Stand: November 2026

FACHHANDBUCH

GESAMTAUSGABE · FÜNF FACHHANDBÜCHER IN EINEM BAND

Gesamthandbuch Sicherheitsdienstleistungen

Das Fachhandbuch für Unternehmen, Betreiber und KRITIS

FACHPORTALE UND MARKEN VON SECUCONCEPT

A Videoüberwachung & Videoaufschaltung KRITIS · B Aufschaltung, Alarmverfolgung & Prävention
C Wachschutz oder Werkschutz · D Empfangsdienst & Pförtner
E KRITIS: Sicherheitsdienste als All-in-One-Lösung? · Quellenverzeichnis

Qualität durch Vertrauen

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

ZU DIESEM HANDBUCH

Fünf Fachhandbücher, ein Band

Sicherheit entsteht aus dem Zusammenspiel von Recht, Technik, Leitstelle und Menschen vor Ort. Dieses Gesamthandbuch bündelt die fünf SecuConCept-Fachhandbücher zu einem Nachschlagewerk – mit durchgängiger Kapitelzählung, Querverweisen zwischen den Teilen und einem gemeinsamen Quellenverzeichnis.

So nutzen Sie dieses Handbuch

Teil	Thema	Besonders relevant für
A	Videoüberwachung & Videoaufschaltung für KRITIS	Betreiber kritischer Anlagen, technische Leitung, Datenschutz
B	Aufschaltung, Alarmverfolgung & Prävention	Facility- und Security-Management, Filial- und Objektverantwortliche
C	Wachschutz oder Werkschutz	Geschäftsführung, Werks- und Standortleitung, Einkauf
D	Empfangsdienst & Pförtner	Office- und Standortleitung, Facility-Management, Datenschutz
E	KRITIS: Sicherheitsdienste als All-in-One-Lösung?	Geschäftsleitung von KRITIS-Unternehmen, Vergabestellen

- **Kapitelnummern** setzen sich aus Teil und Kapitel zusammen: **B3** ist Kapitel 3 in Teil B, **B3.6** der Abschnitt darin.
- **Querverweise** sind grün unterstrichen und im PDF anklickbar; das Inhaltsverzeichnis und die Lesezeichen ebenfalls.
- **Jeder Teil** beginnt mit einer Trennseite, die seine Kapitel und die verwandten Teile zeigt.
- **Kostenbeispiele** bauen aufeinander auf: Der tarifbasierte Modellsatz aus Kapitel C7 wird in Kapitel D8 und Kapitel E8 angewendet.

Wichtiger Hinweis zur Rechtsverbindlichkeit

Dieses Handbuch ist eine fachliche Orientierung und ersetzt keine Rechts-, Steuer- oder Vergabeberatung. Gesetze, Verordnungen, Tarifverträge und behördliche Auslegungen ändern sich – insbesondere die zum Recherchestand (November 2026) noch nicht in Kraft getretene KRITIS-Verordnung. Die Zuordnung einzelner Tätigkeiten zum Bewachungsrecht trifft das zuständige Gewerbeamt. Alle Kostenangaben sind Modellrechnungen und unverbindliche Orientierungswerte (netto) und ersetzen kein objektbezogenes Angebot.

Inhalt

Teil A · Videoüberwachung & Videoaufschaltung für KRITIS-relevante Einrichtungen 5

A1 Auf einen Blick . . . 6
A2 Rechtsrahmen KRITIS 2026 . . . 7
A3 Videoüberwachung im Resilienzkonzept . . . 10
A4 Technik, Normen und Cybersicherheit . . . 12
A5 Videoaufschaltung auf die Leitstelle . . . 14
A6 Datenschutz und DSGVO . . . 16
A7 Kostenbeispiele und Wirtschaftlichkeit . . . 18
A8 Projekt-Checkliste für Betreiber . . . 20
A9 Häufige Fragen (FAQ) . . . 21

Teil B · Aufschaltung von Gefahrenmeldeanlagen, Alarmverfolgung und präventive Gefahrenabwehr 22

B1 Auf einen Blick . . . 23
B2 Gefahrenmeldeanlagen und Aufschaltung . . . 24
B3 Leitstelle und Alarmverfolgung . . . 27
B4 Mitwirkung des Auftraggebers . . . 30
B5 Präventive Gefahrenabwehr . . . 32
B6 Recht, Haftung und Datenschutz . . . 33
B7 Kostenbeispiele und Wirtschaftlichkeit . . . 34
B8 Checkliste für Auftraggeber . . . 36
B9 Häufige Fragen (FAQ) . . . 37

Teil C · Sicherheitsdienste in der Praxis: Wachschutz oder Werkschutz 38

C1 Auf einen Blick . . . 39
C2 Wachschutz und Werkschutz . . . 40
C3 Recht, Qualifikation und Arbeitsschutz . . . 42
C4 Eigenpersonal oder Dienstleister . . . 44
C5 Praxis im Objekt . . . 46
C6 Qualität und Vergabe . . . 48
C7 Was eine Stunde Sicherheit kostet . . . 49
C8 Checkliste für Auftraggeber . . . 51
C9 Häufige Fragen (FAQ) . . . 52

Teil D · Empfangsdienst & Pförtnerdienst – Einlass mit Kontrolle 53

D1 Auf einen Blick . . . 54
D2 Empfang, Pforte, Werkstor . . . 55
D3 Zutritt und Einlasskontrolle . . . 56
D4 Recht und Datenschutz am Empfang . . . 57
D5 Notfall, Bedrohung und Deeskalation . . . 59
D6 Personal, Qualität und Mitwirkung . . . 60
D7 Technik am Empfang . . . 61
D8 Kostenbeispiele und Wirtschaftlichkeit . . . 62
D9 Checkliste für Auftraggeber . . . 63
D10 Häufige Fragen (FAQ) . . . 64

Teil E · KRITIS: Sicherheitsdienste als All-in-One-Lösung? 65

E1 Auf einen Blick . . . 66
E2 Was KRITIS-Betreiber nachweisen müssen . . . 67
E3 Was „All-in-One“ bedeutet . . . 68
E4 Chancen einer integrierten Lösung . . . 69
E5 Risiken und Grenzen . . . 70
E6 Kriterien für ein belastbares Modell . . . 71
E7 Vergabe: privat und öffentlich . . . 72
E8 Kostenbeispiel und Wirtschaftlichkeit . . . 73
E9 Entscheidungshilfe und Checkliste . . . 74
E10 Häufige Fragen (FAQ) . . . 75

SecuConCept: integriert und unabhängig 76

Quellenverzeichnis 77

TEIL A

Videoüberwachung & Videoaufschaltung für KRITIS-relevante Einrichtungen

Rechtsrahmen nach KRITIS-Dachgesetz und BSIG, Technik und Normen, Videoaufschaltung auf eine Leitstelle, Datenschutz und Kostenbeispiele für Betreiber kritischer Anlagen.

KAPITEL

A1 Auf einen Blick
A2 Rechtsrahmen KRITIS 2026
A3 Videoüberwachung im Resilienzkonzept
A4 Technik, Normen und Cybersicherheit
A5 Videoaufschaltung auf die Leitstelle
A6 Datenschutz und DSGVO
A7 Kostenbeispiele und Wirtschaftlichkeit
A8 Projekt-Checkliste für Betreiber
A9 Häufige Fragen (FAQ)

VERWANDTE TEILE

Teil B Aufschaltung von Gefahrenmeldeanlagen, Alarmverfolgung und präventive Gefahrenabwehr – Aufschaltung und Leitstelle
Teil E KRITIS: Sicherheitsdienste als All-in-One-Lösung? – Rechtsrahmen und Dienstleistermodell

KERNAUSSAGEN FÜR ENTSCHEIDER

A1 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 A7).

KRITIS-DACHGESETZ · BSIG / NIS-2 · ZUSAMMENSPIEL

A2 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.

A2.1 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.

A2.2 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 A4.3).
- **§ 65 BSIG – Bußgelder:** bis 10 Mio. € oder 2 % des weltweiten Jahresumsatzes (besonders wichtige Einrichtungen).

A2.3 Weitere relevante Vorschriften

Regelwerk	Relevanz für Video & Aufschaltung
DSGVO / BDSG / Landesdatenschutzgesetze	Zulässigkeit, Transparenz, Speicherfristen, DSFA – siehe Kapitel A6
§ 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

Querverweise

→ E2 Was KRITIS-Betreiber nachweisen müssen
→ E7 Vergabe: privat und öffentlich

SCHUTZZIELE · SICHERUNGSKETTE · GRENZEN

A3 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.

A3.1 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.

A3.2 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

A4 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.

A4.1 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

A4.2 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

A4.3 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

A5 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.

A5.1 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.

A5.2 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

A5.3 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.

Querverweise

→ B2 Alarmübertragung nach DIN EN 50136
→ B3 Leitstelle und Alarmverfolgung

RECHTSGRUNDLAGE · TRANSPARENZ · SPEICHERUNG · DSFA

A6 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.

A6.1 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).

A6.2 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

A6.3 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

A7 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

A8 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

A9 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 A7.

TEIL B

Aufschaltung von Gefahrenmeldeanlagen, Alarmverfolgung und präventive Gefahrenabwehr

Gefahrenmeldeanlagen und Übertragungswege, Leitstelle und Intervention, Haus- und Wegerecht, Mitwirkung des Auftraggebers und Prävention.

KAPITEL

B1 Auf einen Blick
B2 Gefahrenmeldeanlagen und Aufschaltung
B3 Leitstelle und Alarmverfolgung
B4 Mitwirkung des Auftraggebers
B5 Präventive Gefahrenabwehr
B6 Recht, Haftung und Datenschutz
B7 Kostenbeispiele und Wirtschaftlichkeit
B8 Checkliste für Auftraggeber
B9 Häufige Fragen (FAQ)

VERWANDTE TEILE

Teil A Videoüberwachung & Videoaufschaltung für KRITIS-relevante Einrichtungen – Videoaufschaltung
Teil C Sicherheitsdienste in der Praxis: Wachschutz oder Werkschutz – Interventionskräfte in der Praxis
Teil D Empfangsdienst & Pförtnerdienst – Einlass mit Kontrolle – Fernpforte und Zutritt

KERNAUSSAGEN FÜR ENTSCHEIDER

B1 Auf einen Blick

Die zehn wichtigsten Fakten für Betreiber, die Gefahrenmeldeanlagen aufschalten, Alarmverfolgung beauftragen oder ihre Prävention verbessern wollen.

1	**Die Normenbasis ist klar:** DIN VDE 0833 (Gefahrenmeldeanlagen), DIN EN 50131 (Einbruch- und Überfallmeldeanlagen, Grade 1–4), DIN EN 50136 (Alarmübertragung), DIN EN 50518 (Alarmempfangsstelle).
2	**Grad und Klasse bestimmen die Anlage:** Die Polizei empfiehlt für Einbruchmeldeanlagen die Grade 2 bis 4; Versicherer fordern häufig VdS-anerkannte Anlagen der Klassen A, B oder C.
3	**Brandmeldeanlagen mit Aufschaltung zur Feuerwehr** laufen über die Alarmübertragungsanlage des örtlichen Konzessionärs nach DIN 14675 – nicht über eine private Leitstelle.
4	**Übertragungswege altern:** Die 2G-Netze werden ab 2028 abgeschaltet. Übertragungseinrichtungen mit reinem GSM-Ersatzweg müssen rechtzeitig umgerüstet werden.
5	**Alarmverfolgung ist Interventionsdienst nach DIN 77200-1:** vereinbarte Maßnahmen auf ein nicht regelmäßiges Ereignis innerhalb einer bestimmten Frist.
6	**Sicherheitskräfte haben keine Polizeibefugnisse:** Sie handeln mit übertragenem Hausrecht und den Jedermannsrechten – und ohne Sonderrechte im Straßenverkehr.
7	**Ohne Mitwirkung des Auftraggebers geht es nicht:** Aktueller Alarmplan, erreichbare Ansprechpartner und geschulte Mitarbeitende sind die wirksamsten Mittel gegen Fehlalarme.
8	**Fehlalarme kosten:** Je nach Bundesland können Gebühren für Polizeieinsätze anfallen; Gerichte haben z. B. 120 € je ungerechtfertigter Alarmierung bestätigt.
9	**Prävention zuerst:** Mechanischer Widerstand, Organisation und sichtbare Kontrollen verhindern Taten – Melde- und Interventionstechnik begrenzt den Schaden.
10	**Versicherungsschutz hängt an Obliegenheiten:** Wer eine vereinbarte Einbruchmeldeanlage nicht scharf schaltet, riskiert Leistungskürzungen (§ 28 VVG).

ANLAGENARTEN · GRADE UND KLASSEN · AUFSCHALTWEGE · ÜBERTRAGUNG

B2 Gefahrenmeldeanlagen und Aufschaltung

Gefahrenmeldeanlagen (GMA) erkennen Einbruch, Überfall, Brand oder technische Störungen und melden sie an eine ständig besetzte Stelle. Welche Stelle das ist und welche Anforderungen gelten, hängt von der Art der Meldung ab.

B2.1 Anlagenarten im Überblick

Anlagenart	Typische Meldungen	Maßgebliche Regelwerke
Einbruchmeldeanlage (EMA)	Öffnung, Durchstieg, Bewegung, Glasbruch, Sabotage	DIN EN 50131, DIN VDE 0833-1/-3, VdS 2311
Überfallmeldeanlage (ÜMA)	Stiller Alarm, Bedrohung, Personennotsignal	DIN EN 50131, DIN VDE 0833-3, ÜEA-Richtlinie
Brandmeldeanlage (BMA)	Rauch, Wärme, Handfeuermelder, Löschanlagenauslösung	DIN EN 54, DIN VDE 0833-2, DIN 14675
Technische Alarme	Temperatur, Wasser, Stromausfall, Kühlung, Gas	Herstellerangaben, objektbezogene Festlegung
Video- und Perimeteralarme	Zaundetektion, Videoanalytik, Sabotage	DIN EN 62676, siehe Teil A

B2.2 Grade nach DIN EN 50131 und VdS-Klassen

Die Normenreihe DIN EN 50131 teilt Einbruch- und Überfallmeldeanlagen in vier Grade ein. In Deutschland ergänzt DIN VDE 0833-1 und -3; für versicherungsrelevante Anlagen gilt zusätzlich die Richtlinie VdS 2311 mit den Klassen A bis C.

Grad	Risiko / Einsatzbereich	VdS-Klasse (Näherung)	Hinweis
Grad 1	geringes Risiko	–	von der Polizei nicht empfohlen
Grad 2	geringes bis mittleres Risiko, Wohnen, kleines Gewerbe	Klasse A	Mindeststandard für Aufschaltung
Grad 3	mittleres bis hohes Risiko, Gewerbe, Lager	Klasse B	häufige Versicherungsauflage
Grad 4	hohes Risiko, Banken, Hochwertlager, Sonderobjekte	Klasse C	Inspektion viermal jährlich

Die Zuordnung von Graden und VdS-Klassen ist eine Näherung; maßgeblich sind Versicherungsvertrag, Errichterattest und Planung im Einzelfall.

B2.3 Wohin wird aufgeschaltet?

Ziel	Für welche Meldungen	Voraussetzungen
Private Notruf- und Serviceleitstelle (NSL)	Einbruch, Überfall, Technik, Video, Störungen, Scharf-/Unscharf-Überwachung	Vertrag, Alarmplan, Schlüsselhinterlegung; NSL nach DIN EN 50518 / VdS 3138
Polizei (Überfall-/Einbruchmeldeanlage mit Anschluss)	Überfall- und ausgewählte Einbruchmeldungen	ÜEA-Richtlinie, i. d. R. Grad 3 oder 4, Antrag und Abnahme; regional sehr unterschiedlich
Feuerwehr (über Konzessionär)	Brandmeldungen bauordnungsrechtlich geforderter BMA	DIN 14675, Brandmelde- und Alarmierungskonzept, Anschlussbedingungen der Feuerwehr, Schlüsseldepot

Brandmeldeanlagen: Feuerwehr zuerst, Leitstelle ergänzend

Brandmeldungen bauordnungsrechtlich geforderter BMA gehen über die Übertragungseinrichtung zur Alarmübertragungsanlage des örtlichen Konzessionärs direkt an die Feuerwehr. Vor der Errichtung ist ein Brandmelde- und Alarmierungskonzept nach DIN 14675 mit der Feuerwehr abzustimmen. Nach einem Beschluss des Bundeskartellamts darf die Konzession nur noch die Empfangseinrichtung bei der Feuerwehr umfassen; Übertragungseinrichtung und Übertragungsweg sind im Wettbewerb frei wählbar.

Eine private Leitstelle kann zusätzlich Störungs- und Zustandsmeldungen übernehmen und im Brandfall Schlüssel, Einweisung der Feuerwehr und Nachsorge organisieren – sie ersetzt die Feuerwehraufschaltung aber nicht.

B2.4 Alarmübertragung nach DIN EN 50136

Der Übertragungsweg ist das unsichtbare Glied der Sicherungskette: Fällt er unbemerkt aus, ist die beste Anlage wirkungslos. DIN EN 50136-1 unterscheidet Einweg-Übertragung (Single Path, SP 1 bis SP 6) und Zweiwege-Übertragung (Dual Path, DP 1 bis DP 4). Je höher die Kategorie, desto kürzer die Überwachungsintervalle und desto schneller wird ein Ausfall erkannt.

