Stand: November 2026

FACHHANDBUCH

KRITIS & PHYSISCHE SICHERHEIT

Videoüberwachung & Videoaufschaltung

für KRITIS-relevante Einrichtungen

FACHPORTALE UND MARKEN VON SECUCONCEPT

Rechtsrahmen KRITIS-Dachgesetz & NIS-2 / BSIG · DSGVO-konforme Umsetzung
Technik & Normen · Alarmverifikation über Notruf- und Serviceleitstelle
Kostenbeispiele & Wirtschaftlichkeit · Checklisten für Betreiber

Qualität durch Vertrauen

SecuConCept · Security – Consulting – Conception · www.secuconcept.de 0800 666 000 4 · vertrieb@secuconcept.de

ZU DIESEM HANDBUCH

Physischer Schutz ist Pflicht – und planbar

Mit dem KRITIS-Dachgesetz (in Kraft seit 17. März 2026) ist der physische Schutz kritischer Anlagen erstmals sektorübergreifend gesetzlich geregelt. Parallel gilt seit 6. Dezember 2025 das neu gefasste BSI-Gesetz zur Umsetzung der NIS-2-Richtlinie. Videoüberwachung mit professioneller Aufschaltung auf eine Notruf- und Serviceleitstelle (NSL) ist eines der wirksamsten Instrumente, um Perimeter, Zufahrten und unbesetzte Außenanlagen rund um die Uhr zu sichern – vorausgesetzt, Technik, Abläufe und Datenschutz greifen sauber ineinander.

Dieses Handbuch richtet sich an Geschäftsführungen, Security- und Facility-Management, technische Leitungen, Einkauf sowie Bau- und Projektleitungen in Energie, Wasser, Gesundheit, Transport, Logistik und weiteren schutzbedürftigen Bereichen. Es bündelt Rechtsrahmen, Normen, Datenschutzanforderungen, Kostenbeispiele und Checklisten in einem Dokument.

Inhalt

1 Auf einen Blick . . . 3
2 Rechtsrahmen KRITIS 2026 . . . 4
3 Videoüberwachung im Resilienzkonzept . . . 7
4 Technik, Normen und Cybersicherheit . . . 9
5 Videoaufschaltung auf die Leitstelle . . . 11
6 Datenschutz und DSGVO . . . 13
7 Kostenbeispiele und Wirtschaftlichkeit . . . 15
8 Projekt-Checkliste für Betreiber . . . 17
9 Häufige Fragen (FAQ) . . . 18
10 Ihr Partner für KRITIS-Sicherheit . . . 19
11 Quellen, Normen und Rechtsstand . . . 20

KERNAUSSAGEN FÜR ENTSCHEIDER

01 Auf einen Blick

Die zehn wichtigsten Fakten für Betreiber kritischer Anlagen, die Videoüberwachung und Videoaufschaltung planen oder modernisieren.

1	**KRITIS-Dachgesetz gilt seit 17.03.2026** (BGBl. 2026 I Nr. 66). Es regelt den physischen Schutz und die Resilienz kritischer Anlagen in zehn Sektoren.
2	**Konkrete Pflichten hängen an der KRITIS-Verordnung.** Schwellenwerte und Stichtage legt eine Rechtsverordnung des BMI fest; Referentenentwurf seit 26.05.2026. Die ursprüngliche Registrierungsfrist 17.07.2026 wurde gestrichen.
3	**§ 13 KRITISDachG nennt ausdrücklich** Liegenschaftsabgrenzungen, Instrumente zur Überwachung der Umgebung, Detektionsgeräte und Zugangskontrollen – das Kernfeld der Videoüberwachung.
4	**Vorfälle sind binnen 24 Stunden zu melden** (§ 18 KRITISDachG); ein ausführlicher Bericht folgt spätestens nach einem Monat. Lückenlose Videodokumentation erleichtert beides.
5	**Die Geschäftsleitung haftet** für Umsetzung und Überwachung der Resilienzmaßnahmen (§ 20 KRITISDachG).
6	**NIS-2 / BSIG seit 06.12.2025:** Netzwerkkameras, Rekorder und Videomanagement sind IT-Systeme und gehören in das Risikomanagement nach § 30 BSIG.
7	**Datenschutz bleibt voll anwendbar:** KRITIS-Status begründet ein starkes berechtigtes Interesse, ersetzt aber weder Interessenabwägung, Transparenz noch Datenschutz-Folgenabschätzung.
8	**Aufschaltung statt reiner Aufzeichnung:** Erst die Live-Verifikation in einer NSL nach DIN EN 50518 macht aus Bildern eine Reaktion – mit definierter Interventionskette.
9	**Planung nach DIN EN 62676-4:** Schutzziel je Kamera (Detektieren, Erkennen, Identifizieren) bestimmt Auflösung, Objektiv und Standort.
10	**Wirtschaftlich:** Eine aufgeschaltete Perimeterlösung kostet je nach Objekt oft nur einen Bruchteil einer 24/7-Präsenzbewachung – ersetzt sie aber nicht in jedem Szenario (siehe Kapitel 7).

Wichtiger Hinweis zur Rechtsverbindlichkeit

Dieses Handbuch ist eine fachliche Orientierung und ersetzt keine Rechtsberatung. Gesetzeslage, Verordnungen und behördliche Auslegungen ändern sich – insbesondere die noch ausstehende KRITIS-Verordnung zum KRITIS-Dachgesetz. Rechtsstand der Recherche: November 2026. Prüfen Sie vor Entscheidungen den aktuellen Stand bei BBK, BSI und Ihrer Datenschutzaufsicht und binden Sie Ihren Datenschutzbeauftragten sowie ggf. Rechtsberatung ein. Alle Kostenangaben sind unverbindliche Orientierungswerte (netto) und ersetzen kein objektbezogenes Angebot.

