Mehr Sicherheit für Kritische Infrastrukturen

Der BHE Bundesverband Sicherheitstechnik e.V. informiert www.bhe.de

Vorsorgemaßnahmen zum Schutz lebenswichtiger Anlagen und Einrichtungen

© BHE/ Stand 10.02.2025

BHE Bundesverband Sicherheitstechnik e.V.
Feldstraße 28, 66904 Brücken
Telefon: 06386 9214-0, E-Mail: info@bhe.de,
Internet: www.bhe.de

KRI-40002-2025-02

Inhaltsverzeichnis

Vorwort

In einer zunehmend komplexen und vernetzten Welt, in der Abhängigkeiten zwischen verschiedenen Sektoren allgegenwärtig sind, ist die Sicherheit Kritischer Infrastrukturen (KRITIS) ein zentrales Element gesellschaftlicher Stabilität und Ordnung. Der Schutz dieser lebenswichtigen Einrichtungen und Anlagen, von der Energie- und Wasserversorgung über das Gesundheitswesen bis hin zu Kommunikations- und Verkehrssystemen, ist für das Wohlergehen und die Sicherheit der deutschen Gesellschaft von zentraler Bedeutung. Jüngste Entwicklungen und Bedrohungsszenarien zeigen, wie verwundbar die deutschen Infrastrukturen durch gezielte Angriffe, Naturkatastrophen und technisches Versagen sind.

Die Einführung eines Gesetzes zum Schutz von KRITIS in Deutschland ist daher ein wichtiger Schritt, um bundesweit einheitliche Mindeststandards für den physischen Schutz dieser Einrichtungen zu etablieren. Mit dem geplanten und vorerst (Stand: Februar 2025) gescheiterten KRITIS-Dachgesetz sollten erstmals sektorübergreifende Regelungen für den physischen Schutz getroffen werden, die die bestehenden IT-Sicherheitsmaßnahmen ergänzen und so ein ganzheitliches Sicherheitskonzept schaffen. Unabhängig davon, dass sich das nationale Gesetzgebungsverfahren nun auf unbestimmte Zeit verlängert, ist die Umsetzung von Schutzmaßnahmen in KRITIS-Betrieben notwendig und sinnvoll, um sie gegen alle denkbaren Bedrohungen, seien es Naturereignisse, technisches Versagen oder gezielte Sabotageakte abzusichern und ihre Funktionsfähigkeit sicherzustellen. Regelmäßige Risikoanalysen und die Erstellung von Resilienzplänen versetzen die Betreiber nicht nur in die Lage, potenzielle Gefährdungen zu erkennen und ihnen präventiv zu begegnen, sondern auch die Resilienz ihrer Infrastrukturen nachhaltig zu stärken.

Der Schutz von KRITIS erfordert umfassendes Fachwissen und einen integrativen Ansatz, bei dem bauliche, technische und organisatorische Maßnahmen ineinandergreifen. Nur durch das koordinierte Zusammenspiel dieser verschiedenen Schutzmaßnahmen kann die notwendige Sicherheit erreicht werden, um sowohl Sabotageversuchen als auch Naturkatastrophen standhalten zu können. Die Kombination von physischen Sicherheitsvorkehrungen wie Einbruch- und Brandschutz, Perimetersicherheit, Zutrittssteuerungssystemen und Videotechnik mit fortschrittlichen Cyber-Sicherheitsmaßnahmen ist dabei unerlässlich. So entsteht ein umfassender Schutzschild, der den besonderen Anforderungen und Bedrohungslagen Kritischer Infrastrukturen gerecht wird.

Die vorliegende Broschüre soll die Bedeutung und die grundlegenden Anforderungen an die physische Sicherheit im Bereich der KRITIS praxisnah verdeutlichen. Angesichts der stetig wachsenden Bedrohungslage und der Interdependenzen zwischen den einzelnen Sektoren darf die Sicherheit Kritischer Infrastrukturen nicht nur als Aufgabe einzelner Betreiber verstanden werden. Sie ist vielmehr ein gesamtgesellschaftliches Anliegen, das die Zusammenarbeit aller Beteiligten erfordert - von staatlichen Stellen über Sicherheitsbehörden bis hin zu privaten Unternehmen und spezialisierten Sicherheitsdienstleistern. Nur durch diese gemeinsame Verantwortung und die kontinuierliche Anpassung an neue Bedrohungsszenarien kann die Sicherheit und Stabilität Deutschlands dauerhaft gewährleistet werden.

Axel Schmidt,
BHE-Vorstandsvorsitzender

Stephan Holzem,
BHE-Vorstandsmitglied

Carl J. Becker-Christian,
BHE-Geschäftsführer

1. Allgemeiner Überblick bzw. Problemstellung

Die EU hat in den letzten Jahren zwei zentrale Richtlinien eingeführt, um den Schutz kritischer Infrastrukturen zu verbessern:

- die **CER-Richtlinie** (Critical Entities Resilience) zur Stärkung der physischen Resilienz – auch bekannt unter dem Namen **„RCE-Richtlinie"** (Resilience of Critical Entities) – und
- die **NIS2-Richtlinie** für die Stärkung der Cybersicherheit.

Diese Vorgaben zielen darauf ab, die Funktionsfähigkeit wichtiger Dienste in Krisensituationen sicherzustellen und die Widerstandskraft gegenüber unterschiedlichen Bedrohungen zu erhöhen. Neben den eigentlichen kritischen Liegenschaften sind davon auch direkt oder indirekt weite Teile der Wirtschaft betroffen.

Die Richtlinien werden im Folgenden näher vorgestellt.

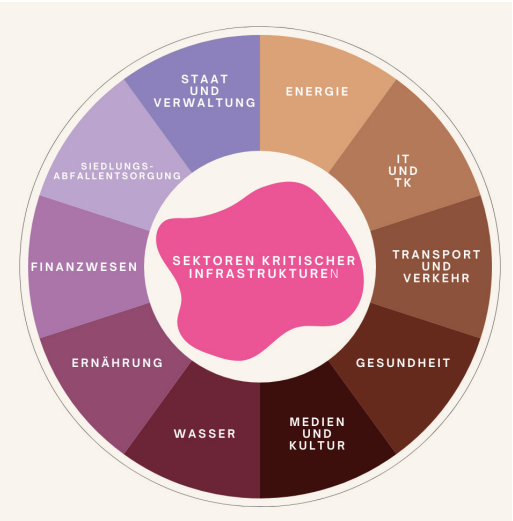
1.1 CER-Richtlinie (bzw. RCE-Richtlinie) und KRITIS-Dachgesetz

Die EU-Richtlinie über die Resilienz kritischer Infrastrukturen (CER-Richtlinie) ist im Januar 2023 in Kraft getreten und sollte ursprünglich bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden, in Deutschland über das sogenannte **„KRITIS-Dachgesetz"**. Am 6. November 2024 hat das Bundeskabinett den Entwurf des KRITIS-Dachgesetzes beschlossen und in das parlamentarische Verfahren eingebracht. Im Januar 2025 sind die weiterführenden Gespräche zwischen den Regierungsparteien gescheitert, wodurch das KRITIS-Dachgesetz nach der Bundestagswahl im Februar 2025 erneut eingebracht werden muss (Stand: Februar 2025).

Mit dem KRITIS-Dachgesetz sollen erstmals auf Bundesebene Kritische Infrastrukturen identifiziert und Mindeststandards für den physischen Schutz für diese festgelegt werden. Bisher gab es solche bundesgesetzlichen Regelungen nur für die IT-Sicherheit Kritischer Infrastrukturen. Die Regelungen des KRITIS-Dachgesetzes zum physischen Schutz sollen die bestehenden IT-Sicherheitsmaßnahmen ergänzen. Damit soll die Widerstandsfähigkeit der Kritischen Infrastrukturen gegenüber Bedrohungen insgesamt gestärkt werden.

Kritische Infrastrukturen sind zunehmend gefährdet. Ereignisse mit katastrophalen Auswirkungen treten immer häufiger auf, werden immer komplexer und verstärken sich oft gegenseitig. Dies haben die letzten Jahre gezeigt. KRITIS werden zwar in verschiedene Sektoren unterschieden, diese sind jedoch so miteinander verzahnt, dass in der Regel Abhängigkeiten voneinander bestehen. Kommt es zu Ausfällen in einem Sektor, z.B. Energie, IT oder Logistik, kann dies gravierende Auswirkungen auf andere Sektoren und damit auf die gesamte Wertschöpfungskette haben. Dennoch gibt es in Deutschland mit Ausnahme des Bereichs der IT-Sicherheit Kritischer Infrastrukturen keine sektor- und gefahrenübergreifenden Regelungen.

Das KRITIS-Dachgesetz soll erstmals ein „Dach" über die Sektoren **Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Trinkwasser, Abwasser, Siedlungsabfallentsorgung, Informationstechnik und Telekommunikation, Ernährung, Raumfahrt und öffentliche Verwaltung** legen und die bestehenden Regelungen für die IT-Sicherheit Kritischer Infrastrukturen ergänzen. Ausgangspunkt sind alle denkbaren Risiken, die durch Naturereignisse oder von Menschen verursacht werden können („All-Gefahren-Ansatz") - sei es ein Unwetter, menschliches Versagen oder ein Sabotageakt.
Im Fokus des Gesetzes stehen alle Kritischen Infrastrukturen. Es soll festlegen, welche Unternehmen und Einrichtungen verpflichtende Resilienzmaßnahmen für den physischen Schutz und die Stabilität der Gesamtwirtschaft ergreifen müssen.



Das Gesetz soll auch die Interdependenzen zwischen den Kritischen Infrastrukturen berücksichtigen: So sind z.B. vom Energiesektor alle anderen Sektoren abhängig. Ebenso sind Wasser und Verkehrswege für die anderen Sektoren unverzichtbar. Daher ist vorgesehen, dass im KRITIS-Dachgesetz erstmals sektorübergreifende Ziele formuliert werden: die Verhinderung von Störungen und Ausfällen, die Begrenzung ihrer Folgen und die Wiederherstellung der Funktionsfähigkeit nach einem Vorfall.

Um diese Ziele zu erreichen, müssen die KRITIS-Betreiber auf die spezifischen Risiken ihrer Anlagen mit maßgeschneiderten Maßnahmen reagieren. Diese sind in so genannten **Resilienzplänen** darzustellen. Eine wesentliche Grundlage hierfür sind **Risikoanalysen und -bewertungen,** die regelmäßig sowohl vom Staat als auch von den Betreibern der betroffenen Sektoren durchgeführt werden sollen.

Das KRITIS-Dachgesetz sieht vor, dass die Betreiber **geeignete und verhältnismäßige Maßnahmen** ergreifen müssen, um die vorgegebenen Ziele zu erreichen. Aufgrund der Unterschiedlichkeit der Sektoren können die Maßnahmen sehr vielfältig sein. Hierfür soll den Betreibern ermöglicht werden, in Zusammenarbeit **mit Branchenverbänden gemeinsame Standards zu erarbeiten und damit zu konkretisieren**, was jeweils für ihren Sektor (z.B. Energie) und ihre Branche (z.B. Strom) als geeignete und verhältnismäßige Maßnahme anzusehen ist. Mindeststandards sollen geschaffen und Lücken geschlossen werden. Bereits bestehende sektorspezifische Regelungen bleiben unberührt.

Darüber hinaus soll das Gesetz ein **zentrales Meldewesen für erhebliche Störungen** vorsehen, das das bereits bestehende Meldewesen im Bereich der IT-Sicherheit Kritischer Infrastrukturen ergänzen würde.

Ferner soll die Zusammenarbeit aller Akteure im KRITIS-Bereich institutionalisiert werden. Die Zuständigkeiten der zahlreichen Akteure beim Schutz Kritischer Infrastrukturen sollen klarer definiert werden. Bei der Umsetzung des KRITIS-Dachgesetzes soll das **Bundesamt für Bevölkerungsschutz (BBK) eine koordinierende Rolle** erhalten. Es wird eng mit den zuständigen Aufsichtsbehörden des Bundes zusammenarbeiten.

