EMDION
SAFETY SYSTEMS

KRITIS-Schutzstrategie

Leitfaden zur Erstellung eines umfassenden Sicherheitskonzepts für kritische Infrastrukturen

EU RCE/CER-RICHTLINIE & KRITIS-DACHGESETZ

Inhaltsverzeichnis

Vorwort 5

1 Gefährdungsanalyse 6
- 1.1 Bedrohungsanalyse 6
- 1.2 Täterprofilanalyse 7
  - 1.2.1 Wichtige Fragestellungen zum Täterprofil 7
  - 1.2.2 Kontaktaufnahme mit Behörden 7

2 Risikoanalyse 8
- 2.1 Schutzzieldefinition 8
- 2.2 Schwachstellenanalyse 8
- 2.3 Risikobewertung 9

3 Definition von Schutzmaßnahmen 12
- 3.1 Entscheidungsfindung 12
- 3.2 Erstellung eines Maßnahmenpakets 12
- 3.3 Ganzheitlicher Ansatz bei der Auswahl von Schutzmaßnahmen 12
  - 3.3.1 Organisatorische Maßnahmen 13
  - 3.3.2 Mechanische Absicherung 13
  - 3.3.3 Technische Maßnahmen 13
  - 3.3.4 Personelle Maßnahmen 13
- 3.4 Vorteile von EMDION 14
- 3.5 Überprüfung der ausgewählten Schutzmaßnahmen 14

4 Entwicklung des Schutzkonzepts 15

5 Erweiterung der Dokumentation 16

6 Realisierung/Integration 17
6.1 Projektierung und Planung 17
6.2 Projektleitung und Detailplanung 17
6.3 Fertigung und Systemtest 17
6.4 Implementierung, Inbetriebnahme und Abnahme 18
6.5 Schulung des Betreiberpersonals 18

7 Betrieb 19
7.1 Begehung der Anlage 19
7.1.1 Verantwortung des Betreibers 19
7.1.2 Schulung zur Begehung 20
7.2 Fachgerechte Instandhaltung 20
7.3 Zusatzleistungen 20

8 Nachhaltige Resilienz 21
8.1 Aktualisierte Analyse des Gefahrenbildes 21
8.2 Maßnahmen bei Abweichungen von Schutzzielen 21
8.3 Proaktiver und vorausschauender Ansatz 22
8.4 Sicherstellung langfristiger Sicherheits- und Betriebsanforderungen 22

Vorwort

In einer Welt, die von ständig verändernden Bedrohungen und Risiken geprägt ist, liegt der Schutz von Menschen, Sachwerten und Informationen in der Verantwortung jedes Unternehmens. Um diesen Schutz effektiv und nachhaltig zu gewährleisten, erfordert es eine fundierte Planung, eine durchdachte Sicherheitsstrategie und ein systematisches Risikomanagement.

Die EMDION GmbH orientiert sich an anerkannten Standards und Best Practices, so auch an der DIN ISO 31000, die die Grundlage für den Ablauf des hier beschriebenen Vorgehens bildet. Das EMDION-Team entwickelt maßgeschneiderte Sicherheitslösungen, die nicht nur die individuellen Anforderungen der Kunden berücksichtigen, sondern auch eine hohe Flexibilität und Effizienz bieten. Durch die kompakte Struktur ist EMDION in der Lage, schnell und zielgerichtet auf unterschiedliche Bedürfnisse zu reagieren – unabhängig von Systemen oder Herstellern. EMDION findet stets die optimale Lösung für Ihren Schutz und setzt diese gezielt und nachhaltig um.

Die Erstellung eines Sicherheitskonzepts basiert auf einer detaillierten Analyse der bestehenden Gefährdungen und Risiken. EMDION identifiziert potenzielle Bedrohungen und leitet daraufhin konkrete Schutzmaßnahmen ab, die passgenau auf die spezifischen Anforderungen abgestimmt sind. Dies stärkt langfristig die Resilienz und Sicherheit des Unternehmens und sorgt dafür, dass Risiken effektiv gemanagt werden.

EMDIONs Philosophie geht über die reine Lieferung eines Schutzkonzepts hinaus: Das EMDION-Team begleitet den gesamten Prozess – von der Gefährdungsanalyse über die Umsetzung bis hin zur kontinuierlichen Betreuung. Mit dem klaren Fokus auf eine nachhaltige Resilienz wird sichergestellt, dass Ihr Unternehmen nicht nur heute, sondern auch in Zukunft optimal geschützt ist.

Dieses Dokument beschreibt, wie EMDION Ihr Unternehmen bei der Umsetzung der EU RCE/CER-Richtlinie und den Anforderungen aus dem daraus abgeleiteten KRITIS-Dachgesetz unterstützt. Für die Transparenz gegenüber den Kunden legt EMDION den gesamten Prozess offen und macht Ihnen gerne ein individuelles, unverbindliches Angebot.

1 Gefährdungsanalyse

Die Gefährdungsanalyse ist die Grundlage für die Erstellung eines Schutzkonzepts. Sie liefert ein Gefahrenbild, das die Basis für das weitere Vorgehen bildet. Dabei wird eine Gefahr folgendermaßen definiert:

EINE GEFAHR HAT DAS POTENTIAL SCHÄDEN ZU VERURSACHEN.