KRITIS-DACHGESETZ · BSIG / NIS-2 · ZUSAMMENSPIEL

02 Rechtsrahmen KRITIS 2026

Für Betreiber kritischer Anlagen greifen zwei Regelwerke ineinander: das KRITIS-Dachgesetz für die physische Resilienz und das BSI-Gesetz für die Cybersicherheit. Videoüberwachungssysteme liegen genau an der Schnittstelle.

2.1 KRITIS-Dachgesetz (KRITISDachG)

Das Gesetz setzt die EU-Richtlinie (EU) 2022/2557 (CER-Richtlinie) um. Der Bundestag beschloss es am 29.01.2026, der Bundesrat stimmte am 06.03.2026 zu; verkündet wurde es am 16.03.2026, in Kraft ist es seit 17.03.2026.

Erfasste Sektoren (§ 4 i. V. m. Anlage 1)

Sektoren nach KRITISDachG	
Energie	Transport und Verkehr
Wasser	Gesundheitswesen
Ernährung	Finanzwesen [1]
Informationstechnik und Telekommunikation [1]	Weltraum
Siedlungsabfallentsorgung [2]	Sozialversicherung und Grundsicherung [2]

[1] Für IT/TK sowie Finanzunternehmen (DORA) entfallen Risikoanalyse-, Resilienz-, Nachweis- und Meldepflichten weitgehend, da Spezialregelungen greifen. [2] Hier bleibt im Wesentlichen die Pflicht zur Risikoanalyse. Als Regel-Schwellenwert gilt eine Versorgung von rund 500.000 Menschen; maßgeblich sind die sektorspezifischen Werte der KRITIS-Verordnung.

Pflichten und Fristen für Betreiber

Pflicht	Rechtsgrundlage	Frist (ab Einstufung als kritisch)
Registrierung beim BBK (gemeinsames Portal BBK/BSI)	§ 8	spätestens 3 Monate
Risikoanalyse und -bewertung	§ 12	nach 9 Monaten; danach bei Bedarf, mind. alle 4 Jahre
Resilienzmaßnahmen und Resilienzplan	§ 13	nach 10 Monaten
Meldung erheblicher Vorfälle	§ 18	binnen 24 h; ausführlicher Bericht binnen 1 Monat
Umsetzungs- und Überwachungspflicht der Geschäftsleitung	§ 20	nach 10 Monaten
Bußgelder	§ 24	gestaffelt, bis zu 1 Mio. €

Aktueller Stand (November 2026)

Die starre Registrierungsfrist zum 17.07.2026 wurde durch Gesetz vom 21.07.2026 (BGBl. 2026 I Nr. 221) gestrichen. Nach Auskunft des BBK besteht derzeit keine Registrierungspflicht, solange die KRITIS-Verordnung nicht in Kraft ist. **Empfehlung:** Die Fristen laufen nach Inkrafttreten sehr kurz. Wer Risikoanalyse und Schutzkonzept jetzt vorbereitet, vermeidet Beschaffungsengpässe und Zeitdruck bei Ausschreibung, Genehmigung und Montage.

§ 13 KRITISDachG – Resilienzmaßnahmen mit Bezug zur Videoüberwachung

§ 13 verpflichtet Betreiber zu geeigneten und verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen. Ziel ist unter anderem ein angemessener physischer Schutz der Liegenschaften. Abs. 3 nennt beispielhaft:

- Objektschutz durch **Liegenschaftsabgrenzungen** (Zäune, Barrieren)
- **Instrumente und Verfahren zur Überwachung der Umgebung** – hierunter fällt Videoüberwachung einschließlich Perimeterdetektion
- **Detektionsgeräte** und **Zugangskontrollen**
- festgelegte **Alarm- und Reaktionsabläufe**, Personalsicherheitsmanagement, Schulungen und Übungen – ausdrücklich auch für Personal externer Dienstleister (Abs. 3 Nr. 5)

Die Erwägungen hinter der Maßnahmenauswahl müssen nachvollziehbar dokumentiert sein (§ 13 Abs. 4). Ein schriftliches Sicherheitskonzept mit Schutzzielen, Gefährdungsanalyse und Begründung je Kamera ist daher nicht nur Datenschutz-, sondern auch KRITIS-Nachweis.

2.2 BSI-Gesetz nach NIS-2 (NIS2UmsuCG)

Das NIS-2-Umsetzungsgesetz hat das BSIG neu gefasst und gilt seit 06.12.2025 ohne Übergangsfrist. Rund 29.500 Unternehmen fallen als „wichtige“ oder „besonders wichtige Einrichtungen“ (§ 28 BSIG) unter die Aufsicht des BSI. Die reguläre Registrierungsfrist endete am 06.03.2026, die vom BSI eingeräumte Nachfrist am 31.07.2026; eine Registrierung ist weiterhin nachzuholen.

- **§ 30 BSIG – Risikomanagement:** Mindestkatalog von zehn Maßnahmen, u. a. Sicherheit in Beschaffung und Wartung, Zugriffskontrolle, Kryptografie, Lieferkettensicherheit. Videoanlagen, Kameras und VMS sind Teil dieses Geltungsbereichs.
- **§ 32 BSIG – Meldepflichten:** Frühwarnung binnen 24 h, Meldung binnen 72 h, Abschlussbericht binnen eines Monats.
- **§ 38 BSIG – Geschäftsleitung:** Billigung und Überwachung der Maßnahmen, Schulungspflicht, persönliche Haftung.
- **§ 41 BSIG – kritische Komponenten:** Das BMI kann den Einsatz bestimmter Komponenten untersagen, etwa bei Kontrolle des Herstellers durch einen Drittstaat. Herstellerauswahl ist damit auch eine Compliance-Frage (siehe Kapitel 4.3).
- **§ 65 BSIG – Bußgelder:** bis 10 Mio. € oder 2 % des weltweiten Jahresumsatzes (besonders wichtige Einrichtungen).