Unabhängig davon, wann das KRITIS-Dachgesetz erscheint – die Richtung ist erkennbar: Zukünftig wird eine Kombination aus physischer Sicherheit (z.B. durch Perimeterschutz, Zutrittssteuerung, Einbruch- und Brandmeldetechnik, Videotechnik sowie Alarmmanagement) und Cyber-Security der Systeme erforderlich sein. Dies hat erhebliche Auswirkungen auf KRITIS-Betreiber und Sicherheitsunternehmen, da sowohl Fachkompetenz im Bereich der physischen Sicherheit als auch im Bereich der sicheren Netzwerkarchitektur und des Fernzugriffs erforderlich ist.

1.2. NIS2-Richtlinie und NIS2-Umsetzungsgesetz

Die NIS2-Richtlinie soll ein Mindestmaß an Cybersicherheit in der gesamten EU gewährleisten. Sie gilt für alle Unternehmen und Einrichtungen, die kritische Dienste und Infrastrukturen betreiben. Die Mitgliedstaaten müssen sicherstellen, dass diese Betreiber ihre Netze und IT-Systeme gegen Cyber-Angriffe schützen. In Deutschland soll die Umsetzung der NIS2-Richtlinie durch das NIS2-Umsetzungsgesetz (NIS2UmsuCG) erfolgen, die Aufsicht übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI). Wie das KRITIS-Dachgesetz ist auch das NIS2-Umsetzungsgesetz vorerst gescheitert, so dass das Gesetz nach der Bundestagswahl 2025 erneut eingebracht werden muss.

Das kommende NIS2-Umsetzungsgesetz wird weitreichende Änderungen in der deutschen KRITIS-Regulierung bringen und über 30.000 Unternehmen im Land betreffen. Das Gesetz soll klare Anforderungen an die Betreiber kritischer Anlagen und wesentlicher Einrichtungen definieren, um Sicherheitslücken zu schließen und den Schutz gegenüber Cyberangriffen zu verbessern.

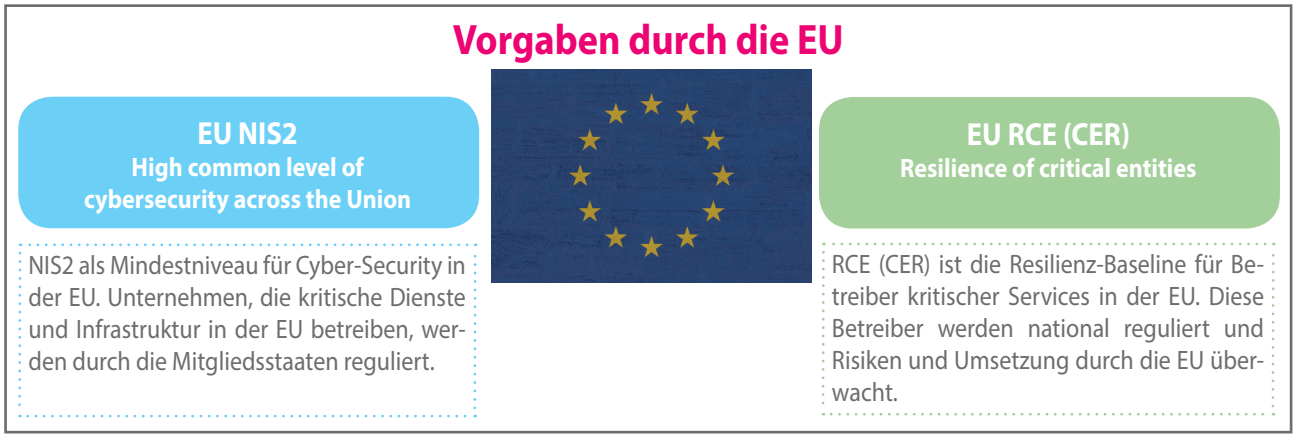
Signifikante Punkte des Gesetzes sind voraussichtlich:

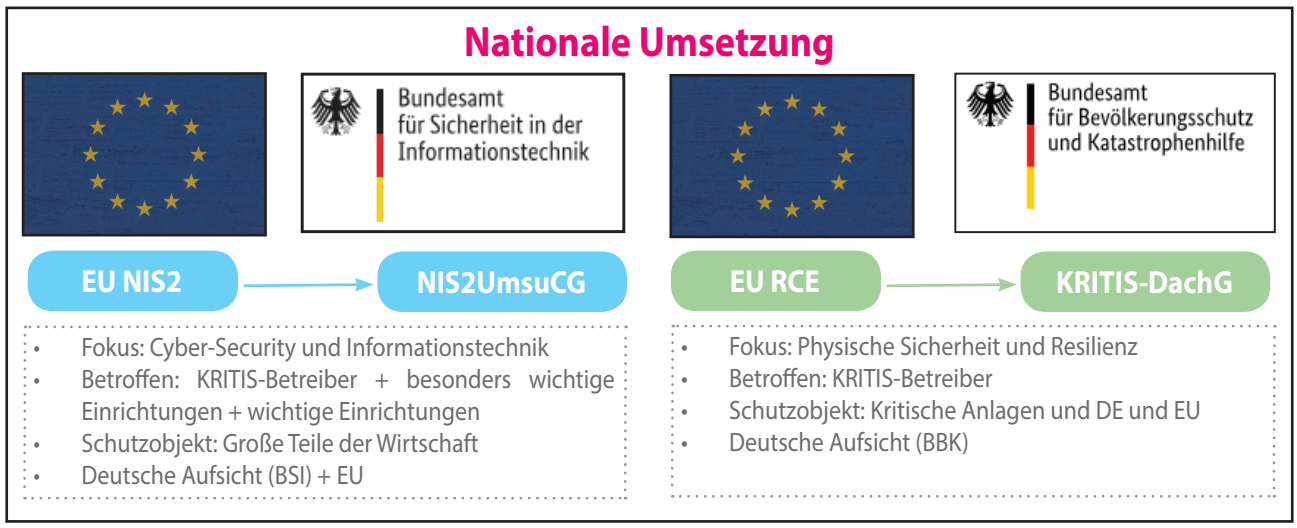
1. **Betroffene Unternehmen:** Zusätzlich zu den Betreibern kritischer Anlagen stehen bei der NIS2-Richtlinie besonders wichtige und wichtige Einrichtungen, je nach Größe und wirtschaftlicher Bedeutung, sowie einige Bundeseinrichtungen im Fokus.

2. **Erweiterte Sektoren:** Neben den klassischen KRITIS-Sektoren, wie Energie, Gesundheit und Wasser, deckt NIS2 nun auch größere Teile der Wirtschaft ab, z. B. das verarbeitende Gewerbe und den digitalen Bereich. Das bedeutet, dass auch Einrichtungen außerhalb der bisher regulierten kritischen Sektoren unter die neuen Cybersicherheitsauflagen fallen können.
3. **Maßnahmenumfang:** Die Richtlinie fordert von den betroffenen Einrichtungen u.a. umfassende Maßnahmen für Cyber-Sicherheit und Risikomanagement, die das gesamte Unternehmen abdecken. Hierzu zählt bspw. auch eine Meldepflicht für Sicherheitsvorfälle.
4. **Nachweispflicht:** KRITIS-Betreiber müssen im 3-Jahres-Rhythmus nachweisen, dass sie die Anforderungen des Gesetzes erfüllen. Für wichtige Einrichtungen soll es eine Dokumentationspflicht und stichprobenartige Prüfungen durch die Behörden geben, um die Wirksamkeit der getroffenen Sicherheitsmaßnahmen zu gewährleisten.
5. **Staatliche Aufsicht und Sanktionen:** Durch das NIS2-Umsetzungsgesetz wird das BSI zur Aufsichtsbehörde für die betroffenen Unternehmen, die künftig Registrierungs-, Nachweis- und Meldepflichten gegenüber dem BSI zu erfüllen haben. Sollten die geforderten Vorgaben nicht eingehalten werden, drohen Unternehmen hohe Geldstrafen. Je nach Verstoß und Größe des Unternehmens werden Bußgelder zwischen 100.000 und 10 Millionen Euro oder bis zu 2 Prozent des weltweiten Umsatzes verhängt, je nachdem, welcher Betrag höher ist. Diese Sanktionsvorschriften sollen sicherstellen, dass die vorgeschriebenen Cybersicherheitsmaßnahmen konsequent umgesetzt werden.

Die **NIS-2-Betroffenheitsprüfung des BSI** bietet in wenigen Schritten eine erste Orientierung, ob ein Unternehmen von der NIS2-Richtlinie der EU betroffen ist.

Die nachfolgenden Grafiken zeigen die unterschiedliche Zielrichtung der vorgenannten Richtlinien im Überblick:





1.3. Auswirkungen auf die Dienstleister der Sicherheitstechnik

Das KRITIS-Dachgesetz und das NIS2-Umsetzungsgesetz werden voraussichtlich weitreichende Auswirkungen auf die Anforderungen an Errichter und Planer physischer Sicherheitssysteme haben:

1. Ganzheitliche Sicherheitskonzepte und „hybride" Ansätze

Anbieter physischer Sicherheitstechnik sind gefordert, ihre Produkte in ganzheitliche Sicherheitskonzepte einzubinden. Hierbei ist die Kombination von physischen Schutzmaßnahmen, wie zum Beispiel einer Zutrittssteuerung mit deren Cyber-Security-Anforderungen zu berücksichtigen - d.h. diese Zutrittssteuerung muss in sichere Netzstrukturen eingebunden werden.
Dies bedeutet, dass bspw. Zutrittssteuerungssysteme nicht mehr isoliert betrachtet werden können, sondern eng mit IT-basierten Überwachungssystemen und Notfallplänen verknüpft werden müssen. Nur so lässt sich ein umfassender Schutz gewährleisten, der auf die Anforderungen der NIS2- und KRITIS-Regulierungen zugeschnitten ist.

2. Beratung zur Erhöhung der Resilienz und geeigneten Schutzmaßnahmen

Eine der zentralen Erwartungen an Sicherheitsdienstleister ist die Fähigkeit, Betreiber Kritischer Infrastrukturen kompetent zur Auswahl der richtigen Sicherheitsmaßnahmen zu beraten. Hierbei spielt die Resilienz – also die Widerstandsfähigkeit gegen Bedrohungen und die Fähigkeit zur schnellen Wiederherstellung nach Störungen – eine wesentliche Rolle. Anbieter müssen daher in der Lage sein, individuelle Bedarfsanalysen zu erstellen, die auf die spezifischen Risiken der jeweiligen Einrichtung abgestimmt sind. Dies umfasst auch die Empfehlung von Schutzmaßnahmen, die nicht nur die aktuellen Risiken adressieren, sondern auch auf zukünftige Bedrohungen vorbereitet sind.

3. Risikobewertung und Verhältnismäßigkeit der Maßnahmen

Das KRITIS-Dachgesetz und das NIS2-Umsetzungsgesetz setzen voraus, dass Sicherheitsmaßnahmen auf einer fundierten Risikobewertung basieren. Anbieter von physischen Sicherheitssystemen müssen daher in der Lage sein, ihre Produkte und Dienstleistungen in einen Gesamtprozess der Risikoanalyse einzubetten. Sie sollten gemeinsam mit den Betreibern und gegebenenfalls auch Behörden eine genaue Risikobewertung durchführen und Lösungen entwickeln, die verhältnismäßig und auf den spezifischen Kontext der jeweiligen Kritischen Infrastruktur zugeschnitten sind. Dieser Prozess verlangt auch die Einbeziehung organisatorischer Maßnahmen, wie zum Beispiel die Schulung des Sicherheitspersonals oder die Einrichtung klar definierter Zugangs- und Interventionsprotokolle.