Das Gefahrenbild zeigt die Gefährdungslage für Menschen, Sachwerte und Informationen auf. Darauf aufbauend können im nächsten Schritt Schutzmaßnahmen abgeleitet werden. Gefährdungen können aus verschiedenen Bereichen kommen: der Umwelt, der Nachbarschaft, technischen Störungen sowie aus Kriminalität, Anschlägen oder Krisen.

Man kann die Gefährdungsanalyse in zwei Abschnitte unterteilen:

- **Bedrohungsszenario:** Hier wird dargestellt, welche Gefahren bestehen.
- **Täterprofile:** Hier wird beschrieben, mit welchen Tätern im Falle einer Gefährdung durch Menschen zu rechnen ist.

Um das Gefahrenbild zu erstellen, werden die zwei Schritte separat voneinander durchgeführt.

1.1 Bedrohungsanalyse

In der Bedrohungsanalyse wird ermittelt, welche Bedrohungen auftreten können. Mögliche Bedrohungen können bspw. durch Umweltgefahren, Anschläge, Krisen, technische Störungen, Ausspähen, Spionage, Vandalismus, Sabotage, Einbruch, Diebstahl oder Gefährdung von Personen entstehen. Um diese Gefahren zu ermitteln, gibt es verschiedene Hilfsmittel, wie die Liste elementarer Gefährdungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[1] oder den GeoRiskReport des VdS. Letzterer liefert eine standortbezogene Analyse von Naturgefahren sowie Informationen über nahe Verkehrsinfrastruktur und Schadstoffemissionen umliegender Gewerbebetriebe.

Die Liste elementarer Gefährdungen des BSI enthält verschiedene Gefahren, die das BSI als gefährdend für Betreiber kritischer Infrastruktur identifiziert hat.

Diese werden in vier Hauptkategorien unterteilt:

- **Cyberangriffe:** Sie zählen zu den häufigsten und schwerwiegendsten Bedrohungen für KRITIS-Betreiber, da sie Betriebsprozesse erheblich stören oder sensible Daten kompromittieren können.
- **Physische Bedrohungen:** Neben digitalen Gefahren können auch physische Gefahren erhebliche Auswirkungen auf KRITIS-Anlagen haben.
- **Technische Risiken:** Technische Schwachstellen stellen innerhalb von IT- und OT-Systemen ein erhebliches Sicherheitsrisiko dar.
- **Spezifische Gefahren:** Je nach KRITIS-Sektor müssen branchenspezifische Bedrohungsszenarien berücksichtigt und durch geeignete Maßnahmen entschärft werden.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/Elementare_Gefaehrdungen.pdf?__blob=publicationFile&v=4

1.2 Täterprofilanalyse

Bei der Täterprofilanalyse geht es bei mutwillig herbeigeführter Bedrohung um die Abschätzung, mit welchen Tätern zu rechnen ist. Dazu werden mögliche Täter anhand unterschiedlicher Merkmale charakterisiert.

1.2.1 Wichtige Fragestellungen zum Täterprofil

→ Wie viele Täter sind zu erwarten?
→ Handelt es sich um Einzeltäter oder Tätergruppen?
→ Wie gut kennen die Täter den Ort?
→ Sind sie ortsfremd oder Insider[2]?
→ Welche Professionalität weisen die Täter auf?
→ Sind es Gelegenheitstäter oder besteht eine Verbindung zur organisierten Kriminalität?
→ Über welche Kenntnisse und welche Ausrüstung verfügen die Täter?
→ Handelt es sich um Laien oder Profis?
→ Wie risikobereit sind die Täter?

1.2.2 Kontaktaufnahme mit Behörden

Für eine umfassende Täterprofilanalyse wird empfohlen Behörden zu konsultieren, um zusätzliche Informationen zu sammeln und ein präziseres Bild der potenziellen Täter zu erhalten. Hierzu zählen insbesondere Gespräche mit der ortsansässigen Polizei, die durch ihre Erfahrungen und Kenntnisse lokale Kriminalitätsmuster und Täterprofile bestens beurteilen kann. Darüber hinaus können auch andere Sicherheitsbehörden, wie bspw. das Landeskriminalamt oder spezialisierte Ermittlungsbehörden, wertvolle Informationen liefern. Der Austausch mit diesen Institutionen hilft, potenzielle Tätergruppen zu identifizieren und mögliche Risiken zu minimieren, indem gezielte Schutzmaßnahmen auf Grundlage der gesammelten Informationen entwickelt werden.

Diese Anfragen müssen in der Regel durch den Betreiber gestellt werden, da die Behörden aus Datenschutz- und Vertraulichkeitsgründen keine Auskünfte an Dritte erteilen. EMDION unterstützt den Betreiber jedoch umfassend bei diesem Prozess, indem ihm bei der Formulierung der Anfragen, der Identifikation der richtigen Ansprechpartner und der Vorbereitung der notwendigen Unterlagen zur Seite gestanden wird. Auf diese Weise wird sichergestellt, dass alle relevanten Informationen effizient und zielgerichtet gesammelt werden, um fundierte Täterprofile zu erstellen.

[2] Insider können z. B. aktuelle oder ehemalige Mitarbeiter, Lieferanten, Handwerker oder Kunden sein.

2 Risikoanalyse

Die Risikoanalyse baut auf dem Gefahrenbild der Gefährdungsanalyse auf. Sie untersucht, wie wahrscheinlich es ist, dass eine Gefahr tatsächlich eintritt. Dabei wird ein Risiko wie folgt definiert:

EIN RISIKO IST DIE WAHRSCHEINLICHKEIT, DASS EINE GEFAHR SCHÄDEN VERURSACHT.