2.3 Weitere relevante Vorschriften

Regelwerk	Relevanz für Video & Aufschaltung
DSGVO / BDSG / Landesdatenschutzgesetze	Zulässigkeit, Transparenz, Speicherfristen, DSFA – siehe Kapitel 6
§ 34a GewO, Bewachungsverordnung	Erlaubnis- und Qualifikationspflicht für Bewachungs- und Interventionspersonal
§ 201 StGB	Verbot heimlicher Tonaufnahmen – Kameras ohne Audioaufzeichnung betreiben
§ 87 Abs. 1 Nr. 6 BetrVG	Mitbestimmung des Betriebsrats bei technischen Überwachungseinrichtungen
EU-KI-Verordnung (EU) 2024/1689	Einschränkungen biometrischer Fernidentifizierung; Analytik ohne Biometrie bevorzugen
Cyber Resilience Act (EU) 2024/2847	Sicherheitsanforderungen und Update-Pflichten für vernetzte Produkte (gestaffelte Geltung bis 2027)
Bauordnungsrecht / Netzbetreiber-Vorgaben	Masten, Fundamente, Leitungsführung, ggf. Genehmigungen in Schutzzonen

SCHUTZZIELE · SICHERUNGSKETTE · GRENZEN

03 Videoüberwachung im Resilienzkonzept

Kameras schützen nicht – Prozesse schützen. Videoüberwachung entfaltet ihre Wirkung erst als Glied einer geschlossenen Sicherungskette aus Erschweren, Erkennen, Verifizieren, Reagieren und Dokumentieren.

3.1 Die Sicherungskette

Erschweren	Erkennen	Verifizieren	Reagieren	Dokumentieren
Zaun, Tore, Beleuchtung, Poller	Videoanalytik, Wärmebild, Detektoren	Live-Bild in der NSL, Täteransprache	Intervention, Polizei, Betreiber-Bereitschaft	Ereignisprotokoll, Beweissicherung, Meldung nach § 18

Grün markiert: Kernaufgaben von Videoüberwachung mit Aufschaltung.

Entscheidend ist das Zeitbudget: Die Zeit, die ein Täter zur Überwindung der Barrieren braucht, muss größer sein als die Summe aus Detektions-, Verifikations- und Interventionszeit. Videoüberwachung verkürzt Detektion und Verifikation auf Sekunden; die Interventionszeit bleibt eine Frage der Organisation und der regionalen Verfügbarkeit.

Rechenbeispiel Zeitbudget

Phase	Ohne Aufschaltung	Mit Videoaufschaltung
Detektion des Eindringens	zufällig, oft erst bei Arbeitsbeginn	unter 10 Sekunden (Perimeteranalytik)
Verifikation	entfällt	30–90 Sekunden (Operator in der NSL)
Erste Gegenmaßnahme	keine	Täteransprache nach rund 2 Minuten
Eintreffen Intervention / Polizei	Stunden bis Tage nach der Tat	nach vereinbarter Interventionszeit, z. B. 15–30 Minuten
Ergebnis	**Schaden wird nachträglich festgestellt**	**Tat wird gestört, abgebrochen und lückenlos dokumentiert**

Die Werte sind typische Praxisgrößen und keine Zusage. Sie zeigen: Je länger Zaun, Tore und Gebäudehülle einen Täter aufhalten, desto eher trifft die Intervention noch während der Tat ein. Barrieren und Aufschaltung müssen deshalb gemeinsam geplant werden.

3.2 Typische Schutzziele in KRITIS-Anlagen

Anlagentyp	Hauptrisiken	Videoschwerpunkt
Umspannwerke, Netzstationen	Sabotage, Buntmetall-/Kabeldiebstahl, Brandstiftung	Perimeterdetektion mit Wärmebild, Zufahrten, Trafo-Bereiche
Wasserwerke, Hochbehälter, Pumpstationen	Manipulation, unbefugter Zutritt, Vandalismus	Zugänge, Schächte, Behälterdächer, Zäune
PV- und Windparks, Batteriespeicher	Modul- und Kabeldiebstahl, Sabotage, Brand	Großflächiger Perimeter, autarke Masten, Thermalanalytik
Krankenhäuser	Übergriffe, Diebstahl, Zutritt zu Technikbereichen	Notaufnahme-Zufahrt, Technikzentralen, Medikamentenlager (keine Patientenbereiche)
Logistik, Häfen, Verkehrsknoten	Ladungsdiebstahl, Eindringen, Sabotage	Tore, Rampen, Freiflächen, Kennzeichenerfassung nur mit Rechtsgrundlage
Rechenzentren, TK-Standorte	Sabotage, Zutritt, Diebstahl von Komponenten	Perimeter, Schleusen, Zutrittskontrolle mit Videoverifikation

Advocatus Diaboli: Wo Video an Grenzen stößt

Video ersetzt keine Barriere: Ohne Zaun und Verzögerung kommt jede Intervention zu spät. Analytik erzeugt Falschalarme durch Wild, Wetter und Vegetation – ohne Kalibrierung und Pflege sinkt die Akzeptanz in der Leitstelle. Funk- und Mobilfunkstrecken können gestört werden; KRITIS-Objekte brauchen eine überwachte Übertragung mit Ersatzweg. Und: Eine 24/7-Präsenz ist dort weiterhin erforderlich, wo Personen vor Ort handeln müssen (z. B. Zutrittssteuerung, Brandwache, Werkschutz).

DIN EN 62676 · DETEKTION · IT-SICHERHEIT

04 Technik, Normen und Cybersicherheit

Die Qualität einer Videoanlage entscheidet sich in der Planung. Maßgeblich ist die Normenreihe DIN EN 62676 „Videoüberwachungsanlagen für Sicherheitsanwendungen“; ergänzend gelten die VdS-Richtlinien und Herstellervorgaben.

4.1 Auflösungsstufen nach DIN EN 62676-4

Für jede Kamera wird das Schutzziel festgelegt. Daraus ergibt sich die erforderliche Pixeldichte am Zielort, gemessen in Pixel pro Meter (px/m) bzw. als Personenhöhe im Bild.