Kategorie	Prinzip	Typischer Einsatz
SP 1 – SP 3	ein Übertragungsweg, längere Überwachungsintervalle	Wohnobjekte, kleines Gewerbe (Grad 2)
SP 4 – SP 6	ein Übertragungsweg mit enger Überwachung	Gewerbe mit höherem Risiko
DP 1 – DP 4	Erst- und Ersatzweg, z. B. IP-Festverbindung plus Mobilfunk	Grad 3 und 4, Filialnetze, KRITIS
BMA zur Feuerwehr	mindestens SP 6 oder DP 3	nach DIN 14675 / Anschlussbedingungen

B2.5 Schnelle Störungserkennung

Ältere Wählverbindungen brauchen für den Verbindungsaufbau 10 bis 15 Sekunden. Moderne, ständig überwachte IP-Verbindungen erkennen Ausfall oder Sabotage der Zentrale oder der Übertragungseinrichtung deutlich schneller; nach den Hinweisen von VdS und BHE soll die Leitstelle spätestens nach 180 Sekunden informiert sein. Bestandsanlagen sollten auf diesen Stand umgerüstet werden.

2G-Abschaltung: Bestandsanlagen jetzt prüfen

Die Telekom will ihr 2G-Netz bis 30. Juni 2028 abschalten, Vodafone im September 2028, Telefónica Ende 2028. Vodafone lässt die 2G-Versorgung für kritische Anwendungen wie ältere Alarmanlagen bis Ende 2030 weiterlaufen. Übertragungseinrichtungen, deren Ersatzweg nur GSM beherrscht, verlieren damit ihren zweiten Weg – oft unbemerkt bis zum Ernstfall.

Empfehlung: Bestand inventarisieren, Übertragungswege mit LTE/5G und IP planen und die Umrüstung mit der ohnehin fälligen Wartung verbinden. Das 3G-Netz ist bereits seit 2021 abgeschaltet.

Upgrade statt neu

Für den Wechsel des Übertragungswegs muss die Einbruchmeldeanlage selten komplett ersetzt werden. Häufig genügt der Tausch der Übertragungseinrichtung oder ein Zusatzmodul. SecuConCept prüft Bestandsanlagen zuerst auf Weiterverwendung – das spart Kosten und Ressourcen und reduziert den ökologischen Fußabdruck.

Bezug zu KRITIS

Für Betreiber kritischer Anlagen nennt § 13 KRITIS-Dachgesetz ausdrücklich Detektionsgeräte, Zugangskontrollen und festgelegte Alarmabläufe als Resilienzmaßnahmen. Aufschaltung, Alarmplan, Intervention und Prävention sind damit Teil des gesetzlichen Nachweises. Details enthält Teil A dieses Handbuchs, insbesondere Kapitel A2 und Kapitel A5.

DIN EN 50518 · DIN 77200-1 · ALARMPLAN · EINSATZ VOR ORT

B3 Leitstelle und Alarmverfolgung

In der Notruf- und Serviceleitstelle (NSL) laufen alle Meldungen zusammen. Sie bewertet, entscheidet und alarmiert – rund um die Uhr, nach einem mit dem Auftraggeber vereinbarten Alarmplan.

B3.1 Ablauf der Alarmbearbeitung

1	**Eingang**	Meldung mit Objekt, Meldergruppe und Zeitstempel geht in der NSL ein und wird quittiert.
2	**Bewertung**	Operator prüft Meldungsart, Verlauf und ggf. Video- oder Audioverifikation.
3	**Rückruf / Codewort**	Kontakt mit dem Objekt oder Rückrufberechtigten; Abfrage des vereinbarten Codeworts.
4	**Alarmierung**	Interventionsdienst, Polizei oder Feuerwehr nach Alarmplan; parallel Information der Ansprechpartner.
5	**Begleitung**	Führung der Interventionskraft, Abgleich der Lage, Nachalarmierung bei Bedarf.
6	**Abschluss**	Protokoll, Einsatzbericht, Wiederherstellung des Scharfzustands, Meldung an den Auftraggeber.

B3.2 Meldungsarten und Reaktion

Meldung	Typische Reaktion der NSL
Einbruchalarm	Verifikation, Alarmverfolgung, bei Anzeichen einer Tat sofort Polizei
Überfall / stiller Alarm	keine Rückfrage im Objekt, sofortige Polizeialarmierung
Sabotage / Leitungsstörung	Rückruf, Technikdienst, bei Verdacht Alarmverfolgung
Technischer Alarm	Ansprechpartner oder Bereitschaft nach Alarmplan, ggf. Fachfirma
Scharfschaltüberwachung	Anlage zur vereinbarten Zeit nicht scharf: Rückruf, ggf. Kontrolle vor Ort
Unscharfschaltung außerhalb der Zeiten	Codewortabfrage, bei Abweichung Alarmverfolgung

B3.3 Qualitätsmerkmale einer Leitstelle

- Zertifizierung als Alarmempfangsstelle nach **DIN EN 50518**, idealerweise mit VdS-Anerkennung nach **VdS 3138**
- Redundante Technik, Notstrom, ständige Besetzung und dokumentierte Ausweichlösung
- Geschultes Personal mit Erlaubnis und Qualifikation nach **§ 34a GewO**
- Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO und nachvollziehbare Protokollierung
- Monatliches Berichtswesen: Alarme, Reaktionszeiten, Fehlalarmquote, Verfügbarkeit

Der Alarmplan – das wichtigste Dokument

Der Alarmplan legt je Meldungsart fest, wer in welcher Reihenfolge informiert wird, welche Maßnahmen die Leitstelle ergreift, welches Codewort gilt und wo Schlüssel liegen. Er wird vom Auftraggeber freigegeben und bei jeder Personal- oder Nummernänderung aktualisiert. Ein veralteter Alarmplan ist die häufigste Ursache für verzögerte Reaktionen.

B3.4 Alarmverfolgung nach DIN 77200-1

Die DIN 77200-1 (aktuelle Fassung 2022-10) beschreibt Mindestanforderungen an Sicherheitsdienstleister. Sie unterscheidet stationäre Dienstleistungen wie den Alarmdienst und mobile Dienstleistungen wie Revier-, Kontroll- und Interventionsdienst. Der Interventionsdienst umfasst vereinbarte Maßnahmen auf ein besonderes, nicht regelmäßiges Ereignis innerhalb einer bestimmten Frist. Die Interventionskraft ist der verlängerte Arm der Leitstelle; jede Alarmverfolgung ist als möglicher Echtalarm zu behandeln.

B3.5 Ablauf vor Ort

1	**Anfahrt**	Auftragsbestätigung an die NSL, Anfahrt unter Beachtung der Straßenverkehrsordnung.
2	**Annäherung**	Eigensicherung, Außenkontrolle, Spuren erkennen und nicht zerstören.
3	**Lagebewertung**	Bei Hinweisen auf Täter im Objekt: kein Betreten, Polizei anfordern, Objekt beobachten.
4	**Innenkontrolle**	Nur bei unauffälliger Lage: Schlüssel entnehmen, Objekt begehen, Ursache feststellen.
5	**Sicherung**	Notverschluss, Anlage zurücksetzen und scharf schalten, ggf. Objektbewachung bis Schadensbehebung.
6	**Bericht**	Einsatzbericht mit Zeiten, Feststellungen und Fotos an Leitstelle und Auftraggeber.

B3.6 Rechte und Grenzen der Interventionskraft

Private Sicherheitskräfte haben keine hoheitlichen Befugnisse. Sie handeln auf Grundlage des vom Auftraggeber übertragenen Hausrechts und der sogenannten Jedermannsrechte:

- **Notwehr und Nothilfe** (§ 32 StGB) sowie **rechtfertigender Notstand** (§ 34 StGB)
- **Vorläufige Festnahme** bei frischer Tat (§ 127 Abs. 1 StPO) – eng auszulegen, nur verhältnismäßige Mittel
- **Besitzwehr und Selbsthilfe** nach §§ 859, 229 BGB
- **Durchsetzung des Hausrechts**, z. B. Aufforderung zum Verlassen und Hausverbot im Namen des Auftraggebers

Haus- und Wegerecht – was im Einsatz gilt

Hausrecht: Es steht dem Eigentümer oder Besitzer zu und folgt aus Eigentum und Besitz (§§ 858 ff., 903, 1004 BGB). Der Sicherheitsdienst kann es nur ausüben, wenn der Auftraggeber es ihm überträgt – am besten schriftlich, mit klarer Beschreibung des Geländes und der Befugnisse (z. B. Hausverbote aussprechen, Personen des Geländes verweisen). Wer trotz Aufforderung bleibt, kann Hausfriedensbruch begehen (§ 123 StGB); die Tat wird nur auf Strafantrag verfolgt, den der Berechtigte stellen muss.

Wegerecht im zivilrechtlichen Sinn: Führt die Zufahrt über fremde Grundstücke – etwa in Gewerbeparks, Mietobjekten oder Werksgeländen mit mehreren Nutzern –, braucht die Interventionskraft ein abgesichertes Zufahrtsrecht, z. B. aus einer Grunddienstbarkeit (§ 1018 BGB), dem Mietvertrag oder einer Vereinbarung mit dem Grundstückseigentümer. Rechte Dritter (Nachbarn, Mitnutzer) darf der Sicherheitsdienst nicht einschränken; das Hausrecht endet an der Grundstücksgrenze des Auftraggebers.

Wegerecht im Straßenverkehr: Private Sicherheitsdienste haben keine Sonder- oder Wegerechte nach §§ 35, 38 StVO – kein Blaulicht, kein Martinshorn, keine Ausnahmen von Geschwindigkeitsgrenzen. Die Interventionszeit muss deshalb realistisch nach Entfernung und Verkehrslage vereinbart werden.

Praxis: Übertragung des Hausrechts, Zufahrts- und Schließberechtigungen (Schranken, Tore, Codes) sowie Ansprechpartner von Grundstückseigentümern gehören schriftlich in den Alarmplan.

B3.7 Schlüssel- und Zugangsmanagement

- Hinterlegung im zertifizierten Schlüsseltresor der Interventionsstelle oder im objektnahen Schlüsseldepot
- Versiegelte, codierte Schlüsseltaschen ohne Objektadresse; Entnahme und Rückgabe werden protokolliert
- Regelmäßige Funktionsprüfung der Schlüssel und Codes, sofortige Meldung bei Schlossänderungen

Querverweise

→ C5 Rechte der Sicherheitskräfte in der Praxis
→ D4 Hausrecht und Personalausweis am Empfang
→ D7 Fernpforte

AUFTRAGGEBER · MITARBEITENDE · UNTERWEISUNG · FEHLALARME VERMEIDEN

B4 Mitwirkung des Auftraggebers

Die beste Leitstelle kann nur so gut reagieren, wie die Informationen sind, die sie erhält. Ein großer Teil aller Fehlalarme und verzögerten Einsätze hat organisatorische Ursachen im Objekt – und lässt sich mit klarer Mitwirkung vermeiden.

B4.1 Mitwirkungspflichten des Auftraggebers

Mitwirkung	Warum sie wichtig ist
Alarmplan freigeben und aktuell halten	Falsche oder veraltete Nummern verzögern jede Reaktion
Mindestens zwei erreichbare Rückrufberechtigte benennen	Entscheidungen vor Ort brauchen eine verantwortliche Person
Schlüssel, Codes und Zufahrtsberechtigungen übergeben	Ohne Zugang endet die Intervention vor der Tür
Hausrecht schriftlich übertragen	Rechtssicherheit für Maßnahmen der Interventionskraft
Änderungen am Objekt melden (Umbau, Mieterwechsel, Lagerung)	Melder können verdeckt oder neu ausgerichtet werden müssen
Wartungs- und Revisionsarbeiten vorab anmelden	Vermeidet Fehlalarme und unnötige Einsätze
Abweichende Arbeitszeiten und Sonderöffnungen ankündigen	Unscharfschaltungen werden sonst als Verdachtsfall bearbeitet
Instandhaltung nach DIN VDE 0833 beauftragen	Pflicht des Betreibers, oft Versicherungsauflage
Einsatzberichte prüfen und Mängel beheben lassen	Wiederkehrende Ursachen werden nur so abgestellt

B4.2 Mitwirkung der Mitarbeitenden

Mitarbeitende schalten die Anlage scharf und unscharf, öffnen Türen und Fenster und sind oft als erste vor Ort. Sie brauchen deshalb eine kurze, regelmäßig wiederholte Unterweisung:

- **Scharfschalten:** Vorher Fenster, Türen und Tore schließen, Bewegungsbereiche räumen, keine Gegenstände vor Meldern abstellen
- **Codes und Codewort:** persönliche Codes nicht weitergeben; Codewort kennen, das die Leitstelle beim Rückruf abfragt
- **Fehlbedienung sofort melden:** Wer versehentlich Alarm auslöst, ruft unverzüglich die Leitstelle an – das spart einen Einsatz
- **Überfall- und Notsituationen:** stillen Alarm kennen und auslösen, sich selbst nicht gefährden, nicht mit Tätern verhandeln
- **Neue Mitarbeitende:** Einweisung vor erster Schlüssel- oder Codeausgabe, Codes ausgeschiedener Personen sofort löschen

B4.3 Häufige Fehlalarm-Ursachen und Gegenmaßnahmen

Ursache	Gegenmaßnahme
Fehlbedienung bei Scharf- oder Unscharfschaltung	Unterweisung, Blockschloss oder Zwangsläufigkeit, klare Bedienanleitung
Offene Fenster, Türen, Tore beim Scharfschalten	Verschlussüberwachung, Checkliste am Ausgang
Tiere, Heizungsluft, Ballons, Dekoration	Melderauswahl und -ausrichtung prüfen lassen
Bauarbeiten, Staub, Feuchtigkeit	Arbeiten vorab melden, Melder abdecken lassen, nach Abschluss prüfen
Veraltete oder verschmutzte Melder	Instandhaltung nach DIN VDE 0833, Tausch statt Dauerprovisorium

Versicherung: Obliegenheiten ernst nehmen

Viele Gewerbe-Versicherungsverträge vereinbaren das Vorhandensein und Scharfschalten einer Einbruchmeldeanlage als Obliegenheit. Wird sie vorsätzlich oder grob fahrlässig verletzt – etwa weil die Anlage nicht scharf geschaltet oder nicht gewartet war –, kann der Versicherer nach § 28 VVG seine Leistung kürzen oder ganz verweigern. Scharfschaltprotokolle der Leitstelle sind im Schadensfall ein wichtiger Nachweis.

Datenschutz und Mitbestimmung

Alarmpläne enthalten Namen und Telefonnummern, Scharfschaltprotokolle zeigen, wer wann das Objekt betreten oder verlassen hat. Mitarbeitende sind nach Art. 13 DSGVO zu informieren. Lassen sich aus den Daten Verhalten oder Leistung ableiten, hat ein vorhandener Betriebsrat ein Mitbestimmungsrecht (§ 87 Abs. 1 Nr. 6 BetrVG) – eine kurze Betriebsvereinbarung schafft Klarheit.

Querverweise

→ C5 Mitwirkung im Objektschutz
→ D6 Mitwirkung am Empfang

ERSCHWEREN · ERKENNEN · ORGANISIEREN

B5 Präventive Gefahrenabwehr

Der beste Alarm ist der, der nie ausgelöst wird. Präventive Gefahrenabwehr verbindet mechanischen Widerstand, organisatorische Regeln und sichtbare Präsenz – und macht Meldetechnik und Intervention erst wirksam.

B5.1 Grundsatz: Mechanik, Elektronik, Organisation

Die polizeiliche Beratung folgt dem Grundsatz, dass mechanische Sicherungen den Täter aufhalten und elektronische Meldetechnik ihn entdeckt. Erst wenn der Widerstand länger hält, als Alarmierung und Intervention brauchen, wird eine Tat verhindert statt nur gemeldet. Die kriminalpolizeilichen Beratungsstellen beraten dazu kostenfrei und herstellerneutral; SecuConCept ergänzt dies um ein objektbezogenes Gesamtkonzept mit Aufschaltung, Intervention und Prävention aus einer Hand.

Widerstandsklasse DIN EN 1627	Tätertyp und Vorgehen	Typischer Einsatz
RC 2	Gelegenheitstäter mit einfachem Werkzeug	Wohnobjekte, Büros, Nebeneingänge
RC 3	Täter mit zusätzlichem Werkzeug, z. B. Brecheisen	Gewerbe, Lager, Rückseiten von Filialen
RC 4 – RC 6	erfahrene Täter mit Elektrowerkzeug	Hochwertlager, Technikräume, Sonderobjekte

B5.2 Bausteine der Prävention

Baustein	Inhalt
Schwachstellenanalyse	Begehung bei Tag und Nacht, Täterperspektive, Bewertung von Zugängen, Beleuchtung, Sichtachsen
Sicherheitskonzept	Schutzziele, Maßnahmenmix aus Mechanik, Technik und Organisation, Verantwortlichkeiten
Revier- und Kontrolldienst	Unregelmäßige Kontrollen zu wechselnden Zeiten, sichtbare Präsenz, Mängelmeldungen
Schließ- und Öffnungsdienst	Kontrolliertes Verschließen, Scharfschalten und Protokollieren am Abend
Zutritts- und Schlüsselmanagement	Berechtigungen nach Bedarf, Verlustprozess, regelmäßige Bereinigung
Beleuchtung und Gelände	Bewegungslicht, freie Sichtachsen, keine Aufstiegshilfen an Fassaden
Notfall- und Krisenmanagement	Alarm- und Notfallpläne, Ansprechpartner, Übungen, Nachbereitung
Brandschutz-Prävention	Brandschutzordnung, Brandschutzhelfer, Brandwachen bei Heißarbeiten

§ 34A GEWO · FEHLALARMGEBÜHREN · DSGVO

B6 Recht, Haftung und Datenschutz

Aufschaltung und Alarmverfolgung berühren Gewerbe-, Polizei-, Zivil- und Datenschutzrecht. Diese Punkte sollten vertraglich geregelt sein.

