Dallmeier

NIS-2

NIS2-ANFORDERUNGEN & LIEFERKETTENSICHERHEIT

Sicherheit für Ihre Lieferkette mit cybersicherer Videosicherheitstechnik

WHITEPAPER

Version 1.0, Januar 2026

MADE IN GERMANY

See more.

INHALT

1 EINFÜHRUNG

Die Jahre 2025 und 2026 stehen für wesentliche und wichtige Einrichtungen ganz im Zeichen verstärkter Regulierungen bezüglich der Informations- und Cybersicherheit und auch der physischen Sicherheit, getrieben durch eine stetig wachsende Anzahl an Cyberattacken, physischen Sicherheitsbedrohungen und eine geopolitisch angespannte und volatile Sicherheitslage.

Da der Markt allein das Thema IT-Sicherheit augenscheinlich nur unzureichend selbst regelt (eine Art von „Marktversagen"), werden Märkte und vor allem kritische, essenzielle und wichtige Unternehmen und Einrichtungen zunehmend reguliert. Diese Unternehmen und Einrichtungen sind von hoher Bedeutung für das Funktionieren des Gemeinwesens, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Eine Vielzahl von Verordnungen, Richtlinien und Gesetzesinitiativen auf EU-Ebene und international zielt darauf ab, die Cyberresilienz und auch die physische Resilienz dieser Unternehmen und Einrichtungen zu erhöhen.

Was bedeutet NIS-2 für Hersteller von Videoüberwachungssystemen?
Videoüberwachungssysteme sind heute hochvernetzt. Sie sind häufig Teil komplexer IT- und OT-Umgebungen. Damit gelten sie als sicherheitsrelevant und potenzielles Einfallstor für Cyberangriffe – was sie direkt oder indirekt in den Fokus der NIS2-Vorgaben rückt. Die Hersteller von Videoüberwachungslösungen tragen also Verantwortung für die Cybersicherheit ihrer Produkte – insbesondere im Einsatz bei NIS-2-Einrichtungen und Betreibern kritischer Anlagen und unter Berücksichtigung der neuen europäischen NIS-2-Richtlinie.

Die EU hat mit der NIS-2-Richtlinie die Sicherheitsanforderungen an NIS-2-Einrichtungen und Betreiber kritischer Anlagen verschärft. In vielen Fällen schließt dies auch Hersteller und Vorlieferanten mit ein, über die gesetzliche Pflicht zur „Sicherheit in der Lieferkette".

Auch wenn die NIS2-Richtlinie nicht direkt Hersteller adressiert, zwingt sie diese durch Lieferkettendruck und Sicherheitsanforderungen der betroffenen Einrichtungen dazu, ein hohes Maß an Cybersecurity-Reife zu erreichen. Wer als Hersteller oder Vorlieferant frühzeitig Sicherheitsprozesse, Transparenz und Kooperationsstrukturen etabliert, wird nicht nur bevorzugter Partner und Trusted Advisor, sondern schützt sich auch vor Reputationsverlust und Haftungsrisiken. Dieses Whitepaper behandelt explizit das Thema Cybersicherheit und Cyberresilienz im Kontext der EU NIS-2-Richtlinie auf europäischer Ebene (nationale Umsetzungen werden nur beispielhaft erwähnt).

Ein weiteres Whitepaper (still to come) wird sich explizit mit dem Thema „Physische Sicherheit und Physische Resilienz" im Kontext der EU RCE-Richtlinie beschäftigen.

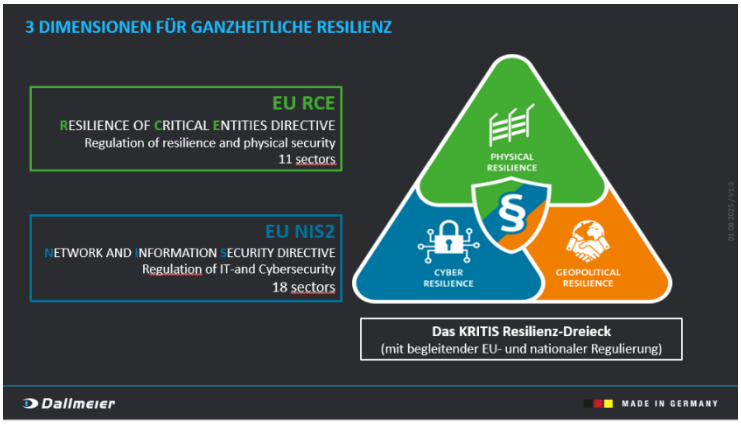


Abb.: Drei Dimensionen von Resilienz, visualisiert in einem Resilienz-Dreieck, mit den begleitenden europäischen Regulierungen

2 NIS-2 RICHTLINIE DER EUROPÄISCHEN UNION

2.1 Was ist die NIS-2 Richtlinie?

Die NIS-2-Richtlinie (Netz- und Informationssicherheit Richtlinie) ist eine EU-weite Gesetzgebung zur Verbesserung der Cybersicherheit, die im Januar 2023 in Kraft getreten ist. Sie ersetzt die vorherige NIS-1 Richtlinie und zielt darauf ab, das Sicherheitsniveau von Netz- und Informationssystemen in der EU zu erhöhen und zu harmonisieren. NIS-2 erweitert den Kreis der bis dato betroffenen sogenannten Betreiber kritischer Anlagen (KRITIS-Betreiber) um Einrichtungen (NIS2-Einrichtungen | „essential and important entities“) und legt strengere Anforderungen an das Cyber-Risikomanagement, das Business Continuity und Schwachstellen-Management und an die Nachweis-, Melde- und Bußgeldpflichten fest. Die NIS-2 erweitert nicht nur den Betroffenheitskreis und die Anforderungen, sondern erweitert diese auch über die Unternehmensgrenzen hinweg auf Hersteller, Vorlieferanten und Dienstleister im Rahmen der Pflicht zur „Sicherheit in der Lieferkette“. Die Folgen der Nichteinhaltung von gesetzlichen Vorschriften durch NIS2-Einrichtungen können hohe Geldstrafen für die Einrichtung sein und rechtliche Konsequenzen für die NIS2-Geschäftsleitung in Form einer persönlichen Haftung sein.

- NIS-2 Originaldokument und Quellen
  - NIS-2 Network and Information Security Directive
  - Amtliches Dokument RICHTLINIE (EU) 2022/2555:
    „Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in der Union“
  - PDF: Deutsche Version | Englische Version | Sprachauswahlseite

- Umsetzung der NIS-2 Richtlinie in den 27 EU-Mitgliedsstaaten
  Die EU-Mitgliedstaaten müssen die NIS2-Richtlinie in nationales Recht („Gesetze“) umsetzen. Die ursprüngliche Deadline 18. Oktober 2024 haben die meisten EU-Länder nicht eingehalten. Kroatien z.B. hat die NIS-2 vorbildlich und innerhalb der Deadline umgesetzt. Die noch offenen Umsetzungen werden nun in den Jahren 2025/2026 erwartet.

- Online-Übersicht zum Stand der nationalen NIS2-Umsetzungen:
  NIS2 Directive Transposition Tracker, von ECSO:
  https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

- Beispiel Deutschland (Stand Dezember 2025):
  In Deutschland trat das NIS-2-Umsetzungsgesetz am 06.12.2025 in Kraft.
  Der Titel des Gesetzes: „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“.

  Das Gesetz im Bundesgesetzblatt: https://www.recht.bund.de/bgbl/1/2025/301/VO.html

  Das Gesetz im Bundesgesetzblatt als PDF:
  https://www.recht.bund.de/bgbl/1/2025/301/regelungstext.pdf?__blob=publicationFile&v=3

  Als Artikelgesetz ändert dieses Umsetzungsgesetz viele Einzelgesetze, v.a. aber das **BSI-Gesetz**, als wichtigstes Gesetz für die Aufgaben des BSI und die Sicherheit in der Informationstechnik von Einrichtungen. Statt bisher etwa 4.500 Einrichtungen (KRITIS-Betreiber, UBI, weitere) werden künftig rund 29.500 Organisationen unter die regulative Aufsicht des BSI (Bundesamt für Sicherheit in der Informationstechnik) gestellt.

2.2 Wer ist von NIS-2 betroffen?

DIREKT:
NIS-2 betrifft direkt und primär alle wesentlichen und wichtigen Einrichtungen, die wesentliche oder wichtige Leistungen für die europäische Wirtschaft und Zivilgesellschaft erbringen.

INDIREKT:
NIS-2 betrifft indirekt und sekundär auch Hersteller, Lieferanten, Zulieferer und Dienstleister, da betroffene Einrichtungen technische und organisatorische Sicherheitsmaßnahmen entlang ihrer Supply Chain nachweisen müssen (Drittanbieter-Risikomanagement). Über die explizite Anforderung an NIS2-Einrichtungen „Sicherheit in der Lieferkette“ unterliegen Hersteller oder Vorlieferanten möglicherweise vertraglichen Cybersicherheitsanforderungen seitens ihrer NIS-2-Kunden. Wie ein NIS2-konformes Herstellerprofil für eine sichere Lieferkette auszusehen hat, erläutern wir in Kap. 4.

3 DIREKTE ANFORDERUNGEN VON NIS-2 AN EINRICHTUNGEN

3.1 Definition und Klassifizierung von wesentlichen und wichtigen Einrichtungen

Die NIS-2-Richtlinie unterscheidet zwischen:

- „Wesentlichen Einrichtungen“ und
- „Wichtigen Einrichtungen“

Die NIS-2-Kriterien, welche Einrichtungen als „wesentliche“ oder „wichtige“ definieren und klassifizieren, sind:

- Sektoren (Zugehörigkeit)
    - siehe Anhang I und Anhang II von NIS-2
- Mitarbeiteranzahl und Umsatz/Bilanzsumme
    - kaufmännische Schwellenwerte | Size Cap
    - mittlere und große Einrichtungen

Besonderheit:
Betreiber kritischer Anlagen (die klassischen KRITIS-Betreiber nach technischen Schwellenwerten) gehören automatisch zu den wesentlichen Einrichtungen.

Anforderungen kurz gesagt:
Die wesentlichen Einrichtungen, dabei insbesondere die Betreiber kritischer Anlagen, unterliegen strengeren Anforderungen und einer stärkeren behördlichen Aufsicht als die wichtigen Einrichtungen.

Sonderfälle und Ausnahmen (u.a. IKT und öffentliche Verwaltung) sind nachfolgend der Übersichtlichkeit halber nicht aufgeführt.

Sektoren mit hoher Kritikalität (Anhang 1 der NIS-2)

- **Energie:** Strom, Fernwärme, Erdöl, Erdgas, Wasserstoff
- **Verkehr:** Luft-, Schienen-, Schiffs- und Straßenverkehr
- **Bankwesen:** Kreditinstitute
- **Finanzmarktinfrastrukturen:** Börsen, Handelsplätze
- **Gesundheitswesen:** Gesundheitsdienstleister, Pharmazeutika, Medizinprodukte
- **Trinkwasser:** Wasserversorgung
- **Abwasser:** Abwasserentsorgung
- **Digitale Infrastruktur:** Internet-Knoten, DNS-Dienste, Cloud-Anbieter, Rechenzentren, CDNs, Vertrauensdienste, Kommunikationsnetze
- **IKT-Dienstleistungsmanagement:** Managed Service Provider, Managed Security Service Provider (B2B)
- **Öffentliche Verwaltung:** Zentral- und Regionalregierungen
- **Weltraum:** Bodeninfrastruktur

Sonstige kritische Sektoren (Anhang 2 der NIS-2)

- **Post- und Kurierdienste:** Postdienste
- **Abfallwirtschaft:** Entsorgung von Abfällen
- **Chemie:** Chemieindustrie
- **Lebensmittel:** Lebensmittelproduktion und -handel
- **Verarbeitendes Gewerbe:** Maschinenbau, Fahrzeugbau, elektrische und optische Ausrüstung
- **Digitale Dienste:** Online-Marktplätze, Suchmaschinen, soziale Netzwerke
- **Forschungseinrichtungen:** Einrichtungen für Forschung und Entwicklung

Tabellarische Klassifizierung „wesentliche Einrichtungen“ und „wichtige Einrichtungen“

Einrichtungen nach NIS2	
Sektoren hohe Kritikalität 1	**Sonstige kritische Sektoren** 2
= Anhang 1 (NIS2)	= Anhang 2 (NIS2)
• Energie • Verkehr • Bankwesen • Finanzmarkt-infrastrukturen • Gesundheitswesen • Trinkwasser • Abwasser • Digitale Infrastruktur • IKT-Dienstleistungs-management • Öffentliche Verwaltung • Weltraum	• Post- und Kurierdienste • Abfallwirtschaft • Chemie • Lebensmittel • Verarbeitendes Gewerbe • Digitale Dienste • Forschungseinrichtungen

Einrichtung	Sektoren	Größe
Wesentlich	1	Große Einrichtungen
Wichtig	1	Mittlere Einrichtungen
	2	Große Einrichtungen Mittlere Einrichtungen

Größenklassen nach:
- Mitarbeitendeanzahl und
- Umsatz oder Bilanzsumme

Große Einrichtungen:
> 250 Mitarbeitende oder
> 50 Mio. EUR Umsatz und 43 Mio. EUR Bilanzsumme

Mittlere Einrichtungen:
> 50 Mitarbeitende oder
> 10 Mio. EUR Umsatz und 10 Mio. EUR Bilanzsumme

Zusammenfassend und vereinfacht gesagt:

Wesentlichen Einrichtungen:
= Große Einrichtungen aus dem Anhang 1

Wichtige Einrichtungen:
= Große und Mittlere Einrichtungen aus dem Anhang 2 + Mittlere Einrichtungen aus dem Anhang 1

3.2 Anforderungen und Pflichten für wesentliche und wichtige Einrichtungen

Die NIS2-Richtlinie legt für wesentliche und wichtige Einrichtungen eine Reihe verbindlicher Pflichten fest, um die Cybersicherheit in der EU zu stärken.

Diese Pflichten lassen sich in folgende Hauptbereiche gliedern:

2) Identifizierungspflicht und Registrierungspflicht

Einrichtungen müssen Ihre Betroffenheit selbst identifizieren. Kriterien für Einrichtungen sind die Zugehörigkeit zu Sektoren und Mitarbeiteranzahl und Umsatz/Bilanzsumme (siehe Tabelle oben unter 3.1). Besonderheit: Betreiber kritischer Anlagen (die klassischen KRITIS-Betreiber) gehören automatisch zu den wesentlichen Einrichtungen. Als Hilfestellung zur eigenen Betroffenheitsprüfung gibt es zahlreiche sogenannte NIS2-Betroffenheitschecker im Internet, z. B. in Deutschland die NIS-2-Betroffenheitsprüfung des BSI als erste Orientierung. Betroffene Einrichtungen müssen sich bei der zuständigen nationalen Aufsichtsbehörde (in Deutschland z.B. beim BSI) registrieren, damit diese sie klassifizieren und beaufsichtigen kann. Zudem ist eine Kontaktstelle zu benennen.

3) Meldepflicht von Vorfällen

Die NIS2-Richtlinie verpflichtet wesentliche und wichtige Einrichtungen, erhebliche Sicherheitsvorfälle unverzüglich zu melden. Innerhalb von 24 Stunden nach Bekanntwerden muss eine Frühwarnung an die zuständige nationale Behörde erfolgen, gefolgt von einer detaillierten Meldung innerhalb von 72 Stunden. Zusätzlich kann ein Abschlussbericht innerhalb eines Monats verlangt werden, der Ursachen, Auswirkungen und ergriffene Maßnahmen dokumentiert.

4) Kooperation und Informationsaustausch mit Aufsichtsbehörde

Betroffene Einrichtungen müssen die Bereitschaft zur Zusammenarbeit mit der Aufsichtsbehörde aufweisen, etwa bei Untersuchungen oder zur Gefahrenabwehr. Dies umfasst auch die Bereitstellung der benötigten Informationen und des Zugangs zu Systemen für Zwecke der behördlichen Aufsicht.

5) Verantwortung Management - Persönliche Haftung

Umsetzungs-, Überwachungs- und Schulungspflicht | Persönliche Haftung Geschäftsleitung
Cybersecurity wird strategische Chefsache: Die Geschäftsleitung (z. B. Geschäftsführung oder Vorstand) ist direkt verantwortlich für die Einhaltung der NIS2-Pflichten. Sie muss die Sicherheits- und Risikomanagementmaßnahmen umsetzen, die Einhaltung überwachen, geeignete Mittel bereitstellen und für Verstöße persönlich haftbar gemacht werden können. Zudem ist eine Schulungspflicht für Geschäftsleitungen vorgesehen.

6) Nachweis- und Dokumentationspflichten

Alle Sicherheitsmaßnahmen und Prozesse müssen nachvollziehbar dokumentiert und regelmäßig überprüft werden (per Audits). Auf Anforderung müssen diese Nachweise und Dokumentationen den Aufsichtsbehörden vorgelegt werden können.

7) Sanktionen und Durchsetzung

Bei Verstößen drohen Bußgelder, die sich je nach Einstufung (wesentlich oder wichtig) unterscheiden können:
Wesentliche Einrichtungen: bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes.
Wichtige Einrichtungen: bis zu 7 Mio. € oder 1,4 % des Umsatzes.

Cybersicherheits- und Resilienzanforderungen:
Die wichtigsten technisch-organisatorischen Cybersicherheits- und Resilienzanforderungen zum Schluss auf einer gesonderten Seite:

1) Risikomanagement- und Cybersicherheitsmaßnahmen

Einrichtungen müssen geeignete, verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um Risiken für die Sicherheit der Netz- und Informationssysteme zu minimieren. Diese Maßnahmen umfassen unter anderem:

- **Policies:** Risikoanalyse und Sicherheitspolitiken
- **Vorfallsbewältigung:** Vorfallbehandlung und -prävention
- **Business Continuity:** Business Continuity Management, Backup- und Disaster-Recovery-Verfahren
- **Supply Chain:** Sicherheit in der Lieferkette
- **Einkauf:** Sicherheit bei Erwerb, Entwicklung und Wartung der IT-Systeme
- **Cyberhygiene, Schulung:** Cyberhygiene (z. B. Updates), Schulungen und Sensibilisierung
- **Kryptografie:** Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- **Personal, Zugriffe, Assets:** Personalsicherheit, Zugriffskontrolle und Asset Management
- **Authentifizierung:** MFA oder kontinuierliche Authentifizierung
- **Kommunikation:** Sichere Sprach-, Video- und Text-Kommunikation
- **Technologie:** „Stand der Technik“ einsetzen

NIS-2, Artikel 21, Originalwortlaut, Screenshot:

Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Pflichten von NIS-2-Einrichtungen auf einen Blick in Tabellenform:

Pflichten nach NIS2-Richtlinie

Pflichtenbereich	Inhalt / Maßnahmen	Gilt für
1. Risikomanagement & Sicherheit	- Risikoanalyse & Sicherheitsstrategien - Vorfallbehandlung & Notfallplanung - Business Continuity & Disaster Recovery - Zugriffskontrollen & Verschlüsselung - Lieferkettensicherheit - Schulungen und Sensibilisierung	Wesentliche & Wichtige
2. Meldepflichten	- Frühwarnung (innerhalb 24 Std.) - Detaillierte Meldung (innerhalb 72 Std.) - Abschlussbericht (innerhalb 1 Monats)	Wesentliche & Wichtige
3. Registrierungspflicht	- Registrierung bei der nationalen Behörde (z. B. BSI in Deutschland) - Aktualisierung bei Änderungen	Wesentliche & Wichtige
4. Zusammenarbeit & Austausch	- Kooperation mit Behörden - Teilnahme an EU-/nationalen Austauschformaten - Beitrag zur Cybersicherheitslageerfassung	Wesentliche & Wichtige
5. Verantwortung des Managements	- Direkte Rechenschaftspflicht der Unternehmensleitung - Pflicht zur Bereitstellung von Ressourcen - Potenzielle persönliche Haftung	Wesentliche & Wichtige
6. Dokumentationspflichten	- Nachvollziehbare Dokumentation aller Maßnahmen - Nachweispflicht gegenüber Behörden - Regelmäßige Überprüfungen und Audits	Wesentliche & Wichtige
7. Sanktionen bei Verstößen	- Wesentliche Einrichtungen: bis zu 10 Mio. € oder 2 % Umsatz - Wichtige Einrichtungen: bis zu 7 Mio. € oder 1,4 % Umsatz	Je nach Einstufung

4 INDIREKTE ANFORDERUNGEN VON NIS-2 AN HERSTELLER

4.1. NIS2-konformer Hersteller für eine sichere Lieferkette

Die NIS2-Richtlinie richtet sich primär an sogenannte wesentliche und wichtige Einrichtungen, aber indirekt hat sie erhebliche Auswirkungen auf deren Hersteller und Vorlieferanten – insbesondere im Bereich IT, OT, Software, Hardware und Dienstleistungen. Diese Auswirkungen ergeben sich daraus, dass betroffene Einrichtungen gemäß NIS2 umfangreiche Sicherheits- und Risikomanagementpflichten entlang ihrer Lieferkette erfüllen müssen und demnach auch ein Drittanbieter-Risikomanagement implementieren sollten.