Im Rahmen der Risikoanalyse wird festgelegt, welches Schutzniveau angestrebt wird und welche Schutzziele erreicht werden sollen. Zudem werden Schwachstellen identifiziert. Dieser Prozess kann als Soll-Ist-Vergleich betrachtet werden. Die Ergebnisse der Risikoanalyse bilden die Grundlage für die anschließende Definition von Schutzmaßnahmen, die darauf abzielen, das gewünschte Schutzniveau zu erreichen. Während der Risikoanalyse werden noch keine konkreten technischen oder organisatorischen Vorschläge festgelegt.

2.1 Schutzzieldefinition

Der erste Baustein der Risikoanalyse ist die Schutzzieldefinition. Schutzziele sind die spezifischen Sicherheitsziele, die durch das Schutzkonzept erreicht werden sollen. Dabei geht es in der Regel um den Schutz von Menschen, Sach- und Vermögenswerten sowie um die Aufrechterhaltung von Ordnung und Recht. Die Motivation für diese Ziele resultiert oft aus betrieblichem Selbstschutz, der Fürsorgepflicht des Unternehmens, Kundenanforderungen oder gesetzlichen Vorgaben. Bei der Definition der Schutzziele spielt die Wirtschaftlichkeit in der Regel ebenfalls eine wichtige Rolle.

In enger Zusammenarbeit entwickelt EMDION zusammen mit dem Auftraggeber die individuellen Schutzziele. Zu Beginn empfiehlt es sich, grobe Ziele wie bspw. den Schutz vor unbefugtem Zutritt oder Vandalismus festzulegen und diese später in präzisere, messbare Feinziele umzuwandeln (SMART-Formulierung[3]). Dabei sollte auf mögliche Kollisionen zwischen verschiedenen Schutzzielen geachtet werden.

2.2 Schwachstellenanalyse

Die Schwachstellenanalyse erfolgt, ohne bereits technische Lösungen zu berücksichtigen. Ziel dieser Phase ist es, zunächst eine umfassende Bestandsaufnahme aller potenziellen Schwachstellen zu erstellen, ohne sich von möglichen Lösungsvorschlägen oder Maßnahmen ablenken zu lassen. Dabei liegt der Fokus auf der objektiven Identifizierung von Schwächen, sei es durch bauliche Mängel, unzureichende Sicherheitsvorkehrungen oder organisatorische Lücken. Erst im späteren Verlauf werden geeignete Maßnahmen zur Behebung dieser Schwachstellen entwickelt.

[3] Ein Ziel ist smart, wenn es spezifisch (d. h. das Ziel ist deutlich beschrieben), messbar (d. h. Erfolg ist objektiv erkennbar), ausführbar (d. h. das Ziel ist mit vorhandenen Mitteln erreichbar), realistisch (d. h. das Ziel ist sicher erreichbar) und terminiert (d. h. ein Zeitrahmen ist festgelegt) ist.