B6.1 Gewerberecht

- Bewachungsunternehmen brauchen eine **Erlaubnis nach § 34a GewO**; die Mitarbeitenden sind im **Bewacherregister** erfasst und benötigen je nach Tätigkeit eine **Unterrichtung** oder **Sachkundeprüfung** vor der IHK.
- Die Bewachungsverordnung regelt u. a. Haftpflichtversicherung, Dienstanweisungen und Ausweispflicht.

B6.2 Fehlalarme und Gebühren

Ob und in welcher Höhe Polizei oder Feuerwehr Gebühren für Fehlalarme erheben, regelt das Landesrecht bzw. die kommunale Gebührensatzung. Das Bundesverwaltungsgericht hält angemessene Gebühren für einen durch eine Alarmanlage veranlassten Polizeieinsatz für zulässig. Das VG Neustadt bestätigte 120 € für die ungerechtfertigte Alarmierung durch eine Einbruchmeldeanlage; als ungerechtfertigt gilt ein Alarm, wenn die Polizei keine Ursache feststellen kann. Feuerwehren berechnen Fehlalarme meist nach Zeit, Personal und Fahrzeugen. In Baden-Württemberg wurden in einem Jahr rund 29.500 Feuerwehreinsätze als Fehlalarm eingestuft.

B6.3 Haftung und Vertrag

- Leistungsumfang, Interventionszeit, Schlüsselhaftung, Haftungsgrenzen und Fremdschäden bei Notöffnung schriftlich festlegen
- Die Leitstelle verantwortet Bearbeitung und Alarmierung, nicht die Funktion der Anlage im Objekt
- Nachweis der Betriebshaftpflicht- und Schlüsselversicherung des Dienstleisters anfordern

B6.4 Datenschutz

Thema	Umsetzung
Rollen	NSL und Interventionsdienst arbeiten in der Regel als Auftragsverarbeiter: AV-Vertrag nach Art. 28 DSGVO
Datenumfang	Nur erforderliche Kontaktdaten im Alarmplan; Codes und Codewörter getrennt und geschützt
Speicherfristen	Alarmprotokolle und Einsatzberichte nach vereinbarter Frist löschen, Ausnahmen bei Schäden und Verfahren
Video, Audio und Technik	Verifikation nur zur Alarmprüfung; verschlüsselte Übertragung, rollenbasierter und protokollierter Zugriff

ORIENTIERUNGSWERTE · INVESTITION · BETRIEB

B7 Kostenbeispiele und Wirtschaftlichkeit

Die Beispiele zeigen typische Kostenstrukturen für Budgetplanung und Vergleich. Alle Werte netto, Marktniveau 2026; tatsächliche Kosten hängen von Objektgröße, Grad, Übertragungsweg, Entfernung zur Interventionsstelle und Leistungsumfang ab.

Beispiel A – Lager- und Bürogebäude, 1.500 m², EMA Grad 3 / VdS-Klasse B

Position	Menge	Einzelpreis	Gesamt
Schwachstellenanalyse und Planung	pauschal		1.200 €
Einbruchmelderzentrale mit Bedienteil	1	2.400 €	2.400 €
Bewegungsmelder	24	95 €	2.280 €
Öffnungs- und Verschlussüberwachung	12	65 €	780 €
Außensignalgeber mit Blitzleuchte	1	450 €	450 €
Übertragungseinrichtung IP/LTE, Dual Path	1	650 €	650 €
Montage und Inbetriebnahme	pauschal		3.800 €
Abnahme und Installationsattest	pauschal		450 €
Investition gesamt (netto)			**12.010 €**

Laufende Kosten pro Jahr	Berechnung	Betrag
Aufschaltung NSL inkl. Scharfschaltüberwachung	49 € × 12 Monate	588,00 €
Schlüsselhinterlegung	15 € × 12 Monate	180,00 €
Mobilfunktarif Ersatzweg	9,90 € × 12 Monate	118,80 €
Instandhaltung nach DIN VDE 0833	2 × 290 €	580,00 €
Alarmverfolgung (Annahme: 6 Einsätze)	6 × 95 €	570,00 €
Abschreibung Investition (10 Jahre linear)	12.010 € ÷ 10	1.201,00 €
Jährliche Gesamtkosten		**3.237,80 €**

Entspricht rund 270 € pro Monat bzw. knapp 9 € pro Tag für die Absicherung des gesamten Objekts.

Beispiel B – Was Fehlalarme kosten und was Prävention spart

Position	Vorher (12 Fehlalarme)	Nachher (3 Fehlalarme)
Alarmverfolgung à 95 €	1.140,00 €	285,00 €
Polizeigebühr à 120 € (Annahme: 4 bzw. 1 Fall)	480,00 €	120,00 €
Interner Aufwand (1,5 h à 45 € je Fehlalarm)	810,00 €	202,50 €
Kosten pro Jahr	**2.430,00 €**	**607,50 €**

Einmaliger Aufwand für Unterweisung der Mitarbeitenden und Melderoptimierung (Annahme): 750 €. Ersparnis im ersten Jahr: 1.822,50 € − 750 € = 1.072,50 €, ab dem zweiten Jahr 1.822,50 € jährlich.

Beispiel C – Präventiver Revierdienst ergänzend zur Aufschaltung

Position	Berechnung	Betrag
Nachtkontrolle an allen Tagen	365 × 22 €	8.030 €
Zusätzliche Tageskontrolle am Wochenende	104 × 22 €	2.288 €
Revierdienst pro Jahr		**10.318 €**

Advocatus Diaboli: Billig aufgeschaltet ist teuer bezahlt

Niedrige Monatspreise für die Aufschaltung sagen wenig über die Leistung. Entscheidend sind Zertifizierung der Leitstelle, vereinbarte Interventionszeit, Qualifikation der Einsatzkräfte, Schlüsselhaftung und Berichtswesen. Ein Angebot ohne verbindliche Interventionszeit oder ohne Nachweis nach DIN EN 50518 ist nicht vergleichbar – und im Schadensfall oft auch nicht versicherungsfest.

VON DER ANALYSE BIS ZUM REGELBETRIEB

B8 Checkliste für Auftraggeber

Die Checkliste eignet sich für interne Abstimmung, Ausschreibung und Nachweis gegenüber Versicherer, Aufsicht und Prüfern.

Phase 1 – Analyse	
☐	Schutzziele, Werte und Risiken je Objekt festlegen; Versicherungsauflagen prüfen
☐	Schwachstellenanalyse mit Begehung bei Tag und Nacht
☐	Bestandsanlagen erfassen: Grad/Klasse, Alter, Übertragungsweg, 2G-Abhängigkeit
☐	Aufschaltziele klären: NSL, Polizei, Feuerwehr über Konzessionär

Phase 2 – Konzeption und Vergabe	
☐	Sicherheitskonzept aus Mechanik, Meldetechnik, Organisation und Intervention
☐	Leistungsbeschreibung mit Interventionszeit, Berichtswesen und Haftung
☐	Nachweise anfordern: DIN EN 50518 / VdS 3138, § 34a GewO, Versicherungen, AV-Vertrag
☐	Zufahrts- und Wegerechte bei fremden Grundstücken klären

Phase 3 – Inbetriebnahme	
☐	Alarmplan, Codewort und Rückrufberechtigte festlegen und freigeben
☐	Schlüssel, Codes und Zufahrtsberechtigungen protokolliert übergeben
☐	Hausrecht schriftlich übertragen
☐	Mitarbeitende unterweisen, Datenschutzinformation und ggf. Betriebsvereinbarung
☐	Probealarm über alle Übertragungswege durchführen

Phase 4 – Regelbetrieb	
☐	Alarmplan bei jeder Änderung aktualisieren, mindestens jährlich prüfen
☐	Instandhaltung nach DIN VDE 0833 und Prüfung der Übertragungswege
☐	Monatliches Reporting auswerten, wiederkehrende Fehlalarme abstellen
☐	Unterweisung jährlich und bei neuen Mitarbeitenden wiederholen

KURZ UND BELASTBAR BEANTWORTET

B9 Häufige Fragen (FAQ)

Was ist der Unterschied zwischen Aufschaltung und Alarmverfolgung?

Die Aufschaltung verbindet die Gefahrenmeldeanlage mit einer ständig besetzten Leitstelle, die Meldungen bewertet. Die Alarmverfolgung ist der Einsatz vor Ort, den die Leitstelle nach dem Alarmplan auslöst.

Kann ich meine Brandmeldeanlage auf eine private Leitstelle aufschalten?

Bauordnungsrechtlich geforderte Brandmeldeanlagen müssen über den Konzessionär auf die Feuerwehr aufgeschaltet werden. Eine private Leitstelle kann ergänzend Störungen überwachen und Schlüssel sowie Einweisung im Einsatz organisieren.

Wie schnell ist die Interventionskraft vor Ort?

Das hängt von Entfernung, Verkehrslage und Vertrag ab. Sicherheitsdienste haben keine Sonderrechte im Straßenverkehr; seriöse Anbieter vereinbaren eine realistische, messbare Interventionszeit je Objekt.

Darf die Interventionskraft einen Täter festhalten?

Nur im Rahmen der Jedermannsrechte, insbesondere der vorläufigen Festnahme bei frischer Tat nach § 127 StPO, und mit verhältnismäßigen Mitteln. Eigensicherung und Polizeialarmierung haben Vorrang.

Wer zahlt bei einem Fehlalarm?

Einsätze des Interventionsdienstes werden nach Vertrag abgerechnet. Gebühren der Polizei oder Feuerwehr richten sich nach Landesrecht bzw. kommunaler Satzung und treffen in der Regel den Betreiber der Anlage.

Funktioniert meine Alarmanlage nach der 2G-Abschaltung noch?

Wenn die Übertragungseinrichtung nur GSM nutzt, nicht mehr zuverlässig. Lassen Sie den Übertragungsweg jetzt prüfen – oft genügt ein Modul- oder Gerätetausch.

Welche Mitwirkung wird von uns erwartet?

Ein aktueller Alarmplan, erreichbare Ansprechpartner, übergebene Schlüssel und Codes, das schriftlich übertragene Hausrecht, angemeldete Wartungsarbeiten und unterwiesene Mitarbeitende.

Brauchen wir für die Aufschaltung eine neue Alarmanlage?

Meist nicht. Bestehende Anlagen lassen sich häufig mit einer neuen Übertragungseinrichtung aufschalten, sofern Grad und Zustand zum Risiko passen.

TEIL C

Sicherheitsdienste in der Praxis: Wachschutz oder Werkschutz

Abgrenzung von Wach- und Werkschutz, § 34a GewO und Qualifikationen, Eigenpersonal oder Dienstleister, Praxis im Objekt und die Kalkulation eines Stundensatzes.

KAPITEL

C1 Auf einen Blick
C2 Wachschutz und Werkschutz
C3 Recht, Qualifikation und Arbeitsschutz
C4 Eigenpersonal oder Dienstleister
C5 Praxis im Objekt
C6 Qualität und Vergabe
C7 Was eine Stunde Sicherheit kostet
C8 Checkliste für Auftraggeber
C9 Häufige Fragen (FAQ)

VERWANDTE TEILE

Teil B Aufschaltung von Gefahrenmeldeanlagen, Alarmverfolgung und präventive Gefahrenabwehr – Rechte und Hausrecht im Einsatz
Teil D Empfangsdienst & Pförtnerdienst – Einlass mit Kontrolle – Empfang und Pforte
Teil E KRITIS: Sicherheitsdienste als All-in-One-Lösung? – Integriertes Dienstleistermodell

KERNAUSSAGEN FÜR ENTSCHEIDER

C1 Auf einen Blick

Die zehn wichtigsten Fakten für alle, die Sicherheitsdienste beauftragen, organisieren oder neu aufstellen.

1	**Wachschutz schützt Objekte, Werkschutz schützt Betriebe:** Werkschutz ist tiefer in Prozesse, Gefahrenabwehr und Notfallorganisation eines Standorts eingebunden.
2	**Eigenes Personal braucht keine Erlaubnis nach § 34a GewO:** Die Bewachung des eigenen Unternehmens durch eigene Mitarbeitende ist keine gewerbliche Bewachung.
3	**Externe Dienstleister brauchen sie immer:** Erlaubnis des Unternehmens, Unterrichtung (40 Stunden) oder Sachkundeprüfung der Mitarbeitenden, Eintrag im Bewacherregister.
4	**Die DGUV Vorschrift 23** regelt Eignung, Dienstanweisung, Objekteinweisung und Ausrüstung – und verbietet Weisungen, die dem Sicherungsauftrag widersprechen.
5	**Tariflöhne sind allgemeinverbindlich:** 2026 liegen die Stundengrundlöhne je nach Land und Tätigkeit etwa zwischen 15 und 19 Euro – deutlich über dem Mindestlohn von 13,90 Euro.
6	**Ein seriöser Stundensatz** liegt deshalb meist bei rund dem Doppelten des Tariflohns. Deutlich günstigere Angebote sind ein Warnsignal.
7	**Ein 24/7-Posten** umfasst 8.760 Stunden im Jahr und braucht rund fünf bis sechs Vollzeitkräfte inklusive Urlaub, Krankheit und Schulung.
8	**Vorsicht Scheinwerkvertrag:** Wer externen Sicherheitskräften direkt Weisungen erteilt, riskiert eine unerlaubte Arbeitnehmerüberlassung.
9	**Qualität ist messbar:** mit klarer Leistungsbeschreibung, Kennzahlen, Rundgangsnachweisen, Audits und einem festen Objektleiter.
10	**Das stärkste Modell ist oft hybrid:** eigene Werkschutzleitung mit Betriebskenntnis, operative Leistung durch einen qualifizierten Dienstleister.

BEGRIFFE · ABGRENZUNG · LEISTUNGSARTEN

C2 Wachschutz und Werkschutz

Im Alltag werden Wachschutz, Objektschutz und Werkschutz oft gleichgesetzt. Für die Planung lohnt die Unterscheidung: Sie bestimmt Aufgaben, Qualifikation, Einbindung in den Betrieb – und damit die Kosten.

C2.1 Der Unterschied im Überblick

Merkmal	Wachschutz / Objektschutz	Werkschutz
Schutzziel	Gebäude, Gelände, Sachwerte	Gesamter Betrieb: Menschen, Anlagen, Prozesse, Know-how
Typische Objekte	Büros, Wohnanlagen, Lager, Baustellen, Leerstand	Industrie, Chemie, Energie, Logistikzentren, KRITIS
Einbindung	Auftrag mit klar abgegrenzten Aufgaben	Teil der Betriebsorganisation, enge Abstimmung mit Werksleitung, HSE und Werkfeuerwehr
Aufgabentiefe	Kontrolle, Präsenz, Meldung, Erstmaßnahmen	Zutritt, Werksverkehr, Material- und Fahrzeugkontrolle, Notfall- und Störfallorganisation
Qualifikation	Unterrichtung oder Sachkunde nach § 34a GewO	zusätzlich Werkschutzfachkraft, Brandschutz, Gefahrstoffkenntnis, Ersthelfer
Organisation	überwiegend externer Dienstleister	eigenes Personal, Dienstleister oder hybrides Modell

C2.2 Leistungsarten nach DIN 77200-1

Die DIN 77200-1 (Fassung 2022-10) beschreibt Mindestanforderungen an Sicherheitsdienstleister und unterscheidet stationäre und mobile Sicherungsdienstleistungen sowie den Veranstaltungssicherungsdienst.

Leistung	Inhalt	Typischer Einsatz
Separatwach- / Objektschutzdienst	dauerhafte Präsenz an einem Objekt, Kontrollgänge, Meldungen	Industrie, Verwaltung, Baustellen
Empfangs- und Pfortendienst	Zutritt, Besucher- und Schlüsselmanagement, Telefon	Firmensitze, Werkstore
Kontrolldienst	Kontrollen an festgelegten Punkten und Zeiten	Leerstand, Technikbereiche
Revierdienst	mehrere Objekte im Wechsel, unregelmäßige Kontrollen	Gewerbegebiete, Filialnetze
Interventionsdienst	Einsatz auf Alarm innerhalb vereinbarter Frist	aufgeschaltete Objekte
Veranstaltungsdienst	Einlass, Ordnungsdienst, Brandschutz	Messen, Werksfeste, Events

C2.3 Typische Aufgaben im Werkschutz

- **Zutritt und Werksverkehr:** Ausweis- und Besuchermanagement, Fremdfirmenkontrolle, Lkw-Abfertigung, Verkehrsregelung im Werk
- **Material- und Fahrzeugkontrollen:** Warenausgang, Stichproben nach Betriebsvereinbarung, Ladungs- und Plombenkontrolle
- **Gefahrenabwehr:** Brandschutzrundgänge, Erste Hilfe, Unterstützung der Werkfeuerwehr, Einweisung von Rettungskräften
- **Störfall- und Notfallorganisation:** Alarmierung, Evakuierung, Absperrung, Lagemeldung an die Werksleitung
- **Technik:** Bedienung von Gefahrenmanagement, Video, Zutrittskontrolle und Leitstelle

Aus der Praxis

Im industriellen Werkschutz – insbesondere in der Chemie – ist der Sicherheitsdienst Teil der betrieblichen Gefahrenabwehr. Wer dort arbeitet, muss Anlagen, Fluchtwege, Sammelplätze und Alarmstufen kennen. Diese Betriebskenntnis ist der eigentliche Mehrwert des Werkschutzes – und sie entsteht nur durch feste Teams, gründliche Objekteinweisung und regelmäßige Übungen.