Die explizite Anforderung für Einrichtungen nach „Sicherheit in der Lieferkette“ ist kodifiziert in NIS-2, Artikel 21 (2) d).

Merksätze:

- Eine Sicherheitskette ist nur so stark wie ihr schwächstes Glied
- Keine sichere Lieferkette ohne sichere Herstellerprodukte und Herstellerprozesse

Indirekte Auswirkungen von NIS-2 auf Hersteller und Vorlieferanten

1) Erhöhte Nachweis- und Vertragspflichten seitens der Kunden (der betroffenen Einrichtungen):

Kunden fordern Nachweise über Cybersicherheitsmaßnahmen und Zertifizierungen (z.B. Nachweis zertifiziertes ISMS nach ISO 27001)

- Kunden fordern vertragliche Vereinbarungen ein (z. B. in Form von Security SLAs oder Compliance-Nachweisen).

2) Erhöhte Transparenzpflichten:

- Offenlegung von Sicherheitslücken, Support- und Patchstrategien, sowie Produktlebenszyklen.

3) Potenzielle Ausschlussrisiken bei mangelnder Cybersecurity oder geopolitischen Risiken

- Hersteller ohne nachweisbare Sicherheitsprozesse könnten von Lieferketten ausgeschlossen werden
- Hersteller auf internationalen Black-/Ban-Lists könnten von Lieferketten ausgeschlossen werden (z.B. NDAA)
- Hersteller von kritischen Komponenten könnten von Lieferketten ausgeschlossen werden (siehe z.B. „Lex Huawei“ in Deutschland, Artikel 9b aktuelles BSI-Gesetz bzw. Artikel 41 geplantes neues BSI-Gesetz (Entwurf))

4) Reputations- und Haftungsrisiken:

- Auch wenn Hersteller nicht direkt adressiert werden, können sie durch Sicherheitsvorfälle in Einrichtungen haftbar gemacht werden (Produkthaftung, Regress).

Wie Hersteller & Vorlieferanten NIS2-Einrichtungen bei der NIS2-Compliance unterstützen können

1) Technische Funktionen und Maßnahmen

Bereich	Maßnahmen
Security by Design | by Default Privacy by Design | by Default	• IT-/OT-Produkte nach Sicherheitsprinzipien entwickeln • Minimalrechte, Härtung, sichere Standards • kryptographische Standards, Verschlüsselung • Trust Plattform Standards, sichere Authentifizierung • personenbez. Daten schützen / Datenschutz nach DSGVO
Patch- und Vulnerability-Management	• Klare Prozesse für Schwachstellenmanagement • Schnelle Bereitstellung Sicherheitspatches
Sicherer Software-Lebenszyklus	• Integration von Sicherheitsprüfungen (u.a. Penetrationstest) in alle Phasen der Entwicklung • Bereitstellung sicherer Updates
Produktzertifizierungen & Standards	• Orientierung und Zertifizierung nach Standards wie ISO/IEC 27001, Common Criteria • CRA zertifizierte Produkte: Der Cyber Resilience Act der EU verpflichtet Hersteller von Produkten mit digitalen Elementen ab dem Jahre 2026/2027 zu Cybersicherheitsmaßnahmen auf Produktebene (u.a. SBOM)
Transparenz (SBOM)	• Offenlegung der verwendeten Softwarekomponenten (Software Bill of Materials)
Stand der Technik	• Produkte nach dem „Stand der Technik“ liefern

2) Organisatorische Prozesse & Kooperationen

Bereich	Maßnahmen
Lieferketten-Compliance und „Sicherheit in der Lieferkette“	• Selbst verpflichtende Sicherheitsstandards und Audits • Teilnahme an Assessments durch Einrichtungen • ISMS nach ISO 27001 einsetzen und nachweisen • sichere Produkte (Security by Design, SBOM, etc.) • Transparente eigene Produktions-, Liefer- und Herkunftsketten • Regelmäßige Sicherheitsupdates / Patchpolitik
Incident-Response-Management	• Klare Eskalations- und Kommunikationsprozesse bei Vorfällen • Vorhalten von PSIRT/SIRC-Teams • Sicherheits-Advisories
Support- und Wartungsverträge	• Sicherheits- und Lifecycle-Management • Sicherheitsagreements, Sicherheitsleitlinien • Technische Sicherheitsdokumentationen,
Awareness & Schulungen	• Trainings und Sensibilisierung für Sicherheit • Sicherheitsawareness schaffen durch z.B. Advisories, Whitepapers, Best-Practices, Praxisleitfäden, Webinare • Schulungspflicht für Geschäftsleitungen (NIS-2)
Kooperation bei Risikoanalysen	• Unterstützung bei Taktiken, Techniken und Verfahren, Risikoanalysen, Sicherheitsbewertungen
Vertragliche Sicherheitsvereinbarungen	• Lieferverträge mit Sicherheitsanforderungen, z. B. zertifiziertes ISMS nach ISO 27001, NDAA-Konformität • geopolitische Sicherheitsvereinbarungen wie z. B. vertrauenswürdige Herstellerländer und Wertschöpfungsketten, „Made in Germany“ als freiwillig-optionales Sicherheits- und Vertrauenssiegel

4.2 NIS2-konformer Hersteller Dallmeier – unsere technischen Antworten im Detail

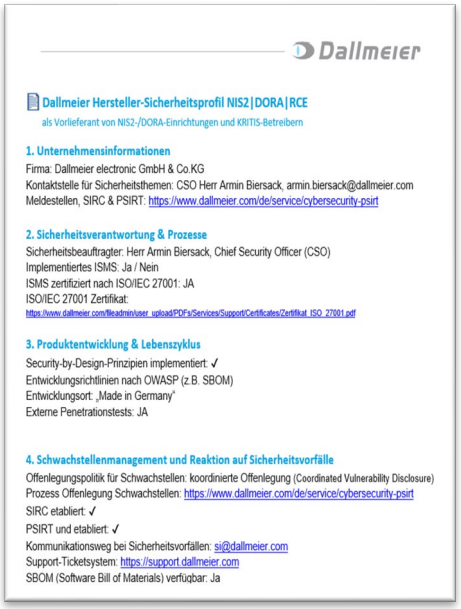
Nachfolgend wird im technischen und organisatorischen Detail beschrieben, wie wir als Hersteller Dallmeier und als Vorlieferant die Anforderungen an Einrichtungen, die von der NIS-2-Richtlinie betroffen sind, erfüllen bzw. wie wir die NIS2-Einrichtung bei der Erfüllung ihrer Anforderungen unterstützen.

Wichtige Anmerkung vorweg: Dallmeier selbst NIS-2-Einrichtung

- Dallmeier ist sowohl indirekt betroffen als Vorlieferant seiner NIS-2-betroffenen Kunden
- Dallmeier ist auch direkt betroffen, ist als Unternehmen eine NIS-2-Einrichtung.
- Sektor „Verarbeitendes Gewerbe“, nach NACE, Abschnitt C, Abt 26
- d.h. wir kennen beide Seiten der Medaille
- alle Anforderungen aus der Lieferanten- als auch aus der NIS2-Betroffenheitssicht
- Bedeutet für unsere Kunden: **Sicherheit hoch 2**.

Zweite Anmerkung:

- Es wird in Kürze ein 3-seitiges PDF-Dokument geben, welches eine Extrem-Kurzfassung dieses Kapitel 4.2. bietet und als schnelles Handout dienen soll
- Titel: Dallmeier Hersteller-Sicherheitsprofil gemäß NIS2|DORA|RCE
- Auch als Art „Bewerbungsdeckblatt Dallmeier für eine Zusammenarbeit mit Ihnen als NIS2-/DORA-Einrichtung und KRITIS-Betreiber“



Dallmeier

Dallmeier Hersteller-Sicherheitsprofil NIS2|DORA|RCE

als Vorlieferant von NIS2-/DORA-Einrichtungen und KRITIS-Betreibern

1. Unternehmensinformationen

Firma: Dallmeier electronic GmbH & Co.KG
Kontaktstelle für Sicherheitsthemen: CSO Herr Armin Biersack, armin.biersack@dallmeier.com
Meldestellen, SIRC & PSIRT: https://www.dallmeier.com/de/service/cybersecurity-psirt

2. Sicherheitsverantwortung & Prozesse

Sicherheitsbeauftragter: Herr Armin Biersack, Chief Security Officer (CSO)
Implementiertes ISMS: Ja / Nein
ISMS zertifiziert nach ISO/IEC 27001: JA
ISO/IEC 27001 Zertifikat:
https://www.dallmeier.com/fileadmin/user_upload/PDFs/Services/Support/Certificates/Zertifikat_ISO_27001.pdf

3. Produktentwicklung & Lebenszyklus

Security-by-Design-Prinzipien implementiert: ✓
Entwicklungsrichtlinien nach OWASP (z.B. SBOM)
Entwicklungsort: „Made in Germany“
Externe Penetrationstests: JA

4. Schwachstellenmanagement und Reaktion auf Sicherheitsvorfälle

Offenlegungspolitik für Schwachstellen: koordinierte Offenlegung (Coordinated Vulnerability Disclosure)
Prozess Offenlegung Schwachstellen: https://www.dallmeier.com/de/service/cybersecurity-psirt
SIRC etabliert: ✓
PSIRT und etabliert: ✓
Kommunikationsweg bei Sicherheitsvorfällen: si@dallmeier.com
Support-Ticketsystem: https://support.dallmeier.com
SBOM (Software Bill of Materials) verfügbar: Ja

4.2.1 Stand der Technik

Die Anforderung nach „Stand der Technik“ wird in der NIS2-Richtlinie an mehreren Stellen genannt, am deutlichsten in Artikel 21 Absatz 1.

Artikel 21 Absatz 1 lautet sinngemäß:

- Die Mitgliedstaaten stellen sicher, dass die in den Anwendungsbereich fallenden Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um Risiken für die Sicherheit der Netz- und Informationssysteme **unter Berücksichtigung des Standes der Technik** zu bewältigen.

Auch in **Erwägungsgrund 85** wird „Stand der Technik“ erwähnt – hier wird klargestellt, dass sich der Begriff auf aktuelle, allgemein anerkannte und verfügbare Sicherheitsstandards bezieht, die dem wirtschaftlich Vertretbaren entsprechen.

Was NIS2 fordert

- **Maßnahmen orientieren sich am Stand der Technik:**
  Unternehmen müssen ihre Sicherheitsvorkehrungen so ausrichten, dass sie dem aktuellen technischen und organisatorischen Entwicklungsstand entsprechen – nicht an veralteten oder minimalen Standards.

- **Dynamische Anpassung:**
  Sicherheitsmaßnahmen müssen regelmäßig überprüft und bei Bedarf an neue technologische Entwicklungen, Bedrohungen und Schwachstellen angepasst werden.

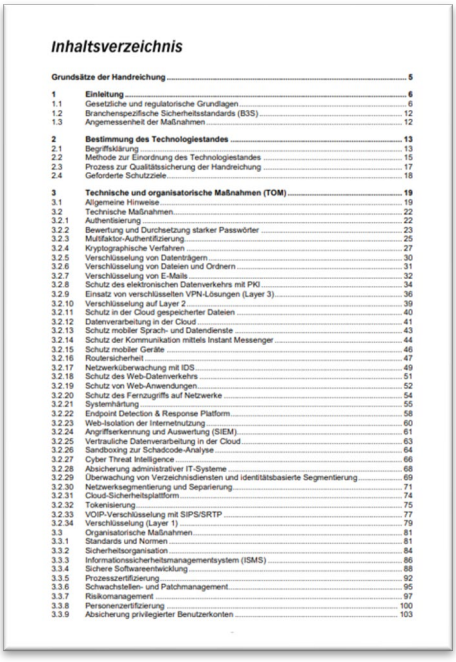
- **Verhältnismäßigkeit:**
  Die Umsetzung muss wirtschaftlich angemessen sein, aber darf nicht hinter dem allgemein anerkannten Sicherheitsniveau zurückbleiben.

- **Dokumentation & Nachweis:**
  Es ist zu erwarten, dass Behörden bei Prüfungen Belege sehen wollen, wie Unternehmen den Stand der Technik ermittelt und umgesetzt haben (z. B. durch Normen wie ISO 27001)

Kernaussage:
„Stand der Technik“ in NIS2 ist keine einmalige Hürde, sondern eine laufende Verpflichtung, Sicherheitsmaßnahmen fortlaufend auf dem neuesten anerkannten Niveau zu halten – sowohl technisch als auch organisatorisch.

„Stand der Technik“ allgemein:
Stand der Technik ist ein gängiger juristischer Begriff. Der Stand der Technik steht nach der im Kalkar-Beschluss entwickelten Drei-Stufen-Theorie zwischen den bewährten anerkannten Regeln der Technik und dem weiter fortgeschrittenen Stand der Wissenschaft. Die technische Entwicklung ist schneller als die Gesetzgebung. Daher hat es sich in vielen Rechtsbereichen seit vielen Jahren bewährt, in Gesetzen auf den „Stand der Technik“ abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen. Was zu einem bestimmten Zeitpunkt „Stand der Technik“ ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise DIN oder ISO oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln oder ableiten (Beschreibung lt. BSI).

„Stand der Technik in der IT-Sicherheit“
Bei der NIS-2 wird vorrangig auf den „Stand der Technik in der IT-Sicherheit“ abgestellt.
Ein sehr gutes Rahmenwerk, eine etablierte und oft referenzierte (z.B. referenziert vom deutschen BSI) Handreichung speziell zum Thema „Stand der Technik in der IT-Sicherheit“, sei an dieser Stelle empfohlen zur eigenen Referenzierung und Beurteilung.


Inhaltsverzeichnis

Grundsätze der Handreichung 5

1 Einleitung 6
1.1 Gesetzliche und regulatorische Grundlagen 6
1.2 Branchenspezifische Sicherheitsstandards (B3S) 12
1.3 Angemessenheit der Maßnahmen 12

2 Bestimmung des Technologiestandes 13
2.1 Begriffsklärung 13
2.2 Methode zur Einordnung des Technologiestandes 15
2.3 Prozess zur Qualitätssicherung der Handreichung 17
2.4 Geforderte Schutzziele 18

3 Technische und organisatorische Maßnahmen (TOM) 19
3.1 Allgemeine Hinweise 19
3.2 Technische Maßnahmen 22
3.2.1 Authentisierung 22
3.2.2 Bewertung und Durchsetzung starker Passwörter 23
3.2.3 Multifaktor-Authentifizierung 25
3.2.4 Kryptographische Verfahren 27
3.2.5 Verschlüsselung von Datenträgern 30
3.2.6 Verschlüsselung von Dateien und Ordnern 31
3.2.7 Verschlüsselung von E-Mails 32
3.2.8 Schutz des elektronischen Datenverkehrs mit PKI 34
3.2.9 Einsatz von verschlüsselten VPN-Lösungen (Layer 3) 36
3.2.10 Verschlüsselung auf Layer 2 39
3.2.11 Schutz in der Cloud gespeicherter Dateien 40
3.2.12 Datenverarbeitung in der Cloud 41
3.2.13 Schutz mobiler Sprach- und Datendienste 43
3.2.14 Schutz der Kommunikation mittels Instant Messenger 44
3.2.15 Schutz mobiler Geräte 46
3.2.16 Routersicherheit 47
3.2.17 Netzwerküberwachung mit IDS 49
3.2.18 Schutz des Web-Datenverkehrs 51
3.2.19 Schutz von Web-Anwendungen 52
3.2.20 Schutz des Fernzugriffs auf Netzwerke 54
3.2.21 Systemhärtung 55
3.2.22 Endpoint Detection & Response Platform 58
3.2.23 Web-Isolation der Internetnutzung 60
3.2.24 Angriffserkennung und Auswertung (SIEM) 61
3.2.25 Vertrauliche Datenverarbeitung in der Cloud 63
3.2.26 Sandboxing zur Schadcode-Analyse 64
3.2.27 Cyber Threat Intelligence 66
3.2.28 Absicherung administrativer IT-Systeme 68
3.2.29 Überwachung von Verzeichnisdiensten und identitätsbasierte Segmentierung 69
3.2.30 Netzwerksegmentierung und Separierung 71
3.2.31 Cloud-Sicherheitsplattform 74
3.2.32 Tokenisierung 75
3.2.33 VOIP-Verschlüsselung mit SIPS/SRTP 77
3.2.34 Verschlüsselung (Layer 1) 79
3.3 Organisatorische Maßnahmen 81
3.3.1 Standards und Normen 81
3.3.2 Sicherheitsorganisation 84
3.3.3 Informationssicherheitsmanagementsystem (ISMS) 86
3.3.4 Sichere Softwareentwicklung 88
3.3.5 Prozesszertifizierung 92
3.3.6 Schwachstellen- und Patchmanagement 95
3.3.7 Risikomanagement 97
3.3.8 Personenzertifizierung 100
3.3.9 Absicherung privilegierter Benutzerkonten 103

Bundesverband IT-Sicherheit e.V. (TeleTrusT):
Handreichung „Stand der Technik in der IT-Sicherheit“, Technische und organisatorische Maßnahmen, Ausgabe 2025

Auszug aus der Handreichung zu ISO/IEC 27001:2022:

- Die Norm ISO/IEC 27001:2022 ist **ein international anerkanntes Rahmenwerk für das Informationssicherheitsmanagement (ISMS).** Sie unterstützt Organisationen aller Größen und Branchen dabei, ihre Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten und zu behandeln.

- Neben diesen Kernaspekten betont ISO/IEC 27001:2022 die Bedeutung eines kontinuierlichen Verbesserungsprozesses. Dies stellt sicher, dass Organisationen auf sich verändernde Bedrohungen und geschäftliche Anforderungen reagieren können.

- Ein entscheidender Vorteil von ISO/IEC 27001:2022 ist die **Möglichkeit einer Zertifizierung**.