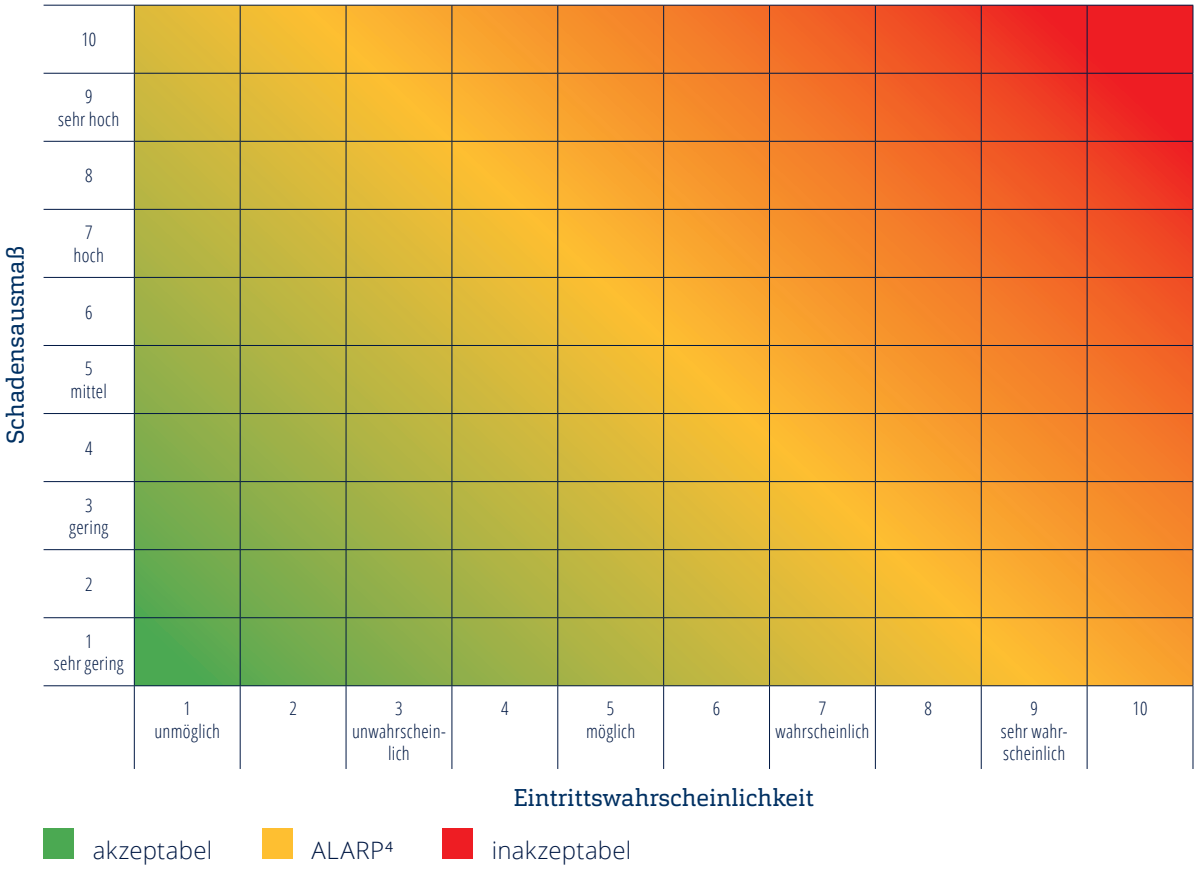
2.3 Risikobewertung

Der dritte Baustein ist die Risikobewertung. Dabei werden die festgelegten Schutzziele und identifizierten Schwachstellen gemeinsam mit dem Auftraggeber bewertet. Diese Bewertung ermöglicht es, die Risiken objektiv zu vergleichen und bildet die Grundlage für die Definition von Schutzmaßnahmen.

Die einfachste Methode zur Risikobewertung ist die Verwendung einer Risikomatrix (vgl. Abbildung 1). Dabei werden für jedes Risiko die Eintrittswahrscheinlichkeit und das potenzielle Schadensausmaß geschätzt und in einem Diagramm eingetragen. Je weiter ein Risiko vom Ursprung des Diagramms entfernt ist, desto höher wird es bewertet.

Um die Bewertung zu verfeinern, kann eine dritte Dimension hinzugefügt werden. Das Vorgehen basiert auf der Ermittlung der Risikoprioritätszahl (RPZ) aus der FMEA (Fehler-Möglichkeit- und Einflussanalyse). Neben dem zu erwartenden Schadensausmaß, der Schwere des Schadens (S, vgl. Tabelle 1) und der Eintrittswahrscheinlichkeit, der Wahrscheinlichkeit des Auftretens (A, vgl. Tabelle 2) wird auch die Wahrscheinlichkeit der Entdeckung (E, vgl. Tabelle 3) bewertet. Diese Bewertung erfolgt auf einer Skala von eins bis zehn.

Abbildung 1 Risikomatrix



[4] As Low As Reasonably Practicable (ALARP), sinngemäß: so niedrig wie vernünftigerweise praktikabel

Tabelle 1 Bewertungskriterien FMEA Schwere **S**

STICHWORT	PAUSCHAL BEI	QUANTIFIZIERUNG	WERT
gefährlich/illegal	Gefährdung von Leib und Leben von Menschen Gesetzesverstößen	individuelles existenzbedrohendes Firmen-risiko (wirtschaftlich, finanzielle Folgen)	10
kritisch	möglichen Gesetzesverstößen	≤ 20 % des individuellen Wertes	9
gravierend		≤ 10 % des individuellen Wertes	8
schwerwiegend		≤ 5 % des individuellen Wertes	7
bedeutend		≤ 2 % des individuellen Wertes	6
deutlich		≤ 1 % des individuellen Wertes	5
erkennbar		≤ 0,5 % des individuellen Wertes	4
geringfügig		≤ 0,2 % des individuellen Wertes	3
unmerklich		≤ 0,1 % des individuellen Wertes	2
keine		<< 0,1 % des individuellen Wertes	1

Tabelle 2 Bewertungskriterien FMEA Wahrscheinlichkeit des Auftretens **A**

STICHWORT	QUANTIFIZIERUNG	WERT
immer	kontinuierlich	10
fast immer	mehrmals pro Stunde	9
sehr oft	einmal pro Stunde	8
oft	einmal pro Tag	7
regelmäßig	einmal pro Woche	6
wiederholt	einmal pro Monat	5
manchmal	einmal pro Quartal	4
selten	einmal pro Jahr	3
sehr selten	einmal pro Jahrzehnt	2
nie	weniger als einmal pro Jahrzehnt	1

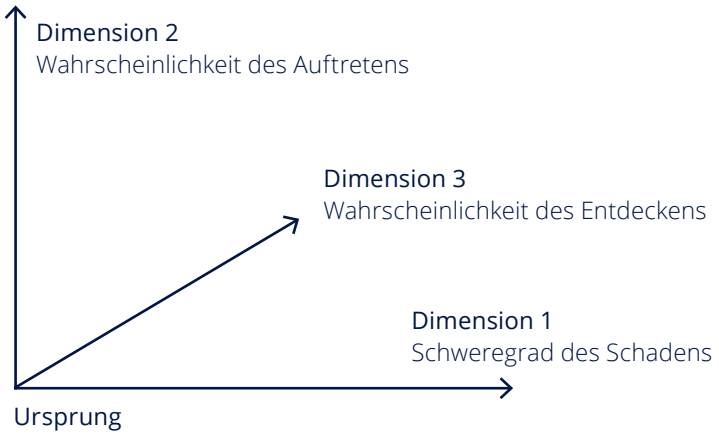
Tabelle 3 Bewertungskriterien FMEA Wahrscheinlichkeit der Entdeckung **E**