§ 34A GEWO · BEWACHERREGISTER · DGUV VORSCHRIFT 23

C3 Recht, Qualifikation und Arbeitsschutz

Wer gewerbsmäßig Leben oder Eigentum fremder Personen bewacht, unterliegt dem Bewachungsrecht. Für eigenes Personal gelten andere Regeln – Arbeitsschutz und Qualifikation bleiben aber in beiden Fällen Pflicht.

C3.1 Wer braucht was?

Konstellation	Erlaubnis § 34a GewO	Qualifikation der Mitarbeitenden
Eigener Werkschutz / eigene Pforte	nicht erforderlich	keine gesetzliche Vorgabe nach § 34a; Qualifikation nach Gefährdungsbeurteilung und DGUV Vorschrift 23
Externer Objekt- und Werkschutz	Unternehmen benötigt Erlaubnis	mindestens Unterrichtung (40 Stunden) bei der IHK
Kontrollgänge im öffentlichen Verkehrsraum oder in Bereichen mit tatsächlich öffentlichem Verkehr	erforderlich	Sachkundeprüfung
Schutz vor Ladendieben, Einlass in Diskotheken	erforderlich	Sachkundeprüfung
Leitende Funktion in Flüchtlingsunterkünften und zugangsgeschützten Großveranstaltungen	erforderlich	Sachkundeprüfung

Bestimmte Berufs- und Fortbildungsabschlüsse ersetzen Unterrichtung bzw. Sachkundeprüfung, etwa Fachkraft oder Servicekraft für Schutz und Sicherheit, Geprüfte Schutz- und Sicherheitskraft, Geprüfte Werkschutzfachkraft sowie Meister für Schutz und Sicherheit (§ 8 BewachV).

C3.2 Qualifikationsstufen im Überblick

Stufe	Abschluss	Typische Rolle
Basis	Unterrichtung nach § 34a GewO (40 Stunden)	Objektschutz, Pforte, Werkschutz (extern)
Erweitert	Sachkundeprüfung nach § 34a GewO	Revierdienst, Veranstaltungen, Schicht- und Teamleitung
Fortbildung	Geprüfte Schutz- und Sicherheitskraft (IHK), Geprüfte Werkschutzfachkraft	Objektleitung, qualifizierter Werkschutz
Ausbildung	Servicekraft (2 Jahre) bzw. Fachkraft für Schutz und Sicherheit (3 Jahre)	Werkschutz, Leitstelle, Führungsnachwuchs
Führung	Meister für Schutz und Sicherheit, Werkschutzmeister	Werkschutzleitung, Niederlassungs- und Bereichsleitung

C3.3 Bewacherregister und Zuverlässigkeit

Seit 1. Juni 2019 erfasst das bundesweite Bewacherregister (§ 11b GewO) Bewachungsunternehmen und deren Mitarbeitende. Vor dem Einsatz prüft die Behörde die Zuverlässigkeit; Wachpersonen tragen im Dienst einen Ausweis und ein Namensschild oder eine Kennnummer. Auftraggeber sollten sich die Anmeldung der eingesetzten Personen bestätigen lassen.

C3.4 Arbeitsschutz: DGUV Vorschrift 23

Die Unfallverhütungsvorschrift „Wach- und Sicherungsdienste“ gilt für alle Wach- und Sicherungstätigkeiten zum Schutz von Personen und Sachwerten – unabhängig davon, ob eigenes Personal oder ein Dienstleister eingesetzt wird. Kernpunkte:

- **Eignung und Befähigung** der eingesetzten Personen, dokumentiert
- **Schriftliche Dienstanweisung** und regelmäßige Unterweisung, u. a. zu Konfrontationen, Überfällen, Brandschutz und Erster Hilfe
- **Objekteinweisung** vor dem ersten Einsatz, Ausrüstung z. B. mit leistungsfähigen Handleuchten
- **Verbot berauschender Mittel** im Dienst
- **Keine Weisungen des Auftraggebers befolgen, die dem Sicherungsauftrag entgegenstehen**

Alleinarbeit absichern

Nachtdienst und Rundgänge finden häufig allein statt. Nach der Gefährdungsbeurteilung kann eine Personen-Notsignal-Anlage erforderlich sein; die DGUV Regel 112-139 beschreibt Auswahl, Betrieb und Betriebsanweisung. Für eigene Werkschutzkräfte trägt der Betrieb diese Verantwortung selbst, beim Dienstleister liegt sie bei dessen Arbeitgeber – die Abstimmung über Gefahren im Objekt bleibt Pflicht beider Seiten (§ 8 ArbSchG).

MAKE OR BUY · HYBRIDMODELL · SCHEINWERKVERTRAG

C4 Eigenpersonal oder Dienstleister

Die Frage „eigener Werkschutz oder externer Dienstleister?“ ist keine reine Kostenfrage. Entscheidend sind Betriebskenntnis, Ausfallsicherheit, Flexibilität, Führungsaufwand und Haftung.

C4.1 Vergleich der Modelle

Kriterium	Eigener Werkschutz	Externer Dienstleister	Hybrid
Betriebskenntnis	sehr hoch	abhängig von Teamkonstanz	hoch durch eigene Leitung
Ausfall, Urlaub, Krankheit	eigenes Risiko	vertraglich beim Dienstleister	beim Dienstleister
Rekrutierung und Schulung	eigener Aufwand	Dienstleister	überwiegend Dienstleister
Flexibilität bei Mehrbedarf	gering	hoch	hoch
Führung und Kontrolle	eigene Linie	über Objektleiter des Dienstleisters	eigene Werkschutzleitung steuert
§ 34a GewO	nicht erforderlich	erforderlich	für externen Teil
Tarif und Arbeitsrecht	Haustarif bzw. Branchentarif des Betriebs	Tarif Sicherheitsdienstleistungen	gemischt

C4.2 Das Hybridmodell

In vielen Industrie- und KRITIS-Betrieben hat sich eine Aufteilung bewährt: Eine eigene Werkschutz- oder Sicherheitsleitung kennt den Betrieb, setzt Standards und ist Ansprechpartner für Werksleitung und Behörden. Der operative Dienst – Pforte, Rundgänge, Leitstelle, Spitzenlasten – wird von einem qualifizierten Dienstleister erbracht, der Ausfälle kompensiert und Personal vorhält. So bleibt die Betriebskenntnis im Haus, ohne dass der Betrieb ein komplettes Sicherheitsunternehmen führen muss.

Scheinwerkvertrag vermeiden

Wird externes Sicherheitspersonal wie eigene Mitarbeitende geführt – also direkt angewiesen, in eigene Dienstpläne eingeplant oder in die Betriebsorganisation eingegliedert –, kann aus dem Dienstvertrag eine verdeckte Arbeitnehmerüberlassung werden. Fehlt die Erlaubnis nach dem Arbeitnehmerüberlassungsgesetz, drohen ein fingiertes Arbeitsverhältnis mit dem Auftraggeber, Bußgelder und Nachzahlungen von Sozialversicherungsbeiträgen.

So bleibt der Vertrag sauber: Leistung und Ergebnis im Vertrag beschreiben, nicht Arbeitszeiten einzelner Personen. Fachliche Anforderungen fließen über die Dienstanweisung ein, die der Dienstleister erlässt. Anliegen aus dem Betrieb laufen über den Objektleiter des Dienstleisters – nicht direkt an einzelne Sicherheitskräfte.

C4.3 Wann welches Modell passt

- **Externer Dienstleister:** Standorte ohne besondere Prozessgefahren, wechselnder Bedarf, mehrere Objekte, Baustellen, Leerstand
- **Eigener Werkschutz:** sehr hohe Anforderungen an Betriebskenntnis und Geheimhaltung, große Standorte mit Werkfeuerwehr und eigener Leitstelle
- **Hybrid:** Industrie, Chemie, Energie, Logistikzentren und KRITIS-Anlagen mit Bedarf an Steuerung im Haus und flexibler Umsetzung

C4.4 Entscheidungsmatrix

Bewerten Sie jedes Kriterium für Ihren Standort mit 1 (gering) bis 5 (hoch) und multiplizieren Sie mit der Gewichtung. Hohe Werte bei den ersten drei Kriterien sprechen für eigene Steuerung, hohe Werte bei den letzten drei für einen Dienstleister – liegen beide Gruppen hoch, ist das Hybridmodell meist die beste Wahl.

Kriterium	Leitfrage	Gewichtung
Betriebskenntnis	Wie stark hängt die Sicherheit von Prozess- und Anlagenwissen ab?	× 3
Vertraulichkeit	Wie sensibel sind Know-how, Zutritt und Informationen?	× 2
Gefahrenabwehr im Betrieb	Ist der Dienst Teil von Brandschutz, Störfall- und Notfallorganisation?	× 3
Schwankender Bedarf	Gibt es Spitzen, Projekte, Baustellen oder saisonale Lasten?	× 2
Ausfallrisiko	Wie kritisch wäre ein unbesetzter Posten?	× 3
Führungskapazität	Fehlen eigene Ressourcen für Rekrutierung, Schulung und Dienstplanung?	× 2

DIENSTANWEISUNG · RUNDGÄNGE · KONTROLLEN · DOKUMENTATION

C5 Praxis im Objekt

Gute Sicherheitsdienste erkennt man nicht an der Uniform, sondern an klaren Abläufen, nachvollziehbarer Dokumentation und Mitarbeitenden, die ihr Objekt kennen.

C5.1 Vom Auftrag zum laufenden Dienst

1	**Objektaufnahme**	Begehung, Schutzziele, Risiken, Schnittstellen zu Technik, Werkfeuerwehr und Haustechnik.
2	**Dienstanweisung**	Aufgaben, Rundgangsplan, Meldewege, Verhalten im Notfall, Befugnisse – vom Dienstleister erlassen, mit dem Auftraggeber abgestimmt.
3	**Objekteinweisung**	Jede Sicherheitskraft vor dem ersten Dienst: Gelände, Technik, Fluchtwege, Ansprechpartner, Gefahrstellen.
4	**Einarbeitung**	Begleitete Dienste, besonders für Pforte, Leitstelle und Werkschutzaufgaben.
5	**Regelbetrieb**	Dienstplan, Schichtübergabe, Rundgänge, Berichte, Mängelmeldungen.
6	**Überprüfung**	Regelmäßige Objektbesuche, Audits, Kennzahlen, Aktualisierung der Dienstanweisung.

C5.2 Rundgänge und Dokumentation

- **Digitale Wächterkontrolle:** Kontrollpunkte per NFC oder QR-Code belegen Zeit und Ort jedes Rundgangs
- **Unregelmäßige Zeiten und Routen:** Vorhersehbare Rundgänge sind für Täter ein offenes Buch
- **Mängelmeldungen mit Foto:** offene Türen, defekte Beleuchtung, Brandlasten, beschädigte Zäune
- **Wachbuch und Schichtübergabe:** lückenlose Übergabe von Besonderheiten, Schlüsseln und offenen Vorgängen
- **Monatsbericht:** Ereignisse, Mängel, Kennzahlen und Empfehlungen für den Auftraggeber

C5.3 Kontrollen von Personen, Taschen und Fahrzeugen

Kontrollen beim Verlassen des Werksgeländes sind im Werkschutz verbreitet, aber rechtlich sensibel. Sicherheitskräfte haben keine Durchsuchungsbefugnis; Kontrollen erfolgen auf Grundlage des Hausrechts, arbeitsvertraglicher Regelungen und – bei vorhandenem Betriebsrat – einer Betriebsvereinbarung, denn Torkontrollen betreffen die Ordnung des Betriebs (§ 87 Abs. 1 Nr. 1 BetrVG). Gegen den Willen der betroffenen Person darf nicht durchsucht werden; bei konkretem Verdacht einer Straftat wird die Polizei hinzugezogen.

Rechte der Sicherheitskräfte

Private Sicherheitskräfte haben keine hoheitlichen Befugnisse. Sie handeln mit dem vom Auftraggeber übertragenen Hausrecht und den Jedermannsrechten: Notwehr und Nothilfe (§ 32 StGB), Notstand (§ 34 StGB), vorläufige Festnahme bei frischer Tat (§ 127 Abs. 1 StPO) sowie Besitzwehr und Selbsthilfe (§§ 859, 229 BGB). Das Hausrecht sollte schriftlich übertragen und das Gelände genau beschrieben sein.

C5.4 Mitwirkung des Auftraggebers

- Einen festen Ansprechpartner benennen und Anliegen über den Objektleiter des Dienstleisters steuern
- Änderungen an Gebäuden, Nutzungen, Zutrittsberechtigungen und Technik rechtzeitig mitteilen
- Mitarbeitende über Aufgaben und Befugnisse des Sicherheitsdienstes informieren – das erhöht Akzeptanz und Wirkung
- Mängelmeldungen aus den Berichten zeitnah abarbeiten und Rückmeldung geben

Querverweise

→ B3 Infobox Haus- und Wegerecht
→ B4 Mitwirkung des Auftraggebers

LEISTUNGSBESCHREIBUNG · KENNZAHLEN · TARIFTREUE

C6 Qualität und Vergabe

Sicherheitsdienstleistungen werden noch zu oft über den niedrigsten Stundensatz vergeben. Das Ergebnis sind hohe Fluktuation, wechselnde Gesichter und sinkende Betriebskenntnis – also genau das Gegenteil von Sicherheit.

C6.1 Bausteine einer guten Ausschreibung

Baustein	Worauf es ankommt
Leistungsbeschreibung	Schutzziele, Aufgaben, Zeiten, Qualifikationen, Ausrüstung, Schnittstellen – Bezug auf DIN 77200-1
Personal	Anteil fest eingesetzter Mitarbeitender, Einarbeitungskonzept, Vertretungsregel, Sprachkenntnisse
Nachweise	Erlaubnis § 34a GewO, Bewacherregister, Haftpflicht- und Schlüsselversicherung, Zertifikate
Tarif und Löhne	Zusicherung der Tariftreue, Offenlegung der Lohngruppen, Regelung zu Nachunternehmern
Bewertung	Bestbieterprinzip: Konzept, Qualität und Referenzen gewichten, nicht nur den Preis
Einstieg	Probephase mit festgelegten Kennzahlen und Abnahme

C6.2 Kennzahlen für den Regelbetrieb

Kennzahl	Aussage	Zielrichtung
Besetzungsquote	Wie viele Soll-Stunden wurden tatsächlich geleistet?	100 %
Rundgangserfüllung	Wie viele Kontrollpunkte wurden zur geplanten Zeit erreicht?	möglichst 100 %
Teamkonstanz	Anteil fest eingesetzter, eingewiesener Mitarbeitender	hoch
Reaktionszeit	Zeit bis zur Maßnahme bei Ereignissen und Alarmen	vertraglich festgelegt
Mängelquote	gemeldete und erledigte Mängel	Abarbeitung nachverfolgen
Beschwerden	Rückmeldungen von Mitarbeitenden, Besuchern, Fremdfirmen	niedrig, mit Auswertung

Advocatus Diaboli: Nachunternehmerketten

Ein Angebot, das unter Tarifniveau kalkuliert ist, funktioniert meist nur mit Nachunternehmern, überlangen Schichten oder fehlenden Ausfallreserven. Für den Auftraggeber entstehen daraus Qualitätsrisiken und – bei Eingliederung des Personals – auch rechtliche Risiken. Lassen Sie sich Nachunternehmer vor dem Einsatz benennen und schriftlich genehmigen, und verlangen Sie dieselben Nachweise wie vom Hauptauftragnehmer.

TARIFLÖHNE · STUNDENSATZ · 24/7-POSTEN · MAKE OR BUY

C7 Was eine Stunde Sicherheit kostet

Ein Stundensatz ist mehr als der Lohn. Die folgende Modellrechnung zeigt, wie ein tarifkonformer Verrechnungssatz entsteht – und warum Angebote weit darunter kaum seriös sein können.

C7.1 Tariflöhne 2026 – Beispiele

Region / Tätigkeit	Stundengrundlohn 2026
Nordrhein-Westfalen, Pfortendienst (ab 01.02.2026)	15,11 €
Baden-Württemberg, Objektschutz / Separatwachdienst	15,14 €
Baden-Württemberg, Revier- und Interventionsdienst	16,30 €
Baden-Württemberg, Geprüfte Schutz- und Sicherheitskraft	18,40 €
Hessen, Spanne über zwölf Lohngruppen	15,15 € – 19,08 €
Gesetzlicher Mindestlohn (2027: 14,60 €)	13,90 €

C7.2 Modellrechnung Verrechnungssatz (Basis Pfortendienst NRW)

Bestandteil	Annahme	Betrag je Stunde
Stundengrundlohn	Tarif NRW 2026	15,11 €
Zuschläge Nacht, Sonn- und Feiertag	Ø 10 %	1,51 €
Zwischensumme Lohn		16,62 €
Ausfallzeiten: Urlaub, Krankheit, Feiertage	22 %	3,66 €
Zwischensumme		20,28 €
Arbeitgeberanteile Sozialversicherung	21 %	4,26 €
Zwischensumme Personalkosten		24,54 €
Schulung, Ausrüstung, Dienstkleidung, Versicherungen	6 %	1,47 €
Zwischensumme		26,01 €
Verwaltung, Einsatzleitung, Leitstelle, Wagnis und Gewinn	18 %	4,68 €
Verrechnungssatz netto		**30,69 €**

Modellrechnung mit typischen Zuschlagssätzen; tatsächliche Werte hängen von Tarifgebiet, Lohngruppe, Einsatzzeiten, Qualifikation und Leistungsumfang ab. Jede Zeile baut auf der vorherigen Zwischensumme auf.