4. Technische Standards und Berücksichtigung von Normen und Richtlinien

Eine zentrale Anforderung an die Anbieter ist die Einhaltung des „Standes der Technik". Die physischen Sicherheitssysteme müssen den neuesten technischen Standards entsprechen und alle relevanten Normen und Richtlinien berücksichtigen, um den erwarteten Anforderungen des KRITIS-Dachgesetzes und der NIS2-Richtlinie gerecht zu werden. Das bedeutet, dass Unternehmen ihre Technologie kontinuierlich anpassen und auf dem aktuellen Stand halten müssen, um Manipulationen, Einbrüche und Sabotage zu verhindern. Das umfasst auch Sicherheitsvorkehrungen wie erweiterte Authentifizierung bei Zutrittssystemen, verschlüsselte Kommunikationswege und moderne Alarmierungssysteme. Es muss sichergestellt werden, dass die Lösungen sowohl gegen die neuesten physischen als auch gegen IT-basierte Bedrohungen widerstandsfähig sind.

2. Das Sicherheitskonzept

2.1. Beschreibung

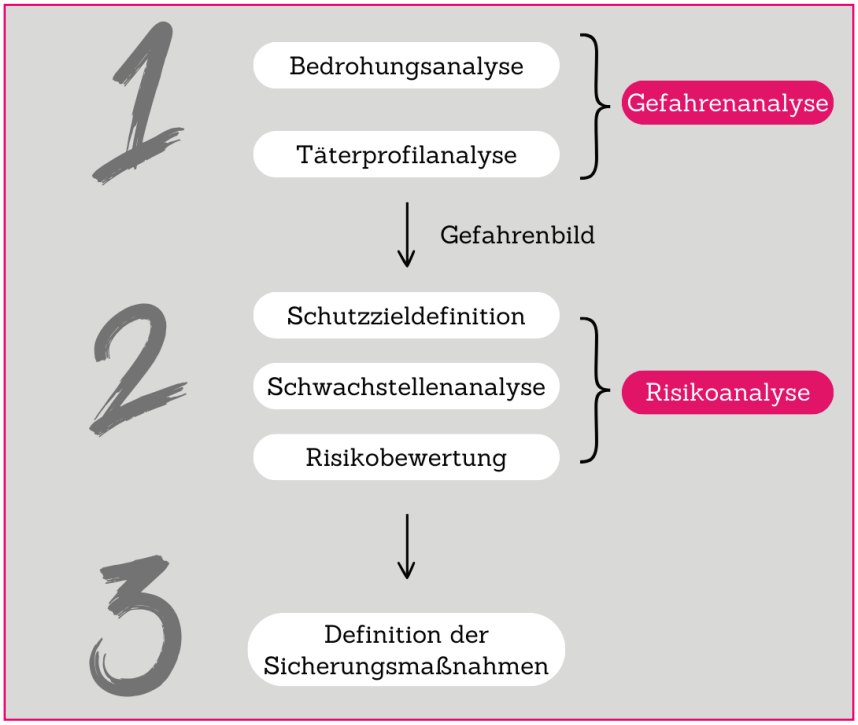
„Ohne ein Konzept ist alles nichts!". Diese Aussage verdeutlicht, nicht nur für Betreiber von Kritischen Infrastrukturen, dass vor jeder Planung und Projektierung einer sicherheitstechnischen Anlage die Erstellung eines Sicherheitskonzeptes, unter Berücksichtigung der baulichen, organisatorischen und personellen Sicherheit, unerlässlich ist. Ein solches Konzept bildet die Grundlage für eine qualifizierte und zielgerichtete Ausführung der Sicherheitstechnik. Eine elektronische sicherheitstechnische Anlage kann nur dann ihre optimale Wirkung entfalten, wenn sie - wie ein Zahnrad in einem komplexen Getriebe – optimal auf die anderen angrenzenden Fachbereiche abgestimmt ist: die bauliche Sicherheit (z.B. Perimeter, Sicherheitstüren und -fenster), die organisatorische Sicherheit (z.B. Definition von Interventionsmaßnahmen) und die personelle Sicherheit (u.a. Quantität und Qualität der Sicherheitsmitarbeiter).

Ein Sicherheitskonzept ermöglicht es, Sicherheit messbar zu machen, zu bewerten und darauf basierend effiziente und notwendige Maßnahmen abzuleiten. Ein solches Konzept ist nicht nur einmalig zu erstellen, sondern muss permanent angepasst und fortgeschrieben werden, z.B. bei Änderung der Gefahrenlage, baulichen Modifikationen oder nutzungstechnischen Änderungen. Viele sicherheitstechnische Normen definieren diese Notwendigkeit als Betreiberpflicht bzw. als Auftraggeberpflicht, d.h. der Betreiber hat das Konzept gemeinsam bzw. mit Unterstützung oder Genehmigung der beteiligten Stellen, wie Behörden, Versicherer, Planer und Errichter, zu erstellen und fortzuschreiben.

Dies ist insbesondere bei KRITIS-Objekten unerlässlich, da sich hier durch veränderte Gefährdungslagen und Vorgehensweisen der Täter immer wieder neue Bewertungsgrundlagen ergeben können. Dieser kontinuierliche Verbesserungsprozess leitet sich aus der allgemeinen Risikomanagementnorm ISO 31000 ab.

Für die Sicherheitsbranche hat sich in den vergangenen Jahren diese typische Vorgehensweise bzw. Gliederung bei der Erstellung von Konzepten abgeleitet.

Ablauf Gefahren- und Risikoanalyse (Ableitung aus ISO 31000)



2.2 Normen und Richtlinien

Für Sicherheitskonzepte existieren neben der ISO 31000 für das Risikomanagement keine nennenswerten speziellen Normen. Vielmehr wird in allen wesentlichen Normen und Regelwerken der Sicherheitstechnik (siehe andere Kapitel) und den angrenzenden Fachbereichen, wie der personellen Sicherheit, die dringende Notwendigkeit eines Sicherheits- bzw. Sicherungskonzeptes betont sowie

- Betreiber-/Auftraggeberpflichten (z.B. Begehungen gemäß DIN VDE 0833-1),
- Qualifikationen der handelnden Personen (z.B. Sachkundige Person gemäß DIN VDE 0833-1)
- Mindestinhalte und
- Sicherungsgrade definiert.

Dies sind beispielsweise die

- Normenreihe für alle Gefahrenmeldeanlagen DIN VDE 0833,
- für Videosicherheitstechnik DIN EN ISO/IEC 62676-4,
- Perimetersicherung DIN VDE V 0826-20,
- Notfall- und Gefahren-Reaktions-Systeme (NGRS) DIN VDE V 0827-1
- etc.

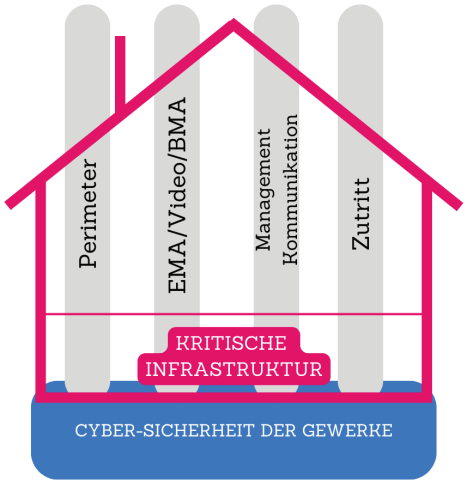
	Dokument	Typ	Titel	Veröffentlichung	Gültigkeit
1	ISO 3100	Allgemeine Anforderungen, nicht fachspezifisch	Risikomanagement - Leitlinien	2018-02	international
2	DIN EN IEC 31010	Allgemeine Anforderungen zur Risikobeurteilung, nicht fachspezifisch	Risikomanagement - Verfahren zur Risikobeurteilung	2024-12	international

3. Mindest-Standards der physischen Sicherheit

Im Folgenden werden die notwendigen Mindeststandards dargestellt, die in den verschiedenen sicherheitstechnischen Gewerken einzuhalten sind, um die physische Sicherheit einer Kritischen Infrastruktur zu gewährleisten.

Physische Schutzmaßnahmen

- **Perimeterschutzanlagen**
  - Physischer Schutz und Detektion
- **Zutrittssteuerungsanlagen**
  - Zufahrts- und Zugangsschutz der Ein- und Ausfahrten, Ein- und Ausgänge, Schranken und Schleusen
- **Einbruchmeldeanlagen, Brandmeldeanlagen und Videosicherheitssysteme**
  - Schutz der Gebäude und Gelände - Detektion
- **Gefahrenmanagementsysteme**
  - Notfallmanagement (Standard-Handlungsabläufe)
  - Abarbeitung organisatorischer Maßnahmen - auch in Krisensituationen
  - Vorausschauender Überblick zur Sicherheitslage und „Systemgesundheit“



3.1. Einbruchmeldeanlage (EMA) bzw. Überfallmeldeanlage (ÜMA)

3.1.1. Beschreibung

Einbruchmeldeanlagen (EMA) und Überfallmeldeanlagen (ÜMA) spielen eine zentrale Rolle beim Schutz Kritischer Infrastrukturen und dienen der umfassenden Sicherung von Gebäuden und Anlagen. Diese sicherheitstechnischen Systeme bieten eine präzise, schnelle und wirksame Erkennung und Meldung von Einbruchs- oder Überfallsituationen und sind für den Schutz hochsensibler Bereiche unverzichtbar.

Einbruchmeldeanlagen sind technische Systeme, die frühzeitig Einbruchsversuche und Manipulationen erkennen und Alarm auslösen. Zur Detektion potenzieller Eindringlinge steht eine Vielzahl unterschiedlicher Sensoren zur Auswahl, z. B. Bewegungsmelder, Glasbruchsensoren oder magnetische Kontakte an Fenstern und Türen. Diese Systeme überwachen kontinuierlich alle sensiblen Bereiche einer Kritischen Infrastruktur und bieten so eine wirksame Verteidigungslinie. Im Ereignisfall leiten EMAs automatisch Maßnahmen ein, die in der Regel die Alarmierung einer Sicherheitsleitstelle oder der zuständigen Sicherheitskräfte umfassen. Dies ermöglicht eine schnelle Reaktion auf Bedrohungen und verhindert unbefugten Zugriff auf sicherheitsrelevante Informationen oder Anlagen.

Überfallmeldeanlagen ergänzen EMAs, indem sie auf manuelle Alarmierungen in Notsituationen ausgelegt sind. ÜMAs ermöglichen es dem Personal, im Fall eines Überfalls oder bei Bedrohungen durch Dritte gezielt Alarm auszulösen. Diese Anlagen bestehen häufig aus strategisch platzierten Panikknöpfen oder mobilen

Auslösern und sind so konzipiert, dass sie diskret bedient werden können, um eine sofortige Intervention zu ermöglichen. Bei Auslösung einer ÜMA erfolgt eine schnelle Alarmübermittlung an Sicherheitskräfte, was insbesondere für Bereiche mit Publikumsverkehr oder für kritische Schaltzentralen und Steuerungsräume eine hohe Bedeutung hat.

Durch die Möglichkeit, in akuten Bedrohungssituationen Alarm zu geben, tragen ÜMAs zur unmittelbaren Sicherheit des Personals und zur Sicherstellung der operativen Funktionalität bei.

Die Detektions- und Reaktionszeiten müssen eng aufeinander abgestimmt sein, um bei sicherheitsrelevanten Ereignissen, wie z. B. Einbrüchen, rasch intervenieren zu können. Besonders bei Kritischen Infrastrukturen wie Umspannwerken, die eine essenzielle Rolle in der Stromversorgung spielen, kann ein solcher Vorfall weitreichende Folgen haben. Ein gestohlener Kabelstrang führt nicht nur zu finanziellen Schäden, sondern kann auch gravierende Auswirkungen auf die Versorgungssicherheit haben. Krankenhäuser, Versorgungsunternehmen oder andere lebenswichtige Einrichtungen könnten von der Stromzufuhr abgeschnitten werden, was ernsthafte Gefährdungen nach sich zieht. Die Einbruch- oder Überfallmeldeanlage dient in diesem Fall weniger dem Schutz vor klassischem Diebstahl. Ihr primärer Zweck ist es, Sabotage oder andere Angriffe auf Kritische Infrastrukturen frühzeitig zu erkennen und eine direkte Reaktion, etwa durch Sicherheitsdienste oder die Polizei, zu ermöglichen.