STICHWORT	QUANTIFIZIERUNG	WERT
nie	weniger als einmal pro Quartal	10
sehr selten	einmal pro Quartal	9
selten	einmal pro Monat	8
manchmal	einmal pro Woche	7
wiederholt	mehrmals pro Woche	6
regelmäßig	einmal pro Tag	5
oft	mehrmals pro Tag	4
sehr oft	einmal pro Stunde	3
fast immer	mehrmals pro Stunde	2
immer	kontinuierlich	1

Die Risikoprioritätszahl (RPZ) wird durch die Multiplikation der einzelnen Werte berechnet:

$$RPZ = S \times A \times E$$

Je höher die RPZ, desto höher ist das Risiko zu bewerten. Auch lassen sich hieraus Prioritäten für die zukünftigen Schritte ableiten. Wenn nötig, können auch komplexere Bewertungsmethoden wie die Nutzwertanalyse eingesetzt werden.



3 Definition von Schutzmaßnahmen

Auf Grundlage der identifizierten und bewerteten Risiken und der Schutzziele werden nun geeignete Schutzmaßnahmen zur Risikominderung festgelegt. Dieser Prozess erfolgt im Rahmen des Risikomanagements. Die zentrale Fragestellung dabei lautet:

KANN DAS RISIKO VERMIEDEN, GETRAGEN ODER VERSICHERT WERDEN?

3.1 Entscheidungsfindung

Zunächst muss entschieden werden, ob ein Risiko akzeptiert oder verringert werden muss. Neben den regulatorischen Anforderungen, die als Referenz dienen, können auch die Ergebnisse der Risikoanalyse herangezogen werden. Wenn eine dreidimensionale Risikomatrix verwendet wird, die an die FMEA angelehnt ist, entspricht die Risikoprioritätszahl (RPZ) der Priorität für die Entwicklung von Schutzmaßnahmen. Eine Risikoprioritätszahl von RPZ ≥ 125 kann als Schwelle für die zwingende Notwendigkeit von Schutzmaßnahmen betrachtet werden. Ebenso müssen hohe Einzelbewertungen beachtet werden. Bei einer Bewertung der Schwere (S) ≥ 8 sind Schutzmaßnahmen zu ergreifen, wenn diese umsetzbar sind. Bei einer hohen Wahrscheinlichkeit des Auftretens (A ≥ 8) oder Wahrscheinlichkeit der Entdeckung (E ≥ 8) sind Schutzmaßnahmen dann zu entwickeln, wenn sie verhältnismäßig sind.

3.2 Erstellung eines Maßnahmenpakets

Sobald entschieden wurde, welche Risiken verringert werden sollen, wird ein Maßnahmenpaket zur Risikominderung erstellt. Zunächst werden geeignete Maßnahmen zur Risikominderung ermittelt und eine Kostenschätzung durchgeführt. Auf dieser Basis werden dann die passenden Maßnahmen ausgewählt. Diese werden abschließend in einem Gesamtkonzept zusammengefasst.

3.3 Ganzheitlicher Ansatz bei der Auswahl von Schutzmaßnahmen

Bei der Auswahl der Maßnahmen sollte ein ganzheitlicher Ansatz verfolgt werden, der sowohl organisatorische, mechanische, technische als auch personelle Schutzmaßnahmen umfasst. Im Folgenden wird die Reihenfolge der Schutzmaßnahmen beschrieben:

3.3.1 Organisatorische Maßnahmen

Diese Maßnahmen fokussieren sich auf die strukturelle und organisatorische Gestaltung der Prozesse.

Hierzu gehören unter anderem:

- **Zutrittsregelungen und Verhaltensvorschriften** (z. B. kein Zutritt für unbefugtes Personal wie Lieferanten oder externe Dienstleister),
- **Umstrukturierungen** (z. B. der Umzug von Abteilungen an strategisch günstigere Standorte zur Minimierung von Risiken),
- **Verstärkung der Sicherheitsrichtlinien und Notfallplanung** zur schnellen und effektiven Reaktion auf Vorfälle.

3.3.2 Mechanische Absicherung

Diese Maßnahmen spielen eine zentrale Rolle bei der physischen Absicherung von Anlagen und Bereichen.

Hierzu zählen unter anderem:

- **Einfriedungen** (z. B. Zäune, Tore, Türen),
- **Einbruchhemmende Türen und Fenster, Physische Barrieren** zur Eindämmung und Kontrolle von Zugangsbereichen.

3.3.3 Technische Maßnahmen

Diese Maßnahmen beziehen sich auf den Einsatz von Technologien zur Überwachung, Erkennung und Meldung von Vorfällen.

Hierzu gehören:

- **Einbruchmeldeanlagen (EMA),**
- **Brandmeldeanlagen (BMA),**
- **Zutrittskontrollsysteme und Videoüberwachung**,
- **Alarmsysteme** zur frühzeitigen Erkennung von Bedrohungen.

3.3.4 Personelle Maßnahmen

Diese Maßnahmen stellen sicher, dass qualifiziertes Personal für die Überwachung, Kontrolle und Intervention zur Verfügung steht.