C7.3 Beispiel: 24/7-Posten – Dienstleister oder eigenes Personal

Modell	Berechnung	Kosten pro Jahr
Dienstleister zum Modellsatz	8.760 h × 30,69 €	268.844 €
Eigenes Personal: 5,5 Vollzeitkräfte	5,5 × 42.000 € Brutto × 1,21	279.510 €
Eigenes Personal inkl. Schulung, Ausrüstung, Führung (+8 %)	279.510 € × 1,08	301.871 €

Annahmen: 8.760 Stunden je Jahr, rund 1.600 produktive Stunden je Vollzeitkraft, 42.000 € Jahresbrutto inklusive Zuschlägen, 21 % Arbeitgeberanteile. Rekrutierung, Ausfallmanagement und Ersatz bei Kündigungen sind beim Eigenpersonal noch nicht enthalten.

Advocatus Diaboli: Der Preis ist nicht der Vergleich

Rechnerisch liegen beide Modelle nah beieinander. Den Unterschied machen Faktoren, die keine Tabelle zeigt: Wer trägt das Ausfallrisiko in der Grippewelle? Wer rekrutiert bei Kündigungen? Wie schnell lässt sich der Dienst bei einer Lageverschärfung verdoppeln? Und wie viel Betriebskenntnis geht verloren, wenn das Personal ständig wechselt? Diese Fragen entscheiden über das Modell – nicht der Stundensatz allein.

Querverweise

→ D8 Modellsatz angewendet: Empfang und Pforte
→ E8 Modellsatz angewendet: KRITIS-Jahrespaket

VON DER BEDARFSANALYSE BIS ZUM REGELBETRIEB

C8 Checkliste für Auftraggeber

Die Checkliste eignet sich für interne Entscheidungsvorlagen, Ausschreibungen und die jährliche Überprüfung.

Phase 1 – Bedarf und Modell	
☐	Schutzziele, Risiken und Aufgaben je Standort festlegen; Wachschutz oder Werkschutz?
☐	Personalbedarf aus Besetzungszeiten ableiten (24/7-Posten = 8.760 Stunden)
☐	Modellentscheidung: Eigenpersonal, Dienstleister oder hybrid – mit Bewertung von Ausfallrisiko und Betriebskenntnis
☐	Mitbestimmung klären: Betriebsrat bei Kontrollen und Technik einbinden

Phase 2 – Ausschreibung und Vergabe	
☐	Leistungsbeschreibung nach DIN 77200-1 mit Kennzahlen und Probephase
☐	Nachweise: § 34a GewO, Bewacherregister, Versicherungen, Tariftreue, Nachunternehmer
☐	Bestbieterprinzip: Konzept, Qualität, Referenzen und Preis gewichten
☐	Vertrag als Dienst- oder Werkvertrag sauber vom Personalverleih abgrenzen

Phase 3 – Start	
☐	Objektaufnahme, Dienstanweisung, Objekteinweisung jeder Sicherheitskraft
☐	Hausrecht schriftlich übertragen, Schlüssel und Berechtigungen protokolliert übergeben
☐	Ansprechpartner und Kommunikationsweg über den Objektleiter festlegen
☐	Mitarbeitende des Betriebs über Aufgaben des Sicherheitsdienstes informieren

Phase 4 – Regelbetrieb	
☐	Monatsbericht und Kennzahlen auswerten, Mängel abarbeiten
☐	Regelmäßige Audits und unangekündigte Kontrollen
☐	Dienstanweisung bei Änderungen und mindestens jährlich aktualisieren
☐	Übungen für Notfall, Evakuierung und Störfall gemeinsam durchführen

KURZ UND BELASTBAR BEANTWORTET

C9 Häufige Fragen (FAQ)

Was ist der Unterschied zwischen Wachschutz und Werkschutz?

Wachschutz sichert Gebäude, Gelände und Sachwerte. Werkschutz ist in die Organisation eines Betriebs eingebunden und übernimmt zusätzlich Zutritt, Werksverkehr, Kontrollen und Aufgaben der betrieblichen Gefahrenabwehr.

Braucht unser eigener Werkschutz eine Erlaubnis nach § 34a GewO?

Nein. Die Bewachung des eigenen Unternehmens durch eigene Mitarbeitende ist keine gewerbliche Bewachung. Arbeitsschutz, Qualifikation nach Gefährdungsbeurteilung und die DGUV Vorschrift 23 gelten trotzdem.

Welche Qualifikation brauchen externe Sicherheitskräfte?

Mindestens die 40-stündige Unterrichtung nach § 34a GewO. Für bestimmte Tätigkeiten, etwa Kontrollgänge im öffentlichen Verkehrsraum, ist die Sachkundeprüfung Pflicht. Höhere Abschlüsse ersetzen beides.

Wie viele Mitarbeitende braucht ein 24/7-Posten?

Ein Posten rund um die Uhr umfasst 8.760 Stunden im Jahr. Mit Urlaub, Krankheit und Schulung sind dafür rund fünf bis sechs Vollzeitkräfte nötig.

Warum unterscheiden sich Stundensätze so stark?

Weil Tarifgebiet, Lohngruppe, Zuschläge, Ausfallreserve, Schulung und Führung unterschiedlich kalkuliert werden. Angebote deutlich unter dem Tarifniveau deuten auf Lücken bei Lohn, Ausfallreserve oder Qualität hin.

Dürfen Sicherheitskräfte Taschen kontrollieren?

Nur auf Grundlage des Hausrechts und betrieblicher Regelungen, bei vorhandenem Betriebsrat mit Betriebsvereinbarung. Eine Durchsuchung gegen den Willen der Person ist nicht zulässig.

Dürfen wir den Sicherheitskräften direkt Anweisungen geben?

Fachliche Anliegen ja, aber über den Objektleiter des Dienstleisters. Direkte Weisungen und Eingliederung in die eigene Organisation können zu einer verdeckten Arbeitnehmerüberlassung führen.

Was ist ein Hybridmodell?

Eine eigene Werkschutz- oder Sicherheitsleitung steuert, ein Dienstleister erbringt den operativen Dienst. So bleibt die Betriebskenntnis im Haus, Ausfälle und Spitzen trägt der Dienstleister.

TEIL D

Empfangsdienst & Pförtnerdienst – Einlass mit Kontrolle

Zonenkonzept und Besucherprozess, Personalausweis und Datenschutz am Empfang, Notfall und Deeskalation, Technik und Fernpforte.

KAPITEL

D1 Auf einen Blick
D2 Empfang, Pforte, Werkstor
D3 Zutritt und Einlasskontrolle
D4 Recht und Datenschutz am Empfang
D5 Notfall, Bedrohung und Deeskalation
D6 Personal, Qualität und Mitwirkung
D7 Technik am Empfang
D8 Kostenbeispiele und Wirtschaftlichkeit
D9 Checkliste für Auftraggeber
D10 Häufige Fragen (FAQ)

VERWANDTE TEILE

Teil B Aufschaltung von Gefahrenmeldeanlagen, Alarmverfolgung und präventive Gefahrenabwehr – Leitstelle und Fernpforte
Teil C Sicherheitsdienste in der Praxis: Wachschutz oder Werkschutz – Stundensatz und Personal

KERNAUSSAGEN FÜR ENTSCHEIDER

D1 Auf einen Blick

Die zehn wichtigsten Fakten für alle, die einen Empfangs- oder Pförtnerdienst aufbauen, beauftragen oder verbessern.

1	**Empfang ist Service und Sicherheit zugleich:** Jede Person, die unkontrolliert hineinkommt, umgeht alle anderen Schutzmaßnahmen im Gebäude.
2	**Externe Pforte mit Zugangskontrolle** ist Bewachung im Sinne von § 34a GewO: Das Personal braucht mindestens die 40-stündige Unterrichtung.
3	**Eigene Angestellte am Empfang** bewachen kein fremdes Gebäude – für sie gilt § 34a GewO nicht. Schulung und Unterweisung bleiben trotzdem nötig.
4	**Der Personalausweis ist kein Pfand:** Ihn hinterlegen zu lassen, ist nach dem Personalausweisgesetz unzulässig.
5	**Kopien des Ausweises** sind nur mit Zustimmung des Inhabers erlaubt, müssen als Kopie erkennbar sein und sind am Empfang fast nie erforderlich.
6	**Offene Besucherlisten sind ein Datenschutzverstoß:** Jeder nachfolgende Gast sieht Namen und Firmen der vorherigen.
7	**Ein Zonenkonzept** regelt, wer sich wo bewegen darf – der Empfang setzt es durch, Technik unterstützt.
8	**Im Notfall** ist der Empfang Anlaufstelle für Feuerwehr und Rettungsdienst und hält die Übersicht, welche Gäste im Haus sind.
9	**Ohne Mitwirkung geht es nicht:** Gastgeber melden Besuch an, holen ab und begleiten; Mitarbeitende tragen ihre Ausweise sichtbar.
10	**Nicht jede Tür braucht rund um die Uhr Personal:** Ein besetzter Tagesempfang mit Fernpforte über eine Leitstelle kann deutlich günstiger sein.

AUFGABEN · ABGRENZUNG · LEISTUNGSPROFILE

D2 Empfang, Pforte, Werkstor

Empfang, Pforte und Werkstor haben dieselbe Kernaufgabe – kontrollierter Zutritt –, aber unterschiedliche Schwerpunkte. Ein Empfang, der nur freundlich ist, wird umgangen; einer, der nur kontrolliert, schreckt Gäste ab. Professionelle Kräfte verbinden beides – auf Grundlage einer Dienstanweisung, die eindeutig regelt, wer ohne Begleitung passieren darf.

D2.1 Drei Einsatzformen im Vergleich

Merkmal	Empfang / Rezeption	Pforte	Werkstor
Typischer Ort	Firmensitz, Verwaltung, Bürohaus	Betriebsgelände, Behörde, Klinik	Industrie, Logistik, Chemie, Energie
Schwerpunkt	Gäste, Service, Repräsentation	Zutritt, Schlüssel, Kontrolle	Personen- und Fahrzeugverkehr, Material
Kontrolltiefe	Identität, Anmeldung, Ausweis	Berechtigung, Zonen, Schlüssel	Ausweise, Ladung, Fremdfirmen, Werksverkehr
Besetzung	meist werktags tagsüber	oft im Schichtbetrieb	häufig rund um die Uhr
Anforderungen	Service, Sprachen, IT	Kontrolle, Technik, Deeskalation	Werkschutzkenntnis, Gefahrstoffe, Notfall

D2.2 Aufgaben im Überblick

Bereich	Typische Aufgaben
Zutritt	Identität prüfen, Berechtigung abgleichen, Besucherausweise ausgeben und zurücknehmen, Tailgating verhindern
Besucher	Voranmeldungen bearbeiten, Gastgeber informieren, Wartezone betreuen, Begleitung organisieren
Fremdfirmen und Lieferanten	Auftrag prüfen, Sicherheitsunterweisung nachweisen, Arbeitsbereiche zuweisen, Anlieferung lenken
Post und Pakete	Annahme, Sichtprüfung, Weiterleitung, Umgang mit verdächtigen Sendungen
Schlüssel und Ausweise	Ausgabe, Rücknahme, Protokoll, Sperrung bei Verlust
Service	Telefon, Konferenzräume, Taxi, Fundsachen, Auskünfte
Sicherheit	Gefahrenmeldetechnik beobachten, Kontrollgänge, Alarmierung, Erstmaßnahmen im Notfall

ZONENKONZEPT · BESUCHERPROZESS · FREMDFIRMEN · POST

D3 Zutritt und Einlasskontrolle

Einlasskontrolle beginnt nicht an der Theke, sondern mit einem Konzept: Wer darf wohin, wann und mit wessen Begleitung?

D3.1 Das Zonenkonzept

Zone	Beispiele	Zutritt
Öffentlich	Vorplatz, Foyer bis zur Theke	alle Personen
Halböffentlich	Besprechungsräume im Empfangsbereich, Kantine	angemeldete Gäste, ggf. ohne Begleitung
Intern	Büros, Produktionsflächen, Lager	Mitarbeitende; Gäste nur mit Begleitung
Sicherheitskritisch	Serverräume, Technikzentralen, Labore, Kassen	namentlich berechtigte Personen, protokolliert

D3.2 Der Besucherprozess

1	**Voranmeldung**	Gastgeber meldet Besuch mit Name, Firma, Zeit und Zielbereich an – per Formular oder Besuchermanagement.
2	**Ankunft**	Begrüßung, Abgleich mit der Anmeldung, Identität durch Vorzeigen eines Ausweises prüfen – nicht kopieren, nicht einbehalten.
3	**Ausweis und Hinweise**	Besucherausweis mit Gültigkeit ausgeben; Hinweise zu Sicherheit, Fotografierverbot und Verhalten im Notfall.
4	**Abholung**	Gastgeber holt im Empfangsbereich ab; ohne Abholung kein Zutritt in interne Zonen.
5	**Begleitung**	Gäste bewegen sich in internen Zonen nur in Begleitung; Weitergabe des Ausweises ist untersagt.
6	**Abmeldung**	Ausweisrückgabe, Austragung, Löschung der Daten nach festgelegter Frist.

D3.3 Fremdfirmen, Lieferanten und Post

- **Fremdfirmen:** Auftrag und Ansprechpartner prüfen, Nachweis der Sicherheitsunterweisung, Arbeitserlaubnis für besondere Arbeiten, Werkzeug- und Materialliste bei Bedarf
- **Lieferanten:** feste Anlieferzone und -zeiten, keine Durchfahrt in interne Bereiche ohne Freigabe, Fahrer bleiben beim Fahrzeug oder werden begleitet
- **Post und Pakete:** zentrale Annahme, Sichtprüfung auf Auffälligkeiten (fehlender Absender, ungewöhnliches Gewicht, Austritte, Drähte, Gerüche)
- **Verdächtige Sendung:** nicht öffnen, nicht bewegen, Raum verlassen und sichern, Polizei über 110 alarmieren

§ 34A GEWO · HAUSRECHT · PERSONALAUSWEIS · DSGVO

D4 Recht und Datenschutz am Empfang

Am Empfang treffen Bewachungsrecht, Hausrecht und Datenschutz aufeinander. Die wichtigsten Regeln sind einfach – werden im Alltag aber häufig verletzt.

D4.1 Brauchen Empfangskräfte eine Qualifikation nach § 34a GewO?

Konstellation	Anforderung
Eigene Angestellte an Empfang oder Pforte	keine Bewachung im Sinne von § 34a GewO; Schulung nach Gefährdungsbeurteilung
Externer Dienstleister, reiner Service-Empfang ohne Kontrollaufgaben	Zuordnung im Einzelfall durch das Gewerbeamt
Externer Dienstleister, Pforte oder Empfang mit Zugangskontrolle	Erlaubnis des Unternehmens, Unterrichtung (40 Stunden) der Mitarbeitenden
Einlasskontrolle bei zugangsgeschützten Großveranstaltungen in leitender Funktion	Sachkundeprüfung

D4.2 Hausrecht

Das Hausrecht erlaubt dem Inhaber, über Zutritt und Verbleib zu entscheiden – auch, einzelnen Personen den Einlass zu verweigern oder ein Hausverbot auszusprechen. Der Empfang übt es im Auftrag aus; für externe Dienstleister sollte es schriftlich übertragen werden. Hausverbote werden dokumentiert, mit Foto nur bei klarer Erforderlichkeit, und in einer geschützten Liste geführt, die regelmäßig überprüft wird.

Personalausweis: vorzeigen ja, abgeben nein

Kein Pfand: Nach § 1 Abs. 1 Satz 3 Personalausweisgesetz darf vom Inhaber nicht verlangt werden, den Ausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Ausweise gegen Besucherkarten „einzutauschen“ ist damit unzulässig.

Kopien nur ausnahmsweise: Eine Ablichtung ist nur durch den Inhaber oder mit seiner Zustimmung erlaubt und muss eindeutig und dauerhaft als Kopie erkennbar sein (§ 20 Abs. 2 PAuswG). Nach dem Grundsatz der Datenminimierung reicht am Empfang fast immer das Vorzeigen und das Notieren des Namens.

Praxis: Als Pfand für Besucherausweise eignen sich eine kleine Kaution, die Visitenkarte oder einfach die Abholung durch den Gastgeber.

D4.3 Datenschutz bei Besucherdaten

Thema	Regel
Besucherliste	Nie offen auslegen; Einzelerfassung am Bildschirm oder auf Einzelbögen
Umfang	Nur erforderliche Daten: Name, Firma, Gastgeber, Zeiten; keine Ausweisnummern ohne besonderen Grund
Speicherdauer	Löschung nach festgelegter Frist, sobald der Zweck erfüllt ist; Ausnahmen bei Sicherheitsvorfällen dokumentieren
Information	Datenschutzhinweise nach Art. 13 DSGVO am Empfang oder in der Einladung
Fotos auf Besucherausweisen	Nur bei begründetem Sicherheitsbedarf und mit Löschkonzept
Videoüberwachung im Foyer	Beschilderung, Interessenabwägung; Arbeitsplatz der Empfangskräfte nicht dauerhaft erfassen

D4.4 Taschen- und Personenkontrollen

Empfangs- und Pfortenpersonal hat keine Durchsuchungsbefugnis. Kontrollen sind nur freiwillig oder auf Grundlage klarer Zutrittsbedingungen möglich; wer sie ablehnt, kann vom Hausrecht ausgeschlossen werden. Für Mitarbeitende gelten Betriebsvereinbarung und Mitbestimmung (§ 87 Abs. 1 Nr. 1 BetrVG). Bei Verdacht einer Straftat wird die Polizei hinzugezogen.

Querverweise

→ B3 Infobox Haus- und Wegerecht
→ A6 Datenschutz bei Videoüberwachung

EVAKUIERUNG · RETTUNGSKRÄFTE · SCHWIERIGE SITUATIONEN

D5 Notfall, Bedrohung und Deeskalation

Wenn etwas passiert, ist der Empfang der Ort, an dem alle Informationen zusammenlaufen – und an dem Feuerwehr, Rettungsdienst und Polizei zuerst ankommen.