3.1.2. Normen und Richtlinien

Die nachfolgenden Normen und Richtlinien sind für Einbruch- und Überfallmeldeanlagen relevant:

	Dokument	Typ	Titel	Veröffentlichung
1	DIN VDE 0833-1	Norm	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Teil 1: Allgemeine Festlegungen	2014-10
2	DIN VDE 0833-3	Norm	Festlegungen für Einbruch- und Überfallmeldeanlagen	2020-10
3	DIN EN 50131	Normenreihe	Alarmanlagen - Einbruch- und Überfallmeldeanlagen	
4	VdS 2311*)	Richtlinie	Einbruchmeldeanlagen, Planung und Einbau	2021-10 (06)
5	VdS 2347*)	Richtlinie	Integrierte Gefahrenmeldeanlagen - Anforderungen	2002-01 (02)

*) Hintergründe/Relevanz von VdS-Richtlinien siehe Link

3.1.3. Mindeststandards für KRITIS

Bei Objekten, die der KRITIS-Kategorie zugeordnet werden, muss in vielen Fällen mit professionellen Tätern gerechnet werden, wobei insbesondere die organisierte Kriminalität, Extremisten und Terroristen zu nennen sind. Daher wird die Verwendung von Komponenten des Grad 3 gemäß DIN EN 50131 oder höher (sofern verfügbar) dringend empfohlen, um einen umfassenderen Schutz gegen Überwindung und Sabotage zu gewährleisten. Beispielhaft seien hier Bewegungsmelder mit integrierter Abdeckküberwachung, Magnetkontakte mit integrierter Fremdfeldüberwachung sowie Übertragungswege zur Alarmempfangsstelle mit (Dual-Path-4) DP4-Technologie genannt.

Die Kombination unterschiedlicher Detektionstechnologien kann die Widerstandsfähigkeit gegenüber Überwindungsversuchen deutlich erhöhen. Die genannten Normen beziehen sich dabei nicht nur auf die Geräte, sondern enthalten auch konkrete Vorgaben für deren fachgerechte Installation. Die Einbruchmeldeanlage (EMA) oder Überfallmeldeanlage (ÜMA) sollte an einem Ort installiert werden, der für unbefugte Personen weder einsehbar noch erreichbar ist, um einen Schutz vor Sicht und Zugriff sicherzustellen.

Weitere Informationen zum fachgerechten Einbau einer EMA oder ÜMA finden sich im BHE-Praxisratgeber „Sicherungstechnik" sowie in den zuvor genannten Normen.

3.2 Brandmeldeanlagen (BMA)

3.2.1. Beschreibung

Brandmeldeanlagen für Kritische Infrastrukturen sind im Kontext dieser Informationsschrift so zu verstehen, dass über die bereits bestehenden üblichen bauordnungsrechtlichen Anforderungen hinaus Gebäude, Anlagenteile oder auch Geräte/Schränke etc. schutzzielorientiert überwacht werden.

Dies erfolgt größtenteils mithilfe sogenannter Sondertechnik, also nicht mit den klassischen punktförmigen automatischen Brandmeldern.

Ein Zusammenwirken mit Löschanlagen sowie die Möglichkeit, bereits bei Vorinformation der Systeme entsprechende Maßnahmen einzuleiten, wird über den normativen Bereich hinaus meist im Sicherungskonzept beschrieben.

3.2.2. Normen und Richtlinien

Bei Brandmeldeanlagen gelten grundlegend die DIN VDE 0833 Teil 1 und Teil 2 sowie die DIN 14675 bei Aufschaltung auf die öffentlichen Feuerwehren. Bei Berücksichtigung versicherungstechnischer Vorgaben sind zusätzliche Anforderungen aus der VdS-Richtlinie 2095 umzusetzen.

Die aktuelle DIN VDE 0833 Teil 2 geht in den Anhängen „A" Überwachung von Räumen mit elektrischen und elektronischen Einrichtungen und „E" Überwachung von Räumen für Datenverarbeitungsanlagen und ähnliche Einrichtungen bereits auf Bereiche ein, die durchaus schon Maßnahmen innerhalb von KRITIS definieren.

	Dokument	Typ	Titel	Veröffentlichung
1	DIN VDE 0833-1	Norm	Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Teil 1: Allgemeine Festlegungen	2014-10
2	DIN VDE 0833-2	Norm	Festlegungen für Brandmeldeanlagen	2022-06
3	DIN 14675	Norm	Brandmeldeanlagen	2020-01
4	VdS 2095	Richtlinie	Automatische Brandmeldeanlagen, Planung und Einbau	2022-06

3.2.3. Mindeststandards für KRITIS

Die Auswahl verfügbarer Bauprodukte oder die Möglichkeit der individuellen Systemanpassung gemäß den geltenden Normen und Vorschriften sollten bereits im Brandschutzkonzept (Sicherungskonzept) beschrieben werden. Während sich bei der Überwachung von Traforäumen und Geräteüberwachungen Ansaug-

rauchmelder etabliert haben, können bei großen Überwachungsbereichen linienförmige Rauchmelder in unterschiedlichen Varianten (2D/3D) angewendet werden. Der Einsatz von Videosicherheit für die Detektion von Feuer und Rauch oder aber der Einsatz reiner Thermalüberwachungen ist je nach Gefährdungsanalyse umsetzbar. Systemkomponenten, die nicht als Bauprodukt zertifiziert oder harmonisiert sind, können eingesetzt werden, wenn ihr Einsatz zur Erreichung des Schutzziels erforderlich ist und sie in den gängigen Normen aufgeführt werden. Dies gilt auch, wenn diese Komponenten nicht in einem System nach DIN EN 54-13 enthalten sind.

Die Überwachung von Verteilern, Datenschränken und EDV-Anlagen, der Stromversorgung und der zugehörigen Notstromversorgung erfordert ebenso ein hohes Maß an Fachkompetenz wie z.B. die Überwachung von Flugzeughangars oder Kavernen von Wasserkraftwerken.

3.3 Videosicherheitssysteme (VSS)

3.3.1. Beschreibung

Zur nachhaltigen Sicherung Kritischer Infrastrukturen bieten Videosicherheitssysteme in Ergänzung zu anderen Sicherheitstechniken den zusätzlichen Nutzen, sensible und/oder unübersichtliche Bereiche oder Räume aus (großer) Entfernung einsehbar zu machen. Dabei kann das konkrete Geschehen vor Ort (auch standortübergreifend) gleichzeitig beobachtet und aufgezeichnet werden.

Durch das intelligente Zusammenspiel der verschiedenen sicherheitstechnischen Gewerke mit moderner Videosicherheitstechnik, deren Systeme vernetzt zusammenarbeiten, ergibt sich ein großes Potential der Kriminalprävention, da es möglich ist, mutmaßliche Täter so frühzeitig zu erkennen, dass diese bereits vor dem Betreten sensibler Bereiche detektiert und mittels Videotechnik erkannt werden.

Wird die Videosicherheitstechnik zusätzlich mit bidirektionaler Audiotechnik ausgestattet, kann von einer Leitstelle bzw. einer rund um die Uhr besetzten Notruf- und Serviceleitstelle (NSL) eine gezielte Ansprache der mutmaßlichen Täter direkt aus der Ferne erfolgen. Dadurch wird in den meisten Fällen verhindert, dass ein Täter in einen sensiblen Bereich eindringt bzw. diesen betritt.

Die Anforderungen an ein VSS zur Absicherung einer Kritischen Infrastruktur sind daher in der Regel deutlich höher anzusetzen als bei einer Standard-Videosicherung im gewerblichen oder industriellen Bereich. Es wird daher dringend empfohlen, bei der Absicherung Kritischer Infrastrukturen nach dem aktuellen Stand der Normen zu arbeiten.

3.3.2. Normen und Richtlinien

Die Standardisierung der Videosicherheitstechnik wird in Deutschland durch die Normenreihe DIN EN 62676 geregelt, die mit der Reihe VDE-0830-7-5 identisch ist.

Die wichtigste Norm dieser Reihe ist die DIN EN 62676-4, die die Anwendungsregeln für Videosysteme in Sicherheitsanwendungen beschreibt. Diese Norm wird derzeit überarbeitet und voraussichtlich 2025 in einer überarbeiteten Fassung vorliegen. Sie beschreibt unter anderem Details zu den Themen Sicherungskonzeption, Auswahl, Planung, Errichtung, Bildqualitätsnachweis, Betrieb und Dokumentation.

	Dokument	Typ	Titel	Veröffentlichung
1	DIN EN 62676-1-2 VDE 0830-7-5-12	Norm	Videoüberwachungsanlagen für Sicherungsanwendungen Teil 1-2: Systemanforderungen – Allgemeine Anforderungen an die Videoübertragung	2014-11
2	DIN EN 62676-4	Norm	Anwendungsregeln für Videosysteme in Sicherheitsanwendungen	2016-07 (in Überarbeitung)

Für den Nachweis einer ordentlichen Anlagendokumentation gemäß der DIN EN 62676-4 hat der „Fachausschuss Video" des BHE eine Checkliste in Form einer Excelliste veröffentlicht. Diese steht BHE-Mitgliedsunternehmen unter folgendem Link zur Verfügung.

3.3.3. Mindeststandards für KRITIS

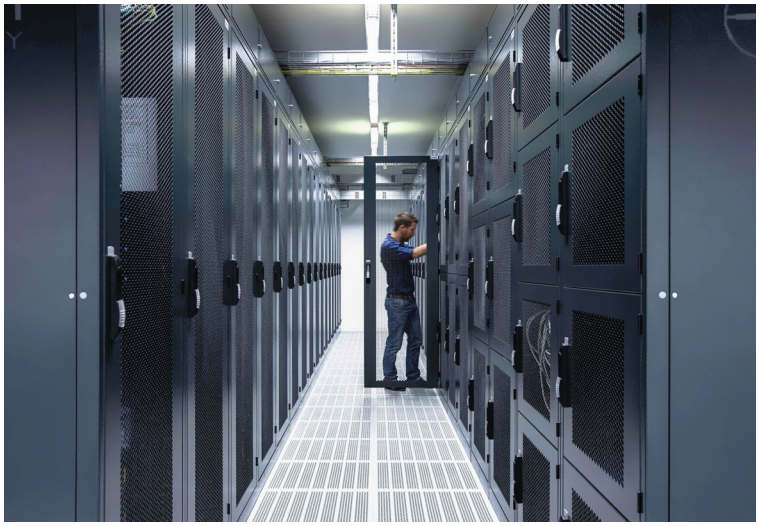
In der überarbeiteten Fassung der DIN EN 62676-4 (voraussichtlich ab 2025 verfügbar) wird explizit auf die Definition von Sicherungsgraden eingegangen. Je nach Sektor und Untersektor der Kritischen Infrastruktur empfiehlt die Norm unterschiedliche Sicherungsgrade, die tabellarisch dargestellt werden.

Ausführliche und weiterführende Informationen zu den Videosicherheitssystemen können dem BHE-Praxis-Ratgeber „Videosicherheit", der bereits in der 6. Auflage (2023) zur Verfügung steht, entnommen werden.

3.4 Zutrittssteuerung

3.4.1. Beschreibung

Zutrittssteuerungssysteme sind zentrale Bestandteile der Absicherung Kritischer Infrastrukturen, da sie den Zugang zu besonders schutzbedürftigen Bereichen gezielt regeln und überwachen. Ihre Hauptfunktion besteht darin, nur autorisierten Personen den Zutritt zu sicherheitsrelevanten Bereichen zu gewähren und gleichzeitig potenzielle unbefugte Zugriffe zu verhindern. Für die Betreiber Kritischer Infrastrukturen ist es von höchster Bedeutung, das bestmögliche Schutzniveau zu erreichen und von den Vorteilen moderner technischer Systeme zu profitieren.