Stufe	Pixeldichte	Was erreicht wird	Typischer KRITIS-Einsatz
Überwachen	12,5 px/m	Personen- und Fahrzeugbewegungen grob verfolgen	Übersicht großer Freiflächen
Detektieren	25 px/m	Feststellen, ob eine Person vorhanden ist	Perimeter- und Zaunlinien mit Analytik
Beobachten	62,5 px/m	Charakteristische Details, z. B. Kleidung	Lager- und Technikflächen
Erkennen	125 px/m	Bekannte Person wiedererkennen	Zugänge, Tore, Schleusen
Identifizieren	250 px/m	Person zweifelsfrei identifizieren	Zufahrtskontrolle, Haupteingang
Inspizieren	1.000 px/m	Feinste Details, z. B. Schriftzüge	Sonderfälle, Kennzeichen-/Detailaufnahmen

4.2 Detektionstechnologien im Vergleich

Technologie	Stärken	Grenzen
Wärmebildkamera mit Analytik	Nachtsicht ohne Beleuchtung, Reichweite, geringe Falschalarmrate bei korrekter Kalibrierung	keine Identifizierung, höhere Kosten pro Kamera
Tag/Nacht-Kamera mit IR und KI-Analytik	Erkennung und Klassifizierung von Personen/Fahrzeugen, Farbinformation am Tag	IR-Reichweite begrenzt, wetterempfindlicher
PTZ-/Speed-Dome	Nachverfolgung durch Leitstelle, Zoom für Verifikation	nur ein Blickfeld zur Zeit; nie alleinige Detektion
Radar / Zaundetektion (ergänzend)	wetterunabhängige Detektion, Kamera-Nachführung	zusätzliche Integration und Kalibrierung
Mobile, autarke Kameratürme	schnell verfügbar, Bauphasen, Interimsschutz, Solar/Akku	Energie- und Mobilfunkabhängigkeit, Vandalismusrisiko

4.3 Cybersicherheit der Videoanlage

Vernetzte Kameras sind ein bekanntes Einfallstor in Unternehmensnetze. Für Betreiber, die unter das BSIG fallen, sind die folgenden Maßnahmen Teil des Risikomanagements nach § 30 BSIG:

- Eigenes, physisch oder logisch getrenntes Videonetz (VLAN/Segmentierung, Firewall), kein direkter Internetzugriff auf Kameras
- Verschlüsselte Übertragung zur NSL (VPN/TLS), Authentisierung mit individuellen Zugangsdaten, keine Standardpasswörter
- Firmware- und Patchmanagement mit dokumentierten Intervallen; Herstellerzusagen zu Sicherheitsupdates (Cyber Resilience Act)
- Rollen- und Rechtekonzept im VMS, Protokollierung von Zugriffen und Exporten
- Lieferkettenprüfung: Herkunft, Supportzeitraum und Risikobewertung von Kameras und Software – herstellerunabhängig bewertet
- Überwachung der Übertragungswege (Leitungsüberwachung, Ersatzweg via LTE/5G) und Sabotagealarme bei Bildverlust oder Verstellen

Achtung bei Herstellern aus Drittstaaten – insbesondere China

Nach **§ 41 BSIG** kann das Bundesministerium des Innern den Einsatz kritischer Komponenten untersagen – unter anderem, wenn der Hersteller unmittelbar oder mittelbar von der Regierung eines Drittstaats kontrolliert wird. Eine Untersagung kann auch bereits eingebaute Komponenten betreffen. Eine allgemeine „Freigabeliste“ des BSI gibt es nicht; das frühere Anzeigeverfahren mit Garantieerklärung des Herstellers (§ 9b BSIG a. F.) ist mit dem neuen BSIG entfallen. Das Risiko einer Fehlentscheidung liegt damit beim Betreiber.

Welche Produkte als kritische Komponenten gelten, legt eine Rechtsverordnung fest – bisher vor allem für Telekommunikation und in Ansätzen für Energie. Videotechnik ist (Stand November 2026) nicht ausdrücklich erfasst, der Anwendungsbereich kann aber auf alle KRITIS-Sektoren ausgeweitet werden. International ist die Entwicklung weiter: In den USA stehen die beiden weltweit größten chinesischen Kamerahersteller auf der „Covered List“ der FCC; seit 16.07.2026 gilt die Beschränkung auch für ältere, bereits zugelassene Modelle.

Empfehlung: Herkunfts- und Kontrollrisiko des Herstellers in der Risikoanalyse dokumentieren. Bevorzugen Sie Komponenten mit nachvollziehbarer Eigentümerstruktur, transparenter Firmware, langfristigem Support in der EU und ohne Cloud-Zwang in Drittstaaten – das vermeidet einen erzwungenen Austausch während der Nutzungsdauer und Probleme bei Drittlandübermittlungen nach Art. 44 ff. DSGVO.

Herstellerunabhängigkeit als Sicherheitsfaktor

SecuConCept unterhält keine Provisions- oder Vertriebsbeziehungen zu Herstellern. Die Auswahl der Komponenten richtet sich ausschließlich nach Schutzziel, IT-Sicherheit, Lieferkettenrisiko, Wartbarkeit und Wirtschaftlichkeit – ein Vorteil, wenn Sie Beschaffungsentscheidungen gegenüber Aufsicht, Prüfern oder Geschäftsleitung begründen müssen.

NSL · ALARMVERIFIKATION · INTERVENTION

05 Videoaufschaltung auf die Leitstelle

Bei der Videoaufschaltung übertragen Kameras und Detektoren Alarmereignisse samt Live- und Ereignisbildern an eine Notruf- und Serviceleitstelle (NSL). Dort bewerten geschulte Operatoren die Lage in Sekunden und lösen die vereinbarte Maßnahmenkette aus.