D5.1 Aufgaben des Empfangs im Notfall

1	**Alarmieren**	Notruf 112 oder 110 absetzen, interne Alarmkette auslösen, Leitstelle informieren.
2	**Lenken**	Zugang für Rettungskräfte freihalten, Aufzüge und Zufahrten sichern, Schaulustige fernhalten.
3	**Informieren**	Rettungskräfte einweisen: Lage, Weg, Schlüssel, Laufkarten der Brandmeldeanlage.
4	**Übersicht halten**	Liste der anwesenden Gäste und Fremdfirmen für die Vollzähligkeitskontrolle am Sammelplatz bereitstellen.
5	**Dokumentieren**	Zeiten, Maßnahmen und Beteiligte festhalten; Medienanfragen an die zuständige Stelle verweisen.

D5.2 Schwierige Besucher und Bedrohungslagen

- **Deeskalation:** ruhig bleiben, Abstand halten, Namen nennen, zuhören, klare Alternativen anbieten, nicht provozieren lassen
- **Eigenschutz:** Theke als Distanzzone, Fluchtweg hinter dem Arbeitsplatz frei halten, keine gefährlichen Gegenstände in Reichweite
- **Stiller Alarm:** Überfall- oder Notrufknopf mit Aufschaltung auf Leitstelle oder Polizei; Auslösung regelmäßig üben
- **Zweite Person:** Bei bekannten Konfliktlagen (Kündigungen, Sozialbehörden, Kliniken) Empfang doppelt besetzen oder Sicherheitskraft im Hintergrund
- **Nachsorge:** Vorfall dokumentieren, Hausverbot prüfen, Betroffene entlasten und bei Bedarf Unterstützung anbieten

Übung macht sicher

Empfangskräfte sollten Evakuierung, Einweisung der Feuerwehr und das Auslösen des stillen Alarms mindestens einmal jährlich praktisch üben – gemeinsam mit Brandschutzbeauftragten und Haustechnik. Nach jeder Übung gehören Erkenntnisse in die Dienstanweisung.

ANFORDERUNGSPROFIL · KENNZAHLEN · AUFGABEN DES AUFTRAGGEBERS

D6 Personal, Qualität und Mitwirkung

Am Empfang wirkt jede Person nach außen. Auswahl, Einarbeitung und Teamkonstanz bestimmen, ob der Empfang als professionell wahrgenommen wird – und ob er im Ernstfall funktioniert.

D6.1 Anforderungsprofil

Kompetenz	Inhalt
Service	Auftreten, Kommunikation, Telefon, Umgang mit VIP-Gästen
Sprache	sicheres Deutsch, je nach Standort Englisch oder weitere Sprachen
Sicherheit	Zutrittsregeln, Erkennen von Auffälligkeiten, Alarmierung, Erste Hilfe
Technik	Besuchermanagement, Zutrittskontrolle, Gefahrenmeldetechnik, Video
Konfliktfähigkeit	Deeskalation, Durchsetzen von Regeln ohne Eskalation
Rechtliches	Hausrecht, Datenschutz, Grenzen der Befugnisse; bei Bedarf Unterrichtung nach § 34a GewO

D6.2 Kennzahlen

Kennzahl	Aussage
Wartezeit am Empfang	Wie schnell werden Gäste begrüßt und an Gastgeber übergeben?
Ausweisrücklauf	Wie viele Besucherausweise kommen am Tagesende zurück?
Voranmeldequote	Wie viele Besuche sind vorher angemeldet?
Feststellungen	Tailgating, unberechtigte Zutrittsversuche, offene Türen
Teamkonstanz	Anteil fest eingesetzter, eingearbeiteter Kräfte

D6.3 Mitwirkung von Auftraggeber und Mitarbeitenden

- **Gastgeber** melden Besuche an, holen ihre Gäste ab, begleiten sie und melden sie wieder ab
- **Mitarbeitende** tragen ihre Ausweise sichtbar, halten Unbekannten keine Türen auf und melden verlorene Ausweise sofort
- **Personalabteilung** meldet Ein- und Austritte zeitnah, damit Berechtigungen angelegt oder gesperrt werden
- **Führungskräfte** unterstützen den Empfang, wenn Regeln durchgesetzt werden – auch gegenüber eigenen Mitarbeitenden
- **Auftraggeber** hält Zutrittsregeln, Hausverbotsliste und Ansprechpartner aktuell und steuert über den Objektleiter des Dienstleisters

BESUCHERMANAGEMENT · ZUTRITTSKONTROLLE · FERNPFORTE

D7 Technik am Empfang

Technik entlastet den Empfang von Routine und schafft Nachweise – sie ersetzt aber nicht das Urteil eines Menschen.

Technik	Nutzen	Worauf achten
Software für Besuchermanagement	Voranmeldung, Einladung mit QR-Code, Ausweisdruck, Anwesenheitsliste	Löschfristen, Rollen, Datenschutzhinweise
Self-Service-Terminal	schnelle Registrierung bei hohem Besucheraufkommen	alternativer Weg über besetzten Empfang
Zutrittskontrolle	Berechtigungen nach Zonen und Zeiten, Protokoll	Sperrprozess bei Verlust, Mitbestimmung
Vereinzelung	Drehsperren, Schleusen gegen Tailgating	Barrierefreiheit, Fluchtwege, Brandschutz
Überfall- und Notrufknopf	stiller Alarm an Leitstelle oder Polizei	regelmäßige Funktionsprüfung
Fernpforte / Video-Gegensprechanlage	Zutritt außerhalb der Besetzungszeiten über eine Leitstelle	klare Regeln, Verifikation, Interventionszeit

Tailgating – die häufigste Lücke

Die meisten unberechtigten Zutritte entstehen nicht durch Gewalt, sondern durch Höflichkeit: Jemand hält die Tür auf. Vereinzelungsanlagen wie Drehsperren oder Schleusen helfen, ersetzen aber nicht die Aufmerksamkeit des Empfangs und klare Regeln für Mitarbeitende. Wer Unbekannte freundlich anspricht („Kann ich Ihnen helfen?“), verhindert mehr als jede Schranke.

Biometrie nur mit Augenmaß

Gesichtserkennung oder Fingerabdruck am Empfang verarbeiten besondere Kategorien personenbezogener Daten (Art. 9 DSGVO). Für Besucher sind sie praktisch nie erforderlich; für Mitarbeitende kommen sie nur mit freiwilliger Einwilligung und gleichwertiger Alternative in Betracht. Ausweis, PIN oder begleiteter Zutritt sind in aller Regel ausreichend.

Querverweise

→ B3 Leitstelle und Alarmverfolgung
→ A5 Videoaufschaltung auf die Leitstelle

PRÄSENZ RUND UM DIE UHR · TAGESEMPFANG MIT FERNPFORTE

D8 Kostenbeispiele und Wirtschaftlichkeit

Die Beispiele zeigen typische Größenordnungen auf Basis des tarifbasierten Modellsatzes aus Teil C, Kapitel C7 (30,69 € netto je Stunde Pfortendienst).

Beispiel A – Präsenz rund um die Uhr

Position	Berechnung	Kosten pro Jahr
Empfang werktags 7–19 Uhr (12 h × 250 Tage = 3.000 h)	3.000 h × 33,50 €	100.500,00 €
Pfortendienst außerhalb der Empfangszeiten	5.760 h × 30,69 €	176.774,40 €
Gesamt	**8.760 h**	**277.274,40 €**

Beispiel B – Tagesempfang plus SecuConCept-Fernpforte

Position	Berechnung	Kosten pro Jahr
Empfang werktags 7–19 Uhr	3.000 h × 33,50 €	100.500 €
Fernpforte über Leitstelle (Annahme: Pauschale)	1.250 € × 12 Monate	15.000 €
Technik: Video-Gegensprechanlage, Fernöffnung (Annahme)	18.000 € ÷ 5 Jahre	3.600 €
Gesamt		**119.100 €**

Differenz zu Beispiel A: 277.274,40 € − 119.100 € = 158.174,40 € pro Jahr. Interventionseinsätze außerhalb der Besetzungszeiten werden zusätzlich nach Vertrag abgerechnet. Der Satz von 33,50 € für Empfangsdienst mit Service- und Sprachanforderungen ist eine Annahme.

Advocatus Diaboli: Die Fernpforte passt nicht überall

Das Kombimodell rechnet sich nur, wenn außerhalb der Bürozeiten wenig Personen- und Fahrzeugverkehr herrscht. Bei Schichtbetrieb, regelmäßigen Nachtanlieferungen, Werkschutzaufgaben oder sensiblen Objekten fehlt die Person, die vor Ort reagiert, kontrolliert und im Notfall Rettungskräfte einweist. Die Entscheidung gehört deshalb in die Risikoanalyse – nicht allein in die Kostenrechnung.

VOM KONZEPT BIS ZUM REGELBETRIEB

D9 Checkliste für Auftraggeber

Die Checkliste unterstützt Planung, Ausschreibung und die jährliche Überprüfung von Empfangs- und Pförtnerdiensten.

Phase 1 – Konzept	
☐	Zonenkonzept festlegen: öffentlich, halböffentlich, intern, sicherheitskritisch
☐	Besetzungszeiten und Modell bestimmen: Präsenz, Fernpforte oder Kombination
☐	Prozesse für Besucher, Fremdfirmen, Lieferanten und Post beschreiben
☐	Datenschutz: Datenumfang, Löschfristen, Hinweise nach Art. 13 DSGVO, kein Ausweis als Pfand

Phase 2 – Vergabe und Start	
☐	Leistungsbeschreibung mit Service- und Sicherheitsanforderungen, Sprachen und Kennzahlen
☐	Nachweise: § 34a GewO bei Zugangskontrolle, Versicherungen, Tariftreue
☐	Dienstanweisung, Hausrechtsübertragung, Hausverbotsliste, Ansprechpartner
☐	Einarbeitung am Objekt, Technikschulung, Notfallunterweisung

Phase 3 – Regelbetrieb	
☐	Kennzahlen monatlich auswerten: Wartezeit, Ausweisrücklauf, Feststellungen
☐	Mitarbeitende regelmäßig an Ausweispflicht und Tailgating-Regeln erinnern
☐	Evakuierung und stillen Alarm mindestens jährlich üben
☐	Besucherdaten fristgerecht löschen, Hausverbotsliste regelmäßig prüfen

KURZ UND BELASTBAR BEANTWORTET

D10 Häufige Fragen (FAQ)

Darf der Empfang den Personalausweis als Pfand für den Besucherausweis einbehalten?

Nein. Nach § 1 Abs. 1 Satz 3 Personalausweisgesetz darf nicht verlangt werden, den Ausweis zu hinterlegen. Der Ausweis darf vorgezeigt, aber nicht einbehalten werden.

Dürfen wir den Ausweis von Besuchern kopieren oder scannen?

Nur mit Zustimmung des Inhabers und als erkennbare Kopie – und nur, wenn es erforderlich ist. Für den normalen Besucherempfang ist das fast nie der Fall.

Braucht unsere Empfangskraft eine Unterrichtung nach § 34a GewO?

Eigene Angestellte nicht. Externe Kräfte, die eine Zugangskontrolle durchführen, benötigen mindestens die 40-stündige Unterrichtung.

Ist eine Besucherliste am Empfang erlaubt?

Ja, aber nicht offen ausgelegt. Jeder Gast darf nur seine eigenen Daten sehen; die Daten werden nach Zweckerfüllung gelöscht.

Dürfen wir Taschen von Besuchern kontrollieren?

Nur freiwillig oder als Zutrittsbedingung. Eine Durchsuchung gegen den Willen ist unzulässig; wer ablehnt, kann vom Zutritt ausgeschlossen werden.

Was tun bei einer verdächtigen Postsendung?

Nicht öffnen, nicht bewegen, Raum verlassen und absperren, Polizei über 110 alarmieren und den Ablauf dokumentieren.

Lohnt sich eine Fernpforte?

Wenn außerhalb der Bürozeiten wenig Verkehr herrscht, kann sie die Kosten deutlich senken. Bei Schichtbetrieb oder sensiblen Objekten bleibt Präsenz vor Ort meist notwendig.

Wer ist für Tailgating verantwortlich?

Alle: Der Empfang achtet darauf, Technik erschwert es, und Mitarbeitende halten Unbekannten keine Türen auf. Ohne klare Regeln für das eigene Personal bleibt jede Kontrolle lückenhaft.

TEIL E

KRITIS: Sicherheitsdienste als All-in-One-Lösung?

Was KRITIS-Betreiber nachweisen müssen, Chancen und Risiken eines integrierten Modells, Kriterien, Vergaberecht und ein integriertes Kostenbeispiel.

KAPITEL

E1 Auf einen Blick
E2 Was KRITIS-Betreiber nachweisen müssen
E3 Was „All-in-One“ bedeutet
E4 Chancen einer integrierten Lösung
E5 Risiken und Grenzen
E6 Kriterien für ein belastbares Modell
E7 Vergabe: privat und öffentlich
E8 Kostenbeispiel und Wirtschaftlichkeit
E9 Entscheidungshilfe und Checkliste
E10 Häufige Fragen (FAQ)

VERWANDTE TEILE

Teil A Videoüberwachung & Videoaufschaltung für KRITIS-relevante Einrichtungen – KRITIS-Rechtsrahmen im Detail
Teil C Sicherheitsdienste in der Praxis: Wachschutz oder Werkschutz – Make or Buy
Teil B Aufschaltung von Gefahrenmeldeanlagen, Alarmverfolgung und präventive Gefahrenabwehr – Leitstelle und Intervention

KERNAUSSAGEN FÜR ENTSCHEIDER

E1 Auf einen Blick

Die zehn wichtigsten Punkte für Geschäftsführungen und Sicherheitsverantwortliche in KRITIS-Unternehmen.

1	**Das KRITIS-Dachgesetz gilt seit 17.03.2026.** Die KRITIS-Verordnung mit den Schwellenwerten ist nach Angaben des BBK (Stand Oktober 2026) noch nicht in Kraft – die Vorbereitung sollte trotzdem jetzt beginnen.
2	**§ 13 verlangt einen Maßnahmenmix:** Objektschutz, Überwachung der Umgebung, Detektion, Zugangskontrolle, Notfall- und Krisenmanagement, Personalsicherheit – ausdrücklich auch für Personal externer Dienstleister.
3	**Die Erwägungen müssen dokumentiert sein.** Ein einheitliches Konzept mit durchgängiger Dokumentation erleichtert den Nachweis gegenüber der Behörde erheblich.
4	**Schnittstellen sind ein Risiko:** Bei sechs Dienstleistern und dem Betreiber entstehen rechnerisch 21 Schnittstellen. Jede kann im Ernstfall Zeit kosten.
5	**All-in-One reduziert Schnittstellen** – kann aber ein Klumpenrisiko schaffen, wenn der Partner selbst keine Redundanz besitzt.
6	**Beratung und Umsetzung aus einer Hand** erfordern Transparenz: Das Schutzkonzept muss sich am Risiko orientieren, nicht am eigenen Leistungskatalog.
7	**Herstellerunabhängigkeit** ist die Voraussetzung dafür, dass ein All-in-One-Partner keine technische Abhängigkeit erzeugt.
8	**Öffentliche Auftraggeber** müssen nach § 97a GWB grundsätzlich in Lose aufteilen; eine Gesamtvergabe ist aus technischen oder wirtschaftlichen Gründen mit dokumentierter Begründung zulässig.
9	**Ein Netzwerkmodell** – ein Vertragspartner, viele regionale Fachbetriebe – verbindet einheitliche Steuerung mit mittelständischer Umsetzung vor Ort.
10	**Die Entscheidung gehört in die Risikoanalyse** nach § 12 KRITISDachG: Welches Modell erhöht die Resilienz tatsächlich?

KRITIS-DACHGESETZ · BSIG · BEITRAG DER SICHERHEITSDIENSTE

E2 Was KRITIS-Betreiber nachweisen müssen

Das KRITIS-Dachgesetz verpflichtet Betreiber kritischer Anlagen nicht zu einzelnen Produkten, sondern zu einem nachvollziehbaren Gesamtsystem. Genau hier setzt die Frage nach dem richtigen Dienstleistermodell an.

E2.1 Pflichten und der Beitrag der Sicherheitsdienstleistung

Pflicht	Norm	Beitrag von Sicherheitsdiensten
Risikoanalyse und -bewertung	§ 12 KRITISDachG	Gefährdungs- und Schwachstellenanalyse vor Ort, Täterperspektive, Lagebild aus Vorfällen
Resilienzmaßnahmen und Resilienzplan	§ 13 KRITISDachG	Perimeterschutz, Video, Detektion, Zugangskontrolle, Personal, Alarm- und Reaktionsabläufe
Personalsicherheit inkl. externer Dienstleister	§ 13 Abs. 3 Nr. 5	Bewacherregister, objektbezogene Überprüfung, Schulung, Teamkonstanz
Meldung erheblicher Vorfälle	§ 18 KRITISDachG	Lückenlose Ereignisprotokolle, Erstbericht binnen Stunden
Billigung und Überwachung durch die Leitung	§ 20 KRITISDachG	Berichtswesen, Kennzahlen, Audits
Risikomanagement inkl. Lieferkette	§ 30 BSIG	IT-Sicherheit von Video- und Meldetechnik, sichere Leitstellenanbindung

E2.2 Was „Maßnahmenmix“ in der Praxis bedeutet

§ 13 Abs. 3 KRITISDachG nennt beispielhaft Objektschutz durch Liegenschaftsabgrenzungen, Instrumente zur Überwachung der Umgebung, Detektionsgeräte, Zugangskontrollen, Risiko- und Krisenmanagement sowie ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeitenden, einschließlich des Personals externer Dienstleister. Diese Maßnahmen greifen ineinander: Eine Kamera ohne Leitstelle, eine Leitstelle ohne Intervention oder eine Pforte ohne aktuelle Zutrittsdaten erfüllt den Zweck nur zum Teil. Die Kernfrage ist daher nicht „Wer liefert was?“, sondern „Wer verantwortet, dass alles zusammen funktioniert?“

Aktueller Stand

Das KRITIS-Dachgesetz ist seit 17. März 2026 in Kraft. Die Rechtsverordnung, die über Schwellenwerte bestimmt, welche Anlagen kritisch sind, lag nach Angaben des BBK im Oktober 2026 noch nicht in Kraft; eine Registrierungspflicht bestand daher noch nicht. Nach der Einstufung laufen die Fristen kurz: Registrierung nach drei Monaten, Risikoanalyse nach neun, Resilienzmaßnahmen nach zehn Monaten. Wer sein Dienstleistermodell jetzt klärt, vermeidet Zeitdruck bei Vergabe und Umsetzung. Den Rechtsrahmen im Detail behandelt Kapitel A2.