Hierzu zählen:

- **Sicherheitskräfte** für die Kontrolle von Zutritten und die Überwachung von sicherheitskritischen Bereichen,
- **Schulungen und Sensibilisierungsmaßnahmen für das Personal**, um das richtige Verhalten im Notfall sicherzustellen,
- **Einsatz von Interventionskräften** zur schnellen Reaktion auf sicherheitsrelevante Ereignisse.

3.4 Vorteile von EMDION

Einer der wesentlichen Vorteile von EMDION ist die Herstellerunabhängigkeit. Dies ermöglicht die besten Systeme für die individuellen Anforderungen der Kunden auswählen zu können. Diese Flexibilität erlaubt es, maßgeschneiderte Lösungen zu entwickeln, die optimal zu den jeweiligen Gegebenheiten passen, anstatt auf ein begrenztes Produktportfolio angewiesen zu sein. Dies garantiert, dass immer die besten und effizientesten Technologien zur Risikominderung eingesetzt werden – ganz gleich, ob es sich um mechanische, technische oder organisatorische Maßnahmen handelt.

3.5 Überprüfung der ausgewählten Schutzmaßnahmen

Das Ziel jeder Schutzmaßnahme ist es, Schäden zu verhindern oder zumindest zu minimieren. Jede dieser Maßnahmen kann auf verschiedene Weisen wirken und sollte entsprechend der Risikoeinschätzung und den spezifischen Anforderungen des Projekts ausgewählt und implementiert werden. Um dies sicherzustellen, wird für jede ausgewählte Schutzmaßnahme eine erneute Risikobewertung durchgeführt. Dabei wird ermittelt, ob die betrachtete Schutzmaßnahme wirklich geeignet ist, das Risiko in einen akzeptablen Bereich zu verschieben oder ob ein neuer Ansatz gewählt werden muss. Durch dieses Vorgehen wird sichergestellt, dass alle Aspekte der Sicherheit berücksichtigt werden und eine effektive, nachhaltige Risikominderung erreicht wird.

4 Entwicklung des Schutzkonzepts

Das Schutzkonzept beschreibt, wie die ausgewählten Schutzmaßnahmen – also die Gesamtheit der festgelegten organisatorischen, personellen, technischen und baulichen Maßnahmen – zur Sicherung eines Objektes und zur Abwehr von Gefahren umgesetzt werden sollen. Es fungiert als Lastenheft für die Umsetzung. Je nach Umfang des Konzeptes und nach Gegebenheit des zu schützenden Objektes ist es sinnvoll, abgestufte Schutzzonen zu definieren. Innerhalb dieser Zonen können unterschiedliche Schutzziele festgelegt werden, was eine flexible Anpassung an verschiedene Anforderungen ermöglicht. Eine übliche Unterteilung sieht vier Schutzzonen vor:

Tabelle 4 Übersicht Schutzzonen

SCHUTZZONE	BEZEICHNUNG	ZUGANG
0	Öffentlicher Bereich	Jederzeit für jedermann zugänglich
1	Frei zugänglicher Bereich	Für jedermann während der Geschäftszeit
2	Betrieblicher Bereich	Für Mitarbeiter, Dienstleister, Handwerker und Lieferanten
3	Schutzbereich	Nur für bestimmte Mitarbeiter, Externe nur in Begleitung

Im Schutzkonzept werden die Schutzziele sowie der Umfang der Sicherheitsmaßnahmen für die identifizierten Risiken und die bekannten Rahmenbedingungen festgelegt. Da mit der Erstellung des Schutzkonzeptes die Entwurfs- und Ausführungsplanung beginnt, wird die Implementierung grundlegender Änderungen ab diesem Zeitpunkt deutlich aufwändiger.

5 Erweiterung der Dokumentation

Je nach Typ der umzusetzenden Systeme müssen weitere Dokumente erzeugt werden. Die DIN VDE 0833-1 (Gefahrenmeldeanlagen für Brand, Einbruch und Überfall - Teil 1: Allgemeine Festlegungen) fordert, dass mindestens folgende Angaben enthalten sind:

→ Nutzung des Gebäudes,
→ Risiko für das Objekt,
→ Schutzziele der Gefahrenmeldeanlagen (z. B. Personen- und/oder Sachschutz),
→ Bereiche, die mit automatischen Meldern überwacht werden sollen,
→ Melder, die von Personen manuell betätigt werden müssen,
→ ggf. vorhandene Steuerfunktionen,
→ Personenschutzmaßnahmen,
→ Alarmierungseinrichtungen,
→ Alarmierungsbereiche,
→ hilfeleistende Stellen.

Je nachdem, welche Schutzmaßnahmen geplant und welche Normen und Richtlinien berücksichtigt werden müssen, können die Anforderungen an die Dokumentation unterschiedlich umfangreich sein. Für die Dokumentation von z. B. Einbruchmeldeanlagen ist – außer der DIN VDE 0833-1 – auch die DIN VDE 0833-3 (Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 3: Festlegungen für Einbruch- und Überfallmeldeanlagen) und bei VdS-konformen Anlagen auch die VdS-Richtlinie 2311 (Einbruchmeldeanlagen, Planung und Einbau) zu berücksichtigen.

Weiterhin müssen in jedem Fall Ersatzmaßnahmen definiert werden, falls einzelne Komponenten des Sicherheitskonzeptes abgeschaltet oder gestört sind.