- Organisationen können ihr Informationssicherheitsmanagementsystem (ISMS) durch eine unabhängige Zertifizierungsstelle auditieren lassen, um die Einhaltung der Norm nachzuweisen.

- Die **Zertifizierung dient als international anerkanntes Gütesiegel** und signalisiert Kunden, Partnern und Aufsichtsbehörden, dass die Organisation systematische und wirksame Maßnahmen zum Schutz von Informationen implementiert hat.

- Dies kann nicht nur das **Vertrauen in die IT-Sicherheit** stärken, sondern auch Wettbewerbsvorteile schaffen, indem es Unternehmen hilft, regulatorische Anforderungen zu erfüllen und neue Geschäftsmöglichkeiten zu erschließen.

Tipp:

Siehe Exkurse und Mapping-Tabellen unter:
4.2 Einordnung der Maßnahmen in ISO/IEC 27001:2022
4.3 Einordnung der Maßnahmen in das NIST-Rahmenwerk (USA)
4.5 Absicherung der Lieferkette

und Einzelkapitel: 3.3.12 Software Bill of Materials (SBOM)

Der „Stand der Technik“ in der Videoüberwachungstechnik
Der „Stand der Technik“ in der Videoüberwachungstechnik umfasst eine Vielzahl von Entwicklungen, die sowohl die Video-Hardware als auch die Software betreffen. Aktuell sind hochauflösende Kameras, intelligente KI-basierte Analysefunktionen und die Integration in Netzwerke und andere komplementäre Plattformen wie Gebäudemanagementsysteme oder Sicherheitssysteme wichtige Aspekte. Zusätzlich gewinnen IT-Sicherheitsaspekte und Datenschutzaspekte, wie die Einhaltung der DSGVO, zunehmend an Bedeutung. Auch die Sicherung der Datenübertragung und des Zugriffs gewinnt an Bedeutung (Verschlüsselungstechnologien und Authentifizierungsmethoden).

Wichtige Normen und Richtlinien dabei sind die DIN EN 62676-4 (Videotechnik), die DSGVO (Datenschutz und Datensicherheit) und künftig auch vermehrt der EU AI Act und indirekt auch, wie oben beschrieben, die NIS-2.
Zusammenfassend lässt sich sagen, dass die Videoüberwachungstechnik sich rasant weiterentwickelt und immer mehr in den Bereich der digitalen Infrastruktur integriert wird. Die Berücksichtigung von Datenschutz, IT-Sicherheit und die Integration in andere Systeme sind dabei entscheidende Faktoren.

Dallmeier Antwort und Unterstützung zu „Stand der Technik“:

- Dallmeier Produkte und Prozesse = „Stand der Technik“
- Dallmeier liefert nach den obigen Definitionen, Kriterien, Handreichungen, Normen und unter Berücksichtigung seines intern eingesetzten, ISO 27001 zertifizierten ISMS, den von der NIS-2 geforderten „Stand der Technik“ sowohl bzgl:
  - „Stand der Technik in der Videoüberwachungstechnik“ als auch
  - „Stand der Technik in der IT-Sicherheit“
  - In Summe: „Stand der Technik“

Ihr Nutzen

Nach den obigen Definitionen, Kriterien, Handreichungen, Normen und unter Berücksichtigung des intern eingesetzten, ISO 27001 zertifizierten ISMS, liefert Dallmeier sowohl den „Stand der Technik in der Videoüberwachungstechnik“ als auch den „Stand der Technik in der IT-Sicherheit“.
Damit stellt Dallmeier sicher, dass Kunden die NIS2-Anforderung zu

- Stand der Technik

effizient und rechtssicher erfüllen.

Das stärkt die Cyberresilienz entlang der gesamten Lieferkette und unterstützt den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

4.2.2 Security by Design

Die NIS2-Richtlinie behandelt die Anforderung nach „Security by Design“ direkt in Artikel 21 Absatz 2 Buchstabe e) sowie indirekt in anderen Teilen, die sich mit der Sicherheit von Netz- und Informationssystemen während ihres gesamten Lebenszyklus befassen.

Konkret heißt es in Artikel 21 Absatz 2 Buchstabe e):

- „Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich der Bewältigung und Offenlegung von Schwachstellen.“

Das umfasst ausdrücklich das Prinzip „Security by Design“, also:

- Sicherheit von Anfang an bei der System- und Softwareentwicklung zu berücksichtigen,
- sicherzustellen, dass Sicherheitsmechanismen bereits bei der Planung und Entwicklung eingebaut sind,
- und dass Systeme standardmäßig sicher konfiguriert sind (auch bekannt als „Security by Default“).

Was NIS2 konkret fordert:

Die Richtlinie verlangt, dass Einrichtungen Strukturen und Prozesse schaffen, um Sicherheitsaspekte proaktiv und systematisch in die Entwicklung und Beschaffung von IT-Systemen einzubinden. Dazu gehört auch, dass Lieferanten, Hersteller und Entwickler vertraglich und technisch in Sicherheitsanforderungen eingebunden werden. Ziel ist es, Schwachstellen zu minimieren, bevor ein System in Betrieb geht, anstatt erst im Nachhinein auf Sicherheitslücken zu reagieren.

Dallmeier Antwort und Unterstützung zu „Security by Design“:

- Dallmeier Entwicklungsprinzipien = „Security by Design“ und „Privacy by Design“
- Nach NIS2 (Artikel 21) und DSGVO (Artikel 32 und Artikel 25)
- Bei Dallmeier findet Security by Design sowohl in der Software- als auch in der Hardwareentwicklung Anwendung.
- „Security by Design“ bei Dallmeier verfolgt das Ziel, Sicherheitsaspekte von Anfang an fest in die Planung und Entwicklung von Produkten einzubinden.
- Sicherheitsrelevante Designentscheidungen werden zu Beginn der Softwareentwicklung festgelegt und werden dann im Entwicklungsprozess umgesetzt.
- So wird sichergestellt, dass die Informationssicherheit ein wesentlicher Bestandteil für die Software ist und über alle Ebenen des Systems berücksichtigt wird.
- Dadurch werden potenzielle Schwachstellen frühzeitig minimiert.
- Zudem werden Dallmeier-Produkte standardmäßig mit sicheren Voreinstellungen ausgestattet („Security by Default“).
- Unser weiterer Sicherheitsansatz nach dem Security by Design Prinzip basiert auf den folgenden, weiteren zentralen Elementen:
    - „No Backdoors-Politik” und „Made in Germany”
        - Sicherheit und (digitale) Souveränität by secure and sovereign country and company Prinzip
        - Gerade im Hinblick auf geopolitische Unsicherheiten und steigende Anforderungen an Datenschutz und Souveränität (Daten, Technologie, Betrieb) gewinnen europäische Techniken zunehmend an Bedeutung.
        - Gütesiegel für Qualität, Vertrauen (Trust), Souveränität und hohe Sicherheits- und Datenschutzstandards inkl. hohe Ethikstandards.
        - NDAA-Konformität
        - politisch und wirtschaftlich unabhängig, keine drittstaatlichen Stakeholder/Interessenlagen
        - regelmäßigen Penetrationstests durch unabhängige Sachverständige
        - Höchste Fertigungstiefe in Forschung, Entwicklung und Produktion

- **Zertifizierungen:**
  - ISO 27001 (Information Security Management System/ISMS, Cybersicherheit inkl. Datenschutz)
  - ISO 9001 (Qualitätsmanagement)
  - ISO 45001 (Arbeitsschutzmanagement)


ZERTIFIKAT

Zertifikat-Registrier-Nr.: 12 310 67686 TMS / Auftrags-Nr.: 707167008

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
bescheinigt, dass die Organisation

Dallmeier

Dallmeier electronic GmbH & Co. KG
Bahnhofstr. 16
93047 Regensburg
Deutschland

für den Geltungsbereich

Entwicklung, Betrieb und Support von
Hardware- und Softwarekomponenten für Produkte und Lösungen
im Bereich der Videosicherheitstechnik

ein Informationssicherheitsmanagementsystem gemäß
„Erklärung zur Anwendbarkeit" eingeführt hat und anwendet.
Durch ein Audit wurde der Nachweis erbracht,
dass die Forderungen der

ISO/IEC 27001:2022

erfüllt sind.

Dieses Zertifikat ist gültig vom 05.06.2024 bis 04.06.2027.
Version der Erklärung zur Anwendbarkeit: V1.2 vom 28.02.2024

Fred Wenke
Leiter der Zertifizierungsstelle
München, 05.06.2024

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuvsud.com/de-certificate-validity-check

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Abb.: Dallmeier Zertifizierung nach ISO 27001

- **Sicherheitstechniken und Sicherheitsfunktionen (Produktebene)**
  - Breites Portfolio an technischen und organisatorischen Features für Cybersecurity und Datenschutz
  - Sicherheitsbetriebssystem Domera OS (aktuelle Version 15.0.0.7)
    - Sicherheitskameras sind mit dem abgeschotteten, hardened Linux Betriebssystem Domera® OS ausgestattet.
    - Neben einem Kernel mit Long Term Support bietet es umfangreiche Sicherheitsfunktionen wie die Deaktivierung ungenutzter, unsicherer Ports und Protokolle („Security by Default") oder die Erzwingung strenger Passwörter .
    - sichere Netzwerkauthentifizierung (IEEE 802.1X) (im Sinne eines Zero-Trust Ansatzes)
    - verschlüsselte Datenübertragung (TLS 1.3/AES-256)
    - Fail2Ban-Schutzfunktion gegen Hackerangriffe (Brute-Force-Angriffsschutz)
    - ViProxy als integriertes, optionales Security-Gateway

- Secure-Boot, Signed OS und Trust Plattform
  - mehrschichtige Sicherheitsmechanismen, um die Systemintegrität und Cyberresilienz nachhaltig zu stärken, das Gesamtsystem gezielt gegen Manipulationen und Angriffsversuche im Kontext moderner Cybersicherheitsanforderungen zu härten und zur Erhöhung der „Sicherheit in der Lieferkette“ (eine explizite Anforderung von NIS-2, siehe oben).
  - Funktionen für eine Sicherheits- und Vertrauenskette („chain of security & trust“)
  - Funktionen zur Stärkung eines optionalen „Zero-Trust“-Ansatzes
  - Secure Boot | Signed OS | TrustZone | fTPM

Sicherheitskomponente	Funktion	Nutzen
Secure Boot	Prüft jede Bootstufe	Verhindert Ausführung von manipuliertem Code
Signed OS	Erzwingt signierte Firmware	Schutz vor Supply-Chain-Angriffen
TrustZone	Getrennte Systemumgebungen	Isolierung sensibler Prozesse in Secure World
fTPM	Hochsicherer Kryptografiespeicher im TrustZone-Kontext	Keine dedizierte TPM-Hardware erforderlich

Genaue Funktionsbeschreibung dieser vier Sicherheitskomponenten siehe gerne Technische Mitteilung Domera OS Version 15.0.0.7

- SBOM: Software Bill of Materials
  - Offenlegung der verwendeten Softwarekomponenten
  - Transparenz in der Cybersicherheit und Schwachstellenmanagement
  - Eine SBOM unterstützt das Schwachstellenmanagement automatisiert, indem sie eine vollständige, maschinenlesbare Liste aller verwendeten Softwarekomponenten bereitstellt, die mit bekannten Schwachstellenquellen abgeglichen werden, um Risiken frühzeitig zu erkennen und gezielt zu beheben.

- Software- und Sicherheitskomponenten unterliegen einer permanenten Überwachung, Pflege und Aktualisierung, Wirksamkeit aller Maßnahmen durch regelmäßige externe Penetrationstests sichergestellt.
- Aufzeichnungs-Appliances: ebenfalls abgeschottetes, hardened Linux Sicherheitsbetriebssystem mit entsprechenden Sicherheitsfunktionen, wie oben bei Domera OS beschrieben.
  - zzgl. spezielles TPM 2.0 Modul / Chip (FIPS 140 konform) | kryptografischer Sicherheitsstandard vom National Institute of Standards and Technology (NIST) der USA
- Datensicherheits- und Datenschutzfunktionen nach „Security und Pivacy by Design“: hier online

Ihr Nutzen

Mit diesen, nach ISO 27001 zertifizierten und periodisch von extern auditierten, Entwicklungs- und Herstellungsprinzip „Security by Design“ und den aufgeführten Sicherheitstechniken und Sicherheitsfunktionen auf Produktebene stellt Dallmeier sicher, dass Kunden die NIS2-Anforderung zu

- Security by Design

effizient und rechtssicher erfüllen.

Das stärkt die Cyberresilienz entlang der gesamten Integrations- und Lieferkette und ermöglicht den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

4.2.3 Sicherheit der Lieferkette

Die NIS2-Richtlinie behandelt die Anforderung zu Sicherheit der Lieferkette in Artikel 21, der sich mit den Pflichten zur Umsetzung von Maßnahmen des Risikomanagements im Bereich der Cybersicherheit befasst.

Dort wird in Absatz 2 Buchstaben d) ausdrücklich gefordert:

- „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern“

Die NIS2-Richtlinie behandelt die Anforderung nach „Sicherheit der Lieferkette“ zusätzlich in Artikel 21 Absatz 3 sowie in Erwägungsgrund 85.

- Artikel 21 Absatz 3:
  Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.

- Erwägungsgrund 85:
  Betont ausdrücklich die Notwendigkeit, Risiken entlang der gesamten Lieferkette zu bewerten – inklusive Drittanbietern, Software-Lieferanten, Hosting-Anbietern und Cloud-Diensten.

Was von NIS2 gefordert wird:

- Einrichtungen müssen die Cybersicherheitsrisiken in ihrer Lieferkette systematisch bewerten,

- Drittanbieter und Zulieferer in ihre Sicherheitsprozesse einbinden (z. B. durch vertragliche Anforderungen, Audits, Zertifizierungen)

- bei der Beschaffung von Systemen und Diensten auf deren Sicherheitsniveau und Vertrauenswürdigkeit achten

- Einrichtungen müssen das gesamte ökosystemische Risiko minimieren – denn Schwachstellen bei Zulieferern können direkte Auswirkungen auf die Sicherheit des eigenen Unternehmens haben.

„Sicherheit in der Lieferkette“ nach dem „Stand der Technik“

Siehe Handreichung „Stand der Technik in der IT-Sicherheit“, TeleTrust, 2025
Kapitel 4.5: Absicherung der Lieferkette

Auszug:
„Die Resilienz von Lieferketten wird zunehmend zur zentralen, branchenübergreifenden Anforderung für Unternehmen. Bedingt durch geopolitische Spannungen, Cyber-Bedrohungen und regulatorische Verschärfungen wächst der Druck, Abhängigkeiten nicht nur wirtschaftlich, sondern auch sicherheitsbezogen zu bewerten. Mit der neuen NIS-2-Richtlinie, der aktualisierten ISO/IEC 27001:2022 ..treten konkrete Anforderungen in Kraft, die so-wohl Organisationen als auch ihre Dienstleister und Zulieferer betreffen.“

„Sicherheit in der Lieferkette“ nach BSI (Bundesamt für Sicherheit in der Informationstechnik

BSI-Webseite: #nis2know-Infopaket: Sichere Lieferkette

Wichtige Auszüge BSI:

Sichere Lieferkette – Warum?

- **Resilienz gegenüber Cyberangriffen**
  Ein einziger kompromittierter Zulieferer kann IT-Systeme lahmlegen, Datenlecks verursachen und dadurch den Geschäftsbetrieb stören. Je komplexer die Lieferkette, desto größer die Angriffsfläche für Cyberkriminelle.

- **Vermeidung von Schadsoftware und kompromittierter Hardware**
  Hat eine Lieferkette Schwachstellen, kann bereits bei der Entwicklung oder Auslieferung von Hardware oder Software Schadcode eingeschleust werden (z. B. durch manipulierte Updates oder kompromittierte Komponenten).

- **Schutz sensibler Daten und Systeme**
  Schwachstellen in der Informationssicherheit der Lieferkette erhöhen das Risiko für Datendiebstahl, Industriespionage oder Systemmanipulation.

- **Vertrauen in Produkte und Anbieter**
  Unternehmen müssen sich darauf verlassen können, dass ihre Produkte nicht kompromittiert oder manipuliert werden oder wurden. Eine vertrauenswürdige Lieferkette bedeutet: Verifizierte Herkunft, geprüfte Komponenten und nachvollziehbare Prozesse. Vorfälle gefährden nicht nur sensible Informationen, sondern auch Vertrauen, Handlungsfähigkeit und Reputation eines Unternehmens.

Sichere Lieferkette – Was ist zu beachten?

- Qualifikationen, Zuverlässigkeit und Sicherheitsüberprüfungen des Personals bei Dienstleistern und Outsourcing-Partnern entziehen sich in der Regel der Kontrolle des Auftraggebers.

- Ein umfassendes Risikomanagement muss auch die Ebene der Zulieferer erreichen.

Sichere Lieferkette – Was tun?

- Vertragliche Vereinbarungen (Service Level Agreements) mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen und Patchmanagement abschließen.
- Nachweise von den Zulieferern und Herstellern verlangen, z. B. zertifiziertes ISMS nach ISO 27001, Nachweis über NDAA-Konformität.
- Optional „geopolitische Sicherheitsvereinbarungen“ wie z.B. vertrauenswürdige Herstellerländer und Wertschöpfungsketten, „Made in Europe“ als freiwillig-optionales Sicherheits- und Vertrauenssiegel anfragen.
- Zulieferer und Dienstleister zur Einhaltung von grundsätzlichen Prinzipien wie Security by Design und Security by Default anhalten.
- Zulieferer und Dienstleister zur Berücksichtigung von Empfehlungen des BSI in Bezug auf ihre Lieferkette anhalten.
- Implementierung eines Informationssicherheits-Managementsystems (ISMS) mithilfe bestehender Standards (ISO 27001:2022, BSI-Standard 200-1, etc.). Ein ISMS nach ISO 27001 schafft Strukturen und Methoden, die für ein wirksames C-SCRM (Cyber-Supply Chain Risk Management) notwendig sind. Ohne ISMS müsste man viele Grundlagen erst neu schaffen, was den Aufwand und das Risiko deutlich erhöht.
- Ein umfassendes Risikomanagement muss auch die Ebene der Zulieferer erreichen, manchmal auch über mehrere Zulieferer hinweg.

Dallmeier Antwort und Unterstützung zu „Sicherheit in der Lieferkette“:

Dallmeier liefert Sicherheit² für die Lieferkette unserer Kunden (NIS-2-Einrichtungen)

WARUM Sicherheit²?

- Das BSI schreibt (siehe oben die zwei letzten Punkte zu Was tun?):
  - Ein ISMS nach ISO 27001 schafft Strukturen und Methoden, die für ein wirksames „Cyber-Supply Chain Risk Management“ (C-SCRM) notwendig sind.
  - Dallmeier ergänzt: ISO 27001... für ein wirksames EIGENES C-SCRM und ein wirksames C-SCRM des Zulieferers/Herstellers.
  - Ein umfassendes Risikomanagement muss auch die Ebene der Zulieferer erreichen, manchmal auch über mehrere Zulieferer hinweg.
  - Dallmeier ergänzt: Auch die Zulieferer vom Zulieferer Dallmeier müssen sicherheitstechnisch einbezogen werden.
- Die NIS-2-Richtlinie verpflichtet auch uns selbst als Dallmeier als wichtige Einrichtungen zu umfassenden Risikomanagementmaßnahmen.