5.1 Ablauf eines Alarms

1	**Detektion**	Analytik oder Detektor meldet ein Ereignis in einer definierten Zone (z. B. Zaunlinie, Zufahrt).
2	**Übertragung**	Alarm, Ereignissequenz und Live-Stream erreichen die NSL verschlüsselt und überwacht.
3	**Verifikation**	Operator prüft: Echtalarm, Täuschungsalarm oder technischer Alarm? Kamera-Nachführung über PTZ.
4	**Täteransprache**	Optional über Lautsprecher vor Ort – in der Praxis eine der wirksamsten Maßnahmen zum Abbruch einer Tat.
5	**Intervention**	Alarmierung von Interventionsdienst, Polizei und Betreiber-Bereitschaft gemäß Alarmplan.
6	**Dokumentation**	Lückenloses Ereignisprotokoll mit Zeitstempeln – Grundlage für Meldungen nach § 18 KRITISDachG / § 32 BSIG und Versicherung.

5.2 Qualitätsanforderungen an Leitstelle und Intervention

Kriterium	Anforderung / Norm	Worauf Sie achten sollten
Alarmempfangsstelle	DIN EN 50518, VdS-Anerkennung (VdS 3138)	Zertifikat mit Geltungsbereich und Gültigkeit vorlegen lassen; redundanter Betrieb, Notstrom
Personal Leitstelle	§ 34a GewO, Schulungsnachweise	24/7-Besetzung, Vier-Augen-Prinzip bei kritischen Entscheidungen
Interventionsdienst	§ 34a GewO, DIN 77200 (Sicherungsdienstleistungen)	vertraglich zugesicherte Interventionszeit, Schlüsselmanagement, Objektkenntnis
Alarmplan	Objektbezogen, schriftlich	Eskalationsstufen, Erreichbarkeiten, Freigabe durch Betreiber, regelmäßige Aktualisierung
Datenschutz	Art. 28 DSGVO	Vertrag zur Auftragsverarbeitung mit NSL und Aufschalter, TOM-Nachweis
Berichtswesen	SLA-Kennzahlen	Alarmanzahl, Falschalarmquote, Reaktionszeiten, Verfügbarkeit – monatlich

5.3 Eckpunkte für Vertrag und SLA

Leistungen einer Videoaufschaltung sind nur so gut wie ihre vertragliche Absicherung. Folgende Punkte sollten im Vertrag messbar geregelt sein – sie dienen zugleich als Nachweis gegenüber Aufsicht und Prüfern nach § 13 KRITISDachG:

- **Reaktionszeit der Leitstelle:** Zeit vom Alarmeingang bis zur Bewertung durch den Operator, mit monatlichem Nachweis
- **Interventionszeit:** vereinbarte maximale Anfahrtszeit je Objekt und Regelung für Ausnahmen (Wetter, Großlagen)
- **Verfügbarkeit und Ausfallmeldung:** Überwachung der Übertragungswege, Meldung bei Bild- oder Verbindungsverlust binnen Minuten
- **Alarmplan und Eskalation:** Freigabe durch den Betreiber, Pflege bei Personal- oder Nummernänderungen, jährliche Übung
- **Datenschutz und Datenzugriff:** AV-Vertrag, Speicherorte, Zugriffsrechte, Herausgabe von Aufzeichnungen an Behörden
- **Melde- und Berichtsfristen:** Vorfallbericht so rechtzeitig, dass Betreiber die 24-Stunden-Meldung nach § 18 KRITISDachG einhalten können

So arbeitet SecuConCept

Die eingesetzte Alarmempfangsstelle ist nach DIN EN 50518 / VdS zertifiziert und redundant aufgebaut. Interventionen setzt SecuConCept bundesweit mit geprüften Fachunternehmen des eigenen Unternehmernetzwerks **SecuNET** um – aktuell mehr als 350 Mitgliedsbetriebe mit einheitlichen Qualitätsanforderungen. Ihr Vertragspartner bleibt immer SecuConCept: ein Ansprechpartner, ein Alarmplan, ein Berichtswesen.

RECHTSGRUNDLAGE · TRANSPARENZ · SPEICHERUNG · DSFA

06 Datenschutz und DSGVO

Auch bei kritischen Anlagen gilt: Videoüberwachung verarbeitet personenbezogene Daten. Der KRITIS-Status stärkt das Sicherheitsinteresse in der Abwägung erheblich – die formalen Anforderungen der DSGVO bleiben jedoch vollständig bestehen.

6.1 Rechtsgrundlage

Betreiber	Rechtsgrundlage	Hinweis
Private Unternehmen (z. B. Netzbetreiber, Logistik, private Kliniken)	Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)	§ 4 BDSG ist für nicht-öffentliche Stellen nach Auffassung von DSK und BVerwG nicht anwendbar
Öffentliche Stellen des Bundes	§ 4 BDSG i. V. m. Art. 6 Abs. 1 lit. e DSGVO	Aufgabenbezug und Erforderlichkeit begründen
Kommunale / Landeseinrichtungen (z. B. Stadtwerke als Eigenbetrieb, Wasserverbände)	jeweiliges Landesdatenschutzgesetz	Rechtsform prüfen: GmbH-Stadtwerke sind i. d. R. nicht-öffentliche Stellen
Beschäftigte im Erfassungsbereich	Art. 6 Abs. 1 lit. f bzw. Betriebsvereinbarung (Art. 88 DSGVO)	Nach EuGH C-34/21 (30.03.2023) ist die Tragfähigkeit von § 26 Abs. 1 BDSG umstritten

Die Interessenabwägung erfolgt in drei Stufen: **(1)** berechtigtes Interesse konkret benennen (z. B. Schutz vor Sabotage, dokumentierte Vorfälle, gesetzliche Resilienzpflicht), **(2)** Erforderlichkeit prüfen – gibt es mildere, gleich wirksame Mittel?, **(3)** Abwägung mit den Interessen der Betroffenen, insbesondere ihrer vernünftigen Erwartung (Erwägungsgrund 47 DSGVO).

