine Melde-Mitwirkung des Partners, Zertifikate für jeden getauschten Datenträger und ein Beschluss der Geschäftsleitung zu den kritischen Entscheidungen — das ist der Umfang. Die Prüf-Matrix in Kapitel 5 und die Klausel-Checkliste in Kapitel 12 machen ihn abarbeitbar.

Die weniger bequeme Nachricht: Der Prüfer kommt selten mit Termin. Er kommt als Großkunde mit Lieferanten-Fragebogen, als Versicherer, als Wirtschaftsprüfer, der § 38 BSIG in seine Prüfung einbezieht — oder nach einem Vorfall, wenn die 24-Stunden-Frist bereits läuft. Wer die Nachweise dann erst zusammensucht, verliert nicht nur Zeit, sondern die Beweislast.

Herstellerunabhängige Wartung ist in dieser Lage kein Risiko, sondern ein Hebel: Sie macht den Weiterbetrieb bewährter Systeme möglich, liefert die Betriebs- und Ersatzteil-Fakten, die der Betreiber für seine Risiko-Akzeptanz braucht — und ein Partner, der die zwölf Klauseln aus Kapitel 12 vertraglich trägt, wird im Audit vom Prüfgegenstand zum Beleg.

> **IN EINEM SATZ**
>
> NIS2 fragt nicht, ob Ihre Hardware gewartet wird — sondern ob Sie es beweisen können.

KAPITEL 14

Über TechCare & Quellen

Über TechCare Solutions

TechCare Solutions GmbH mit Sitz in Hahnstätten wartet Server-, Storage- und Netzwerk-Hardware aller großen Enterprise-Hersteller herstellerunabhängig — auch über das End of Service Life hinaus. Unsere Wartungsverträge sind auf die Anforderungen von NIS2, DORA, KRITIS, BAIT, TISAX und ISO 27001 ausgelegt: SLA-Performance-Reports, dokumentierte Incident-Response innerhalb 24 Stunden, Sub-Outsourcing-Transparenz, Chain-of-Custody für Ersatzteile und Lösch-Zertifikate für jeden getauschten Datenträger. Ein Compliance-Officer begleitet Audits als Eskalationsinstanz.

Kontakt: techcaresolutions.de · 24/7 Service-Desk (DE/EN) · Hahnstätten

Methodik & Transparenz

Alle konkreten Zahlen dieses Whitepapers stammen aus den unten genannten, öffentlich zugänglichen Quellen (EU-Rechtsakte, deutsches Gesetz, BSI-Veröffentlichungen, ISO-Norm, Behörden- und Branchenstudien). Wo Quellen Spannen oder Schätzungen enthalten, ist dies sprachlich gekennzeichnet („rund", „etwa", „nach Schätzung"). Die Prüf-Matrix (Kapitel 5), die Verantwortungsmatrix (Kapitel 11) und die Klausel-Checkliste (Kapitel 12) sind eigene Arbeitshilfen von TechCare Research, abgeleitet aus den zitierten Regelwerken; sie stellen keine Rechtsberatung dar. Maßgeblich ist im Einzelfall der Gesetzestext und die Einschätzung der zuständigen Aufsicht.

Quellen

[1] Richtlinie (EU) 2022/2555 (NIS2), insb. Art. 6, 20, 21, 22, 23. eur-lex.europa.eu/eli/dir/2022/2555

[2] Europäische Kommission — NIS2 Directive (Policy-Überblick). digital-strategy.ec.europa.eu/en/policies/nis2-directive

[3] NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) / BSI-Gesetz (BSIG), insb. §§ 28, 30–33, 38, 65. gesetze-im-internet.de/bsig

[4] BSI — NIS-2: Informationen für Unternehmen, Betroffenheitsprüfung. bsi.bund.de/nis-2

[5] BSI — IT-Grundschutz-Kompendium, Edition 2023: OPS.1.1.3, OPS.2.3, CON.6, DER.2.1, ORP.4, INF.2. bsi.bund.de/grundschutz

[6] BSI — Die Lage der IT-Sicherheit in Deutschland 2024. bsi.bund.de/lagebericht

[7] Durchführungsverordnung (EU) 2024/2690 der Kommission (technische Anforderungen, Anhang). eur-lex.europa.eu

[8] ISO/IEC 27001:2022, Anhang A — Controls 5.9, 5.19–5.22, 5.30, 7.10, 7.13, 7.14, 8.8. iso.org

[9] Verordnung (EU) 2022/2554 (DORA), Art. 28–30 IKT-Drittparteienrisiko. eur-lex.europa.eu/eli/reg/2022/2554

[10] Verordnung (EU) 2024/2847 (Cyber Resilience Act). eur-lex.europa.eu/eli/reg/2024/2847

[11] CISA — Known Exploited Vulnerabilities (KEV) Catalog. cisa.gov/known-exploited-vulnerabilities-catalog

[12] NIST SP 800-88 Rev. 1 — Guidelines for Media Sanitization. csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

[13] Uptime Institute — Annual Outage Analysis 2024. uptimeinstitute.com

[14] ENISA — Threat Landscape 2024. enisa.europa.eu/publications/enisa-threat-landscape-2024

[15] Bitkom — Wirtschaftsschutz 2024 (Schäden durch Cyberangriffe). bitkom.org

[16] OpenKRITIS — NIS2-Umsetzung in Deutschland, Betroffenheits-Schätzungen. openkritis.de

[17] Hersteller-Sicherheitshinweise: Cisco PSIRT, HPE Security Bulletins, Dell Security Advisories. cisco.com · support.hpe.com · dell.com/support