- Dazu zählt auch „die Sicherheit der Lieferkette **(unsere eigene Lieferkette !!)** einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unseren unmittelbaren Anbietern“.
- Bindende Hilfestellung zur Umsetzung der Anforderung nach Sicherheit in der Lieferkette liefert uns unser eingesetztes Information Security Management System (ISMS), welches nach dem internationalen Standard ISO 27001 zertifiziert ist.
- Das ist nicht nur eine Hilfestellung, sondern eine Pflicht aus der Zertifizierungssicht.
- Die ISO 27001 verpflichtet uns also abseits der NIS-2 bereits zu Sicherheit in der (eigenen!) Lieferkette.
- Konkret nach den ISO 27001-Normkapitel/Controls A.5.19 bis A.5.23

TIPP:
Nutzen sie gerne als NIS-2-Einrichtung die Mapping-Tabelle NIS2 zu ISO 27001 unseres CSO Armin Biersack (gerne auf Anfrage komplett) oder die Mapping-Tabelle auf OpenKRITIS.

Auszug Dallmeier Mapping NIS2 zu ISO 27001 - Sicherheit der Lieferkette:

EU-NIS2 (EU 2022/2555) Anforderungen	**Typische Auditfragen**	**ISO 27001:2022 / ISO 27002:2022** Normkapitel und Controls
Artikel 21.2 (d) & 21.3: Management der Lieferkette	Sicherheit in der Lieferkette und bei Dienstleistern – Welche Maßnahmen ergreifen Sie, um sicherzustellen, dass auch Ihre Dienstleister die Anforderungen an die Informationssicherheit erfüllen? – Wie überprüfen Sie Ihre Dienstleister?	A.5.19 Informationssicherheit in Lieferantenbeziehungen A.5.20 Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen A.5.21 Management der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT) A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendiensten A.5.23 Informationssicherheit bei der Nutzung von Cloud-Diensten

„NIS-2 verlangt nachweisbare Cybersicherheit – Vertrauen und Sicherheit für die Lieferkette schafft nur eine zertifizierte und periodisch auditierte ISO 27001.“

Jürgen Seiler, Head of Business Development bei Dallmeier electronic

Weitere organisatorische und technische Aspekte Dallmeier:

- Dallmeier verfolgt beim Thema Cybersicherheit einen umfassenden Lebenszyklusansatz – von der Entwicklung über Vertrieb und Betrieb bis hin zur Stilllegung – und setzt dabei auf konsequente Risikominderung entlang der gesamten Lieferkette.
- Das Unternehmen Dallmeier entwickelt und produziert sämtliche Kamera- und Aufzeichnungssysteme und Software am Standort Regensburg in Deutschland.
- Die Dallmeier Komponenten der Kamera- und Aufzeichnungssysteme und Software werden von Dallmeier zertifizierten Unternehmen aus einem Umkreis von weniger als 200 km gefertigt.
- Manche Komponenten lassen sich allerdings in Qualität oder Funktion nicht mehr regional beschaffen. Beim „Global Sourcing“ dieser Komponenten folgen wir akribisch den strengen deutschen Vorgaben nach ISO und führen mehrmals im Jahr Besuche und Audits bei unseren Lieferanten durch.

- Im Folgenden technische Beispiele und Funktionen, wie Dallmeier die Sicherheit der Lieferkette gewährleistet (in Kurzform, da oben bereits ausführlich gelistet):
  - Security by Design Entwicklungsprinzipien
  - Produkte nach dem „Stand der Technik“ (auch „Stand der Technik in der IT-Sicherheit“)
  - Regelmäßige Sicherheitsupdates / Patchpolitik / Lebenszyklus-Sicherheitsmanagement
  - Vorhalten Vorhalten von PSIRT/SIRC-Teams für proaktives und reaktives Schwachstellenmanagement; Sicherheits-Advisories
  - SBOM: Software Bill of Materials
    - Offenlegung der verwendeten Softwarekomponenten
    - Transparenz in der Cybersicherheit und Schwachstellenmanagement
    - Eine SBOM unterstützt das Schwachstellenmanagement automatisiert, indem sie eine vollständige, maschinenlesbare Liste aller verwendeten Softwarekomponenten bereitstellt, die mit bekannten Schwachstellenquellen abgeglichen werden, um Risiken frühzeitig zu erkennen und gezielt zu beheben.
  - Kryptografische Prüfverfahren: Secure-Boot, Signed OS und Trust Plattform
  - Sichere, Port-basierte Netzwerkauthentifizierung nach IEEE 802.1X auf Basis von Zertifikaten
  - Verschlüsselte Datenübertragung (TLS 1.3/AES-256)
  - CRA zertifizierte Produkte: Der Cyber Resilience Act der EU verpflichtet uns als Hersteller Dallmeier von Produkten mit digitalen Elementen ab dem Jahre 2026/2027 zu verpflichtenden Cybersicherheitsmaßnahmen auf Produktebene (u.a. SBOM); wir werden den CRA auf Produktebene erfüllen und CRA-zertifizierte Produkte liefern.
  - Mit Hersteller-Vorprodukten (von Dallmeier), die nach CRA ihre CE-Konformität nicht nur bezüglich Safety, sondern auch bezüglich Security nachweisen können, kann die NIS-2-betroffene Einrichtung die Sicherheit in der Lieferkette leichter bewerkstelligen.
  - Lesetipp Blogartikel:
    - CRA, CE und NIS-2: Was bedeutet digitale Resilienz und Cybersecurity über die gesamte Liefer- und Wertschöpfungskette hinweg?

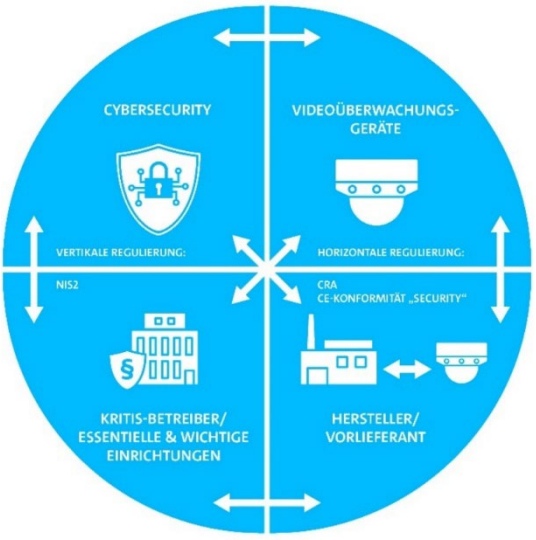


Abb.: Zusammenhang CRA und NIS-2, dargestellt am Beispiel Videoüberwachungshersteller/Produkte für NIS-2-Einrichtungen, NIS2 als vertikale Regulierung, CRA als horizontale Regulierung

Ihr Nutzen

Mit diesen, nach ISO 27001 zertifizierten und periodisch von extern auditierten, Sicherheitsprozessen und Sicherheitsfunktionen stellt Dallmeier sicher, dass Kunden die NIS2-Anforderung zu

- **Sicherheit der Lieferkette**

effizient und rechtssicher erfüllen.

Das stärkt die Cyberresilienz entlang der gesamten Lieferkette und ermöglicht den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

4.2.4 Sicherheit der Integrationskette

NIS-2 fordert indirekt bzw. fast auch direkt die Sicherheit der Integrationskette in Artikel 21 (2) d) und e):

Über die direkten, expliziten Anforderungen nach:

- „Sicherheit in der Lieferkette..einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen..ihren unmittelbaren Anbietern oder Diensteanbietern“ und
- „Sicherheitsmaßnahmen bei Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen“

Jedes Unternehmen bzw. jede NIS-Einrichtung hat andere Anforderungen an ein Videosystem bzw. ein ganzheitliches Sicherheitssystem. Videomanagement, Videoanalytik, Drittsysteme wie Einbruchmeldeanlagen (EMA), Zutrittskontrollsysteme (ZuKo), Intercomsysteme oder andere Komplementär-Technologien oder übergeordnete Sicherheitsplattformen werden bei anspruchsvollen Sicherheitsprojekten oft durch Integrationen und Schnittstellen verbunden. Aktuell sind Integrationen (egal welche Integrationsrichtung und welche Integrationstiefe) in komplementäre Plattformen wie Gebäudemanagementsysteme/PSIM-Systeme oder 3rd party Videomanagementsysteme oder 3rd party Videoanalytiksysteme, wie oben geschrieben, „Stand der Technik in der Videosicherheitstechnik“.

- Aber sind solche Integrationen auch „Stand der Technik bzgl. IT-Sicherheit“?
- Hier muss erneut und insbesondere die obige Frage nach der expliziten NIS2-Anforderung „Sicherheit in der Lieferkette“ gestellt werden.
- Hier muss genauer gesagt nach „Sicherheit in der Integrations-Lieferkette | Integrationskette“ gestellt werden.

Zur Sensibilisierung nochmal die obigen Merksätze, auf die Sicherheit von Integrationen abgestellt:

- Eine Sicherheits- und Integrationskette ist nur so stark wie ihr schwächstes Glied.
- Keine sichere Integrationskette ohne sichere Integrationsprodukte der beteiligten Hersteller.
- Ein umfassendes Risikomanagement muss auch die Ebene der Integrations-Zulieferer erreichen, manchmal auch über mehrere Integrations-Zulieferer hinweg.

Die von Dallmeier angebotenen Integrationen von und zu anderen Sicherheitssystemen und Plattformen wie Videomanagement (VMS), Videoanalytik und Gebäudemanagement/PSIM-Systeme von Dallmeier Technologiepartnern sind bzgl. ihrer Sicherheits- und Prozessanforderungen nach dem Security by Design-Prinzip entwickelt und ausgiebig getestet. Dieses Vorgehensweise nach dem Security by Design-Entwicklungs- und Testprinzip und dieses Level der Sicherheit von Integrationen ist Standard und stellt auch nur „Standardsicherheit“ her.

Wo unterscheiden wir uns als Dallmeier nun bei Integrationssicherheit?

Dallmeier Antwort und Unterstützung zu „Sicherheit der Integrationskette“:

Dallmeier liefert Sicherheit² für die Integrationskette unserer Kunden (NIS-2-Einrichtungen)

WARUM Sicherheit²?

- Nicht nur unsere eigenen Produkte und Prozesse, sondern auch unsere Integrationslösungen und Integrationsprozesse werden im Rahmen unserer internen Sicherheits- und Prüfprozesse streng nach ISO 27001 zertifiziert und periodisch und kontinuierlich in zeitlichen Abständen von extern auditiert.
- Dallmeier bietet damit eine sichere Integrationskette mit offizieller Akkreditierung und offiziellem Nachweis nach dem internationalen Zertifizierungs-Standard ISO 27001.

  Nochmal obiges Zitat, hier abgestellt auf Integrationen und Schnittstellen:

> *"NIS-2 verlangt nachweisbare Cybersicherheit – Vertrauen und Sicherheit für die Liefer- und Integrationskette schafft nur eine zertifizierte und periodisch auditierte ISO 27001."*
>
> *Jürgen Seiler, Head of Business Development bei Dallmeier electronic*

NIS2-Mapping-Tabelle auf ISO 27001 - 27002

EU-NIS2 (EU 2022/2555) Anforderungen	**Typische Auditfragen**	**ISO 27001:2022 / ISO 27002:2022** Normkapitel und Controls
Artikel 21.2 (d) & 21.3: Management der Lieferkette	Sicherheit in der Lieferkette und bei Dienstleistern – Welche Maßnahmen ergreifen Sie, um sicherzustellen, dass auch Ihre Dienstleister die Anforderungen an die Informationssicherheit erfüllen? – Wie überprüfen Sie Ihre Dienstleister?	A.5.19 Informationssicherheit in Lieferantenbeziehungen A.5.20 Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen A.5.21 Management der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT) A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendiensten A.5.23 Informationssicherheit bei der Nutzung von Cloud-Diensten
Artikel 21.2 (e): Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzen und Informationssystemen	Sicherheit in Entwicklung, Beschaffung und Wartung – Welche Sicherheitsprinzipien wenden Sie bei der Softwareentwicklung oder bei der Beschaffung und Wartung von Software an?	A.5.20 Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen A.5.24 Planung und Vorbereitung des Informationssicherheitsvorfallmanagements A.5.36 Einhaltung von Richtlinien, Regeln und Standards zur Informationssicherheit A.5.37 Dokumentierte Betriebsverfahren A.6.08 Meldung von Informationssicherheitsereignissen A.8.09 Konfigurationsmanagement A.8.19 Installation von Software auf Betriebssystemen A8.20 Netzwerksicherheit A8.21 Sicherheit von Netzwerkdiensten

Abb.: Dallmeier Sicherheit in Liefer- und Integrationskette, geprüft und zertifiziert nach ISO27001

Ihr Nutzen

Mit diesen, nach ISO 27001 zertifizierten und periodisch von extern auditierten, Entwicklungs- und Integrationsprozessen stellt Dallmeier sicher, dass Kunden die indirekte NIS2-Anforderung zu

- Sicherheit der Integrationskette

effizient und rechtssicher erfüllt.

Das stärkt die Cyberresilienz entlang der gesamten Integrations- und Lieferkette und ermöglicht den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

4.2.5 Regelmäßige Updates und Sicherheitspatches

Die NIS2-Richtlinie behandelt die Anforderungen zu regelmäßigen Updates und Sicherheitspatches in Artikel 21, der sich mit den Pflichten zur Umsetzung von Maßnahmen des Risikomanagements im Bereich der Cybersicherheit befasst.

Dort wird in Absatz 2 Buchstaben e) und g) ausdrücklich gefordert:

- „Sicherheitsmaßnahmen bei Erwerb, bei Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen“
- Grundlegende Verfahren im Bereich der Cyberhygiene

Das schließt folgerichtig ein:

- die zeitnahe Installation von Updates, Sicherheitsupdates und Patches
- die kontinuierliche Überwachung von Schwachstellen,
- sowie Prozesse zur Schwachstellenbehandlung und -meldung.

Regelmäßige Updates und Sicherheitspatches sind entscheidend, um Sicherheitslücken zu schließen, die Stabilität zu gewährleisten und die Kompatibilität der IT-Komponenten im Gesamtsystem zu erhalten. In der heutigen Zeit ist es unerlässlich, dass komplexe Systeme wie Kameras und Aufzeichnungssysteme für Videoüberwachung auf dem neuesten Stand gehalten werden. Hierfür sorgt der Dallmeier Device Manager. Dieses leistungsstarke Tool vereinfacht nicht nur die Verwaltung Ihres gesamten Dallmeier Systems, sondern sorgt auch dafür, dass Ihre Systeme stets mit den neuesten Funktionen und Sicherheitsupdates ausgestattet sind.

Auch alle anderen Netzwerkkomponenten (Firewalls, Router, Switches etc.) des kompletten Systems sollten insbesondere in Bezug auf Sicherheitspatches stets auf dem aktuellsten Software-Stand sein. Auch die Betriebssysteme von Servern und Client-PCs sollten unbedingt regelmäßig auf Sicherheitspatches geprüft und falls erforderlich entsprechend aktualisiert werden.

Dallmeier Antwort und Unterstützung zu „Regelmäßige Updates und Sicherheitspatches“:

- Dallmeier liefert nach seinem Lebenszyklus-Sicherheitsmanagement regelmäßige Updates und Sicherheitspatches.
- Dallmeier Schwachstellenmanagement (SIRC/PSIRT): siehe Kapitel 4.2.8
- Sicheres und zuverlässiges Updatemanagement: Dallmeier Device Manager

Der „Dallmeier Device Manager“ ist ein Tool zur Geräteverwaltung, das es NIS-2-Einrichtungen und Kunden sehr einfach macht, die Software auf allen Dallmeier Systemen auf dem neuesten Versionsstand und damit auf dem aktuellsten Sicherheitsstand zu halten. Darüber hinaus melden Dallmeier-Systeme optional automatisch, sobald neue Softwareversionen zur Verfügung stehen.

Zu jedem Update wird eine technische Mitteilung veröffentlicht, die über alle sicherheitsrelevanten Aspekte und Neuerungen informiert. Alle Updates sollten zunächst ausgiebig in einer Testumgebung auf Kompatibilität und einwandfreie Funktionsweise geprüft werden, um den laufenden Betrieb des IT-Systems nicht zu gefährden. Zudem sollte das Einspielen von Updates stets sorgfältig geplant und dokumentiert werden.

Dallmeier Device Manager: Device Management & Firmware/Software Rollout

- Zentrales Management Tool für ein stets aktuelles und sicheres Videoüberwachungssystem
- Halten Sie die Firmware/Software von Kameras und Recordern immer auf dem neuesten Stand und profitieren Sie von neuen Funktionen und Sicherheitspatches.
- Halten Sie auch Ihre Windows-Installation und die Management-Clients auf dem neuesten Stand.
- Die sichere Konfiguration von Kameras, Recordern und zumindest des Management-Clients ist ein wesentlicher Bestandteil einer cybersicheren Videoüberwachungslösung.
- Produktlebenszyklusbegleitende Sicherheitsupdates:
  Freiwillige und künftig verpflichtende produktlebenszyklusbegleitende Updates gemäß neuer CRA-Vorgaben (Cyber Resilience Act)
- **Warum regelmäßige Updates so wichtig sind?**
  - **Neue Funktionen:** Mit jedem Update erhalten Sie Zugriff auf innovative Funktionen, die die Leistungsfähigkeit Ihres Systems steigern und neue Anwendungsmöglichkeiten eröffnen.
  - **Erhöhte Sicherheit:** Regelmäßige Updates schließen Sicherheitslücken und schützen Ihr System vor Cyberangriffen.
  - **Kompatibilität:** Durch die Installation der neuesten Softwareversionen stellen Sie sicher, dass alle Komponenten Ihres Systems reibungslos zusammenarbeiten.
  - **Sichere Updates**: Updates von Dallmeier sind immer gegen Veränderungen durch Dritte abgesicherten. Sobald nur ein einziges Bit der Update-Datei modifiziert wurde, wird es nicht mehr als gültig akzeptiert und der Update-Vorgang wird nicht eingeleitet.
  - **Gesetzlich verpflichtende Updates**: Der Cyber Resilience Act (CRA) verpflichtet Hersteller von digitalen Produkten, über die gesamte Lebensdauer ihrer Produkte Sicherheitsupdates bereitzustellen.

- **Wie funktioniert die Update-Funktionalität des DDM?**
  Der DDM bietet eine intuitive Benutzeroberfläche, über die Sie alle Geräte und deren Softwareversionen einsehen können. Mit nur wenigen Klicks können Sie:
  - **Verfügbare Updates prüfen:** Der DDM scannt beim Start der Applikation nach neuen verfügbaren Softwareversionen und informiert Sie, sobald Updates verfügbar sind.
  - **Updates planen:** Sie können Updates für Ihre Systeme planen und ausführen, um den Betrieb während wichtiger Ereignisse nicht zu unterbrechen.
  - **Updates kontrollieren**: Updates werden nicht automatisch ausgerollt – Sie haben die Kontrolle!
  - **Updates durchführen:** Der DDM startet die Updates der Systeme auf Ihren Wunsch und informiert Sie, sobald die Systeme wieder online sind.
- Dallmeier Device Manager: Firmware Rollout & Update Management
- Dallmeier Device Manager: Webseite
- Praxistipp: Wie Sie die Sicherheit Ihres Videosystems erhöhen
- Best-Practice Guide: Cybersichere Videoüberwachung

Ihr Nutzen

Mit diesen Updatemechanismen du Tools stellt Dallmeier sicher, dass Kunden die NIS2-Anforderungen zu

- Regelmäßige Updates und Sicherheitspatches

effizient und rechtssicher erfüllen.