6 Realisierung/Integration

6.1 Projektierung und Planung

Die Realisierung des Schutzkonzepts beginnt mit der Projektierung. In dieser Phase werden die Anlagenteile ausgewählt und so platziert, dass die spätere Anlage die festgelegten Zielsetzungen erfüllt. Das EMDION-Team bringt dabei seine umfangreiche Erfahrung und Expertise ein, um sicherzustellen, dass alle Komponenten optimal aufeinander abgestimmt sind. Der Einsatz hochqualifizierter Ingenieure und Techniker gewährleistet, dass die Planung und Ausführung auf höchstem Niveau erfolgt. Durch die langjährige Erfahrung und zahlreichen Zertifizierungen ist sichergestellt, dass alle Planungs- und Ausführungsschritte mit höchster Qualität und Effizienz durchgeführt werden.

6.2 Projektleitung und Detailplanung

Neben der Auswahl und Platzierung der Anlagenteile übernimmt EMDION auch die Projektleitung, die Werks- und Montageplanung sowie die vollständige Dokumentation der Prozesse. Dieser integrierte Ansatz ermöglicht eine reibungslose Umsetzung aller Aufgaben. Zentraler Bestandteil dieses Ansatzes ist, dass jedes Projekt durchgehend und umfassend von der selben Ansprechperson mit entsprechender Vertretung begleitet wird, welche sich selbst mit dem Projekt identifiziert.

6.3 Fertigung und Systemtest

Durch die eigene Werkstatt kann EMDION eine hohe Integrationstiefe gewährleisten und durch die Durchführung von Vorkonfigurationen und Systemtests grundlegende Herausforderungen erkennen. Dies ermöglicht ein frühzeitiges Reagieren und trägt dazu bei, die Montagezeit möglichst kurz zu halten. Auf Wunsch können außerdem Vorabnahmen wie einen FAT (Factory Acceptance Test) angeboten werden, um sicherzustellen, dass die Anlage alle Anforderungen erfüllt, bevor sie endgültig in Betrieb genommen wird.

6.4 Implementierung, Inbetriebnahme und Abnahme

Die Implementierung umfasst die Montage der Anlagenkomponenten sowie deren Inbetriebnahme. Dabei wird überprüft, ob die Anlage mit der Projektierung übereinstimmt. EMDION übernimmt auch die Koordination der Inbetriebnahme und stellt sicher, dass alle Komponenten fehlerfrei arbeiten. In der abschließenden Prüfung wird nochmals kontrolliert, ob alle Anforderungen aus der Planung, Projektierung, Montage und Inbetriebnahme eingehalten werden. Das EMDION-Team begleitet diesen Prozess kontinuierlich und sorgt für die ordnungsgemäße Ausführung.

Auch die Abnahme selbst begleitet EMDION umfassend und unterstützen den Betreiber bei der Zusammenarbeit mit prüfenden Organisationen. EMDIONS Fachkenntnis stellt sicher, dass die Anforderungen sämtlicher Prüfstellen schnell und effizient erfüllt werden, ohne dass es zu Verzögerungen kommt. Nach erfolgreich abgeschlossener Prüfung erfolgt im Rahmen der Abnahme die formale Übergabe der Anlagenverantwortung vom Errichter an die im Auftrag spezifizierte Stelle.

6.5 Schulung des Betreiberpersonals

Parallel zur Implementierung der Anlage wird begonnen, das relevante Personal des Betreibers in die Grundlagen der Anlagenbedienung einzuweisen.

Diese Einweisung umfasst unter anderem:
→ **die Bedienung und Funktion** der Anlage,
→ **Sicherheitsvorkehrungen** im Umgang mit der Anlage,
→ **alle relevanten Richtlinien und sonstige Vorgaben.**

EMDIONs umfassende Schulungsprogramme sorgen dafür, dass das relevante Personal des Betreibers über alle aktuellen Richtlinien und Betriebsvorgaben informiert ist und die Anlage sicher sowie effizient betrieben werden kann.

7 Betrieb

Während des Betriebs der Anlage(n) müssen regelmäßig Instandhaltungsmaßnahmen durchgeführt werden. Die Häufigkeit dieser Maßnahmen ist in der DIN VDE 0833-1 festgelegt. Instandhaltung umfasst:

EINE KOMBINATION AUS VORBEUGENDEN UND FEHLERBESEITIGENDEN MASSNAHMEN WÄHREND DES BETRIEBS EINER ANLAGE, UM DIE GEFORDERTEN FUNKTIONEN ZU ERHALTEN UND/ODER WIEDERHERZUSTELLEN.

7.1 Begehung der Anlage

Ein wichtiger Teil der Instandhaltung ist die Begehung der Anlage. Dabei wird die Anlage auf sichtbare Störungen und Mängel überprüft. Es ist darauf zu achten, dass die im Sicherheitskonzept festgelegten Überwachungsaufgaben eingehalten werden. Zudem sollte geprüft werden, ob sich die Raumnutzung, die Raumgestaltung oder die Umgebungsbedingungen geändert haben, ob es bauliche Veränderungen gab, ob Hilfsmittel für Einsatzkräfte, wie bspw. Feuerwehrlaufkarten, noch aktuell sind und ob das Betriebsbuch korrekt und vollständig geführt wurde. Besonders wichtig ist die Kontrolle des äußeren Zustands aller Anlagenteile, insbesondere hinsichtlich Befestigung, Beschädigung und Verschmutzung. Die Ergebnisse der Begehung sind im Betriebsbuch festzuhalten. Gegebenenfalls sind weitere Maßnahmen zu veranlassen.