6.2 Die zentralen Pflichten im Überblick

Pflicht	Norm	Praxisumsetzung
Transparenz / Hinweisschild	Art. 12, 13 DSGVO	Vorgelagertes Schild vor Betreten des Erfassungsbereichs (Muster der DSK) plus vollständiges Informationsblatt
Speicherbegrenzung	Art. 5 Abs. 1 lit. e, Art. 17	Regelfall nach DSK: max. 72 Stunden; längere Fristen gesondert begründen (z. B. unbesetzte Anlagen, Wochenenden)
Datenschutz-Folgenabschätzung	Art. 35 DSGVO	Bei systematischer, umfangreicher Überwachung regelmäßig erforderlich; vor Inbetriebnahme durchführen
Verzeichnis der Verarbeitungstätigkeiten	Art. 30 DSGVO	Eigener Eintrag „Videoüberwachung / Aufschaltung“ inkl. Empfänger NSL
Auftragsverarbeitung	Art. 28 DSGVO	AV-Vertrag mit NSL, Errichter (bei Fernwartung) und Cloud-/VMS-Anbieter

Pflicht	Norm	Praxisumsetzung
Technisch-organisatorische Maßnahmen	Art. 32 DSGVO	Verschlüsselung, Zugriffsrechte, Protokollierung, Löschroutinen – deckungsgleich mit § 30 BSIG
Betroffenenrechte	Art. 15–21 DSGVO	Auskunfts- und Löschprozess definieren; Schwärzung Dritter bei Herausgabe
Datenschutz durch Technik	Art. 25 DSGVO	Privatzonen-Maskierung, Erfassungsbereich auf eigenes Gelände begrenzen

6.3 Besondere Konstellationen

- **Öffentlicher Raum und Nachbargrundstücke:** grundsätzlich ausblenden. Ausnahme: ein schmaler Streifen entlang der Grundstücksgrenze, soweit für den Perimeterschutz zwingend erforderlich und begründet.
- **Beschäftigte:** keine Leistungs- und Verhaltenskontrolle; Pausen-, Sozial- und Sanitärbereiche sind tabu. Bei vorhandenem Betriebsrat besteht Mitbestimmung (§ 87 Abs. 1 Nr. 6 BetrVG) – Betriebsvereinbarung frühzeitig abschließen.
- **Krankenhäuser:** Patienten- und Behandlungsbereiche sind regelmäßig ausgeschlossen; schon der Aufenthalt kann ein Gesundheitsdatum sein.
- **Tonaufnahmen:** unzulässig (§ 201 StGB). Lautsprecher für die Täteransprache sind zulässig, Mikrofone nicht.
- **Biometrie und KI:** Objekt- und Bewegungsklassifizierung ist unkritischer als Gesichtserkennung. Biometrische Identifizierung ist nach Art. 9 DSGVO und KI-Verordnung nur in engen Ausnahmen denkbar.
- **Attrappen:** Kameraattrappen erzeugen Überwachungsdruck und können ebenfalls unzulässig sein; im KRITIS-Kontext zudem ohne Schutzwirkung.

Bußgeldrisiko

Verstöße gegen die DSGVO können mit bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes geahndet werden (Art. 83 DSGVO). Häufigste Beanstandungen der Aufsichtsbehörden: fehlende oder unvollständige Beschilderung, zu lange Speicherdauer, Erfassung öffentlicher Flächen und fehlende Dokumentation der Interessenabwägung.

ORIENTIERUNGSWERTE · INVESTITION · BETRIEB

07 Kostenbeispiele und Wirtschaftlichkeit

Die folgenden Beispiele zeigen typische Kostenstrukturen. Sie dienen der Budgetplanung und ersetzen kein objektbezogenes Angebot. Alle Werte netto, Marktniveau 2026; tatsächliche Kosten hängen von Perimeterlänge, Tiefbau, Infrastruktur, Schutzziel und Interventionsentfernung ab.

Beispiel A – Wasserwerk / Hochbehälter, Perimeter ca. 400 m (Festinstallation)

Position	Menge	Einzelpreis	Gesamt
Sicherheitskonzept, Planung, Unterstützung DSFA	pauschal		4.500 €
Wärmebildkamera mit Perimeteranalytik	6	3.200 €	19.200 €
IR-Dome-Kamera (Identifizierung Zufahrt)	2	900 €	1.800 €
Masten, Fundamente, Tiefbau	pauschal		12.000 €
Netzwerk (LWL, Switches), USV	pauschal		6.500 €
Rekorder / Videomanagement inkl. Lizenzen	1	4.800 €	4.800 €
Montage, Inbetriebnahme, Einmessung Analytik	pauschal		7.200 €
Investition gesamt (netto)			**56.000 €**

Laufende Kosten pro Jahr	Berechnung	Betrag
Videoaufschaltung NSL (8 Kanäle, analytikbasiert)	390 € × 12 Monate	4.680 €
Wartung und Inspektion (2 × jährlich)	pauschal	1.800 €
Interventionen (Annahme: 12 Einsätze)	12 × 145 €	1.740 €
Abschreibung Investition (5 Jahre linear)	56.000 € ÷ 5	11.200 €
Jährliche Gesamtkosten		**19.420 €**

Entspricht rund 1.618 € pro Monat bzw. rund 53 € pro Tag für die 24/7-Absicherung des Perimeters.

Beispiel B – Solarpark oder Baustelle, 12 Monate mobile Kameratürme

Position	Berechnung	Betrag
Miete autarker Kameratürme inkl. Aufschaltung	6 Türme × 890 € × 12 Monate	64.080 €
Transport, Aufbau, Einrichtung, Abbau	6 × 450 €	2.700 €
Gesamtkosten Projektzeitraum (netto)		**66.780 €**

Mobile Lösungen eignen sich für Bauphasen, Interimsschutz bis zur Festinstallation und kurzfristige Lageverschärfungen. Ab einer Nutzungsdauer von etwa zwei bis drei Jahren ist eine Festinstallation in der Regel wirtschaftlicher – im Einzelfall rechnen.