Das stärkt die Cyberresilienz entlang der gesamten Lieferkette und ermöglicht den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

4.2.6 Authentifizierung und Autorisierung

Die NIS2-Richtlinie behandelt die Anforderungen zu Authentifizierung und Autorisierung insbesondere in Artikel 21, der sich mit den Pflichten zur Umsetzung von Maßnahmen des Risikomanagements im Bereich der Cybersicherheit befasst.

Dort wird in Absatz 2 Buchstaben i) und j) ausdrücklich gefordert:

- Sicherheit des Personals, **Konzepte für die Zugriffskontrolle** und Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung

Was NIS2 konkret fordert:

Es wird gefordert, dass Unternehmen angemessene technische und organisatorische Maßnahmen umsetzen, einschließlich Zugriffskontrolle und Zugriffssteuerung (Access Control, optional auch physische Zugriffskontrolle per Videoüberwachung / einziger optionaler physischer Sicherheitsaspekt der NIS2!), also insbesondere starke Authentifizierungsverfahren und eine Rollen- bzw. Rechtevergabe, um unbefugten Zugriff zu verhindern.

Unterscheidung allgemein Authentifizierung und Autorisierung:

- Authentifizierung ist der Prozess zur Überprüfung der Identität eines Benutzers oder Systems, meist durch Zugangsdaten wie Passwörter oder Zertifikate.
- Autorisierung regelt, welche Rechte oder Zugriffe eine authentifizierte Person oder ein System innerhalb eines Netzwerks oder einer Anwendung hat.

Im Kontext von Videoüberwachungstechnik:

- Authentifizierung bedeutet z. B., dass nur berechtigte Personen sich an der Überwachungssoftware anmelden dürfen, etwa mit Benutzernamen und Passwort.
- Autorisierung legt dann fest, wer welche Rechte hat, z. B. nur Livebilder sehen, wer Aufzeichnungen löschen oder Systemeinstellungen verändern darf.

Dallmeier Antwort und Unterstützung zu „Authentifizierung und Autorisierung“:

Dallmeier verwendet Authentifizierung und Autorisierung, um den Zugriff auf seine Videosicherheitssysteme zu steuern und zu schützen.

- 4-Augen-Login-Prinzip:
  Sicherheitsmechanismus, bei dem ein zusätzliches Passwort einer zweiten Person erforderlich ist, um den Zugriff auf bestimmte Funktionen zu beschränken.
- Starke Zugriffskontrollen (komplexe Passwörter, regelmäßiger Wechsel)
- Hierarchisches Rechte- und Nutzer-Management:
  Die Benutzerverwaltung ermöglicht dazu die Definition verschiedener Zugriffs- und Konfigurationsrechte für unterschiedliche lokale Benutzergruppen. Falls erforderlich, können den lokalen Benutzergruppen zudem einzelne lokale Benutzer zugeordnet werden. Des Weiteren wird die zentralisierte Benutzerverwaltung über einen Active Directory (AD) Verzeichnisdienst (z.B. Microsoft Windows Server*) oder Linux*) Server mit Samba) mithilfe von LDAP (Lightweight Directory Access Protocol) unterstützt.
- Bei Dallmeier Hemisphere® SeMSy Systemen:
  - Das Hemisphere® Advanced Authentication Module (AAM) ist die zentrale Instanz für die Authentifizierung und Autorisierung aller Benutzer eines Hemisphere® Systems.
  - Es ermöglicht die Anbindung an bestehende LDAP-Benutzerverwaltungssysteme und unterstützt eine kontinuierliche Synchronisierung.

- OAuth2-Standard: Das Modul setzt den modernen und sicheren OAuth2-Standard zur Authentifizierung und Autorisierung von Benutzern und Diensten auf SeMSy® Workstations und Hemisphere® Modulen ein. Das Protokoll bietet hohe Sicherheit und verwaltet die Zugriffe aller Benutzer und Ressourcen auf die geschützten Module und Applikationen des gesamten Hemisphere® Systems.

- Authentifizierungsdienst Kerberos: Das Hemisphere® Advanced Authentication Module kann optional in Kombination mit dem verteilten Authentifizierungsdienst Kerberos genutzt werden. Dieser erlaubt die Authentifizierung aller Benutzer in Applikationen und an Modulen über Single Sign-On mit den Zugangsdaten einer Workstation.

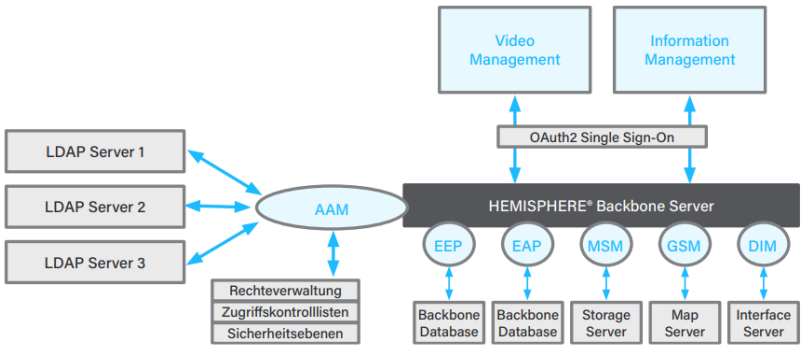
- Dual Login: Die Option Dual Login ermöglicht es, den Anmeldevorgang auf einen Zwei-Benutzer-Login zu erweitern. Melden sich zwei Benutzer nacheinander an einer Workstation an, erlangen sie dadurch höhere Rechte. Damit können bestimmte Bereiche eines Hemisphere® SeMSy® Systems wie beispielsweise Konfigurations- oder Editor-Anwendungen zuverlässig vor unberechtigtem Zugriff geschützt werden.

- Rechteverwaltung: Die Zugriffsrechte auf Hemisphere® Module werden für alle Benutzer über Gruppenberechtigungen verwaltet. Dies erfolgt über eine grafische Benutzeroberfläche, durch einfaches Aktivieren oder Deaktivieren der Zugriffsrechte auf die einzelnen Module.

- Zugriffskontrolllisten: Die definierten Gruppenberechtigungen können durch Zugriffskontrolllisten erweitert werden. Diese Option ermöglicht die Aktivierung zusätzlicher Rechte für einzelne Funktionen und Daten, die in den Hemisphere® Modulen definiert werden können.

- Sicherheitsebenen: Die gespeicherten Mediendateien des Hemisphere® Systems können durch Vergabe von Sicherheitsebenen vor unberechtigtem Zugriff geschützt werden. Benutzergruppen werden hierfür in eine bestimmte Sicherheitsebene eingeordnet und haben somit Zugriff auf alle Dateien bis zu ihrem Level.

- Konfiguration: Das Hemisphere® Advanced Authentication Module bietet eine grafische Benutzeroberfläche für die Konfiguration, auf die plattformunabhängig mit einem Webbrowser zugegriffen werden kann.



- Zudem bietet Dallmeier Tools zur Einrichtung von TLS-Verschlüsselung und zur Konfiguration weiterer Sicherheitseinstellungen, um die Datenübertragung und den Zugriff auf die Systeme zu schützen.

- **Authentifizierung im Netzwerk:** Sichere Authentifizierung nach IEEE 802.1X
  - Aufbau eines Netzwerks mit einer Authentifizierung nach dem Standard IEEE 802.1X.
  - Authentifizierung anhand von Zertifikaten (EAP-TLS) mittels Radius Server
  - Förderung eines Zero-Trust-Ansatzes (Zero-Trust-Netzwerke)

4.2.7 Kryptografie und Datenverschlüsselung

Kryptografie ist die übergeordnete Wissenschaft, die sich mit der Sicherung von Informationen beschäftigt, während Verschlüsselung ein spezifisches Werkzeug innerhalb der Kryptografie ist, das zur Geheimhaltung von Daten dient. Kryptografie umfasst eine Vielzahl von Techniken, darunter Verschlüsselung, digitale Signaturen, Hashfunktionen und mehr.

Verschlüsselung ist ein konkreter Prozess, der innerhalb der Kryptografie eingesetzt wird. Sie wandelt Klartext (lesbare Daten) in Chiffretext (unlesbare Daten) um, wobei ein Schlüssel verwendet wird, um die Umwandlung durchzuführen und die Daten später wiederherzustellen.

Ziel von Kryptografie und Datenverschlüsselung ist es, Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit von Daten und Kommunikation zu gewährleisten.

Die NIS2-Richtlinie behandelt die Anforderung nach „Kryptografie und Datenverschlüsselung“ in Artikel 21 sowie unterstützend in weiteren allgemeinen Vorgaben zur Datensicherheit und Zugangskontrolle.

Dort wird in Artikel 21, Absatz 2 Buchstaben f) ausdrücklich gefordert:

- „Sicherung der Kommunikation, einschließlich gesicherter Sprach-, Video- und Textkommunikation, und gegebenenfalls gesicherter Notfallkommunikationssysteme innerhalb der Einrichtung“

Diese Formulierung schließt den Einsatz von Kryptografie – insbesondere Ende-zu-Ende-Verschlüsselung – als technische Maßnahme zur Vertraulichkeit und Integrität der Kommunikation mit ein.

Außerdem verweist Artikel 21 allgemein auf die Pflicht zur Umsetzung „geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen“, was nach dem Stand der Technik Verschlüsselung und kryptografische Verfahren für die Sicherung sensibler Daten einschließt.

Vgl. gerne dazu Handreichung „Stand der Technik“, Teletrust, 2025:
Kapitel 3.2.4 Kryptographische Verfahren und fortfolgende Kapitel.

Was von NIS2 gefordert wird:

Die NIS2-Richtlinie verlangt, dass Unternehmen:

- Kryptografische Verfahren einsetzen, um Daten und Kommunikation zu verschlüsseln
- sowohl bei der Speicherung als auch bei der Übertragung
- Schlüsselmanagement und Zertifikate sicher handhaben,
- und regelmäßig den Stand der Technik prüfen und die eingesetzten Verschlüsselungsverfahren entsprechend aktualisieren.

Ziel:
Die NIS2-Richtlinie will sicherstellen, dass vertrauliche Informationen nicht kompromittiert oder manipuliert werden können – weder durch interne Fehler noch durch externe Angriffe. Kryptografie ist dabei ein zentrales Werkzeug zur Wahrung von Datensicherheit, Datenschutz, Integrität und Authentizität.

Dallmeier Antwort und Unterstützung zu „Kryptografie und Datenverschlüsselung“:

Dallmeier Produkte ermöglichen eine sichere und „trusted“ Kommunikation, d.h. unsere Softwareprodukte ermöglichen eine verschlüsselte Kommunikation und beinhalten kryptografische Prüfverfahren.

- TLS-Verschlüsselung Video- und Daten:
  - TLS 1.3/AES 256 Bit Verschlüsselung
    Der Einsatz einer End-to-End verschlüsselten Video- und Datenübertragung mit TLS 1.3/AES 256 Bit über DaVids und HTTPs bietet höchsten Schutz vor unberechtigtem Zugriff auch innerhalb eines netzwerkbasierten Videosicherheitssystems. Bei dieser Technik handeln die Netzwerkteilnehmer, beispielsweise eine Kamera und ein Aufzeichnungssystem, einen geheimen Schlüssel zur Kodierung der übertragenen Daten aus. Da dieser nur den Endgeräten bekannt ist, kann ein Mitlesen der Video- und Datenübertragung durch andere Netzwerkteilnehmer verhindert werden.

Erklärvideo zur TLS-Verschlüsselung

  - TLS-Verschlüsselung: Dallmeier Webseite
  - TLS-Setup -Verbindungen von Kameras, Recordern und Clients im Netzwerk verschlüsseln und absichern: Handout (PDF)
    - Kryptografie und kryptografische Prüfverfahren:
      - Secure Boot | Signed OS | TrustZone | fTPM
        - Secure Boot – Verifizierter Systemstart:
          Der Startvorgang des Systems beginnt im fest implementierten und unveränderlichen Boot-ROM des Prozessors, dessen Sicherheitsarchitektur auf Arm TrustZone basiert. Jede nachfolgende Softwarekomponente wird durch kryptografische Prüfverfahren verifiziert und validiert, um die Authentizität und Integrität – und damit die Vertrauenswürdigkeit – der gesamten Boot-Kette („Boot Chain“) sicherzustellen.
        - Signed OS – Signierte Firmware:
          Nur von Dallmeier mit einem privaten (geheimen) Schlüssel digital signierte Firmware-Pakete können installiert werden. Beim Start der Kamera oder bei einem Firmware-Update prüft Secure Boot (s. o.) per öffentlichem Schlüssel (fest im Gerat verankert), ob die Firmware authentisch signiert und damit vertrauenswürdig ist. Dieses Verfahren schützt zuverlässig vor modifizierten oder nicht autorisierten Systemdateien. Dies gewährleistet die Integrität der Systemsoftware und verhindert das Einschleusen von manipuliertem Programmcode bzw. unkontrollierten Kamera-Updates (Supply-Chain-Schutz).
        - Arm TrustZone und fTPM – Isolierte Ausführungsumgebung für kritische Sicherheitsfunktionen:
          - Sicherheitskritische Aufgaben werden in einem speziell geschützten Bereich des Prozessors ausgeführt.

- Arm TrustZone ermöglicht dabei eine hardwaregestutzte Trennung des Systems in zwei logisch isolierte und klar voneinander abgegrenzte Ausführungsumgebungen: die Secure World (sichere Umgebung) und die Normal World (normale Umgebung).
- In der Secure World werden besonders sensible Prozesse – etwa kryptografische Operationen wie die Schlüsselverwaltung und Authentifizierungsmechanismen – isoliert verarbeitet, um ein hohes Mas an Sicherheit zu gewährleisten.
- Das integrierte firmwarebasierte Trusted Platform Module (fTPM) emuliert die Funktionen eines dedizierten TPM-Chips (dTPM) – bildet also die Funktionen eines klassischen TPM-Chips softwareseitig nach.
- Dank der isolierten TrustZone-Umgebung können vertrauliche Daten wie kryptografische Schlüssel sicher abgelegt und verarbeitet werden, ganz ohne zusätzliche physische TPM-Hardware.

Sicherheitskomponente	Funktion	Nutzen
Secure Boot	Prüft jede Bootstufe	Verhindert Ausführung von manipuliertem Code
Signed OS	Erzwingt signierte Firmware	Schutz vor Supply-Chain-Angriffen
TrustZone	Getrennte Systemumgebungen	Isolierung sensibler Prozesse in Secure World
fTPM	Hochsicherer Kryptografiespeicher im TrustZone-Kontext	Keine dedizierte TPM-Hardware erforderlich

Genaue Funktionsbeschreibung dieser vier Sicherheitskomponenten siehe gerne Technische Mitteilung Domera OS Version 15.0.0.7

- TPM 2.0 Modul (Chip) (FIPS 140 konform):
  - kryptografischer Sicherheitsstandard vom National Institute of Standards and Technology (NIST) der USA
  - fips: Federal Information Processing Standard Publication 140
  - implementiert in Dallmeier Aufzeichnungs-Appliances
  - implementiert in den neuen Dallmeier Kamera-Serien

Ihr Nutzen

Mit dieser „gesicherten“ und „vertrauenswürdigen“ Trustmechanismen stellt Dallmeier sicher, dass Kunden die NIS2-Anforderungen zu

- Kryptografie und Datenverschlüsselung

effizient und rechtssicher erfüllen.

Das stärkt die Cyberresilienz entlang der gesamten Lieferkette und ermöglicht den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

4.2.8 Meldewesen und Schwachstellenmanagement

Die NIS2-Richtlinie behandelt die Anforderung nach „Meldewesen, Berichtswesen und Schwachstellenmanagement“ an mehreren zentralen Stellen:

- Schwachstellenmanagement

  Artikel 21 Absatz 2 Buchstabe e) nennt ausdrücklich:

  - „Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich der Bewältigung **und Offenlegung von Schwachstellen**.“

- Interne Dokumentations- und Berichtspflichten
  Artikel 21 Absatz 1 verpflichtet Organisationen zu einem umfassenden Cybersicherheits-Risikomanagement, wozu auch die Erfassung, Auswertung und Dokumentation von Vorfällen und Schwachstellen gehört.

- Meldewesen
  Artikel 23 regelt die Berichtspflichten zur Meldung von Sicherheitsvorfällen.

  - Artikel 23 legt fest, dass betroffene Einrichtungen erhebliche Sicherheitsvorfälle unverzüglich an die zuständige nationale Behörde oder das CSIRT melden müssen.

Was NIS2 konkret fordert:

1) Meldewesen & Berichtswesen

- Klare Meldeprozesse und verantwortliche Stellen im Unternehmen definieren
- Einhaltung der Fristen (24h Frühwarnung, 72h erste Bewertung, 1 Monat Abschlussbericht)
- Bereitstellung relevanter technischer Informationen für Behörden/CSIRT

2) Schwachstellenmanagement

- Kontinuierliche Überwachung auf bekannte und neue Schwachstellen
- Patch-Management-Prozesse zur schnellen Behebung
- Verfahren zur koordinierten Offenlegung (Coordinated Vulnerability Disclosure)

3) Interne Auswertung

- Vorfälle und Schwachstellen müssen analysiert, dokumentiert und in Verbesserungsmaßnahmen überführt werden, um Wiederholungen zu vermeiden.

Dallmeier Antwort und Unterstützung zu „Meldewesen und Schwachstellenmanagement“:

Hier ist eine klare Übersicht, wie Dallmeier Hersteller seine Kunden bei den NIS2-Anforderungen rund um Meldewesen, Berichtswesen und Schwachstellenmanagement unterstützt:

- **Zentrale Meldestelle – SIRC & PSIRT**
  Dallmeier betreibt ein eigenes Security Incident Response Centre (SIRC), das als erste Anlaufstelle für alle Meldungen zu Schwachstellen, Sicherheitsvorfällen oder Bedrohungen dient. Das SIRC übernimmt die Steuerung der Untersuchungen, die Kommunikation mit dem Meldenden sowie die Einbindung interner Fachbereiche – inklusive des Product Security Incident Response Teams (PSIRT) und, falls erforderlich, der Datenschutzabteilung.

- **Koordinierte Schwachstellenbearbeitung**
  Sobald eine Schwachstelle bestätigt ist, veröffentlicht Dallmeier einen Sicherheitshinweis, sobald eine Lösung verfügbar ist. In dringenden Fällen wird bereits vor Release eines Updates ein Hinweis mit notwendigen Maßnahmen herausgegeben.

- **Transparenz und Offenlegung**
  Dallmeier verfolgt eine klare Strategie der koordinierten Offenlegung (Coordinated Vulnerability Disclosure), bei der Meldende dazu angehalten werden, potenzielle Schwachstellen nicht voreilig öffentlich zu machen. Zugleich achtet Dallmeier auf die Interessen der Meldenden, indem Informationen vertraulich behandelt werden und keine NDA notwendig ist.

Abgleich mit den NIS2-Anforderungen

NIS2-Anforderung	**Dallmeier-Unterstützung**
Meldewesen & Berichtswesen	Das SIRC sorgt für schnelle, organisierte Bearbeitung von Sicherheitsvorfällen und Schwachstellenmeldungen. Koordinierte Meldeprozesse erleichtern schnelle Reaktion und rechtzeitige Vorfallsmeldungen gemäß NIS-2
Schwachstellenmanagement	PSIRT bearbeitet Schwachstellen Veröffentlichung von Sicherheitshinweisen und Bereitstellung von Lösungen sowie präventive Hinweise bei kritischen Situationen.
Koordinierte Offenlegung	Umsetzung eines CVD-Prozesses, vertrauensvolle Zusammenarbeit ohne NDA, transparente Kommunikation mit Meldenden.