Gleichzeitig gilt es, Transparenz zu schaffen und „Altlasten" zu beseitigen. Mechanische Schlüssel beispielsweise können weitergegeben werden, gehen leicht verloren oder werden unerlaubt kopiert – ein permanentes Sicherheitsrisiko. Darüber hinaus kann der Ersatz bei Schlüsselverlust schnell teuer werden. Die Verwendung eines verlorenen/entwendeten Schlüssels wird nicht protokolliert oder bemerkt. Um den geforderten höheren Sicherheitsanforderungen gerecht zu werden, können in KRITIS-Einrichtungen ergänzend oder alternativ biometrische Erkennungsverfahren zur Verifikation oder Authentisierung eingesetzt werden. Eine intelligente elektronische Zutrittssteuerung schafft hier wirksame Abhilfe und ist über den gesamten Lebenszyklus betrachtet wesentlich günstiger, da die Betriebskosten deutlich geringer sind als bei mechanischen Systemen.

Durch individuelle oder gruppenspezifische Zutrittsrechte kann genau festgelegt werden, wer wann und wo eine Zutritts- und Zufahrtsberechtigung hat. Gleichzeitig erhalten die Betreiber einen umfassenden Überblick über alle Zutrittsereignisse sowie Meldungen, wenn Zutrittspunkte unberechtigt geöffnet, passiert oder manipuliert werden. Dies bietet Schutz vor Diebstahl, Vandalismus, Sabotage und Wirtschaftsspionage. Bei Verlust oder Diebstahl von Zutrittsmedien kann sofort reagiert werden. Indem Berechtigungen in Echtzeit gelöscht werden, ist das Objekt zu keinem Zeitpunkt ungeschützt. Darüber hinaus können Zutrittsrechte auch im laufenden Betrieb stets aktuell angepasst und beispielsweise mit flexiblen Zutrittszeiten versehen werden.

Ein effizientes elektronisches Zutrittsmanagement spart erhebliche Ressourcen, schafft Flexibilität in der Handhabung und sichert den Überblick durch detaillierte Echtzeitdaten. Darüber hinaus können Sicherheitsabläufe automatisiert und Betriebskosten gesenkt werden. Viele alltägliche Funktionen und Reaktionen auf Vorfälle können ohne manuelle Eingriffe abgewickelt werden. Das spart Zeit, macht die Wartung effizienter und reduziert den Personalbedarf vor Ort.

Sehr vorteilhaft sind auch die vielfältigen Integrationsmöglichkeiten mit Drittsystemen. Die Palette der Möglichkeiten reicht von klassischen Sicherheitsgewerken wie Videosicherheitssystemen, Perimeterschutz, Fluchtwegsteuerung und Physical Security Information Management (PSIM) bis hin zu Raummanagement, Zeiterfassung, Arbeitsschutzunterweisungssystemen, Präsenzmeldung und Gebäudemanagement. Auch Brandmeldeanlagen (BMA) können mit der Zutrittssteuerung interagieren. Die Brandmeldezentrale löst dann z.B. entsprechende Türsteuerungen aus.

3.4.2. Normen und Richtlinien

Die Standardisierung der Zutrittssteuerung erfolgt in Deutschland durch die Normenreihe DIN EN 60839-11. Hier werden viele Fragen zur Zutrittssteuerung beantwortet.

Hinweis: Die folgende Aufstellung nimmt bewusst keinen Bezug auf etwaige Normen, die im Zusammenhang der mechanischen Absicherung (Tür, Schloss, Beschläge, etc.) stehen.

	Dokument	Typ	Titel	Veröffentlichung	Gültigkeit
1	DIN EN 60839-11-1	Technische Spezifikation	Alarmanlagen - Teil 11-1: Elektronische Zutrittskontrollanlagen - Anforderungen an Anlagen und Geräte	2015-10	CENELEC-Mitglieder
2	DIN EN 60839-11-2	Anforderungen an den Betrieb	Alarmanlagen - Teil 11-2: Elektronische Zutrittskontrollanlagen - Anwendungsregeln	2016-04	CENELEC-Mitglieder

Die DIN EN 60839-11-1 stellt die Anforderungen an Zutrittssysteme dar. Dazu werden in 4 Sicherheitsgraden die zu erfüllenden Anforderungen aufgeführt. Hier sind beispielsweise zu nennen: Schnittstelle des Zutrittspunktes, Hinweise und Signalisierung (Anzeige, Alarm, Protokollierung), Bedrohungssignalisierung, Vorrangschaltung (overriding), Systemselbstschutz und Energieversorgung

3.4.3. Mindeststandards für KRITIS

Die Einstufung in einen der 4 Sicherheitsgrade gemäß normativem Anhang A der DIN EN 60839-11-2 erfolgt durch den Betreiber entsprechend seiner sicherheitstechnischen und organisatorischen Anforderungen und einer zuvor durchgeführten Risikoanalyse, ggf. gemeinsam mit dem Sicherheitsanbieter. Hochsicherheitsbereiche der Kritischen Infrastrukturen sind vorrangig in der Sicherheitsstufe 4 auszuführen. Die Risikoanalyse ist nicht Gegenstand der Norm, es werden jedoch Hinweise dazu gegeben.

Bereits in frühen Ausgaben der technischen Richtlinien des BSI wurden als Trägermedium (auch Ausweise, Transponder oder Identifikationsmittel genannt) ausschließlich RFID-Medien nach ISO/IEC 14443, mit Secure Access Module (SAM) und AES 128 Verschlüsselungsverfahren oder gleichwertigen offenen Verfahren, vorgegeben z.B. Mifare Desfire EV3.

Bei Sicherheitsvorfällen muss das System automatisiert und softwaregesteuert folgende Prozesse aktivieren:

- Blockieren des Zutritts zu Gefahrenbereichen
- Schließen von Zutrittsstellen (z.B. Schleusen)
- Öffnen von Notfalltüren
- Auslösung von Alarmen, insbesondere für Rettungskräfte

Ausführliche und weiterführende Informationen zu Zutrittssystemen stehen unter https://www.bhe.de/fachthemen/fachsparten/zutritt/infos-and-papiere zum Download zur Verfügung. Weiterhin bietet der BHE-Praxis-Ratgeber „Zutrittssteuerung" aktuelle und vielfältige Informationen zu den wesentlichen Aspekten der Zutrittssteuerung.

3.5 Perimetersicherung

3.5.1. Beschreibung

Die Perimetersicherung ist der äußerste Baustein für ein wirkungsvolles Sicherungskonzept einer Liegenschaft. Sie besteht aus der Kombination einer mechanischen Sicherung und einem Perimetersicherheitssystem (PSS). Die mechanische Sicherung umfasst die schutzzielkonforme Planung und den Einsatz von Zäunen und Schranken als mechanische Barriere. Das PSS ist ein Detektionssystem für den Außenbereich und erfüllt eine ähnliche Funktion wie eine Einbruchmeldeanlage in einem Gebäude. Es dient der Detektion von Eindringversuchen in externe Bereiche außerhalb geschlossener Gebäude und wird innerhalb des Perimeters aber außerhalb eines Gebäudes installiert.

Durch die frühzeitige Alarmierung bei Annäherung an ein Gelände bzw. bei unbefugtem und oft gewaltsamem Betreten kann die Widerstandszeit deutlich erhöht werden.
Darüber hinaus hat ein Perimetersicherheitssystem eine abschreckende Wirkung auf Gelegenheitstäter. In fast allen Fällen wird das PSS mit einem Videosicherheitssystem kombiniert, um die Ereignisse zu verifizieren und zwischen echten und falschen Alarmen zu unterscheiden.

Die Hauptfunktion eines Perimetersicherheitssystems besteht also darin, die Unversehrtheit der rechtlichen Grenze rund um die Uhr zu gewährleisten. Es muss daher speziell auf die mechanische Barriere (Graben, Mauer, Zaun, Hecke etc.) abgestimmt sein. Weitere Anforderungen ergeben sich aus dem Täterprofil und dem allgemeinen Schutzziel der Anlage.

Die Anforderungen an ein PSS, das zur Sicherung einer Kritischen Infrastruktur eingesetzt wird, sind daher in der Regel deutlich höher anzusetzen als bei einer Standard-Perimetersicherung im gewerblichen Industriebereich. Neben dem Überklettern von Zäunen gehören auch das Unterkriechen, Durchbrechen oder spezielle Fortbewegungsarten wie Kriechen, Robben und Rollen zu typischen Vorgehensweisen, die das Täterprofil ergänzen.

3.5.2. Normen und Richtlinien

Die Standardisierung der Perimetersicherung ist in Deutschland durch zwei Regelwerke geprägt. Zum einen durch die europäische Normenreihe des Europäischen Komitees für elektrotechnische Normung (CENELEC), die DIN CLC/TS 50661-x, und zum anderen durch die von der DKE erarbeitete Anwendungs-Vornorm DIN VDE V 0826-20.

Hinweis: In der folgenden Auflistung wird bewusst auf mögliche Normen, die im Zusammenhang mit der mechanischen Sicherung (Zaun, Mauer, Auslegerkonstruktion etc.) stehen, verzichtet.

	Dokument	Typ	Titel	Veröffentlichung	Gültigkeit
1	DIN CLC/TS 50661-1 (VDE V 0830-100-1)	Technische Spezifikation / Vornorm	Alarmanlagen - Externe Perimeter-Sicherheitsanlagen Teil 1: Systemanforderungen	April 2018	CENELEC-Mitglieder, d.h. auch Deutschland
2	DIN VDE V 0826-20	Vornorm	Überwachungsanlagen - Teil 20: Externe Perimeter Sicherheitsanlagen - Anwendungsregeln	Sept. 2023	Deutschland

In der Vornorm DIN VDE V 0826-20 finden sich zwei wichtige Hilfestellungen zur Dokumentation von PSS, die auch im KRITIS-Bereich Anwendung finden:

a) verbändeübergreifende PSS-Anlagenbeschreibung
b) Checkliste für die Betriebsanforderung PSS

Diese stehen unter folgendem Link zum Download zur Verfügung.

3.5.3. Mindeststandards für KRITIS

Perimetersicherheitssysteme werden nach DIN CLC/TS 50661-1 in zwei verschiedene Kategorien eingeteilt:

- PSS-Eigenschutz und
- PSS-Leistung.

Der „PSS-Eigenschutz" ist ein Maß dafür, inwieweit ein Täter eine Sabotage des Sicherheitssystems in Betracht zieht. KRITIS-Anlagen sollten der Eigenschutzklasse „4" zugeordnet werden. Aufgrund des Täterprofils ist auch ein mehrstufiger Angriff wahrscheinlich. Dabei kann in einem ersten Schritt das Detektionssystem außer Betrieb gesetzt oder zumindest gestört werden. Diese Störung muss weiträumig detektiert und gemeldet werden.

Höhere Klassifikationen einer Leistungskategorie sind für Anlagen vorgesehen, die komplexer sind oder eine größere Flexibilität im Betrieb erfordern. Erst ab der Leistungskategorie „B" sind zwei Alarmstufen, z. B. Voralarm und Alarm, vorgesehen. Aufgrund der besseren Steuerung der Intervention ist dies in einem PSS-System für KRITIS-Anlagen vorzusehen.