Beispiel C – Vergleich mit personeller 24/7-Bewachung

Modell	Berechnung	Kosten pro Jahr
Präsenzbewachung 24/7, 1 Sicherheitskraft (Annahme 32 €/h)	8.760 h × 32 €	280.320 €
Videoüberwachung mit Aufschaltung (Beispiel A)	siehe oben	19.420 €
Hybrid: Beispiel A + Revierdienst (2 Kontrollen/Nacht à 28 €)	19.420 € + 365 × 2 × 28 €	39.860 €

Advocatus Diaboli: Der Vergleich ist kein Gleichsetzen

Die Differenz von rund 260.900 € pro Jahr zwischen Präsenzbewachung und Video-Modell ist real, aber die Leistungen sind nicht identisch: Eine Sicherheitskraft vor Ort kann Zutritte steuern, Brände früh bekämpfen und sofort eingreifen. Video mit Aufschaltung punktet bei großen, unbesetzten Flächen, durchgehender Aufmerksamkeit und Dokumentation. Für viele KRITIS-Anlagen ist das **Hybridmodell** die fachlich und wirtschaftlich stärkste Lösung. Entscheidend ist die Ableitung aus der Risikoanalyse nach § 12 KRITISDachG.

Kostentreiber, die Sie früh klären sollten

- Tiefbau und Stromversorgung an Masten (oft 20–35 % der Investition)
- Netzanbindung: vorhandene LWL-Infrastruktur oder Mobilfunk mit Ersatzweg
- Anzahl der Detektionszonen und Falschalarmverhalten (Vegetation, Wild, Wasserflächen)
- Interventionsentfernung und vereinbarte Interventionszeit
- Integration in bestehende Leit-, Zutritts- und Gefahrenmeldetechnik

VON DER RISIKOANALYSE BIS ZUM REGELBETRIEB

08 Projekt-Checkliste für Betreiber

Die Checkliste folgt dem bewährten Ablauf eines KRITIS-Sicherheitsprojekts. Sie eignet sich als Arbeitsgrundlage für interne Abstimmung, Ausschreibung und Nachweis gegenüber Aufsicht und Prüfern.

Phase 1 – Analyse	
☐	Betroffenheit prüfen: KRITISDachG (Sektor, Schwellenwert) und BSIG (§ 28) – Ergebnis dokumentieren
☐	Risikoanalyse nach § 12 KRITISDachG: Bedrohungen, Schwachstellen, Vorfallhistorie
☐	Schutzziele je Bereich festlegen (Detektieren, Erkennen, Identifizieren)
☐	Bestehende Technik, Infrastruktur und Verträge erfassen

Phase 2 – Konzeption	
☐	Sicherheitskonzept mit Sicherungskette und Zeitbudget (Barriere vs. Interventionszeit)
☐	Kamerakonzept nach DIN EN 62676-4 mit Lageplan und Erfassungsbereichen
☐	Datenschutz: Interessenabwägung, DSFA, Löschkonzept, Beschilderung, VVT-Eintrag
☐	Betriebsrat und Datenschutzbeauftragten einbinden
☐	IT-Sicherheitskonzept: Segmentierung, Verschlüsselung, Patchmanagement, Lieferkette

Phase 3 – Beschaffung und Umsetzung	
☐	Leistungsbeschreibung herstellerunabhängig formulieren (Funktion statt Produkt)
☐	Nachweise anfordern: DIN EN 50518 / VdS, § 34a GewO, Referenzen, AV-Vertrag
☐	Herstellerherkunft und Drittstaatenrisiko prüfen (§ 41 BSIG), Supportzeitraum und Datenflüsse dokumentieren
☐	Montage, Einmessung der Analytik, Test aller Alarmwege inkl. Ersatzweg
☐	Alarmplan erstellen und vom Betreiber freigeben lassen

Phase 4 – Regelbetrieb und Nachweis	
☐	Probebetrieb mit Falschalarm-Optimierung (4–6 Wochen)
☐	Monatliches Reporting: Alarme, Reaktionszeiten, Verfügbarkeit
☐	Wartung, Firmware-Updates, jährliche Übung des Alarm- und Meldeablaufs
☐	Resilienzplan und Risikoanalyse fortschreiben (mind. alle 4 Jahre)

KURZ UND BELASTBAR BEANTWORTET

09 Häufige Fragen (FAQ)

Ist Videoüberwachung für KRITIS-Betreiber gesetzlich vorgeschrieben?

Nein, nicht ausdrücklich. § 13 KRITISDachG verlangt geeignete und verhältnismäßige Maßnahmen zum physischen Schutz und nennt Instrumente zur Überwachung der Umgebung und Detektionsgeräte als Beispiele. Ob Video das passende Mittel ist, ergibt sich aus der Risikoanalyse.

Ab wann müssen sich Betreiber nach dem KRITIS-Dachgesetz registrieren?

Spätestens drei Monate nach Einstufung als kritische Anlage. Die Einstufung hängt an der KRITIS-Verordnung, die nach unserem Kenntnisstand (November 2026) noch nicht in Kraft ist. Die frühere Frist 17.07.2026 wurde gestrichen.

Wie lange dürfen Videoaufnahmen gespeichert werden?

Nach Auffassung der Datenschutzkonferenz im Regelfall bis zu 72 Stunden. Eine längere Speicherung ist möglich, wenn sie konkret begründet und dokumentiert wird – etwa bei unbesetzten Anlagen, die nur in größeren Abständen kontrolliert werden.

Was ist der Unterschied zwischen Videoüberwachung und Videoaufschaltung?

Videoüberwachung zeichnet auf. Videoaufschaltung überträgt Alarme und Live-Bilder an eine ständig besetzte Leitstelle, die verifiziert und Maßnahmen auslöst. Erst die Aufschaltung verhindert Taten, statt sie nur zu dokumentieren.

Ist eine Datenschutz-Folgenabschätzung nötig?

Bei systematischer, umfangreicher Überwachung – typisch für KRITIS-Perimeter – in aller Regel ja (Art. 35 DSGVO). Sie ist vor Inbetriebnahme abzuschließen.

Dürfen Kameras den Gehweg vor dem Gelände erfassen?

Grundsätzlich nein. Öffentliche Flächen sind auszublenden; allenfalls ein schmaler Streifen entlang der Grundstücksgrenze kann bei zwingender Erforderlichkeit zulässig sein.

Welche Zertifizierung sollte die Leitstelle haben?