LEISTUNGSBAUSTEINE · ORGANISATIONSMODELLE

E3 Was „All-in-One“ bedeutet

„All-in-One“ wird sehr unterschiedlich verstanden – vom Facility-Konzern, der Sicherheit mitliefert, bis zum spezialisierten Sicherheitspartner mit Netzwerk. Für KRITIS-Betreiber lohnt die genaue Unterscheidung.

E3.1 Leistungsbausteine

Baustein	Inhalt
Beratung und Konzeption	Risikoanalyse, Schutzziele, Sicherheits- und Resilienzkonzept, Ausschreibungsunterstützung
Sicherheitstechnik	Video, Perimeterdetektion, Einbruch- und Überfallmeldetechnik, Zutrittskontrolle – Planung, Errichtung, Wartung
Leitstelle	Aufschaltung, Alarmverifikation, Fernpforte, Störungsüberwachung, Ereignisdokumentation
Personelle Sicherheit	Werk- und Objektschutz, Empfang und Pforte, Revier- und Interventionsdienst, Brandwachen
Mobile Lösungen	autarke Videotürme für Baustellen, Interimsschutz und Lageverschärfungen
Notfall und Krise	Alarm- und Notfallpläne, Übungen, Unterstützung im Ereignis, Nachbereitung
Nachweise	Berichte, Kennzahlen, Audit-Unterlagen für Behörde, Versicherer und Geschäftsleitung

E3.2 Organisationsmodelle im Vergleich

Modell	Prinzip	Stärken	Schwächen
Einzelvergabe	je Leistung ein eigener Vertrag	Spezialisierung, Wettbewerb je Gewerk	viele Schnittstellen, Koordination liegt beim Betreiber
Facility-Paket	Sicherheit als Teil eines Vertrags über Gebäudedienste	ein Rahmenvertrag, Bündelungseffekte	Sicherheit oft Nebenleistung, wenig KRITIS-Tiefe
Generalunternehmer mit eigenem Personal	ein Anbieter erbringt alles selbst	einheitliche Führung	Abhängigkeit, regionale Lücken, Herstellerbindung möglich
Netzwerkmodell	ein Vertragspartner steuert spezialisierte Fachbetriebe	eine Verantwortung, regionale Stärke, Skalierbarkeit	erfordert einheitliche Standards und straffe Steuerung

SCHNITTSTELLEN · REAKTIONSZEIT · NACHWEIS

E4 Chancen einer integrierten Lösung

Der größte Vorteil eines integrierten Modells liegt nicht im Preis, sondern in der Verantwortung: Einer steht dafür ein, dass die Sicherungskette im Ernstfall geschlossen ist.

E4.1 Weniger Schnittstellen

Zwischen n Beteiligten bestehen rechnerisch n × (n − 1) ÷ 2 mögliche Schnittstellen. Jede steht für Abstimmungen, Übergaben, Zuständigkeitsfragen – und im Ereignisfall für mögliche Verzögerungen.

Konstellation	Beteiligte	Mögliche Schnittstellen
Betreiber und ein integrierter Partner	2	1
Betreiber und drei Dienstleister (z. B. Technik, Leitstelle, Personal)	4	6
Betreiber und sechs Dienstleister	7	21

Beim integrierten Partner verschwinden die inneren Schnittstellen nicht – sie werden aber dort gesteuert, wo die Fachkompetenz liegt, und nicht beim Betreiber.

E4.2 Weitere Vorteile

- **Geschlossene Alarmkette:** Detektion, Verifikation, Intervention und Dokumentation folgen einem gemeinsamen Alarmplan
- **Schnellere Meldung:** Ein einheitliches Ereignisprotokoll erleichtert die 24-Stunden-Meldung nach § 18 KRITISDachG
- **Durchgängiger Nachweis:** Konzept, Maßnahmen, Schulungen und Kennzahlen liegen in einer Struktur vor (§ 13 Abs. 4)
- **Einheitliche Personalsicherheit:** gleiche Anforderungen an Überprüfung, Schulung und Einweisung für alle eingesetzten Kräfte
- **Skalierbarkeit:** Lageverschärfungen, Bauphasen und neue Standorte werden aus einer Hand abgedeckt
- **Entlastung des Betreibers:** weniger Vertrags-, Rechnungs- und Abstimmungsaufwand

Praxisbeispiel: der Alarm um 3:12 Uhr

Perimeteranalytik meldet eine Person am Zaun einer Pumpstation. Im Einzelmodell prüft die Leitstelle von Anbieter A das Bild, beauftragt den Interventionsdienst von Anbieter B und informiert den Betreiber, der den Wartungsdienst von Anbieter C wegen eines beschädigten Kamerastandorts anruft. Im integrierten Modell laufen diese Schritte nach einem Alarmplan, mit einem Protokoll und einem Ansprechpartner – der Betreiber erhält am Morgen einen vollständigen Bericht.

ADVOCATUS DIABOLI · GEGENMASSNAHMEN

E5 Risiken und Grenzen

Resilienz bedeutet, dass ein Ausfall nicht zum Gesamtausfall führt. Ein All-in-One-Modell kann genau diesem Prinzip widersprechen – wenn es nicht entsprechend gebaut ist.

E5.1 Die wichtigsten Risiken und wie man ihnen begegnet

Risiko	Worin es besteht	Gegenmaßnahme
Klumpenrisiko	Fällt der Partner aus, fehlen Technik, Leitstelle und Personal zugleich	Redundante Leitstelle, Ausweichkonzept, regionale Ersatzkräfte, Notfallübergabe
Abhängigkeit (Lock-in)	Wechsel wird teuer oder technisch unmöglich	offene Schnittstellen, Herstellerunabhängigkeit, Datenhoheit beim Betreiber, Exit-Klausel
Interessenkonflikt	Berater empfiehlt bevorzugt eigene Leistungen	risikobasierte Begründung je Maßnahme, Transparenz, Zweitmeinung bei großen Investitionen
Qualität in Nebenleistungen	„Kann alles“ heißt nicht „kann alles gut“	Kennzahlen je Leistungsbereich, Nachweise der Fachbetriebe, Audits
Intransparente Nachunternehmer	Unklar, wer tatsächlich vor Ort arbeitet	Benennung und Genehmigung aller Nachunternehmer, gleiche Nachweispflichten
Wissensverlust beim Betreiber	Eigene Sicherheitskompetenz verkümmert	eigene verantwortliche Person, regelmäßige Berichte, gemeinsame Übungen

Advocatus Diaboli: Ein Vertrag ist kein Resilienzkonzept

Wer alle Sicherheitsleistungen an einen Partner vergibt, hat die Verantwortung nicht abgegeben. Nach § 20 KRITISDachG bleibt die Geschäftsleitung für Umsetzung und Überwachung verantwortlich. Ein All-in-One-Vertrag ist nur dann ein Gewinn, wenn der Betreiber ihn aktiv steuert, die Leistung messbar ist und ein Plan existiert, was passiert, wenn der Partner selbst ausfällt.

E5.2 Wann All-in-One nicht die beste Wahl ist

- Wenn der Betreiber bereits eine starke eigene Sicherheitsorganisation mit Leitstelle besitzt und nur Einzelleistungen ergänzt
- Wenn einzelne Gewerke hoch spezialisiert sind, etwa Brandmeldeanlagen mit Feuerwehraufschaltung oder kerntechnische Anforderungen
- Wenn der Anbieter keine Redundanz nachweisen kann oder Technik nur eines Herstellers anbietet
- Wenn vergaberechtlich keine tragfähige Begründung für eine Gesamtvergabe besteht

WORAN BETREIBER QUALITÄT ERKENNEN

E6 Kriterien für ein belastbares Modell

Die folgenden Kriterien trennen ein tragfähiges integriertes Modell von einem Bündel, das nur auf dem Papier aus einer Hand kommt.

1	**Redundanz**	Ausweich-Leitstelle oder redundanter Betrieb, Ersatzkräfte je Region, dokumentierte Notfallübergabe bei Ausfall des Partners. Lassen Sie sich die Redundanz nachweisen.
2	**Herstellerunabhängigkeit**	Keine Provisionen von Herstellern, offene Protokolle und Schnittstellen, Technik bleibt mit anderen Partnern betreibbar.
3	**Datenhoheit**	Konzepte, Pläne, Zugangsdaten, Video- und Ereignisdaten gehören dem Betreiber und werden bei Vertragsende vollständig übergeben.
4	**Transparenz**	Jede Maßnahme ist aus der Risikoanalyse begründet; Nachunternehmer sind benannt und genehmigt.
5	**Personalsicherheit**	Bewacherregister, objektbezogene Überprüfung nach Betreibervorgaben, Schulung und Teamkonstanz – auch bei Nachunternehmern.
6	**Messbarkeit**	Kennzahlen je Leistungsbereich: Reaktionszeiten, Verfügbarkeit, Besetzungsquote, Rundgangserfüllung, Mängelabarbeitung.
7	**Zertifizierung**	Alarmempfangsstelle nach DIN EN 50518, Dienstleistung nach DIN 77200-1, Arbeitsschutz nach DGUV Vorschrift 23.
8	**Exit-Fähigkeit**	Kündigungs- und Übergangsregeln, Übergabeplan, Mitwirkungspflicht des Partners beim Wechsel.

Mitwirkung des Betreibers

Auch das beste integrierte Modell braucht einen aktiven Betreiber: eine benannte verantwortliche Person, aktuelle Alarm- und Zutrittsdaten, Meldung von Änderungen an Anlagen und Personal, Teilnahme an Übungen sowie die Auswertung der Berichte. Fachliche Anliegen laufen über den Projekt- oder Objektleiter des Partners – direkte Weisungen an einzelne Sicherheitskräfte sind zu vermeiden, um eine verdeckte Arbeitnehmerüberlassung auszuschließen.

Querverweise

→ B3 Qualitätsmerkmale einer Leitstelle
→ C6 Qualität und Vergabe von Sicherheitsdiensten

LOSGRUNDSATZ · GESAMTVERGABE · RAHMENVERTRÄGE

E7 Vergabe: privat und öffentlich

Viele KRITIS-Betreiber – Stadtwerke, Wasserverbände, kommunale Kliniken – sind öffentliche Auftraggeber. Für sie ist „All-in-One“ zuerst eine vergaberechtliche Frage.

E7.1 Der Losgrundsatz

Öffentliche Aufträge sind grundsätzlich in Teil- und Fachlose aufzuteilen, um mittelständische Interessen zu berücksichtigen. Mit dem Gesetz zur Beschleunigung der Vergabe öffentlicher Aufträge wurde dieser Grundsatz zum 1. Juli 2026 aus § 97 Abs. 4 GWB in den neuen § 97a GWB überführt; die Ausnahme für wirtschaftliche oder technische Gründe blieb wortgleich erhalten.

E7.2 Wann eine Gesamtvergabe begründbar ist

- **Technische Gründe:** Leistungen sind so eng verzahnt, dass eine getrennte Vergabe die Funktionsfähigkeit gefährden würde – etwa Detektion, Verifikation und Intervention in einer Alarmkette
- **Besonderes Risikopotenzial:** Die Rechtsprechung hat ein hohes Risikopotenzial und die Gefährdung der Gesamtleistung als Rechtfertigung anerkannt (OLG München, Verg 10/18)
- **Wirtschaftliche Gründe:** unverhältnismäßiger Koordinationsaufwand oder erhebliche Mehrkosten bei Losaufteilung
- **Dokumentation:** Die Begründung muss konkret auf den Einzelfall eingehen und in der Vergabeakte stehen; verwaltungsinterne Bequemlichkeit genügt nicht

Mittelstand trotz Gesamtvergabe

Bei einer Gesamtvergabe können öffentliche Auftraggeber den Auftragnehmer verpflichten, bei Unteraufträgen die Interessen kleiner und mittlerer Unternehmen besonders zu berücksichtigen (§ 97a Abs. 5 GWB). Ein Netzwerkmodell mit regionalen, mittelständischen Fachbetrieben erfüllt dieses Ziel strukturell.

E7.3 Private Betreiber

Private Betreiber sind frei in der Gestaltung. Bewährt haben sich Rahmenverträge mit einheitlichen Standards und Kennzahlen, in denen einzelne Leistungsbereiche gesondert bepreist, gemessen und bei Bedarf auch einzeln gekündigt werden können. So verbindet der Betreiber die Vorteile aus einer Hand mit der Möglichkeit, gezielt nachzusteuern.

REGIONALER WASSERVERSORGER · INTEGRIERTES LEISTUNGSPAKET

E8 Kostenbeispiel und Wirtschaftlichkeit

Das Beispiel zeigt ein typisches integriertes Jahrespaket. Die Ansätze stammen aus den Modellrechnungen in A7, B7, C7 und D8; alle Werte netto und unverbindlich.

Beispiel: Hauptwerk und zwölf Außenanlagen

Leistung	Berechnung	Kosten pro Jahr
Pfortendienst Hauptwerk werktags 6–18 Uhr	3.000 h × 30,69 €	92.070 €
Fernpforte Hauptwerk außerhalb der Besetzungszeiten	1.250 € × 12 Monate	15.000 €
Videoaufschaltung aller 13 Standorte	13 × 390 € × 12 Monate	60.840 €
Revierkontrollen nachts an 4 Schwerpunktanlagen	4 × 365 × 22 €	32.120 €
Intervention (Annahme: 40 Einsätze)	40 × 145 €	5.800 €
Wartung Video- und Meldetechnik	13 × 900 €	11.700 €
Konzept, Resilienzplan-Unterstützung, Übungen	pauschal	12.000 €
Jahrespaket gesamt		**229.530 €**

Entspricht 19.127,50 € pro Monat. Nicht enthalten: Investitionen in Sicherheitstechnik, Zaun- und Bauleistungen sowie Sonderleistungen bei Lageverschärfung.

Wo der wirtschaftliche Vorteil liegt

- **Weniger Koordination beim Betreiber:** ein Vertrag, eine Rechnung, ein Berichtswesen statt sechs
- **Kein Doppelaufwand:** Leitstelle, Intervention und Technik nutzen dieselben Objektdaten und Alarmpläne
- **Bedarfsgerechte Mischung:** Personal dort, wo es nötig ist; Technik und Fernpforte dort, wo sie genügen
- **Rahmenvertragskonditionen:** Bündelung mehrerer Leistungen und Standorte verbessert die Konditionen

Advocatus Diaboli: Integriert heißt nicht automatisch günstiger

Einzelne Leistungen können bei Einzelvergabe günstiger sein, weil Spezialanbieter in ihrem Gewerk scharf kalkulieren. Der Vorteil des integrierten Modells liegt in geringeren Schnittstellenkosten, schnellerer Reaktion und einfacherem Nachweis – Effekte, die in keiner Einzelposition stehen. Vergleichen Sie deshalb Gesamtkosten einschließlich eigenem Steuerungsaufwand, nicht Stundensätze.

IN VIER SCHRITTEN ZUM PASSENDEN MODELL

E9 Entscheidungshilfe und Checkliste

Die Checkliste führt durch die Entscheidung und eignet sich als Grundlage für eine Vorlage an die Geschäftsleitung.

Schritt 1 – Ausgangslage	
☐	Betroffenheit nach KRITISDachG und BSIG prüfen; Fristen ab Inkrafttreten der KRITIS-Verordnung einplanen
☐	Bestehende Verträge, Technik, Leitstellen und Personaldienste erfassen, Laufzeiten und Kündigungsfristen prüfen
☐	Schnittstellen und bekannte Lücken aus Vorfällen und Übungen dokumentieren

Schritt 2 – Bewertung	
☐	Risikoanalyse nach § 12 als Grundlage: Welche Maßnahmen sind nötig, welche Abhängigkeiten entstehen?
☐	Modelle vergleichen: Einzelvergabe, Paket, Generalunternehmer, Netzwerkmodell
☐	Klumpenrisiko bewerten: Was passiert, wenn der Partner ausfällt?
☐	Bei öffentlichen Auftraggebern: Losbildung oder dokumentierte Begründung der Gesamtvergabe

Schritt 3 – Vergabe und Vertrag	
☐	Leistungsbeschreibung mit Kennzahlen je Bereich, Redundanz- und Exit-Regelungen
☐	Nachweise: § 34a GewO, DIN EN 50518, DIN 77200-1, Versicherungen, Nachunternehmer
☐	Datenhoheit, offene Schnittstellen und Übergabepflichten vertraglich sichern

Schritt 4 – Steuerung	
☐	Verantwortliche Person beim Betreiber benennen; Berichte und Kennzahlen monatlich auswerten
☐	Gemeinsame Übungen für Ereignis, Meldung nach § 18 und Ausfall des Partners
☐	Resilienzplan und Risikoanalyse fortschreiben, Modell regelmäßig überprüfen

KURZ UND BELASTBAR BEANTWORTET

E10 Häufige Fragen (FAQ)

Schreibt das KRITIS-Dachgesetz einen bestimmten Sicherheitsdienstleister oder ein bestimmtes Modell vor?