7.1.1 Verantwortung des Betreibers

Die Begehung ist grundsätzlich eine Aufgabe des Betreibers. Er kann diese entweder selbst durchführen oder an eine Fachfirma delegieren. Es ist jedoch wichtig, dass der Betreiber spätestens mit der Abnahme schriftlich auf seine Pflicht zur Begehung hingewiesen wird, da nicht davon ausgegangen werden kann, dass der Betreiber mit allen einschlägigen Normen und Richtlinien vertraut ist.

7.1.2 Schulung zur Begehung

Auch für die Begehung der Anlage können die relevanten Mitarbeiter des Betreibers durch EMDION kontinuierlich geschult werden, um sicherzustellen, dass diese für die Aufgabe der Begehung qualifiziert sind.

Diese Schulungen umfassen unter anderem:

- Korrekte Handhabung von Betriebsmitteln und Sicherheitsausstattungen,
- Schulungen zur Nutzung des Betriebsbuches und der korrekten Dokumentation,
- Einweisungen in die relevanten Normen und Richtlinien,
- Handhabung von Notfällen,
- Umgang mit technischen Mängeln und Eskalation von Problemen an Fachfirmen.

7.2 Fachgerechte Instandhaltung

Die weitere Instandhaltung muss grundsätzlich von einer Fachfirma durchgeführt werden. Sie umfasst die Inspektion, bei der allgemeine, herstellerunabhängige Kriterien überprüft werden, die Wartung, bei der herstellerspezifische Tätigkeiten ausgeführt werden, sowie ggf. notwendige Instandsetzungs- und Verbesserungsarbeiten.

7.3 Zusatzleistungen

Zusätzlich zu den Instandhaltungsaufgaben besteht die Möglichkeit dem Betreiber ein Incident-Management sowie ein 24/7-Service anzubieten, um bei auftretenden Problemen schnell reagieren zu können. Außerdem kann durch regelmäßige Auffrischungsschulungen die Qualifikation bestehender Mitarbeiter zur Bedienung oder Begehung der Anlage erhalten werden sowie neuen Mitarbeiter der Erwerb dieser ermöglicht werden.

8 Nachhaltige Resilienz

Die nachhaltige Resilienz einer Anlage erfordert während des gesamten Betriebs eine kontinuierliche Überwachung und Anpassung an sich verändernde Bedingungen. Es ist unerlässlich, regelmäßig zu überprüfen, ob die festgelegten Schutzziele weiterhin eingehalten werden. Diese Überprüfungen gehen über rein technische Inspektionen hinaus und umfassen auch die Beurteilung der Betriebs- und Sicherheitsanforderungen im Hinblick auf sich verändernde Rahmenbedingungen.

8.1 Aktualisierte Analyse des Gefahrenbildes

Ein zentraler Bestandteil dieser Überprüfungen ist die aktualisierte Analyse des Gefahrenbildes. Das Gefahrenbild muss regelmäßig überprüft und gegebenenfalls neu bewertet werden, da sich äußere Einflüsse wie technologische Entwicklungen, regulatorische Änderungen oder neue Bedrohungsszenarien auf die Funktionsweise und Sicherheit der Anlage auswirken können. Nur durch eine laufende Anpassung an diese Veränderungen kann die Resilienz der Anlage langfristig gewährleistet werden.

8.2 Maßnahmen bei Abweichungen von Schutzzielen

Falls bei der Überprüfung Abweichungen von den ursprünglichen Schutzzielen festgestellt werden, müssen sofortige und gezielte Maßnahmen ergriffen werden.

Diese beinhalten:

- **technische Anpassungen oder Nachrüstungen an der Anlage,**
- **Schulungen für das Personal**, um auf neue Anforderungen oder Risiken vorbereitet zu sein,
- **Aktualisierung von Notfallplänen,** um auf sich verändernde Risiken reagieren zu können.

Es ist entscheidend, dass auf neue Risiken und Veränderungen schnell und effektiv reagiert wird, um die Betriebssicherheit und den Schutz dauerhaft zu gewährleisten.

8.3 Proaktiver und vorausschauender Ansatz

Die nachhaltige Resilienz erfordert einen proaktiven und vorausschauenden Ansatz.

Dies umfasst neben der regelmäßigen Inspektion und Gefährdungsanalyse auch:

- das kontinuierliche Monitoring von sicherheitsrelevanten Systemen,
- die Durchführung von regelmäßigen Risikoanalysen,
- die enge Zusammenarbeit mit Fachkräften und externen Organisationen, um aktuelle und zukünftige Herausforderungen frühzeitig zu identifizieren und zu bewältigen.

8.4 Sicherstellung langfristiger Sicherheits- und Betriebsanforderungen

Mit diesem ganzheitlichen Ansatz stellt EMDION sicher, dass die Anlage nicht nur heute, sondern auch in Zukunft den höchsten Sicherheits- und Betriebsanforderungen entspricht. Durch regelmäßige Überprüfungen, schnelle Reaktionsfähigkeit auf Veränderungen und kontinuierliche Anpassungen kann die langfristige Resilienz der Anlage gewährleistet werden.

Mit Sicherheit Ihr starker Partner für individuelle Sicherheitssysteme

EMDION GmbH
Zweiter Polderweg 18
D-26723 Emden

Tel. +49 (0)4921 3658 – 200
sales@emdion.eu

www.emdion.com

EMDION
SAFETY SYSTEMS