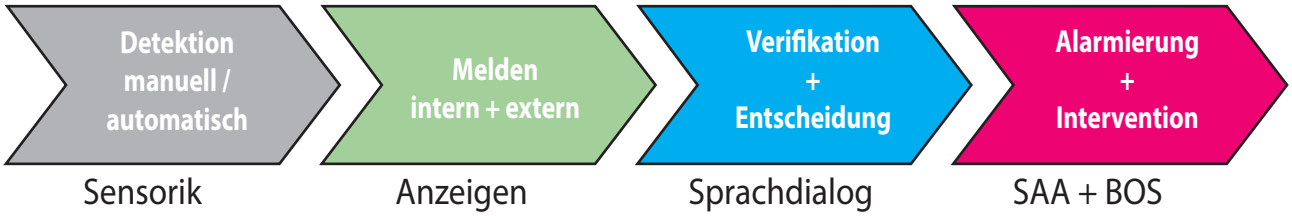
Installationsempfehlungen

	Empfehlungen für PSS im KRITIS-Bereich
PSS-Eigenschutz	Eigenschutzklasse 4 (siehe DIN VDE V 0826-20)
PSS-Leistungskategorie	Leistungskategorie B oder höher
Detektionstechnik	Mehrfach-Detektion mit zwei Detektionssystemen mit jeweils physikalisch anderem Wirkprinzip gemäß Empfehlung der DIN VDE V 0826-20
zu berücksichtigendes Täterprofil	Durchbrechen, Überklettern, Übersteigen, Herumlungern
Notstromüberbrückungszeit	je nach Anforderung und Interventionszeit

Ausführliche und weiterführende Informationen zu den Systemen und Detektionsverfahren können der Broschüre „Perimetersicherheit - BHE-Planungsgrundlagen" entnommen werden.

3.6 Kommunikationssysteme

NGRS-Prozesskette von der Detektion bis zur Intervention



3.6.1. Beschreibung

Die Kommunikation im Krisenfall ist von zentraler Bedeutung für die schnelle und effektive Bewältigung der Situation. Insbesondere in Krisenzeiten müssen die Kommunikationssysteme für alle Meldenden und Entscheidungsträger hochverfügbar sein. In der höchsten Sicherheitsstufe sollte dazu ein von allen anderen Systemen unabhängiges und autarkes Kommunikationssystem mit einem eigenständigen Netz redundant zur Verfügung stehen. In der mittleren Sicherheitsstufe kann auf Redundanz verzichtet werden und in der niedrigen Sicherheitsstufe kann anstelle eines eigenen Netzes ein vorhandenes Sicherheitsnetz mitgenutzt werden. Die Entscheidung über die relevante Sicherheitsstufe wird im Rahmen eines Risikomanagementprozesses getroffen.

In jeder Organisation wird ein etabliertes Kommunikationskonzept genutzt.

Die Hauptaufgaben der darin eingesetzten Kommunikationssysteme liegen in der Unterstützung aller Abläufe, um einen reibungslosen Betrieb zu gewährleisten, sowie in der schnellen und effektiven Behebung von Störungen in den Betriebsabläufen. Diese Störungen können technischer Natur sein oder die Gesundheit der Mitarbeiter betreffen. Durch verschiedene präventive Maßnahmen lassen sich solche innerorganisatorischen Störungen auf ein Minimum reduzieren.

Im Hinblick auf die Anforderungen aus dem KRITIS-Dachgesetz ist das bestehende Kommunikationskonzept einer Organisation zu überprüfen und anzupassen, wobei alle denkbaren Störeinflüsse durch externe Faktoren zu berücksichtigen sind.

Welche Störeinflüsse (Angriffe) in Bezug auf die Art der Ausführung und dem damit verbundenen Schadensumfang im Kommunikationskonzept zur Schadensbewältigung zu berücksichtigen sind, muss im Einzelfall durch eine Risikobeurteilung in einem Risikomanagementprozess ermittelt werden (siehe Grafik).

Jeder Störfall erfordert eine Entscheidung über die Art und den Umfang der zu ergreifenden Maßnahmen. Dabei sind viele Fragen von besonderer Bedeutung, zum Beispiel:

- Ist die bestehende Kommunikationsstruktur der Organisation mit den bestehenden Kommunikationseinrichtungen in der Lage, eine schnelle und fundierte Maßnahmenentscheidung herbeizuführen?
- Ist die bestehende Kommunikationsinfrastruktur im Störfall verfügbar?
- Sind für die Störfallkommunikation die notwendigen Prioritäten vorhanden?
- Besteht eine Notfall-Kommunikationsinfrastruktur?
- Wie lange ist die Notfall-Kommunikationsinfrastruktur bei Stromausfall verfügbar?
- Wie wird die richtige Entscheidung zur Räumungsalarmierung z.B. im Brandfall oder Einschluss-Alarmierung bei Terrorangriff herbeigeführt, wenn beide Ereignisse zeitgleich gemeldet werden?

Diese und viele weitere Fragen sind im Rahmen des Risikomanagements für ein Notfall- und Gefahren-Reaktions-System (NGRS) zu beantworten. Eine Liste von 100 Basisfragen ist in der DIN VDE V 0827-3 zur Erstellung einer „Risiko-Management-Akte“ nach EN 50726-1 als Orientierungshilfe aufgeführt.

In vielen Organisationen, die voraussichtlich unter KRITIS fallen werden, sind in den letzten Jahren Notfall- und Gefahren-Reaktions-Systeme installiert worden, um im Krisenfall schnelle Entscheidungen treffen zu können und das Schadensausmaß erheblich zu reduzieren.

Die Reaktionszeit auf einen Störfall hat großen Einfluss auf das Schadensausmaß. Je kürzer die Reaktionszeit, desto schneller greifen Gegenmaßnahmen und desto kürzer ist die Wirkungsdauer der Störung.

Störfall-Reaktionszeit = Störfall-Meldezeit + Erreichbarkeit-Verantwortlicher + Lageerkundung-Verifikation + Entscheidungszeit + Gegenmaßnahmen einleiten + Hilfe durch Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

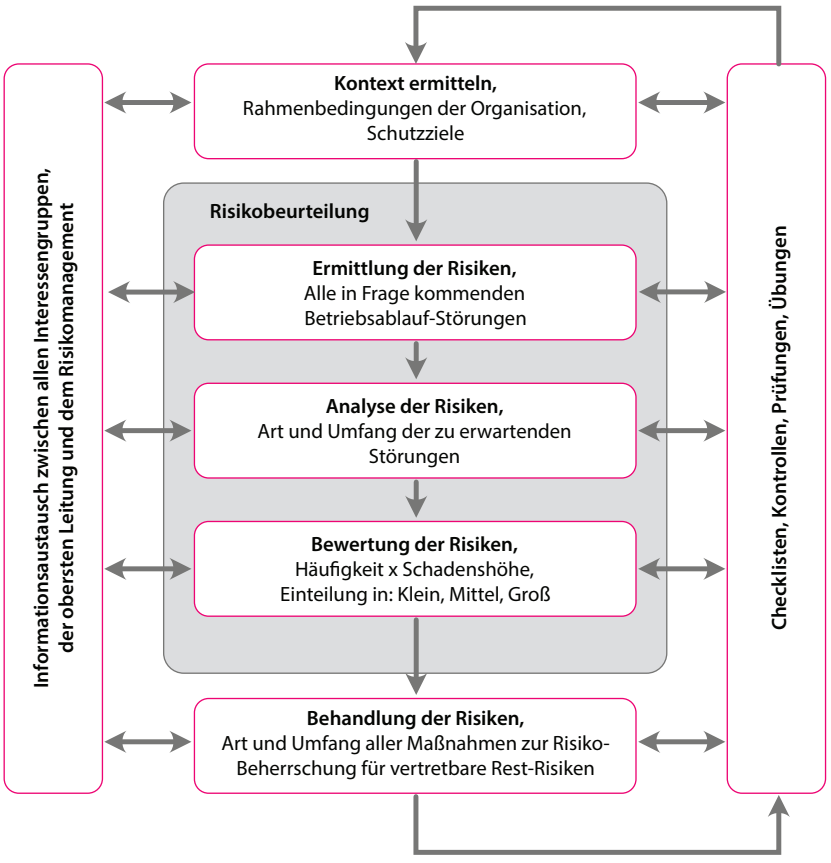
Eine Möglichkeit, die Störfall-Reaktionszeit zu verkürzen besteht darin, sie auf die Meldezeit zu reduzieren, wenn durch Störfall-Meldungen automatisch geeignete Gegenmaßnahmen eingeleitet werden. Dies birgt jedoch die große Gefahr, dass falsche Störfall-Meldungen nicht herausgefiltert werden und dadurch Sekundärschäden entstehen. Außerdem würde bei gleichzeitigem Auftreten von Gefahren mit gegenläufigen Gegenmaßnahmen, wie z.B. bei einer Terroranschlagsmeldung und einer Brandmeldung, möglicherweise die falsche Gegenmaßnahme eingeleitet und die Verhältnismäßigkeit der Gegenmaßnahmen nicht berücksichtigt.

Eine weitere Möglichkeit zur Minimierung der Störfall-Reaktionszeit ist eine optimale Krisen-Störfall-Kommunikation entlang der gesamten Ereigniskette von der Störfall-Meldung bis zur Einleitung von Gegenmaßnahmen. Dadurch können falsche Störfall-Meldungen herausgefiltert, situationsgerechte Gegenmaßnahmen eingeleitet und die Verhältnismäßigkeit berücksichtigt werden.

Welche Krisen- und Störfallkommunikation in Form von Daten, Bildern, Sprache und Alarmierung in Verbindung mit den entsprechenden organisatorischen Notwendigkeiten im Einzelfall erforderlich ist, kann nicht pauschal festgelegt werden, sondern muss im Rahmen eines Risikomanagementprozesses ermittelt werden (siehe Grafik).

Der Risikomanagementprozess für eine NGRS ist ein wesentlicher Bestandteil der EN 50726-1:2024-05-17. Die Norm beschreibt die Anforderungen an ein Notfall- und Gefahren-Reaktions-System (NGRS) in Verbindung mit der notwendigen organisatorischen Kommunikation entlang der Ereigniskette und schließt mit der Prognose der zu erwartenden Restrisiken. Die Restrisiken gelten dabei unter der Annahme, dass alle identifizierten technischen und organisatorischen Maßnahmen zur Risikobeherrschung gemäß der erstellten „Risiko-Management-Akte“ umgesetzt und eingehalten werden.

Der Risikomanagementprozess



Bernd Ammelung, Grafik: Risikobeurteilung (Gefährdungsbeurteilung) als Beitrag zum Risikomanagementprozess

3.6.2. Normen und Richtlinien

	Dokument	Titel	Veröffentlichung
1	EN 50726-1	Emergency and Danger Systems Part-1 Emergency- and Danger Response-System (EDRS) Basic requirements, duties, responsibilities and activities.	2024-05
2	DIN VDE V 0827-1	Notfall und Gefahren-Systeme Teil 1: Notfall- und Gefahren-Reaktions-Systeme (NGR Notfall- und Gefahren-Reaktions-Systeme (NGRS) – Grundlegende Anforderungen, Aufgaben, Verantwortlichkeiten und Aktivitäten	2016-07
3	DIN VDE V 0827-2	Notfall und Gefahren-Systeme Teil 2: Notfall- und Gefahren-Reaktions-Systeme (NGRS) – Ergänzende Anforderungen für Notfall- und Gefahren-Sprechanlagen	2016-07
4	DIN VDE V 0827-3	Notfall- und Gefahren-Systeme Teil 3: Notfall- und Gefahren-Reaktions-Systeme (NGRS) - Risikomanagementakte und Anwendungsbeispiele	2021-12
5	EN 62820-2	Gebäude-Sprechanlagen Teil 2: Anforderungen an Sprechanlagen für Gebäude mit gehobenen Sicherheitsanforderungen (SGGS)	2018-01
6	EN 62820-3-2	Gebäude-Sprechanlagen Teil 3-2: Gebäude-Sprechanlagen für erhöhte Sicherheitsanforderungen – Anwendungsrichtlinien	2018-06
7	DIN EN 31010	Deutsche Fassung, Risikomanagement, Verfahren zur Risikobeurteilung	2019
8	prEN 50726-2	Notfall- und Gefahren-Systeme, Teil 2: Notfall- und Gefahren-Reaktions-Systeme (NGRS) – Besondere Anforderungen für KRITIS-Anwendungsfälle und bei gleichzeitiger Behandlung unterschiedlicher Gefährdungen (Arbeitstitel)	in Vorbereitung

3.6.3. Mindeststandards für KRITIS

Die Mindeststandards für ein Notfall-Krisen-Kommunikationssystem ergeben sich aus dem Risikomanagementprozess nach EN 50726 (VDE 0827) Teil 1 und Teil 3, wobei sehr genau geprüft werden muss, ob die niedrige Sicherheitsstufe für eine KRITIS-Anwendung überhaupt in Frage kommt. Sollte sie dennoch zum Einsatz kommen, ist das Leistungsmerkmal „Sprachkommunikation“ der Sicherheitsstufe 2 zwingend erforderlich, um das Restrisiko zu minimieren.

