Stand: November 2026

FACHHANDBUCH

KRITIS & INTEGRIERTE SICHERHEIT

Sicherheitsdienste als All-in-One-Lösung?

Für KRITIS-Betreiber: Chancen, Grenzen, Entscheidung

FACHPORTALE UND MARKEN VON SECUCONCEPT

KRITIS-Dachgesetz & BSIG: Was Betreiber nachweisen müssen

Ein Anbieter für alles – Schnittstellen, Klumpenrisiko, Vergaberecht

Kriterien für ein belastbares Modell · Kostenbeispiel · Entscheidungshilfe

Qualität durch Vertrauen

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

ZU DIESEM HANDBUCH

Ein Anbieter für alles – Lösung oder Risiko?

Betreiber kritischer Anlagen müssen ihre Resilienz künftig ganzheitlich planen, umsetzen und nachweisen: Risikoanalyse, physischer Schutz, Personal, Alarm- und Meldewege, Übungen. Viele fragen sich deshalb, ob ein einziger Sicherheitspartner für Beratung, Technik, Leitstelle und Personal die bessere Wahl ist als ein Flickenteppich aus Einzelverträgen.

Die ehrliche Antwort lautet: Es kommt darauf an, wie das Modell gebaut ist. Dieses Handbuch zeigt, was All-in-One im KRITIS-Umfeld leisten kann, wo es Risiken schafft, die dem Resilienzgedanken widersprechen, wie öffentliche Auftraggeber vergaberechtlich vorgehen – und an welchen Kriterien Betreiber ein belastbares Modell erkennen.

Inhalt

1 Auf einen Blick . . . 3
2 Was KRITIS-Betreiber nachweisen müssen . . . 4
3 Was „All-in-One“ bedeutet . . . 5
4 Chancen einer integrierten Lösung . . . 6
5 Risiken und Grenzen . . . 7
6 Kriterien für ein belastbares Modell . . . 8
7 Vergabe: privat und öffentlich . . . 9
8 Kostenbeispiel und Wirtschaftlichkeit . . . 10
9 Entscheidungshilfe und Checkliste . . . 11
10 Häufige Fragen (FAQ) . . . 12
11 SecuConCept: integriert und unabhängig . . . 13
12 Quellen und Rechtsstand . . . 14

KERNAUSSAGEN FÜR ENTSCHEIDER

01 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?

Wichtiger Hinweis zur Rechtsverbindlichkeit

Dieses Handbuch ist eine fachliche Orientierung und ersetzt keine Rechts- oder Vergabeberatung. Die KRITIS-Verordnung lag zum Recherchestand (November 2026) noch nicht in Kraft; Schwellenwerte und Fristen können sich ändern. Kostenangaben sind Modellrechnungen und unverbindliche Orientierungswerte (netto).

KRITIS-DACHGESETZ · BSIG · BEITRAG DER SICHERHEITSDIENSTE

02 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.

2.1 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

2.2 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.

LEISTUNGSBAUSTEINE · ORGANISATIONSMODELLE

03 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.

3.1 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

3.2 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

04 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.

4.1 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.

4.2 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

05 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.

5.1 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.

5.2 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

06 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.

LOSGRUNDSATZ · GESAMTVERGABE · RAHMENVERTRÄGE

07 Vergabe: privat und öffentlich

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

7.1 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.

7.2 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.

7.3 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

08 Kostenbeispiel und Wirtschaftlichkeit

Das Beispiel zeigt ein typisches integriertes Jahrespaket. Die Ansätze stammen aus den Modellrechnungen der übrigen SecuConCept-Handbücher; 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

09 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

10 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

11 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

KRITIS-Modellcheck für Ihr Unternehmen

Betroffenheit, bestehende Verträge, Schnittstellen und das passende Dienstleistermodell – mit klarer Handlungsempfehlung.

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

ZUM NACHSCHLAGEN

12 Quellen und Rechtsstand

Rechtsgrundlagen

- KRITIS-Dachgesetz (KRITISDachG) vom 11.03.2026, BGBl. 2026 I Nr. 66, insbesondere §§ 8, 12, 13, 18, 20
- BSI-Gesetz in der Fassung des NIS-2-Umsetzungsgesetzes, insbesondere §§ 30, 32, 38
- Gesetz gegen Wettbewerbsbeschränkungen (GWB), § 97 Abs. 4 und § 97a in der Fassung ab 01.07.2026
- § 34a Gewerbeordnung, Bewachungsverordnung; Arbeitnehmerüberlassungsgesetz

Rechtsprechung und Behörden

- OLG München, Beschluss vom 25.03.2019 – Verg 10/18 (Gesamtvergabe bei hohem Risikopotenzial)
- VK Bund, Beschluss vom 26.02.2024 – VK 2-11/24 (Begründung einer Gesamtvergabe)
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): Informationen zum KRITIS-Dachgesetz, Stand Oktober 2026

Normen

- DIN EN 50518 (Alarmempfangsstelle); DIN 77200-1:2022-10 (Sicherungsdienstleistungen); DGUV Vorschrift 23
- Weitere SecuConCept-Fachhandbücher: Videoüberwachung & Videoaufschaltung für KRITIS · Aufschaltung, Alarmverfolgung & Prävention · Sicherheitsdienste in der Praxis · Empfangsdienst & Pförtner

Rechtsstand und Haftung: Recherchestand November 2026. Die KRITIS-Verordnung war zu diesem Zeitpunkt noch nicht in Kraft. Dieses Handbuch stellt keine Rechts- oder Vergabeberatung dar. Kostenangaben sind Modellrechnungen und unverbindliche Orientierungswerte (netto).

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