Ihr Nutzen

Mit dieser robusten und proaktiven Sicherheitsinfrastruktur und dem etablierten SIRC/PSIRT-System stellt Dallmeier sicher, dass Kunden die **NIS2-Anforderungen** zu

- Meldewesen und Berichtswesen
- Schwachstellenmanagement

effizient und rechtssicher erfüllen.

Das stärkt die Cyberresilienz entlang der gesamten Lieferkette und unterstützt den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

Link Meldestellen, SIRC & PSIRT:
https://www.dallmeier.com/de/service/cybersecurity-psirt

4.2.9 Datenschutz durch IT-Sicherheit

Die NIS2-Richtlinie ist primär eine Cybersicherheitsrichtlinie und keine Datenschutzverordnung wie die DSGVO.

- Dennoch greift die NIS2 den Datenschutz indirekt auf – immer dann, wenn der Schutz personenbezogener Daten ein Teil der Sicherheit von Netz- und Informationssystemen ist.
- Merksatz: Ohne Datensicherheit auch kein Datenschutz

1) **Artikel 20, insb. Artikel 21 Absatz 1**
   Verpflichtet Unternehmen zu geeigneten und verhältnismäßigen technischen, operativen und organisatorischen Maßnahmen, unter Berücksichtigung des Standes der Technik, zum Schutz der Netz- und Informationssysteme – inkl. dem Schutz personenbezogener Daten.

2) **Artikel 23 Absatz 4**
   Bei der Meldung von Sicherheitsvorfällen müssen Unternehmen den Schutz personenbezogener Daten sicherstellen. Das bedeutet, dass Meldungen an Behörden oder CSIRTs keine unnötigen personenbezogenen Informationen enthalten dürfen, es sei denn, sie sind für die Vorfallbearbeitung erforderlich.

3) **Erwägungsgrund 14 und 51**
   Stellen klar, dass NIS2 **die DSGVO nicht ersetzt**. Die Richtlinie gilt **neben** bestehenden Datenschutzvorschriften und ist komplementär – Cybersicherheitsmaßnahmen dienen damit auch der Erfüllung von Datenschutzpflichten.

Was NIS2 fordert

- **Sicherheitsmaßnahmen** müssen so gestaltet sein, dass **personenbezogene Daten** vor unbefugtem Zugriff, Veränderung, Verlust oder Zerstörung geschützt sind.
- Bei Vorfallmeldungen dürfen nur die notwendigen personenbezogenen Daten übermittelt werden.
- **Koordination mit der DSGVO**: Unternehmen müssen sicherstellen, dass NIS2-Meldungen und DSGVO-Meldungen (Art. 33 DSGVO: 72 Stunden Frist) aufeinander abgestimmt sind.

- **Technische Maßnahmen** wie Verschlüsselung, Zugriffskontrollen und Protokollierung sind einzusetzen, um auch Datenschutzverletzungen zu verhindern.

Kernaussage:
NIS2 schreibt Datenschutz nicht gesondert wie die DSGVO vor, bindet ihn aber in den Kontext der Cybersicherheit ein.

Für NIS2-Einrichtungen bedeutet das, dass Datenschutz (auch) durch IT-Sicherheit erreicht wird.

Nachfolgend eine Übersicht „Schnittstelle NIS2 ⟷ DSGVO" – kompakt, aber mit allen relevanten Überschneidungen zwischen den beiden Regelwerken im Bereich Datenschutz.

Thema	NIS2-Pflicht	DSGVO-Pflicht	Überschneidung / Praxisrelevanz
Schutz personenbezogener Daten	Artikel 21 Abs. 1 – Technische & organisatorische Maßnahmen zum Schutz der Informationssysteme (inkl. personenbezogener Daten)	Artikel 32 – Technische & organisatorische Maßnahmen zum Schutz personenbezogener Daten	Gleiche Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit. Umsetzung z. B. durch Verschlüsselung, Zugriffskontrolle, Monitoring.
Vorfallmeldung	Artikel 23 – Meldung erheblicher Sicherheitsvorfälle an zuständige Behörde/CSIRT	Artikel 33 – Meldung von Datenschutzverletzungen an die Aufsichtsbehörde	Bei Sicherheitsvorfällen, die personenbezogene Daten betreffen, sind **beide Meldungen** nötig. Fristen: NIS2 (24h Frühwarnung, 72h Erstbericht), DSGVO (72h Meldung).
Datensparsamkeit in Meldungen	Artikel 23 Abs. 4 – Meldungen nur mit notwendigen personenbezogenen Daten	Artikel 5 Abs. 1 lit. c – Datenminimierung	In beiden Fällen gilt: Nur relevante Daten melden, Pseudonymisierung/Anonymisierung nutzen, wenn möglich.
Stand der Technik	Artikel 21 Abs. 1 – Maßnahmen müssen Stand der Technik entsprechen	Artikel 32 Abs. 1 – Berücksichtigung von Stand der Technik bei Schutzmaßnahmen	Beide fordern regelmäßige Aktualisierung und Anpassung der Maßnahmen an neue Risiken und Technologien.
Dokumentationspflichten	Artikel 21 – Nachweis über Sicherheitsmaßnahmen und Risikomanagement	Artikel 5 Abs. 2 – Rechenschaftspflicht, Nachweisfähigkeit	Technische und organisatorische Schutzmaßnahmen müssen in beiden Regimen dokumentiert und nachweisbar sein.

Abb.: Übersicht „Schnittstelle NIS2 ⟷ DSGVO

Praxis-Tipp für NIS2-Einrichtungen:

1) **Integrierte Vorfallprozesse:** Einen einheitlichen Incident-Response-Plan erstellen, der beide Meldepflichten (NIS2 & DSGVO) abdeckt.

2) **Gemeinsame Risikobewertung:** Datenschutz- und IT-Sicherheitsrisiken gemeinsam betrachten, statt in getrennten Silos.

3) **Dokumentation bündeln:** Sicherheits- und Datenschutzmaßnahmen in einem zentralen Compliance-Register erfassen.

4) **Schulung kombinieren:** Mitarbeiterschulungen zu IT-Sicherheit mit Datenschutzthemen verbinden.

Dallmeier Antwort und Unterstützung zu „Datenschutz durch IT-Sicherheit":

Dallmeiers Unterstützung Datenschutz
Klare Datenschutzrichtlinien & -transparenz
Dallmeier stellt auf seiner Unternehmenswebsite umfassende Datenschutzerklärungen bereit, die die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO und nationalem Recht offenlegen.
Link: https://www.dallmeier.com/de/datenschutz

1) Sichere Datenschutzprozesse durch Dallmeier ISO 27001

Der Geltungsbereich des ISO/IEC 27001-Zertifikats von Dallmeier umfasst Entwicklung, Betrieb und Support von Soft-, und Hardwarekomponenten für Produkte und Lösungen im Bereich der Videosicherheitstechnik.
Obwohl die ISO 27001 nicht explizit Datenschutz als Hauptziel hat, ist sie dennoch ein wichtiger Baustein für den Datenschutz. Durch die Schaffung einer sicheren Umgebung für Informationen erleichtert ISO 27001 die Einhaltung datenschutzrechtlicher Anforderungen. Die Einhaltung von ISO 27001 trägt bei Dallmeier dazu bei, die technischen und organisatorischen Maßnahmen zu implementieren, die die DSGVO fordert, um personenbezogene Daten sicher zu verarbeiten.

- Ja, die ISO 27001 (auch die von Dallmeier) befasst sich auch mit Datenschutz. Sie ist zwar kein Datenschutz-Zertifikat im Sinne der DSGVO, aber sie hilft, Datenschutzgesetze wie die DSGVO zu erfüllen, indem sie den Schutz von Informationen, einschließlich personenbezogener Daten, gewährleistet.

- Beispiel Dallmeier ISO 27001:
  ISO 27001 Control A.5.34: „Privatsphäre und Schutz personenbezogener Daten (PII)“

Siehe gerne nachfolgende hilfreiche Mapping-Tabelle (Auszug)

NIS2-Mapping-Tabelle auf ISO 27001 - 27002

EU-NIS2 (EU 2022/2555) Anforderungen	**Typische Auditfragen**	**ISO 27001:2022 / ISO 27002:2022** Normkapitel und Controls
Artikel 20 : Governance	Organisation der Informationssicherheit – Wer ist in Ihrem Unternehmen für die Informationssicherheit verantwortlich? – Wie ist die interne Organisation der Informationssicherheit aufgebaut?	5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation A.5.01 Richtlinien zur Informationssicherheit A.5.02 Rollen und Verantwortlichkeiten im Bereich Informationssicherheit A.5.03 Aufgabentrennung A.5.04 Managementverantwortlichkeiten A.5.05 Kontakt mit Behörden A.5.06 Kontakt mit Interessengruppen A.5.31 Gesetzliche, gesetzliche, behördliche und vertragliche Anforderungen A.5.34 Privatsphäre und Schutz personenbezogener Daten (PII) A.5.35 Unabhängige Überprüfung der Informationssicherheit A.5.36 Einhaltung von Richtlinien, Regeln und Standards zur Informationssicherheit

Gesamt-Mappingtabelle Datenschutz: NIS2 – DSGVO – ISO 27001

Thema	NIS2-Pflicht	DSGVO-Pflicht	ISO 27001-Kapitel / Controls
Schutz personenbezogener Daten	Art. 21 Abs. 1 – Schutz von Informationssystemen inkl. personenbezogener Daten	Art. 32 – Schutz personenbezogener Daten	
Vorfallmeldung	Art. 23 – Meldung erheblicher Sicherheitsvorfälle (24h/72h)	Art. 33 – Meldung von Datenschutzverletzungen (72h)	
Datensparsamkeit in Meldungen	Art. 23 Abs. 4 – Nur notwendige personenbezogene Daten	Art. 5 Abs. 1 lit. c – Datenminimierung	
Stand der Technik	Art. 21 Abs. 1 – Maßnahmen nach Stand der Technik	Art. 32 Abs. 1 – Stand der Technik	
Dokumentationspflichten	Art. 21 – Nachweis über Sicherheitsmaßnahmen	Art. 5 Abs. 2 – Rechenschaftspflicht	

A.5.34 Privatsphäre und Schutz personenbezogener Daten (PII)

A.5.07 Bedrohungsinformationen
A.5.24 Planung und Vorbereitung des Informationssicherheitsvorfallmanagements
A.5.25 Bewertung und Entscheidung zu Informationssicherheitsereignissen
A.5.26 Reaktion auf Informationssicherheitsvorfälle
A.5.27 Lernen aus Informationssicherheitsvorfällen
A.5.28 Sammlung von Beweisen
A.6.08 Meldung von Informationssicherheitsereignissen
A8.16 Überwachungsaktivitäten

8.10 Löschen von Informationen...
8.11 Datenmaskierung.....
8.12 Verhinderung von Datenlecks.
A.5.01 Richtlinien zur Informationssicherheit

Die ISO 27001 fordert, dass ein Informationssicherheits-Managementsystem (ISMS) insgesamt auf dem "Stand der Technik" basiert.

In der ISO 27001 werden diese Anforderungen nach Dokumentations-und Rechenschaftspflichten hauptsächlich in den folgenden Bereichen des Anhangs A behandelt: Risikomanagement, Incident Response, Business Continuity und Zugangskontrollen.

2) Datenschutzkonforme Videosicherheitssysteme

Im Bereich Videoüberwachung bietet Dallmeier Produkte mit einem höchsten Maß an technischen Vorkehrungen nach dem von der DSGVO geforderten Prinzip „Privacy by Design“ und „Privacy by Default“, damit Kunden datenschutzkonforme Lösungen einfach implementieren können.

Dallmeier bietet viele Praxisleitfäden, Broschüren und Trainings zum Thema Datenschutz und zu DSGVO-konformer Videotechnik an.

Konkrete Funktionen (Beispiele) zu datenschutzkonformer Videosicherheitstechnik – konkret und wirksam:

- Privacy Shield (Datenschutz-Rollo): Ein ferngesteuertes Rollo – sichtbar und gesetzeskonform, z. B. bei öffentlichen Versammlungen – DSGVO, Versammlungsgesetz und Versammlungsfreiheit im Einklang.
- AI Pixelation für eine automatische Objektverpixelung, Private Zonen und MaxAge (maximale Speicherdauer je Kamera) und viele weitere datenschutzfördernde Dallmeier-Datenschutzfunktionen.
- Standardmäßig deaktivierte Audio-Funktionen in Dallmeier Videosicherheitsprodukten.
- Stärkung Datenschutz auch durch technische Cybersicherheitssicherheitsstandards, die auch NIS2-relevante Aspekte wie Kryptografie, Verschlüsselung, Authentifizierung und Systemresilienz abdecken.
- Weitere Informationen zu Dallmeier Datenschutzlösungen finden Sie auf: https://www.dallmeier.com/de/produkte/datenschutz-datensicherheit

Links: Dallmeier Datenschutzkonforme Videosicherheitssysteme

- Webseite Datenschutz & Datensicherheit
- Broschüre: Videosicherheit, Datenschutz und Datensicherheit
- Onlinepräsentation: Datenschutz und Datensicherheit bei Dallmeier

Ihr Nutzen

Mit unseren innovativen Datenschutzfunktionen, entwickelt nach dem „Privacy by Design“-Prinzip, und den integrierten, geprüften und zertifizierten Datenschutzprozessen innerhalb der ISO 27001 stellt Dallmeier sicher, dass Kunden die **NIS2-Anforderung** zu

- Datenschutz nach Artikel 21 Absatz 1
- Schutz der Netz- und Informationssysteme – inkl. dem Schutz personenbezogener Daten

effizient und rechtssicher erfüllen.

Das stärkt die Cyberresilienz und die Datenschutzkonformität entlang der gesamten Lieferkette und unterstützt den lückenlosen Nachweis der NIS2-Compliance und auch der DSGVO-Compliance gegenüber Aufsichtsbehörden.

4.2.10 Schulungen und Awarenessmaßnahmen (Geschäftsleitung, Mitarbeitende, Kunden)

Die NIS2-Richtlinie greift Schulung, Awareness- und Trainingsmaßnahmen in Artikel 21 Absatz 2 Buchstabe h ausdrücklich auf.

Sie ordnet dies als organisatorische Sicherheitsmaßnahme ein – und zwar für alle Ebenen einer Organisation, vom Management bis zu den operativen Mitarbeitenden.

1) Schulungen für die Geschäftsleitung

- Art. 20 Abs. 1 und 2: Die Geschäftsleitung ist verantwortlich für die Umsetzung der Risikomanagementmaßnahmen und muss regelmäßig an entsprechenden Schulungen teilnehmen.
- Art. 21 Abs. 2 lit. g: Pflicht zur Sensibilisierung und Schulung auch auf Leitungsebene.

Was NIS2 für Geschäftsleitungen fordert:

- Management-Trainings zu Cybersicherheitsrisiken, rechtlichen Pflichten und strategische Verantwortung.
- Verständnis der Haftung: Die Geschäftsleitung haftet persönlich für NIS2-Compliance.
- Fähigkeit, Entscheidungen fundiert zu treffen – z. B. Budgetfreigaben für Security-Maßnahmen, Priorisierung von Investitionen.
- Regelmäßige Auffrischung (nicht nur einmalig).

2) Schulungen für Mitarbeitende

- Art. 21 Abs. 2 lit. g „Maßnahmen zur Schulung in der Cybersicherheit und zur Sensibilisierung der Mitarbeiter im Hinblick auf die Risiken in Bezug auf Netz- und Informationssysteme.“

Was NIS2 für Mitarbeitende fordert:

- Awareness-Trainings für alle Beschäftigten, passend zu ihrer Rolle.
- Rollenspezifische Schulungen: z. B. spezielle Inhalte für Administratoren, Entwickler oder Support-Personal.
- Sensibilisierung für aktuelle Bedrohungen wie Phishing, Social Engineering, Malware.
- Regelmäßige Wiederholungsschulungen (mindestens jährlich).
- Nachweis und Dokumentation der Teilnahme für Audits.

Kernbotschaft für Geschäftsleitungen und Mitarbeitende:

- Für die Geschäftsleitung: Fokus auf strategische und rechtliche Verantwortung, Risikomanagement, Compliance-Entscheidungen.
- Für die Mitarbeiter: Fokus auf tägliche Sicherheitspraktiken, Erkennen und Vermeiden von Risiken.

3) Schulungen für Kunden?

Die NIS2-Richtlinie formuliert ihre Schulungs- und Awarenesspflichten primär für die eigene Organisation (Geschäftsleitung und Mitarbeitende) – aber es gibt indirekte Bezüge, aus denen sich auch eine Pflicht zur Kunden-Schulung ableiten lässt, vor allem wenn ein NIS2-Unternehmen als Hersteller, Anbieter oder Dienstleister sicherheitsrelevante Produkte oder Services liefert.

Direkte NIS2-Referenzen

- Art. 21 Abs. 2 lit. g
  → Verpflichtet „Maßnahmen zur Schulung in der Cybersicherheit und zur Sensibilisierung" einzurichten.

  Zwar bezieht sich der Artikel im Wortlaut auf Mitarbeitende, aber:
  Der Erwägungsgrund 88 betont, dass Informations- und Sensibilisierungsmaßnahmen „alle relevanten Akteure" einschließen können, wenn es der Sicherheit der Netze und Informationssysteme dient.

- Art. 21 Abs. 2 lit. d – Lieferkettensicherheit
  → Verpflichtet Unternehmen, die Sicherheit der Lieferkette zu berücksichtigen. Wenn Kunden Teil dieser Lieferkette sind, kann eine Schulung oder Awareness-Maßnahme notwendig sein, um deren Umgang mit den gelieferten Systemen sicherzustellen.

Indirekte Anforderungen aus NIS2

- Erwägungsgrund 88 & 89
  → Betonen die Bedeutung von Informationsaustausch, Awareness und „capacity building" für alle Beteiligten einer Wertschöpfungskette.

- Art. 20 Abs. 1
  → Geschäftsleitung muss sicherstellen, dass geeignete Maßnahmen ergriffen werden, um Risiken zu minimieren – dazu können auch Kundenschulungen gehören, wenn Fehlbedienung oder Unkenntnis beim Kunden die Sicherheit beeinträchtigen könnte.

Was NIS2 für Kunden fordert:

Für Kundenschulungen gibt es keine explizite, allgemeingültige Schulungspflicht.
Allerdings:

- Wenn unsichere Bedienung durch den Kunden zu Sicherheitsvorfällen führen kann, muss der Hersteller/Dienstleister sicherstellen, dass der Kunde die sicheren Betriebsweisen kennt (z. B. durch Schulungen, Handbücher, Online-Trainings).

- In sensiblen Branchen kann das zur vertraglichen Pflicht werden.

- Awareness-Materialien oder Trainings können ein Teil des Sicherheitskonzepts sein, das im Rahmen von Art. 21 verlangt wird.

Gesamtfazit (Geschäftsleitung, Mitarbeitende, Kunden)

- NIS2 verlangt Schulung und Awareness in erster Linie intern (Geschäftsleitung/Mitarbeitende)

- Für Kunden entsteht die Pflicht indirekt über die Anforderungen an Lieferkettensicherheit und Risikomanagement – wenn das Verhalten des Kunden sicherheitsrelevant ist, muss der Anbieter entsprechende Schulungen oder Informationsmaßnahmen anbieten.