4. Cybersicherheit durch resiliente Übertragungstechnik sowie sichere Router und Netze

4.1. Sichere Netze/Router und resiliente Übertragungstechnik

4.1.1. Beschreibung

Die Sicherheitstechnik erfordert insbesondere in Kritischen Infrastrukturen und sensiblen Bereichen höchste Zuverlässigkeit und Schutz vor Ausfällen oder Angriffen. Die DIN EN 50136 spielt hierbei eine zentrale Rolle, da sie die Anforderungen an die Übertragung von Alarmmeldungen über Netzwerke definiert.

Diese Norm bezieht sich speziell auf Alarmübertragungsanlagen, die die Kommunikation zwischen Einbruchmelde-, Brandmelde- und Zutrittssteuerungssystemen sowie den Alarmempfangszentralen sicherstellen.

Um eine maximale Resilienz zu gewährleisten, sind sichere Router und Netzwerke von entscheidender Bedeutung. Die Resilienz eines Systems beschreibt dessen Fähigkeit, gegenüber äußeren Einflüssen wie Cyberangriffen, technischen Störungen oder Netzwerküberlastungen robust zu bleiben und die geforderte Funktion aufrechtzuerhalten. Ziel sollte es daher immer sein, eine sichere und redundante Übertragungsstrecke aufzubauen, so dass sowohl die Überwachung der Übertragungswege als auch die Übertragungszeiten gemäß den geltenden Normen und Richtlinien erfolgen können.

4.1.2. Normen und Richtlinien

Im Bereich der Alarmübertragungstechnik gibt es eine Reihe von Normen und Richtlinien, die sowohl auf europäischer als auch nationaler Ebene relevant sind. Diese Normen und Richtlinien definieren die Anforderungen an die Planung, Installation, den Betrieb und die Überwachung von Systemen zur Alarmübertragung.

Normen	Richtlinien
DIN EN 50136-1	VdS 2465-1
DIN EN 50136-2	VdS 2465-2
DIN EN 50136-3	VdS 2465-3
DIN EN 54-21	VdS 2311
DIN EN 50131-1	VdS 3836
DIN VDE 0833-1	

4.1.3. Mindeststandards für KRITIS

1. Spannungsversorgung

Die Übertragungstechnik muss gegen Spannungseinbrüche und Stromausfälle abgesichert sein, was durch eine unterbrechungsfreie Stromversorgung mittels Akkumulatoren gewährleistet werden kann.

Darüber hinaus sollte die Energieversorgungseinheit der Übertragungseinrichtung kontinuierlich überwacht werden, so dass evtl. Störungen an eine ständig besetzte Stelle gemeldet werden. Eine solche Energieversorgungseinheit sollte den Anforderungen der DIN EN 50131 Grad 4 entsprechen.

2. Redundante Übertragungswege

Es sollte nur Übertragungstechnik eingesetzt werden, die über mindestens zwei voneinander unabhängige Übertragungswege verfügt, z.B. über einen leitungsgebundenen IP-Übertragungsweg (DSL) und einen funkbasierten IP-Übertragungsweg (Mobilfunk).

Beide Übertragungswege sollten vollständig notstromversorgt sein und über eine Ende-zu-Ende-Überwachung zur Alarmempfangszentrale verfügen.

Hinweis: Zur Einhaltung der Überbrückungszeit kann es erforderlich sein, einen der beiden Übertragungswege nach einer gewissen Ausfallzeit abzuschalten.

3. Sabotageschutz

Die Übertragungstechnik muss adäquat gegen mechanische Beschädigung oder Sabotage geschützt werden, bspw. durch ein robustes Gehäuse, Deckelkontakt, Durchbohrungsschutz oder Abreißschutz.

4. Schutz vor Überspannung

Es wird empfohlen, im Rahmen der Risikoanalyse zu prüfen, ob ein zusätzlicher Schutz gegen Überspannungen vorzusehen ist. Dies betrifft u.a. die 230V-Spannungsversorgung, externe Mobilfunkantennen oder TAE/DSL-Anschlüsse.

5. Cybersicherheit

Für die Alarmübertragung sind ausschließlich speziell dafür vorgesehene Protokolle (z.B. VdS SecurIP) zu verwenden, die dem aktuellen Stand der Technik entsprechen.

Das eingesetzte Gerät sollte zudem nach den geltenden Cybersicherheitsanforderungen (z.B. VdS 3836) zertifiziert sein.

Es wird empfohlen, auf Geräte zurückzugreifen, die nach den Prinzipien „Security by Design“ sowie „Security by Default“ entwickelt wurden und über zeitgemäße DoS-Schutzmaßnahmen verfügen, die dem Stand der Technik entsprechen.

Hinweis: Der Einsatz von geschlossenen Netzwerken, wie dem BHE-Sicherheitsnetzwerk, ist zu empfehlen.

Ein Fernzugriff darf nur über Infrastrukturen erfolgen, die dem Stand der Technik nach DIN EN 50710 und TS 50136-10 entsprechen.

Einsatz von zertifizierten Geräten:

Die eingesetzte Übertragungstechnik sollte nach DIN EN 50131-10, DIN EN 50136-2, DIN EN 54-21 geprüft und zertifiziert sein.

Installationsempfehlungen für Aufschaltungen im KRITIS-Bereich		
Aufschaltung	AES gemäß DIN EN 50518 bzw. VdS 3138	
Übertragungseinrichtung inkl. Energieversorgungseinheit	Zulassung gemäß DIN EN 50131, Grad 4	
Cybersicherheits-Standard	Einhaltung der Richtlinie VdS 3836	
Übertragungswege	Dual-Path 4 (nur stehende Verbindungen)	
Übertragungsprotokoll	SecurIP	
Schlüsselgenerierung	Duale Alarmempfangsstelle (PK03)	Durch Übertragungseinrichtung (PK04)* * bspw. notwendig für den Anwendungsbereich BSI-Verschluss-Sachen

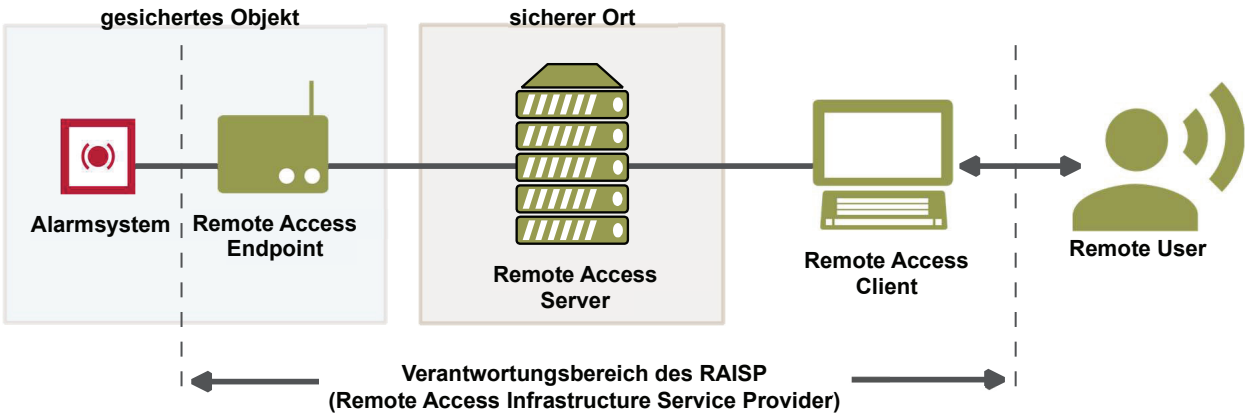
Installationsempfehlungen für Aufschaltungen im KRITIS-Bereich	
Übertragungsnetze	zwei Übertragungsnetze mit geschlossener Benutzergruppe (Keine Erreichbarkeit aus dem öffentlichen Netz)
Notstromüberbrückungszeit	Objektseitig für mindestens einen Übertragungsweg; 60 Stunden
Fernzugriffsoptionen	Gemäß DIN EN 50710 / TS 50136-10 über Übertragungsnetze mit geschlossener Benutzergruppe
Zertifizierungen	DIN EN 50131-10, DIN EN 50136-2, DIN EN 54-21
Passwortsicherheit	Gemäß dem Stand der Technik nur Passwörter mit mindestens 8 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen

4.2. Remote Access und Remote Services

- DIN EN 50710 regelt die „Remote Services“
- TS 50136-10 regelt den sicheren Zugriff „Remote Access“

Die beiden Normen gelten für alle in diesem Dokument beschriebenen sicherheitstechnischen Gewerke.

Die TS 50136-10 „Anforderungen an den Fernzugriff“ regelt die technische Infrastruktur für sichere Fernzugangsverbindungen und die Gesamtverantwortung. Es werden Leistungsmerkmale, Zuverlässigkeit, Integrität und Sicherheitsmerkmale einer Fernzugangsinfrastruktur festgelegt. Eine Plattform übernimmt die zentrale Funktion der Fernzugangsinfrastruktur. Der Betreiber der Fernzugangsinfrastruktur übernimmt die Gesamtverantwortung unter anderem auch für die Cybersicherheit.



Die DIN EN 50710 beschreibt die technischen Möglichkeiten der eigentlichen Remote Services. Diese sind spezifisch für die einzelnen sicherheitstechnischen Gewerke geregelt.

Eine Risikobeurteilung enthält zulässige Betriebsabläufe und Schutzmaßnahmen. Verantwortlichkeiten werden zwischen dem Bereitsteller der Ferndienstleistung sowie dem Auftraggeber geregelt.

5. Anforderungen an die Produkte

Nicht nur im Umfeld von Kritischen Infrastrukturen ist zunehmend auf die Cybersicherheit der eingesetzten Produkte zu achten. Aktuell werden neue Gesetze verabschiedet, die von den Herstellern der Produkte umgesetzt werden müssen. Anwender und Errichter sollten insbesondere im KRITIS-Bereich bereits jetzt auf die Umsetzung der Cyber-Sicherheits-Zielsetzung achten:

5.1. CRA - Cyber Resilience Act

Der Cyber Resilience Act wurde mit der Verordnung (EU) 2024/2847 am 20.11.2024 im Amtsblatt der Europäischen Union veröffentlicht (siehe Regulation - 2024/2847 - EN - EUR-Lex).

Die Verordnung ist am 10. Dezember 2024 in Kraft getreten, und ihre wichtigsten Verpflichtungen werden ab dem 11. Dezember 2027 gelten. Die Meldepflichten gelten ab dem 11. September 2026.

Der CRA beschreibt erstmals branchenübergreifend die Cybersicherheitsanforderungen an digitale Produkte. Dies umfasst sowohl Hardware als auch Software, die vernetzt oder vernetzbar ist.

Ausnahmen gibt es nur für nicht-kommerzielle Open-Source-Projekte und Branchen, in denen es bereits weitergehende Regelungen gibt, wie zum Beispiel bei Medizinprodukten. Diese Anforderungen sind insbesondere für Hersteller von Bedeutung, da sie sicherstellen müssen, dass ihre Produkte den neuen Standards entsprechen.

Nachfolgend finden Sie die wichtigsten Fragen und Antworten rund um den CRA.

Müssen die Anforderungen des CRA erfüllt werden?

Ja, der CRA erweitert den Geltungsbereich des CE-Kennzeichens. Ohne die Anforderungen zu erfüllen, dürfen die Produkte im EU-Binnenmarkt nicht mehr verkauft werden. Dies gilt nicht nur für Hersteller, sondern auch für Händler und Importeure, die Waren im EU-Binnenmarkt in den Verkehr bringen möchten.