Eine Zertifizierung als Alarmempfangsstelle nach DIN EN 50518, idealerweise mit VdS-Anerkennung. Lassen Sie sich Zertifikat, Geltungsbereich und Gültigkeit vorlegen.

Was kostet Videoaufschaltung pro Monat?

Je nach Kanalanzahl, Analytik und Leistungsumfang typischerweise einige hundert Euro pro Objekt und Monat zuzüglich Interventionen. Ein Rechenbeispiel finden Sie in Kapitel 7.

SECURITY · CONSULTING · CONCEPTION

10 Ihr Partner für KRITIS-Sicherheit

SecuConCept verbindet herstellerunabhängige Sicherheitsberatung, Sicherheitskonzeption und operative Umsetzung aus einer Hand – bundesweit, persönlich koordiniert.

Consulting

Risikoanalyse, Betroffenheitsprüfung KRITISDachG/BSIG, Datenschutzunterstützung, Ausschreibungsbegleitung

Conception

Sicherheitskonzepte nach DIN EN 62676-4, Perimeter- und Aufschaltkonzepte, Alarmpläne, Resilienzbausteine

Security

Videoaufschaltung, Intervention, Objekt- und Werkschutz, Revierdienst, mobile Videoüberwachung & Kameratürme

Warum SecuConCept?

- **SecuNET by SecuConCept:** mehr als 350 spezialisierte Fachunternehmen bundesweit – regionale Fachkompetenz, skalierbare Projektumsetzung, einheitliche Qualitätsanforderungen.
- **Ein Vertragspartner:** Auch wenn SecuNET-Partner vor Ort umsetzen, bleibt SecuConCept Ihr Vertragspartner und verantwortlicher Koordinator.
- **Herstellerunabhängig:** keine Provisions- oder Vertriebsbeziehungen zu Herstellern – die Technik folgt Ihrem Schutzziel.
- **Zertifiziert und praxiserprobt:** redundante Alarmempfangsstelle nach DIN EN 50518 / VdS, Erfahrung aus dem Werkschutz großer Chemie- und Industriestandorte.
- **Nachhaltig organisiert:** unternehmensweite Elektromobilität, eigene Photovoltaikanlage und „Upgrade statt neu“ bei Hardware – bestehende Kameras werden geprüft und, wo sinnvoll, weitergenutzt.

Fachportale und Marken

SecuFokus® SICHERHEIT GEMEINSAM STEUERN. BY SECUCONCEPT

SecuFokus by SecuConCept – Sicherheit gemeinsam steuern. Fachinformationen und Werkzeuge, mit denen Betreiber, Partner und Dienstleister Sicherheitsprozesse gemeinsam und transparent steuern.

CCTV-SECURITY.DE VIDEOTÜRME | ALARMZENTRALE | ALARMVERFOLGUNG | REALISIERUNG by SecuConCept

CCTV-Security.de by SecuConCept – Fachportal für Videotürme, Alarmzentrale, Alarmverfolgung und Realisierung von Videoüberwachungslösungen.

KOSTENFREIES ERSTGESPRÄCH

KRITIS-Check für Ihre Anlage

Betroffenheit, Schutzziele, Videokonzept und Datenschutz – in einem strukturierten Termin mit klarer Handlungsempfehlung.

0800 666 000 4 (bundesweit) · **0221 954 917 52** (Köln)
vertrieb@secuconcept.de · www.secuconcept.de
SecuConCept · Inh. Torsten Bentlage · Adolf-Grimme-Allee 3 · 50829 Köln

ZUM NACHSCHLAGEN

11 Quellen, Normen und Rechtsstand

Rechtsgrundlagen

- Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz) vom 11.03.2026, BGBl. 2026 I Nr. 66; Änderung des § 8 durch Gesetz vom 21.07.2026, BGBl. 2026 I Nr. 221
- NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), in Kraft seit 06.12.2025; BSI-Gesetz (BSIG) n. F.
- Verordnung (EU) 2016/679 (DSGVO); Bundesdatenschutzgesetz (BDSG); Landesdatenschutzgesetze
- EuGH, Urteil vom 30.03.2023, C-34/21 (Beschäftigtendatenschutz)
- Verordnung (EU) 2024/1689 (KI-Verordnung); Verordnung (EU) 2024/2847 (Cyber Resilience Act)
- § 34a Gewerbeordnung, Bewachungsverordnung; § 87 Betriebsverfassungsgesetz; § 201 Strafgesetzbuch
- § 41 BSIG (Untersagung des Einsatzes kritischer Komponenten), zuvor § 9b BSIG a. F.; US Federal Communications Commission (FCC): Covered List nach Secure Equipment Act

Normen und Richtlinien

- DIN EN 62676 (Reihe) – Videoüberwachungsanlagen für Sicherheitsanwendungen, insbesondere Teil 4: Anwendungsregeln
- DIN EN 50518 – Alarmempfangsstelle (AES)
- VdS 3138 – Notruf- und Serviceleitstellen; VdS-Richtlinien für Videoüberwachungsanlagen
- DIN 77200 – Sicherungsdienstleistungen

Behördliche Orientierung

- Datenschutzkonferenz (DSK): Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen (2020) inkl. Muster-Hinweisschild; DSK-Kurzpapier Nr. 15
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): Informationen und FAQ zum KRITIS-Dachgesetz – www.bbk.bund.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI): NIS-2-Informationen und Melde-/Registrierungsportal – www.bsi.bund.de

Rechtsstand und Haftung: Recherchestand November 2026. Die KRITIS-Verordnung zum KRITIS-Dachgesetz lag zu diesem Zeitpunkt als Referentenentwurf vor; konkrete Schwellenwerte und Fristen können sich ändern. Dieses Handbuch stellt keine Rechtsberatung dar. Kostenangaben sind unverbindliche Orientierungswerte (netto) auf Basis typischer Projektannahmen.

© 2026 SecuConCept · Inh. Torsten Bentlage · Weitergabe in unveränderter Form ausdrücklich erwünscht.