Dallmeier Antwort und Unterstützung zu: „Schulungen und Awarenessmaßnahmen (Geschäftsleitung, Mitarbeitende, Kunden)“

1) Schulungsblickwinkel / Scope

Dallmeier wird ja in diesem Whitepaper als ihr Vorlieferant/Hersteller in ihrer Lieferkette betrachtet. Daher wäre eigentlich nur der „Kunden-Blickwinkel“ „Wie schulen wir sie als unser Kunde“ für sie interessant.

Da wir, wie oben erwähnt, auch eine NIS2-Einrichtung durch das geplante deutsche NIS2-Umsetzungsgesetz werden, möchten wir hier alle 3 Blickwinkel kurz darstellen.

Aber auch ohne gesetzlichen Zwang würden wir auch freiwillig unsere internen IT-Sicherheits-Schulungen für Geschäftsleitung und Mitarbeitende darstellen, denn es gelten folgende Merksätze:

- Sicherheit (auch Schulungssicherheit) beginnt nicht erst beim Kunden, sondern bereits beim Hersteller.
- Für sie als Kunde bedeutet das: Schulungs-Sicherheit² entlang ihrer Lieferkette

2) Dallmeier Schulungen und Awarenessmaßnahmen

Hier ist eine strukturierte Übersicht, wie Dallmeier als Hersteller alle drei Schulungskategorien – für Mitarbeitende, Geschäftsleitung und Kunden – professionell abdeckt und damit NIS2-Konformität unterstützt:

a) Mitarbeitende

Anforderung: Pflichtschulungen für IT-Sicherheit und Datenschutz, basierend auf ISO 27001.
ISO 27001 Controls: A.6.3 – Awareness, Education and Training; A.5.1 – Informationssicherheitsrichtlinien
Dallmeier-Pflichtunterweisungen:
Standardisierte, jährliche Pflichtunterweisungen / Intranet / online Themen: IT- und Cybersicherheit, Datenschutz
Begleitende wichtige ISO27001 Dokumente:
Unternehmensregelung Informationssicherheit Datenschutz, Datenschutz und Datensicherheit, Richtlinien zur Entwicklungssicherheit, Sicherheitsanforderungen an Lieferanten und Dienstleister

b) Geschäftsleitung

Anforderung: Schulungen zur strategischen Cyber- und Datenschutzverantwortung
ISO 27001 Controls: A.6.3 – Awareness, Education and Training; A.5.1 – Informationssicherheitsrichtlinien
Dallmeier interne Pflicht: Schulung Geschäftsleitung nach ISO27001 (und künftig auch nach NIS2)
Dallmeier externes Angebot: Schulung und Awarenesstrainings
Geschäftsleitungen/Führungskräfte über Individualkundentage/-trainings und periodische Kundentage/Partnertage und jährliche „KRITIS-Tage“

c) Kunden

- Sicherheitsrelevante Produkte
  Anforderung: Kunden müssen für einen sicheren Betrieb ihrer Systeme geschult werden.
  Dallmeier-Angebote: „SIT Point” Programme – Onboarding und Trainings für Kunden, um Videosysteme optimal zu nutzen, Partnertage, Kundentage, Webinare, Individualtrainings

- Vertragsgebundene Pflicht
  Anforderung: Schulungen können vertraglich vorgeschrieben sein (z. B. durch KRITIS-Betreiber oder NIS2-Einrichtung).
  Dallmeier-Angebot: 1:1-Talks mit Dallmeier KRITIS-Experte Jürgen Seiler zur NIS2- und KRITIS-Konformität

- Awareness & unterstützende Formate
  Anforderung: Kunden sollen kontinuierlich über Cybersecurity informiert werden.
  Dallmeier-Angebote (Auszüge):

  - Webinar-Serie „Eye on Security“ – 20-minütige Expertensessions zu aktuellen Sicherheitsthemen

    - Beispiel: Video trifft Cybersicherheit: TPM und FIPS erklärt

  - Whitepaper, Praxisleitfäden, Best-Practice Guides, Broschüren sowie Download-Material

    - Datensicherheit und Datenschutz Webseite

    - Download-Centre

      - Sicherheit 1: DIESES WHITEPAPER

      - Sicherheit 2: Praxisleitfaden Videotechnik für KRITIS-Betreiber und NIS2-Einrichtungen (DE/EN)

      - Sicherheit 3: Best Practice Guide: Cybersecurity bei Videosicherheitssystemen

Fazit: Sichere Schulungsprozesse bei Dallmeier nach ISO 27001

Unser ISMS nach ISO27001 beschreibt Schulungsprozesse für alle 3 obigen Blickwinkel verbindlich vor. Diese Schulungsprozesse sind also, wie schon öfter erwähnt, zertifiziert und werden periodisch durch externe Audits geprüft und gegebenenfalls angepasst.

Ebene	NIS2-Artikel / Pflicht	Inhalt & Ziel	ISO/IEC 27001:2022 (Annex A)
Geschäftsleitung	Art. 20 Abs. 1 und 2 – Verantwortung und Haftung der Leitung; Art. 21 Abs. 2 lit. g – Schulungspflicht	Verständnis der NIS2-Pflichten und Haftung; Strategisches Risikomanagement; Budget- und Ressourcenentscheidungen für Cybersicherheit; Integration von Security in Unternehmensstrategie	A.5.1 – Policies for Information Security; A.5.3 – Responsibilities for Information Security; A.6.3 – Awareness, Education and Training
Mitarbeitende	Art. 21 Abs. 2 lit. g – Schulung & Sensibilisierung aller Mitarbeitenden	Grundlegende Cybersicherheitsawareness; Erkennen von Phishing, Social Engineering, Malware; Rollenspezifische Sicherheitsrichtlinien; Meldung von Sicherheitsvorfällen; Datenschutzgerechtes Arbeiten	A.6.3 – Awareness, Education and Training; A.5.2 – Information Security Objectives
Kunden 1 Sicherheitsrelevante Produkte	Indirekter Artikelbezug: Art. 21 Abs. 2 lit. d – Sicherheit der Lieferkette; Erwägungsgrund 88/89 – 'Capacity building' und Informationsweitergabe an alle relevanten Akteure	Kundenschulung – Sicherheitsrelevante Produkte Bsp: Hersteller von Videoüberwachungssystemen schult Kunden, wie Systeme sicher konfiguriert und betrieben werden	A.5.23 – Information security in supplier relationships
Kunden 2 Vertragsgebundene Pflicht	Indirekter Artikelbezug: Kombination aus Art. 21 Abs. 1 (Risikomanagementmaßnahmen) + Lieferkettensicherheit; Risikominimierung	Kundenschulung – Vertragsgebundene Pflicht Bsp: KRITIS-Betreiber oder NIS2-Einrichtung verpflichtet Lieferanten, Schulungen für Betriebspersonal zu organisieren	A.5.23 & A.5.28 – Monitoring and review of supplier services

Überblick in tabellarischer Form

Zielgruppe	Anforderung	ISO 27001 Controls	Angebot von Dallmeier
Mitarbeitende	Pflichtschulungen IT-Sicherheit/Datenschutz	A.6.3; A.5.1	Onboarding- und Technical Training (Level 1–4)
Geschäftsleitung	Strategische Cyber-/Datenschutzverantwortung	A.5.1; A.5.3	Leadership-/Partnertrainings, Partnertage
Kunden – Sicherheit	Sichere Systemkonfiguration	(indirekt A.6.3)	SIT Point Trainings
Kunden – Vertragsbindung	Schulungspflicht durch KRITIS-Vertrag	(gemischt, A.5.x)	1:1 NIS-2/KRITIS-Talks
Kunden – Awareness	Kontinuierliche Sensibilisierung	A.6.3	Webinare („Eye on Security"), Whitepaper, Leitfäden, Praxismaterial

Pflichtschulungen für IT-Sicherheit und Datenschutz, nach ISO 27001.Jährliche Pflichtunterweisungen / Intranet / online

+ Dallmeier Geschäftsleitung

Ihr Nutzen

Mit unseren permanenten, dreidimensionalen Schulungs- und Awarenessangeboten für Mitarbeitende, Geschäftsleitungen und (NIS2-) Kunden, welche zudem geprüft und zertifiziert sind nach ISO 27001, stellt Dallmeier sicher, dass Kunden die direkten NIS2-Anforderungen zu

- Schulungen für Mitarbeitende und Geschäftsleitung
- Indirekte Schulungsanforderung über ihre Pflicht zu Lieferkettensicherheit und Risikomanagement („Wie schulen wir sie als unser Kunde")

effizient und rechtssicher erfüllen.

Das stärkt ihre Cyberresilienz, ihr Cyber Know-how und ihre Cybersicherheitsawareness sowohl intern als auch entlang der gesamten Lieferkette und unterstützt den lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.

4.3 NIS2-konformer Hersteller Dallmeier – Ihr Nutzen

4.3.1 Sanktionen und Bußgelder für NIS2-Einrichtungen – Vermeidung

Die **NIS2-Richtlinie** behandelt *Sanktionen* und Bußgelder in Artikel 34 („Verhängung von Geldbußen") und Artikel 36 („Sanktionen") sowie teilweise in Artikel 31 („Aufsicht und Durchsetzung") und Artikel 32 („Aufsichts- und Durchsetzungsmaßnahmen").

Dort wird festgelegt, dass die Mitgliedstaaten wirksame, verhältnismäßige und abschreckende Sanktionen für Verstöße einführen müssen.

- Artikel 34 Absatz 1:
  Mitgliedstaaten müssen Sanktionen im nationalen Recht verankern, die wirksam, verhältnismäßig und abschreckend sind.

- Artikel 34 Absatz 4:
  Für wesentliche Einrichtungen kann dies Geldbußen von **bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes** bedeuten – je nachdem, welcher Wert höher ist.

- Artikel 34 Absatz 5:
  Für wichtige Einrichtungen beträgt der Rahmen **bis zu 7 Mio. EUR oder 1,4 % des weltweiten Jahresumsatzes** – ebenfalls der höhere Wert.

- Artikel 31 & 32:
  Ergänzende Durchsetzungsmaßnahmen, wie verbindliche Anweisungen, Fristen zur Mängelbeseitigung, Anordnungen zum Stopp bestimmter Tätigkeiten oder zeitweise Suspendierung der Geschäftsführung.

Was NIS2 konkret fordert

- Einführung nationaler Sanktionssysteme durch die EU-Mitgliedstaaten.
- Abschreckende Bußgelder, die sich an der Schwere des Verstoßes und der Unternehmensgröße orientieren.
- Sanktionen gelten sowohl bei:
  - Nichterfüllung der Risikomanagementmaßnahmen (Art. 21 NIS2)
  - Verletzung der Meldepflichten (Art. 23 NIS2)
- Möglichkeit für Behörden, auch *nicht-finanzielle Maßnahmen* zu ergreifen (z. B. öffentliche Rüge, temporäre Untersagung Geschäftsführung).

NIS2-Artikel	Sanktionsart	Höhe / Umfang	Geltungsbereich	Beispiele für Verstöße
Art. 34 (1)	Allgemeine Pflicht zu Sanktionen	Keine feste Höhe in der Richtlinie, nationale Umsetzung erforderlich	Alle Einrichtungen	Mitgliedstaaten müssen „wirksame, verhältnismäßige und abschreckende" Sanktionen einführen
Art. 34 (4)	Geldbußen – wesentliche Einrichtungen	Bis zu **10 Mio. EUR** oder **2 %** des weltweiten Jahresumsatzes (höherer Wert gilt)	Wesentliche Einrichtungen (z. B. große KRITIS-Betreiber)	Keine Umsetzung der Risikomanagementmaßnahmen (Art. 21), Nichteinhaltung der Meldepflichten (Art. 23)
Art. 34 (5)	Geldbußen – wichtige Einrichtungen	Bis zu **7 Mio. EUR** oder **1,4 %** des weltweiten Jahresumsatzes (höherer Wert gilt)	Wichtige Einrichtungen (z. B. mittlere KRITIS-Betreiber)	Verletzung der Meldepflichten, unzureichende Sicherheitsmaßnahmen
Art. 31	Durchsetzungsmaßnahmen	Anweisungen, Fristen, Audits, Verpflichtung zur Umsetzung von Maßnahmen	Alle Einrichtungen	Anordnung zur Schließung einer Sicherheitslücke, verbindliche Umsetzung eines Patches
Art. 32	Vorübergehende Maßnahmen	Suspendierung von Verantwortlichen, temporäre Untersagung von Tätigkeiten	Alle Einrichtungen	Wiederholte oder besonders schwerwiegende Verstöße, die den Betrieb gefährden

Abb.: Sanktionen und Bußgelder nach NIS2

Nationale Umsetzungsgesetze definieren finale Bußgeldvorschriften

Die Mitgliedstaaten sind verpflichtet, die NIS2-Richtlinie in nationales Recht zu überführen. Dabei definieren dann die nationalen Umsetzungsgesetze die finalen, spezifischen Sanktionen und Bußgelder für Verstöße.

Beispiel: Bußgelder in Deutschland

In Deutschland wird die NIS2-Richtlinie durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ umgesetzt. Der Regierungssentwurf vom 25.07.2025 definiert die Bußgelder in Artikel 65. Das Gesetz sieht für besonders wichtige Einrichtungen und Betreiber kritischer Anlagen Bußgelder von bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes bei Verstößen vor. Für wichtige Einrichtungen können Bußgelder von bis zu 7 Millionen Euro oder 1,4% des Jahresumsatzes verhängt werden.

Dallmeier Antwort und Unterstützung zu „Sanktionen und Bußgelder für NIS2-Einrichtungen“:

Durch all die in diesem Dokument, v.a. in Kapitel 4.2. „NIS2-konformer Hersteller Dallmeier“ beschriebenen technischen und organisatorischen Maßnahmen, Produkte, Sicherheitsfunktionen, Zertifizierungen (v.a. ISO 27001) und vielem mehr möchten wir beitragen zu:

- Ihrer Cyberresilienz entlang der gesamten Lieferkette
- Ihrem lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden
- Ihr monetärer Gesamtnutzen: Vermeidung Sanktionen und Bußgelder!

4.3.2 Persönliche Haftung der NIS2-Geschäftsleitung - Vermeidung

Die persönliche Haftung der Geschäftsleitungen wird in der NIS2-Richtlinie ausdrücklich in Artikel 20 („Governance“) und in Artikel 32 Absatz 6 geregelt.

- Art. 20 „Verantwortung des Leitungsorgans / Governance“
    - Das Leitungsorgan (z. B. Vorstand, Geschäftsführung) muss die Umsetzung der Risikomanagementmaßnahmen nach Artikel 21 billigen und deren Umsetzung überwachen.
    - Es muss die notwendige Schulung erhalten, um Risiken für Netz- und Informationssysteme zu verstehen und Risikomanagementmaßnahmen zu bewerten.
    - Mitgliedstaaten müssen Regeln festlegen, um Verantwortliche bei Verstößen haftbar zu machen.
        - Art. 32 Abs 6: Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung dieser Richtlinie haftbar gemacht werden können.

Damit wird die Grundlage für die **persönliche Haftung von Geschäftsleitungen** geschaffen, die dann in nationales Recht (z. B. das deutsche NIS2-Umsetzungsgesetz, siehe Regierungsentwurf, Artikel 38) übertragen wird.

Was fordert NIS2 konkret?

1) **Persönliche Verantwortung:** Geschäftsleiter haften für mangelhafte Umsetzung der Sicherheits- und Meldepflichten.

2) **Nachweisbare Genehmigung:** Sicherheitsstrategien, -budgets und Risikomanagementpläne müssen formell durch die Geschäftsleitung beschlossen sein.

3) **Awareness & Schulungspflicht:** Geschäftsleitung muss regelmäßig geschult werden

    - NIS2 verknüpft hier Artikel 20 Abs.2 mit der Pflicht aus Art. 21 Abs. 2 lit.g

4) **Sanktionsrisiko:** In Verbindung mit Art. 34 drohen hohe Bußgelder (bis zu 10 Mio. € oder 2 % Umsatz) und organisationsrechtliche Maßnahmen (z. B. Abberufung).

Dallmeier Antwort und Unterstützung zu „Persönliche Haftung der NIS2-Geschäftsleitung“:

Durch all die in diesem Dokument, v.a. in Kapitel 4.2. „NIS2-konformer Hersteller Dallmeier“ beschriebenen technischen und organisatorischen Maßnahmen, Produkte, Sicherheitsfunktionen, Zertifizierungen (v.a. ISO 27001) und vielem mehr möchten wir beitragen zu:

- Ihrer Cyberresilienz entlang der gesamten Lieferkette
- Ihrem lückenlosen Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden
- Ihr monetärer Gesamtnutzen: Vermeidung persönliche Haftung der Geschäftsleitung!

4.3.3 Ihr Gesamtnutzen aus der Zusammenarbeit mit Dallmeier

Als Hersteller von Videoüberwachungslösungen tragen wir die Mit-Verantwortung für die Cybersicherheit unserer (NIS2-) Kunden durch die Cybersicherheit unserer Produkte.

Denn Cybersecurity beginnt nicht erst beim Anwender und Kunden, sondern bereits beim Hersteller.

Oder andersrum ausgedrückt: Cybersecurity endet nicht am Netzwerkperimeter der NIS2-Einrichtung – sie beginnt heute mit der Auswahl, Prüfung und Steuerung externer Dienstleister und Hersteller.

Wir helfen unseren Kunden, das sogenannte „Kuckucksei-Problem“ zu lösen: Unsichere Vorprodukte gefährden die gesamte Sicherheitskette und damit die Gesamtsicherheit der Kunden.

Unsere Systeme und Prozesse sind darauf ausgerichtet, den gestiegenen Anforderungen, seien diese aus der realen, angespannten Sicherheitslage oder aus Regulierungen wie der NIS-2 bedingt, gerecht zu werden – mit besonderem Fokus auf Cybersicherheit, Lieferkettensicherheit, Datenschutz und den „Stand der Technik“.

Dallmeier geht dabei weit über die Mindestanforderungen der NIS-2-Richtlinie hinaus. Durch ISO 27001-Zertifizierung, Security- & Privacy-by-Design, umfassende Update-Strategien, Notfall-Teams (SIRC/PSIRT) und Made-in-Europe-Produktion wird eine belastbare, vertrauenswürdige und compliant-fähige Lieferkette sichergestellt.

Damit profitieren sie als NIS-2-betroffene Einrichtung von einem Partner, der nicht nur Produkte liefert – sondern Sicherheit in ihrer gesamten Wertschöpfungskette.

Dallmeier setzt gezielt technische und organisatorische Funktionen ein, um seine eigene und ihre NIS-2-Konformität als Kunden entlang der gesamten Lieferkette sicherzustellen.

Unser zertifiziertes, internes ISMS nach ISO 27001 garantiert dabei sowohl Vertrauen und Verbindlichkeit als auch geprüfte Sicherheit mit Nachweis in unseren Prozessen und Produkten.

Videosicherheit und Cybersecurity „Made in Germany“, „Made by Dallmeier electronic“.

Was sich für Anwender von Videoüberwachungstechnologie ableiten lässt, lässt sich eigentlich ganz einfach auf drei Punkte reduzieren:

- Wenn Kunden die Sicherheit in der gesamten Lieferkette gewährleisten und garantieren, dass die physischen und Cybersicherheitslösungen auf dem neuesten Stand der Technik sind, ist schon viel erreicht.
- Mit unserer konsequenten geopolitischen Strategie „Made in Germany“, die sich seit vier Jahrzehnten bewährt hat, bieten wir unseren Anwendern zuverlässige Antworten und Mehrwerte auf diese Fragen.
- Sehen sie die NIS-2-Regulierung nicht als bürokratische Bürde, sondern als rahmengebende Chance, sich proaktiv gegen die wachsenden Cyberbedrohungen abzusichern.