Welche Vorgaben müssen umgesetzt werden?

Der CRA legt fest, dass die Informationssicherheit eines Produkts über dessen gesamten Lebenszyklus hinweg gewährleistet sein muss. Dies umfasst Prinzipien wie „Security by Design“ und „Security by Default“ sowie die Sicherstellung der Vertraulichkeit und Integrität der verarbeiteten Daten. Hersteller sind verpflichtet, entdeckte Schwachstellen zu melden und durch Sicherheitsupdates zu beheben. Zudem ist die Pflege einer Software Bill of Materials (SBOM) verpflichtend.

Eine SBOM dokumentiert, welche kommerziellen und freien Software-Bestandteile in Software-Produkten enthalten sind. Sie macht Abhängigkeiten zu Komponenten Dritter transparent und hilft damit Herstellern, Sicherheitsforschenden sowie professionellen Anwendern beim Monitoring von Schwachstellen.

Mit der TR-03183 hat das BSI hierzu bereits eine erste Richtlinie veröffentlicht.

Wie lange ist der beschriebene Produktlebenszyklus?

Der Lebenszyklus eines Produkts mit digitalen Elementen beginnt gemäß CRA mit dem Zeitpunkt des Inverkehrbringens und gilt entweder für die erwartete Lebensdauer des Produkts oder für einen Zeitraum von fünf Jahren ab Inverkehrbringen, je nachdem, welcher Zeitraum kürzer ist.

Wer stellt fest, ob das Produkt die Anforderungen erfüllt?

Im Rahmen des CRA werden Produkte mit digitalen Elementen in zwei Klassen eingeteilt, die das jeweilige Cybersicherheitsrisiko und die damit verbundenen Sicherheitsanforderungen widerspiegeln.

Klasse I umfasst kritische Produkte mit grundlegenden Sicherheitsanforderungen und geringeren Konformitätsauflagen, während Klasse II hochkritische Produkte mit strengeren Sicherheitsvorgaben und intensiverer Konformitätsbewertung abdeckt.

Beide Klassen sind im Anhang III „kritische Produkte mit digitalen Elementen" des CRA beschrieben.

Für den Bereich der Sicherheitstechnik sind u.a. folgende Produkte aus der Klasse I relevant:

- Digitale Elemente mit der Funktion eines virtuellen privaten Netzes (VPN)
- Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)
- Software für Fernzugriff und gemeinsame Datennutzung
- Software für die Mobilgeräteverwaltung
- Physische Netzschnittstellen
- …

Hersteller kritischer Produkte der Klassen I und II müssen die jeweils erforderlichen Konformitätsbewertungsmodule anwenden. Bis Mai 2025 will die EU harmonisierte Standards veröffentlichen, die es ermöglichen sollen, die Produkte eigenständig zu deklarieren. Dies wird jedoch voraussichtlich nur möglich sein, wenn beispielsweise der Entwicklungsprozess selbst nach einem harmonisierten Standard zertifiziert ist.

Hersteller kritischer Produkte der Klasse II müssen einen Dritten (notifizierte Stelle) in ihre Konformitätsbewertung einbeziehen. Zur Klasse II zählen z.B.:

- Public-Key-Infrastrukturen und Aussteller digitaler Zertifikate;
- Firewalls, Angriffserkennungs- und/oder -präventionssysteme für den industriellen Einsatz;
- Router, Modems für die Internetanbindung und Switches für den industriellen Einsatz;
- Sicherheitselemente;
- Geräte für das industrielle Internet der Dinge (IIoT), die zur Verwendung durch wesentliche Einrichtungen gemäß Anhang I der NIS2-Richtlinie bestimmt sind;

Welche Strafen drohen?
Bei Nichtbeachtung drohen empfindliche finanzielle Strafen sowie ein Verkaufsverbot für das Produkt auf dem europäischen Markt.

Warum sollte man sich bereits jetzt mit dem Thema beschäftigen?
Die Etablierung der notwendigen Prozesse benötigt Zeit und mehrere Erfahrungszyklen. Aspekte wie ein sicherer Entwicklungsprozess, Security by Design und Security by Default sollten frühzeitig implementiert werden, um die Konformität mit den später veröffentlichten harmonisierten Normen zu gewährleisten. Andernfalls könnte eine Überlastung der notifizierten Stellen nach Inkrafttreten dazu führen, dass betroffene Produkte nur verzögert in Verkehr gebracht werden dürfen.

5.2 RED (Funkanlagenrichtlinie oder Radio Equipment Directive)

In der Richtlinie RED ist die Cyber-Security im Abschnitt 3.3 beschrieben. Die Erfüllung der Vorgaben kann durch die Hersteller in einer Selbsterklärung mit einer harmonisierten Norm (vermutlich prEN 18031, EN303645 oder IEC 62443) oder nach Prüfung durch eine akkreditierte, notifizierte Stelle erfolgen.

Betroffen von der Richtlinie sind alle Produkte, die drahtlose Standards wie WIFI, Bluetooth oder Zigbee unterstützen. Dies bedeutet im erweiterten Sinne, dass beispielsweise Maschinen, die mit dem Internet verbunden sind, keine „schädlichen Auswirkungen auf das Netz oder seinen Betrieb" ausüben dürfen sowie „Funktionen zum Schutz von Betrug" implementiert sein müssen und der Schutz personenbezogener Daten zu gewährleisten ist.

Stand der Umsetzung

- Stand 11.11.2024 sind noch keine harmonisierten Standards zur Eigendeklaration veröffentlicht -> Prüfung der Produkte durch eine dritte Stelle wäre dann zwingend erforderlich
- Ab 01.08.2025: Produkte müssen gemäß dem harmonisierten Standard für einen weiteren Vertrieb nach RED deklariert sein
- Eine Überlastung der notifizierten Stellen führt dazu, dass Unternehmen betroffene Produkte nur verzögert in Verkehr bringen dürfen

5.3 Produkte aus sicherer Herkunft/Transparenz Lieferkette

Neue bzw. überarbeitete Normen nehmen Hersteller zunehmend in die Pflicht, die Herkunft sowohl digitaler als auch physischer Komponenten ihrer Produkte zu überwachen. Wie bereits erwähnt, fordert der Cyber Resilience Act hierfür die Pflege einer Software Bill of Materials. Externe Software oder Softwarebestandteile, sogenannte Bibliotheken, müssen dokumentiert und überprüft werden. Dies geschieht entweder durch die Verpflichtung des Lieferanten, Sicherheitslücken schnellstmöglich zu melden und zu beheben, oder durch eigene Anstrengungen, insbesondere bei der Einbindung von Open-Source-Projekten, diese auf Fehler oder Sicherheitslücken zu überprüfen.

Die bisher übliche Verwendung von Bibliotheken in Softwareprojekten ist damit nicht mehr ohne weiteres möglich. Bei Auftreten einer Sicherheitslücke ist das Unternehmen verpflichtet, Behörden und Kunden, teilweise innerhalb von 24 Stunden nach Bekanntwerden, qualifizierte Informationen bereitzustellen. Neben der Meldung ist auch eine Bewertung der Schwere des Vorfalls vorzunehmen.

Ähnliches gilt auch für Hardwarekomponenten. Insbesondere chinesische Firmen geraten zunehmend unter Druck und es drohen Sperren für den Einsatz dieser Produkte im KRITIS-Umfeld. Auch über die Hardware können beispielsweise Hintertüren in die Produkte eingeschleust werden. Dabei ist es zum Teil schwierig nachzuweisen, ob das Gerät „nach Hause telefoniert".

Das Netzwerk und die vernetzten Geräte sind die Basis für die Gesamtsicherheit. Dabei ist das Produkt nur so sicher wie das schwächste Glied in der Kette. Mit anderen Worten: Der unsicherste Zulieferer ist entscheidend für die Sicherheit des Produkts. Deshalb muss die gesamte Lieferkette betrachtet werden. Einheitliche Standards in der EU sollen die Zuverlässigkeit der verwendeten Komponenten gewährleisten. Labels wie „Made in Germany bzw. Europe" erhalten damit eine höhere Bedeutung.

6. Auswahl geeigneter Fachfirmen

Von entscheidender Bedeutung für die effektive und zielgerichtete Absicherung von Kritischen Infrastrukturen ist eine professionelle und qualifizierte Beratung und Betreuung der KRITIS-Betreiber durch auf Sicherheitstechnik spezialisierte Unternehmen.

An dieser Stelle ist insbesondere vor unqualifizierten oder gar unseriösen Firmen zu warnen, die versuchen, den KRITIS-Betreibern eine vordergründig günstige Technik quasi „von der Stange" zu verkaufen. Solche Systeme sind in der Regel ungeeignet, da die individuellen Anforderungen der zu schützenden Einrichtung nicht berücksichtigt werden. Leider erkennen Betreiber häufig erst zu spät, dass diese „Standardlösungen" ihren spezifischen Sicherheitsbedürfnissen nicht gerecht werden.

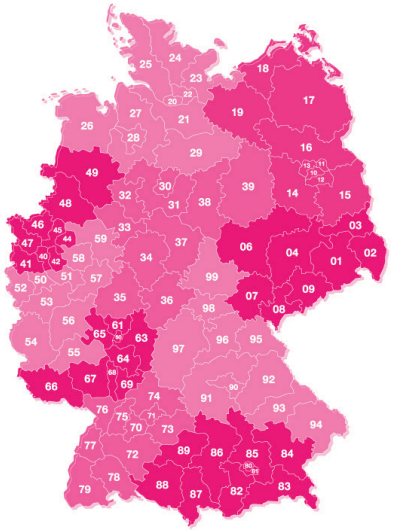
Um sicherzustellen, dass sicherheitstechnische Anlagen im Bedarfsfall voll funktionsfähig sind, müssen sie nicht nur von Fachfirmen installiert, sondern von diesen auch regelmäßig instandgehalten werden.

Durch den Einsatz falscher Produkte und/oder fehlerhafter bzw. fehlender Planung der Sicherheitstechnik kommt es in der Praxis häufig zu Fehlfunktionen.

Die im BHE Bundesverband Sicherheitstechnik e.V. organisierten Fachfirmen zeichnen sie durch Fachkenntnis und Flexibilität aus. KRITIS-Betreiber werden durch diese Firmen fachkundig und seriös beraten.

Sämtliche BHE-Mitglieder sind unter www.bhe.de/fachfirmen-sicherheitstechnik mit Kontaktdaten und Leistungsspektrum aufgelistet.

Verschiedene Suchkriterien helfen, die Ergebnisliste einzugrenzen. So kann nach Postleitzahl inkl. Umkreissuche oder nach Firmennamen gesucht werden. Außerdem ist die gezielte Recherche nach BHE-zertifizierten Fachbetrieben möglich.



Der BHE übersendet auf Anfrage gerne eine vollständige oder regionale Liste der Sicherheitsfachfirmen, die das o.g. Leistungsspektrum anbieten.

BHE Bundesverband Sicherheitstechnik e.V.
Feldstraße 28
66904 Brücken
Tel.: 06386 9214-0
Internet: www.bhe.de
E-Mail: info@bhe.de

Quellen- und Autorenverzeichnis

Bundesministerium des Innern und für Heimat, www.bmi.bund.de

OpenKRITIS, www.openkritis.de

Bernd Ammelung, Ing.-Büro Ammelung

Thomas Hermes, Securiton GmbH Alarm- und Sicherheitssysteme

Stephan Holzem, Telefonbau Arthur Schwabe GmbH & Co. KG

Oliver Jung, CM Security GmbH

Michael Meissner, AEviso DePro Solution Co., Ltd.

Sascha Puppel, Sachverständigen- und Planungsbüro Sascha Puppel GmbH

Axel Schmidt, SALTO Systems GmbH

Raimond Werdin, Planungs- und Sachverständigenbüro Raimond Werdin