Nein. Es verlangt geeignete und verhältnismäßige Maßnahmen und deren nachvollziehbare Dokumentation. Wie der Betreiber sie organisiert, bleibt ihm überlassen.

Kann ich die Verantwortung für die Resilienz an einen Dienstleister übertragen?

Die Umsetzung ja, die Verantwortung nicht. Nach § 20 KRITISDachG bleibt die Geschäftsleitung für Umsetzung und Überwachung verantwortlich.

Ist ein All-in-One-Anbieter nicht ein Klumpenrisiko?

Er kann es sein. Entscheidend sind Redundanz, offene Schnittstellen, Datenhoheit beim Betreiber und ein Plan für den Ausfall des Partners.

Dürfen öffentliche KRITIS-Betreiber Sicherheitsleistungen gesamt vergeben?

Grundsätzlich gilt der Losgrundsatz nach § 97a GWB. Eine Gesamtvergabe ist zulässig, wenn technische oder wirtschaftliche Gründe sie erfordern und dies konkret dokumentiert ist.

Wie wird Personal externer Dienstleister überprüft?

Sicherheitskräfte sind im Bewacherregister erfasst und auf Zuverlässigkeit geprüft. § 13 KRITISDachG verlangt zusätzlich ein angemessenes Sicherheitsmanagement für Mitarbeitende, einschließlich externer Dienstleister.

Wird es mit einem Anbieter günstiger?

Nicht zwingend je Einzelleistung, häufig aber in der Gesamtbetrachtung – durch weniger Koordination, schnellere Reaktion und einfacheren Nachweis.

Was ist ein Netzwerkmodell?

Ein Vertragspartner übernimmt Verantwortung und Steuerung, regionale Fachbetriebe setzen nach einheitlichen Standards um. So entstehen Nähe vor Ort und eine einheitliche Qualität.

SECURITY · CONSULTING · CONCEPTION

SecuConCept: integriert und unabhängig

SecuConCept verbindet herstellerunabhängige Beratung, Sicherheitskonzeption und operative Umsetzung – als ein Vertragspartner mit bundesweitem Netzwerk.

Consulting

Betroffenheitsprüfung, Risikoanalyse, Modellentscheidung, Vergabeunterstützung

Conception

Sicherheits- und Resilienzkonzepte, Alarm- und Notfallpläne, Kennzahlen und Nachweise

Security

Video und Aufschaltung, Fernpforte, Intervention, Werk- und Objektschutz, Empfang, Revierdienst, Videotürme

Warum SecuConCept?

- **Netzwerkmodell SecuNET:** mehr als 350 spezialisierte Fachunternehmen bundesweit – ein Vertragspartner, regionale Umsetzung, einheitliche Qualitätsanforderungen.
- **SecuNET für Firmenkunden:** Firmenkunden mit Exklusivbindung an SecuConCept erhalten einen persönlichen Key Account Manager und 24-Stunden-Support.
- **Redundante Leitstelle:** zertifizierte Alarmempfangsstelle nach DIN EN 50518 / VdS mit redundanter Leitstellenstruktur – für Aufschaltung, Verifikation und Fernpforte.
- **Herstellerunabhängig und erfahren:** keine Provisionen von Herstellern, „Upgrade statt neu“ bei Bestandstechnik, Praxiswissen aus dem Werkschutz großer Chemiestandorte.

Fachportale und Marken

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

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

SecuFokus®
SICHERHEIT GEMEINSAM STEUERN.
BY SECUCONCEPT

SecuFokus by SecuConCept – Sicherheit gemeinsam steuern.
Fachinformationen und Werkzeuge für Betreiber, Partner und Dienstleister.

KOSTENFREIES ERSTGESPRÄCH

Sicherheits-Check für Ihr Unternehmen

Video, Aufschaltung, Personal, Empfang oder KRITIS-Gesamtkonzept – 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

RECHTSGRUNDLAGEN · NORMEN · RECHTSPRECHUNG · ONLINE-QUELLEN

Quellenverzeichnis

Konsolidiertes Verzeichnis aller Teile. Die Buchstaben in Klammern zeigen, in welchen Teilen eine Quelle verwendet wird. Recherchestand und Abruf der Online-Quellen: November 2026.

Gesetze und Verordnungen

- KRITIS-Dachgesetz (KRITISDachG) vom 11.03.2026, BGBl. 2026 I Nr. 66; Änderung von § 8 durch Gesetz vom 21.07.2026, BGBl. 2026 I Nr. 221 (A, B, E)
- BSI-Gesetz in der Fassung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes, in Kraft seit 06.12.2025, insbesondere §§ 28, 30, 32, 38, 41, 65 (A, E)
- Verordnung (EU) 2016/679 (DSGVO); Bundesdatenschutzgesetz; Landesdatenschutzgesetze (A, B, D)
- Gewerbeordnung, insbesondere § 34a und § 11b; Bewachungsverordnung (BewachV) (A, B, C, D, E)
- Personalausweisgesetz, insbesondere § 1 Abs. 1 Satz 3 und § 20 Abs. 2 (D)
- Gesetz gegen Wettbewerbsbeschränkungen, § 97 Abs. 4 und § 97a in der Fassung ab 01.07.2026 (E)
- Arbeitnehmerüberlassungsgesetz; Arbeitsschutzgesetz, insbesondere § 8; Arbeitszeitgesetz; Mindestlohngesetz (C, E)
- Betriebsverfassungsgesetz, § 87 Abs. 1 Nr. 1 und Nr. 6 (A, B, C, D)
- Strafgesetzbuch §§ 32, 34, 123, 201; Strafprozessordnung § 127 (A, B, C, D)
- Bürgerliches Gesetzbuch §§ 229, 858 ff., 903, 917, 1004, 1018; Straßenverkehrs-Ordnung §§ 35, 38 (B, C, D)
- Versicherungsvertragsgesetz § 28 (B)
- Verordnung (EU) 2024/1689 (KI-Verordnung); Verordnung (EU) 2024/2847 (Cyber Resilience Act) (A)

Rechtsprechung

- EuGH, Urteil vom 30.03.2023 – C-34/21 (Beschäftigtendatenschutz) (A)
- BVerwG, Urteil vom 23.08.1991 – 8 C 37.90 (Gebühren für Polizeieinsätze nach Alarmauslösung) (B)
- VG Neustadt an der Weinstraße: Gebühr von 120 € für ungerechtfertigte Alarmierung durch eine Einbruchmeldeanlage (B)
- OLG München, Beschluss vom 25.03.2019 – Verg 10/18 (Gesamtvergabe bei hohem Risikopotenzial) (E)
- VK Bund, Beschluss vom 26.02.2024 – VK 2-11/24 (Begründung einer Gesamtvergabe) (E)

Normen und Regelwerke

- DIN EN 62676 (Reihe) – Videoüberwachungsanlagen für Sicherheitsanwendungen, insbesondere Teil 4 (A)
- DIN EN 50518 – Alarmempfangsstelle; VdS 3138 – Notruf- und Serviceleitstellen (A, B, D, E)
- DIN EN 50131 (Reihe) – Einbruch- und Überfallmeldeanlagen; VdS 2311 – Planung und Einbau von EMA (B)
- DIN EN 50136-1/-2 – Alarmübertragungsanlagen und -einrichtungen (B)
- DIN VDE 0833-1/-2/-3 – Gefahrenmeldeanlagen; DIN 14675 – Brandmeldeanlagen; DIN EN 54 (B)
- DIN EN 1627 – Einbruchhemmung von Türen, Fenstern und Abschlüssen (B)
- DIN 77200-1:2022-10 – Sicherungsdienstleistungen (A, B, C, D, E)
- DGUV Vorschrift 23 „Wach- und Sicherungsdienste“; DGUV Regel 112-139 „Personen-Notsignal-Anlagen“ (C, D, E)
- Richtlinie für Überfall- und Einbruchmeldeanlagen mit Anschluss an die Polizei (ÜEA-Richtlinie) (B)

Behörden, Verbände und Orientierungshilfen

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): Informationen und FAQ zum KRITIS-Dachgesetz, Stand Oktober 2026 (A, E)
- Bundesamt für Sicherheit in der Informationstechnik (BSI): NIS-2-Informationen und Registrierungsportal (A)
- Datenschutzkonferenz (DSK): Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen; Kurzpapier Nr. 15 (A)
- Bundesnetzagentur und Netzbetreiber: Abschaltung der 2G-Netze (B)
- BHE / VdS: Hinweise zur Überwindung von EMA-Zentralen und Übertragungseinrichtungen; Aufschaltung von BMA (B)
- IHK-Merkblätter zur Abgrenzung von Unterrichtung und Sachkundeprüfung im Bewachungsgewerbe (C, D)
- Allgemeinverbindliche Lohn- und Entgelttarifverträge für Sicherheitsdienstleistungen 2026, u. a. NRW, Baden-Württemberg, Hessen (C)
- US Federal Communications Commission (FCC): Covered List (A)

Online-Quellen

Teil	Quelle
A	Wikipedia: Kritis-Dachgesetz https://de.wikipedia.org/wiki/Kritis-Dachgesetz
A	coredinate: KRITIS-Dachgesetz und Sicherheitsdienst https://coredinate.de/blog/kritis-dachgesetz-sicherheitsdienst
A, E	datenraume.de: KRITIS-Dachgesetz 2026 https://datenraume.de/blog/kritis-dachgesetz/
A	DSN Group: NIS-2-Umsetzungsgesetz in Kraft https://www.dsn-group.de/datenschutz-notizen/das-nis-2-umsetzungsgesetz-ist-in-kraft-getreten-welche-schritte-sind-nun-erforderlich-4457509
A	Axians: NIS2UmsuCG – aktueller Stand https://www.axians-secure.de/blog/nis2-umsetzungsgesetz-nis2umsucg
A	PwC Legal: DSK-Orientierungshilfe Videoüberwachung https://legal.pwc.de/de/news/fachbeitraege/datenschutzkonferenz-veroeffentlicht-orientierungshilfe-zur-videoueberwachung
A	OpenKRITIS: Garantieerklärung § 9b BSIG https://www.openkritis.de/betreiber/komponenten_garantieerklaerung.html
A	OpenKRITIS: Kritische Komponenten https://www.openkritis.de/betreiber/kritische-komponenten.html
A	BDEW/VKU: Positionspapier zu § 41 BSIG https://www.bdew.de/media/documents/BDEW_VKU_Positionspapier_41_BSIG_NIS2-UmsuCG_Kritische_Komponenten_1.pdf
A	ictally: FCC Camera Ban 2026 https://ictally.com/resources/blog/fcc-chinese-camera-import-ban-nashville
B, C	DIN Media: DIN 77200-1:2022-10 https://www.dinmedia.de/de/norm/din-77200-1/348823032
B	BHE: Aufschaltung von Brandmeldeanlagen https://www.bhe.de/_Resources/Persistent/d/4/9/9/d49991c5c03ba5fe5262346a3f8250efc96e3fd7/leseprobe_10_kapitel_aufschaltung-von-brandmeldeanlagen-1.pdf

Teil	Quelle
B	BHE: Aufschaltung von BMA auf die Feuerwehr https://www.bhe.de/_Resources/Persistent/b/2/c/8/b2c81ae48267cb526313291896282f8ed52f8ac5/2019-10-21_aufschaltung_von_bma_auf_feuerwehr.pdf
B	VdS/BHE: Überwindung von EMA-Zentralen https://www.VDS.de/fileadmin/Website_Content_Images/VdS_Publikationen/Rundschreiben_Security/30-03-2021_Infopapier_Ueberwindung_EMZ.pdf
B	BHE: Einbruchmeldetechnik https://www.bhe.de/_Resources/Persistent/d/5/d/b/d5db10152a56aff56a99c0945df2e5e546ad346d/Leseprobe%20_2.4_Kapitel_Einbruchmeldetechnik.pdf
B	Bundesnetzagentur: 2G-Abschaltung https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Breitband/2GAbschaltung/artikel.html
B	Verbraucherzentrale: 2G-Abschaltung https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/2gabschaltung-was-damit-auf-verbraucherinnen-zukommt-114129
B	LTO: VG Neustadt zur Fehlalarm-Gebühr https://www.lto.de/recht/nachrichten/n/vg-neustadt-kioskbesitzer-muss-fuer-polizeieinsatz-nach-fehlalarm-bezahlen/print.html
B	anwalt24: BVerwG 8 C 37.90 https://www.anwalt24.de/urteile/bverwg/1991-08-23/bverwg-8-c-3790
B, C	bpb: Private Sicherheitsdienste https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/571071/private-sicherheitsdienste/
B	Nordkurier: Fehlalarme der Feuerwehren https://www.nordkurier.de/panorama/wenn-feuerwehren-umsonst-ausruecken-4579918
C	IHK Köln: Erlaubnis nach § 34a GewO https://www.ihk.de/koeln/hauptnavigation/recht-steuern/bewachungsgewerbe-erlaubnis-nach-34a-gewo-5224494
C	IHK Rostock: Abgrenzung der Tätigkeiten nach § 34a https://www.ihk.de/rostock/aus-und-weiterbildung/weiterbildung/sachkundepruefung/abgrenzung-taetigkeiten-34a-6822272
C	IHK Bonn: Merkblatt Unterrichtung https://www.ihk-bonn.de/fileadmin/dokumente/Downloads/Weiterbildung/Weiterbildungspruefungen/Merkblatt-Unterrichtung_im_Bewachungsgewerbe.pdf
C	DGUV Vorschrift 23 https://publikationen.dguv.de/widgets/pdf/download/article/1105
C	Zoll: Lohntarifvertrag Sicherheit NRW https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/Arbeit/sicherheit_lohntarifvertrag_nrw_20250211.pdf?__blob=publicationFile&v=2
C	BDSW: Allgemeinverbindlichkeit Baden-Württemberg 2026 https://www.bdsw.de/images/tarifvertraege/ave/2026/AVE_BW_LTV_2026_0908.pdf
C	Hessische Landesregierung: Entgelttarifvertrag allgemeinverbindlich https://landesregierung.hessen.de/presse/entgelttarifvertrag-fuer-beschaeftigte-in-sicherheitsbranche-allgemeinverbindlich
C	Bundesregierung: Mindestlohn steigt https://www.bundesregierung.de/breg-de/suche/mindestlohn-steigt-2391010

Teil	Quelle
D	Gesetze im Internet: § 20 PAuswG https://www.gesetze-im-internet.de/pauswg/__20.html
D	Bundestag WD 3-041-19: Ausweis-Scans https://bundestag.de/resource/blob/645674/0204d86f6cff7fd920d54703d7ea874b/WD-3-041-19-pdf-data.pdf
D	GIGA: Personalausweis kopieren https://www.giga.de/ratgeber/specials/personalausweis-kopieren-wie-geht-das-ist-das-erlaubt
D	Dr. Datenschutz: Besuchermanagement im Unternehmen https://www.dr-datenschutz.de/besuchermanagement-im-unternehmen/
D	IHK: Merkblatt Unterrichtung im Bewachungsgewerbe https://www.ihk.de/blueprint/servlet/resource/blob/4244936/9eab9ad2cecb3148f3b13fe41114d836/ihk-merkblatt-unterrichtung-bewachungsgewerbe-72018-data.pdf
D	IHK Hannover / DIHK: Unterrichtung oder Sachkundeprüfung https://www.hannover.ihk.de/blueprint/servlet/resource/blob/5294910/c65a3da3c4cc2401b390efef2cc615b8/merkblatt-up-oder-skp-dihk-data.pdf
E	noba-experts: KRITIS-Dachgesetz, Stand Oktober 2026 https://www.noba-experts.de/wissen/themen/kritis-dachgesetz
E	CMS: KRITIS-Verordnung https://cms.law/de/deu/legal-updates/kritis-verordnung-was-betreiber-kritischer-anlagen-jetzt-wissen-muessen
E	gesetze.legal: § 13 KRITISDachG https://gesetze.legal/bund/kritisdachg/13
E	Lobbyregister: BDSW-Stellungnahme zur Zuverlässigkeitsüberprüfung https://www.lobbyregister.bundestag.de/media/67/e9/612529/Stellungnahme-Gutachten-SG2509080026.pdf
E	cosinex: Gesamt- vs. Losvergabe, § 97a GWB https://blog.cosinex.de/2018/09/13/gesamt-vs-losvergabe-wie-begruendet-man-eine-gesamtvergabe-rechtssicher/
E	vergabeblog: OLG München Verg 10/18 https://vergabeblog.de/2019-07-01/hohes-risikopotential-rechtfertigt-gesamtvergabe-olg-muenchen-beschl-v-25-03-2019-verg-10-18/
E	vergabeblog: VK Bund VK 2-11/24 https://vergabeblog.de/2024-06-10/gesamtvergabe-von-leistungen-auf-eine-gute-begruendung-kommt-es-an-vk-bund-beschl-v-26-02-2024-vk2-11-24/
E	lxgesetze: § 97a GWB https://lxgesetze.de/gwb/97a

Rechtsstand und Haftung: Recherchestand November 2026. Dieses Handbuch stellt keine Rechtsberatung dar. Kostenangaben sind Modellrechnungen und unverbindliche Orientierungswerte (netto).

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