Thomas Dallmeier, CEO bei Dallmeier electronic

4.4. Weiterführende Links & Downloads & Angebot

- Praxisleitfaden: Cybersichere Videotechnik für KRITIS-Betreiber und NIS2-Einrichtungen (DE/EN)
- Best-Practice Guide: Cybersichere Videoüberwachung
- Broschüre: Videosicherheit, Datenschutz und Datensicherheit
- Onlinepräsentation: Datenschutz und Datensicherheit bei Dallmeier
- Blogartikel: CRA, CE und NIS-2: Was bedeutet digitale Resilienz und Cybersecurity über die gesamte Liefer- und Wertschöpfungskette hinweg?
- Blogartikel: Praxistipp: Wie Sie die Sicherheit Ihres Videosystems erhöhen
- Angebot: Kostenloses 30-minütiges 1:1 - Fachgespräch (online)

Bereit für ein NIS-2-konformes Videoüberwachungsprojekt?

Planen Sie ein Videoüberwachungsprojekt und sind unsicher, wie NIS-2 und das KRITIS-Dachgesetz (geplante Umsetzung der RCE-Richtlinie in Deutschland) zu berücksichtigen sind?

Sichern Sie sich Ihren Termin für einen kostenlosen 30-minütigen 1:1 -Talk (online) mit unserem KRITIS-Experten Jürgen Seiler – fundiert und praxisnah.

Letzter Tipp „Compliance-Durchblick behalten“:

Compliance-Durchblick behalten und pragmatisch loslegen
Die Anforderungen einiger EU-Regularien überschneiden sich. Wer hier genau hinschaut, kann Synergien nutzen und seine Compliance effizienter einhalten. Dazu empfehlen wir:

- Hilfreicher Online-Artikel auf Computerwoche.de von Juni 2025:
  Wie Sie den Compliance-Durchblick behalten
- Bitkom Diskussionspapier von April 2025:
  Digitalgesetzgebung der EU: Konfliktzonen und Wege zur Kohärenz

Ich hoffe, dieses Whitepaper ist hilfreich und unterstützt sie wirkungsvoll bei ihrer NIS-2-Compliance und der Umsetzung ihres NIS-2-konformen Videoüberwachungsprojektes. Gerne mit Dallmeier an ihrer Seite.

ANHANG 1

Ihre Nutzenbetrachtung aus verschiedenen Blickwinkeln (technisch, organisatorisch, monetär, etc.)

Nutzentabelle 1:
NIS2-Einzelanforderungen (Kunde) gespiegelt an Dallmeier ISO 27001-Prozessen

NIS2-Anforderung	NIS2-Richtlinie (EU)	NIS2 in DE	Dallmeier als Vorlieferant/ Hersteller	Dallmeier ISO 27001 (Normkapitel/Controls)	Nutzen für NIS2-Kunde
Stand der Technik	Art. 21 (1) EG 85	§ 30	✓	ISO 27001 = technologieneutral ISO als Grundlage für Stand der Technik in der IT-Sicherheit (Handreichung TeleTrust) + Stand der Technik Videoüberwachungstechnik + Hinweis (*): Dallmeier erfüllt	(1) Cyberresilienz entlang der gesamten Lieferkette
Security by Design	Art. 21 (2) e)	§ 30	✓	A.5.20, A.5.24, A.5.36, 5.37,A.6.08, A.8.09, A.8.19, A.8.20,A.8.21	(2) Nachweis der NIS2-Compliance gegenüber Aufsichtsbehörden.
Sicherheit der Lieferkette	Art. 21 (2) d) & 21 (3)	§ 30	✓	A.5.19, A.5.20, A.5.21, A.5.22, A.5.23	
Sicherheit der Integrationskette	Art. 21 (2) d) und e)	§ 30	✓	A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.5.24, A.5.36, 5.37, A.6.08, A.8.09, A.8.19, A.8.20, A.8.21	(3) Vermeidung Ausfallkosten durch stabile Business Continuity
Regelmäßige Updates und Patches	Art. 21 (2) e) und g)	§ 30	✓	A.5.35, A.5.36, A.5.07, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.08, A.8.16	
Authentifizierung und Autorisierung	Art. 21 (2) i) und j)	§ 30	✓	A.5.12, A.5.13, A.5.14, A.5.15, A.5.16, A.5.17,A.5.18, A.8.01, A.8.02,A.8.03	
Kryptografie und Datenverschlüsselung	Art. 21 (2) f)	§ 30	✓	A.8.20, A.8.21, A.8.22, A.8.24	(4) Vermeidung Bußgeld für Einrichtung
Meldewesen und Schwachstellenmanagement	Art. 21 (2) e)	§ 30	✓	A.5.07, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.08, A8.07, A8.08, A8.15, A8.16	
Datenschutz durch IT-Sicherheit	Ableitung aus Art. 20, Art 21 (1), Art.23 (4), EG 14 und 51	§ 30	✓	insbesondere: A.5.34 Privatsphäre und Schutz personenbezogener Daten (PII)	(5) Vermeidung persönliche Haftung Geschäftsleitung
Schulungen und Awarenessmaßnahmen	Art. 20 (1) und (2), Art. 21 (2) d) und g); EG 88 und 89	§ 30	✓	A.5.1, A. 5.2, A.5.3, A.6.3, A. 5.23, A.5.28	

EG: Erwägungsgrund

Hinweis (*)
Es gibt keine Stelle in der ISO 27001 oder in einem Gesetz, die pauschal und verbindlich sagt:
„Wer ISO 27001 erfüllt, erfüllt automatisch den Stand der Technik."

Warum nicht?

- ISO 27001 ist eine internationale Managementnorm für Informationssicherheits-Managementsysteme (ISMS).
- Sie definiert Prozesse und Kontrollen, aber sie ist technologieneutral und sagt nicht, welche konkreten Sicherheitsmaßnahmen „Stand der Technik" sind.

Wo kommt der Bezug ISO 27001 ⟷ „Stand der Technik" her?

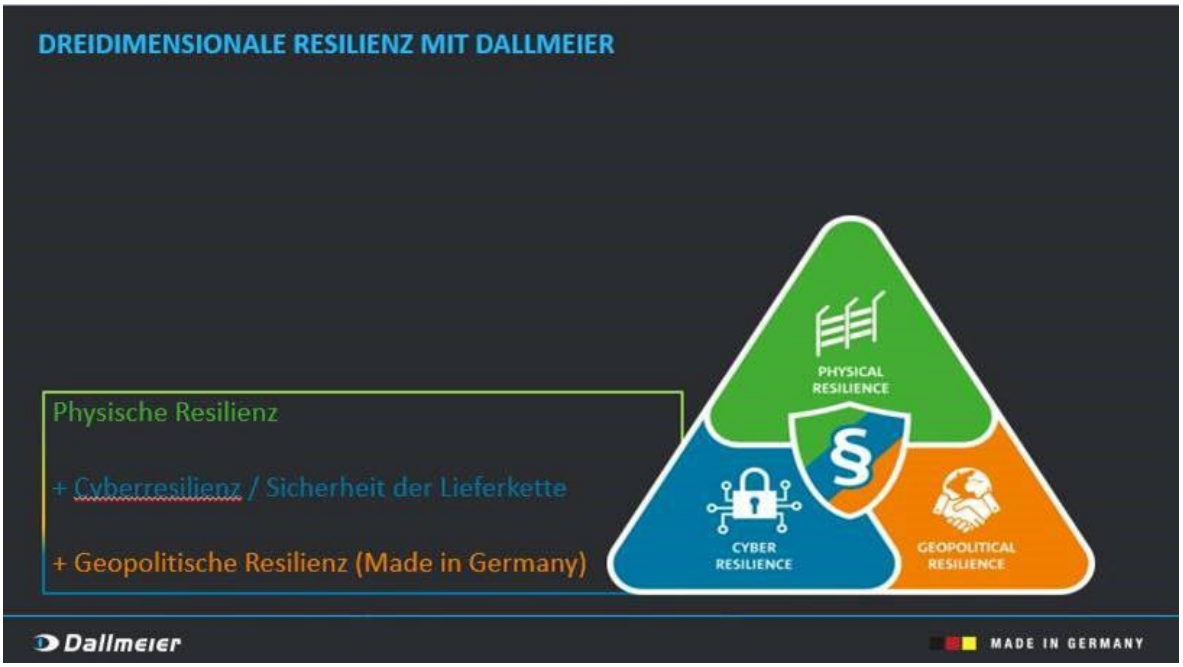
- Behörden wie das BSI oder auch Datenschutzaufsichtsbehörden sagen häufig:
  Die Einführung eines ISMS nach ISO 27001 unterstützt die Einhaltung des Standes der Technik, weil die Norm systematisch Sicherheitsrisiken erfasst und geeignete Maßnahmen auswählt.
- In der Praxis wird ISO 27001 oft als Nachweis akzeptiert, dass man organisatorisch und prozessual Stand der Technik-orientiert arbeitet.
- ISO 27001 allein = gute Grundlage, erfüllt aber nicht automatisch „Stand der Technik".
- Kombination ISO 27001 + aktuelle technische Sicherheitsstandards = starker Nachweis.

Bezug ISO 27001 zu NIS-2:

Thema	ISO 27001	NIS 2
ISMS / systematischer Sicherheitsansatz	✅	✅ (implizit gefordert)
Risikomanagement	✅	✅
Technische & organisatorische Maßnahmen (z. B. Zugriffs-kontrolle, Kryptografie)	✅	✅
Business Continuity / Notfallmanagement	Teilweise	✅ explizit
Lieferketten- und Drittrisiken	Teilweise	✅ stärker betont
Incident-Management	✅ (Prozesse)	✅ inkl. **fester Meldefristen** (24h/72h/1 Monat)
Governance & Verantwortlich-keit der Geschäftsleitung	Teilweise	✅ deutlich konkreter
Rechtliche Compliance & behördliche Zusammenarbeit	Teilweise	✅ sehr konkret

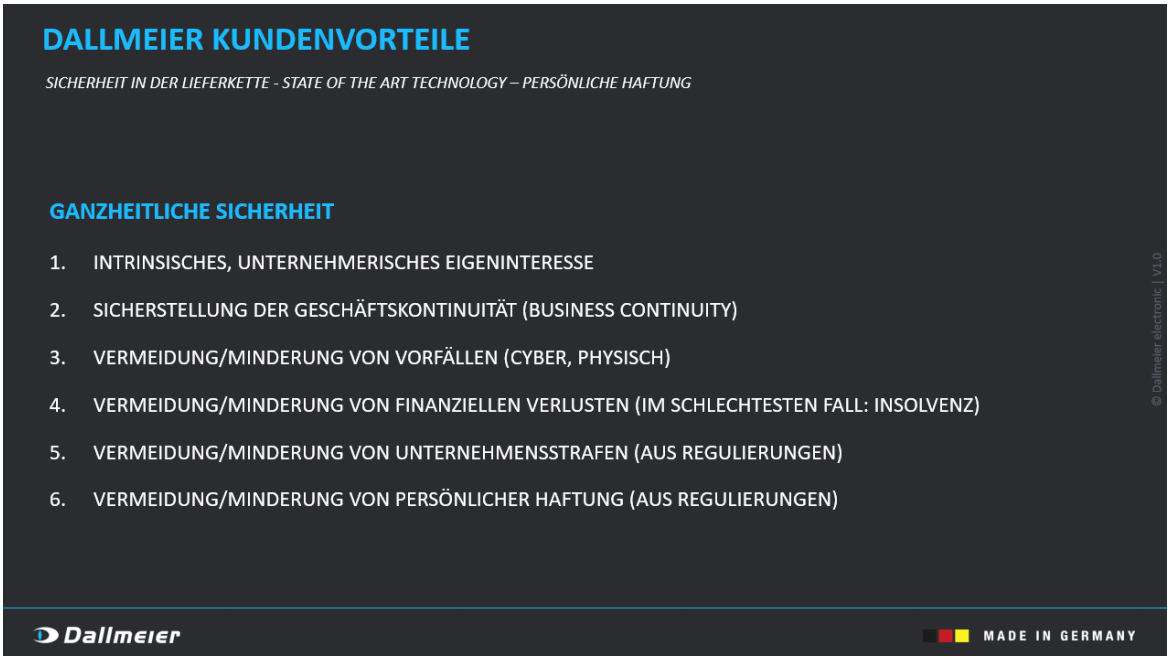
Nutzentabelle 2:

Dallmeier als Geschäftspartner für dreidimensionale Resilienz



Nutzentabelle 3:

Dallmeier als Geschäftspartner für ganzheitliche Sicherheit



ANHANG 2

	KRITIS-RECHTSRAHMEN Europa und Beispiel Deutschland			
EU Richtlinie Kurzform	**EU RCE**	**EU NIS2**		
Regulierungs-bereiche	Regelwerk für Resilienz und physische Sicherheit	Regelwerk für IT-Sicherheit und Cybersicherheit		
Offizielle Kennnummer:	RICHTLINIE (EU) 2022/2557	RICHTLINIE (EU) 2022/2555		
Bezeichnung:	RESILIENCE CRITICAL ENTITIES Resilienz kritischer Einrichtungen	Netz-und Informations Sicherheit „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union"		
in Kraft seit:	Januar 2023	Januar 2023		
EU-Länder	Umsetzung Richtlinie in nationales Gesetz bis 10_2024	Umsetzung Richtlinie in nationales Gesetz bis 10_2024		
Gesetz(e) Deutschland:	KRITIS-Dachgesetz	NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) ⬇ BSI-Gesetz		
Ziele und Inhalte:	• Resilienz • Physische Sicherheit (u.a durch Videoüberwachung) • Business Continuity (BCM) • Risikomanagement	• Cybersicherheit • IT-Sicherheit • Sicherheit in der Lieferkette • Risikomanagement		
Risiko-und Resilienz-maßnahmen (Video)	• geeignete und verhält. TOM • angemessener phys.Schutz • Stand der Technik	• geeignete und verhält. TOM • Sicherheit der Lieferkette • Stand der Technik		
Betroffenheit in Deutschland **WER?**	• **Betreiber kritischer Anlagen** • **Geltungsbereich: Anlagen** • 11 Sektoren (*)	• **Betreiber kritischer Anlagen** (siehe links) **UND:** • **Besonders wichtige Einrichtungen** • **Wichtige Einrichtungen** • **Geltungsbereich: Unternehmen** • Insgesamt 18 Sektoren (**)		
WER Anzahl Bsp: Deutschland	• 2000	• 2000 + 6000 + 22000 = 30000		
Größenklassen	• Größenklassen nach: - technischen Schwellenwerten • Erbringung „kritische Dienstleistung"	• Größenklassen nach: - Mitarbeiteranzahl ODER - Umsatz und Bilanzsumme • Großunternehmen: > 250 MA ODER > 50 Mio | 43 Mio • Mittlere Unternehmen: > 50 MA ODER > 10 Mio | 10 Mio		
Sektoren	**(*) Sektoren der:** **Betreiber kritischer Anlagen:**	**(**) Sektoren der:** **Einrichtungen / Unternehmen nach NIS2:**		
		Sektoren hohe Kritikalität 1	**Sonstige kritische Sektoren** 2	
		= Anhang 1 (NIS2)	= Anhang 2 (NIS2)	
	• Energie • Transport und Verkehr • Finanz-/Versicherungswesen • Gesundheitswesen • Trinkwasser • Abwasser • Ernährung • ITK/Digitale Infrastruktur • Siedlungsabfallentsorgung • Weltraum (Neu) • Bundesverwaltung	• Energie • Transport/Verkehr • Finanz/Versicherung • Gesundheitswesen • Trinkwasser • Abwasser • ITK/Digitale Infrastruktur • Öffentliche Verwaltung • Weltraum	• Post und Kurier • Chemie • Verarbeitendes Gewerbe / Herstellende Industrie • Ernährung • Siedlungsabfall-entsorgung • Digitale Dienste • Forschung	
WER ganz genau in Deutschland betroffen?	• definiert in der Verordnung zur Bestimmung Kritischer Infrastrukturen, Kritisverordnung KritisV	**Einrichtung**	**Sektoren**	**Größe**
		Besonders wichtig	1	Großunternehmen
		Wichtig	1	Mittlere Unternehmen
			2	Großunternehmen Mittlere Unternehmen

Tabelle:

NIS-2-Richtlinie und RCE-Richtlinie | Cybersicherheit und Physische Sicherheit gehören zusammen („Kohärenz")
Rechtsrahmen Europa und Beispiel geplante Umsetzung Deutschland

Über Dallmeier

Dallmeier: Turn Images Into Assets.
Mit wegweisender Videotechnologie aus Deutschland.

Im Jahr 1984 gründete Dieter Dallmeier die heutige Dallmeier electronic GmbH & Co. KG – nicht in der sprichwörtlichen Garage, aber immerhin in einem Gartenhaus in Regensburg. Heute hat das Unternehmen, das sich mit Fug und Recht als Hidden Champion für Videoinformationstechnologie „Made in Germany" bezeichnen darf, weltweit mehrere Hundert Mitarbeitende, davon über 250 allein am Unternehmenssitz in der Regensburger Innenstadt.

Unsere Kunden: Vom Gewerbebetrieb bis zum WM-Stadion

Die Kamera-, Aufzeichnungs-, Software- und Analyselösungen von Dallmeier optimieren Sicherheit und Prozesse bei B2B-Endkunden in den unterschiedlichsten Branchen in über 60 Ländern. Schwerpunktmäßig sind dies Anwender aus den Bereichen Casino, Safe & Smart City, Flughäfen, Logistik, Stadien und Industrie. Aber auch Banken, Einrichtungen der kritischen Infrastruktur (KRITIS) sowie mittelständische Unternehmen aus allen Bereichen gehören zum Kundenkreis.

Niedrige Gesamtbetriebskosten „Made in Germany"

Mit wegweisenden Innovationen gelingt es Dallmeier immer wieder, sich technologisch an die Spitze zu setzen: Vom weltweit ersten Digitalen Bildspeicher mit Bewegungsanalyse im Jahr 1992 über die patentierte „Multifocal-Sensortechnologie" Panomera® mit ihrem „Mountera®" Montagesystem bis hin zur Domera® Kamerafamilie, die bis zu 300 Kameravarianten mit nur 18 Komponenten ermöglicht. Diese und viele weitere Innovationen stiften echten Kundennutzen und können mit ihrem dadurch niedrigen Total Cost of Ownership (TCO) und hohem Return on Investment (ROI) problemlos mit Systemen aus Niedriglohnländern konkurrieren.

Cybersecurity, Datenschutz und ethische Verantwortung durch maximale Fertigungstiefe

Durch 100 % „Made in Germany" garantieren wir unseren Kunden zudem allerhöchste Standards bei den Themen Datenschutz, Cybersecurity und ethischer Verantwortung. Mit hoher Qualität und kurzen Lieferketten sorgen wir – quasi nebenbei – auch noch für Nachhaltigkeit und Umweltschutz. In dem prominenten Gebäude direkt neben dem Regensburger Hauptbahnhof erfolgt deshalb nicht nur die gesamte Entwicklung, sondern auch die komplette Fertigung der Produkte.

www.dallmeier.com

www.panomera.com

Jürgen Seiler, Head of Business Development
Dallmeier electronic GmbH & Co.KG

Juergen.Seiler@dallmeier.com +49 941 8700-0

Dallmeier electronic GmbH & Co.KG

Bahnhofstr. 16
93047 Regensburg
Deutschland

Tel: +49 941 8700-0

info@dallmeier.com