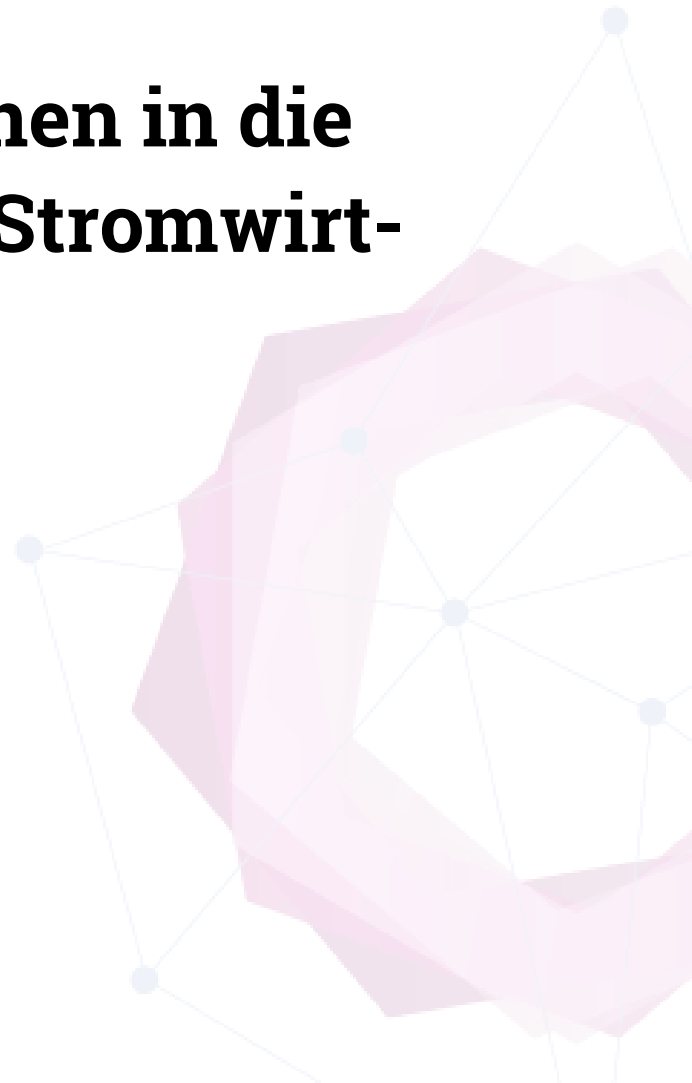




**STUDIE**

# **Cyber-Fit: Investitionen in die Cybersicherheit der Stromwirtschaft**

Rentabilität von Cybersicherheitsmaßnahmen



# Impressum

## Herausgeber:

Deutsche Energie-Agentur GmbH (dena)

Chausseestraße 128 a

10115 Berlin

Tel.: +49 30 66 777-0

Fax: +49 30 66 777-699

E-Mail: **Fehler! Linkreferenz ungültig.**

Internet: **Fehler! Linkreferenz ungültig.**

## Autorinnen und Autoren:

Dennis Rösch, M. Sc., Fraunhofer IOSB-AST

André Kummerow, M. Sc., Fraunhofer IOSB-AST

Thomas Bauer, M. Sc., Fraunhofer IOSB-AST

Katerina Simou, dena

Friederike Wenderoth, dena

## Konzeption & Gestaltung:

Raban Ruddigkeit

## Stand:

09/2024

Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.

## Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2024): Cyber-Fit: Investitionen in die Cybersicherheit der Stromwirtschaft



Bundesministerium  
für Wirtschaft  
und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

# Inhalt

<b>1</b>	<b>Executive Summary .....</b>	<b>5</b>
<b>2</b>	<b>Rolle und Zuständigkeiten der Führungskraft in den neuen KRITIS-Gesetzen.....</b>	<b>6</b>
2.1	Das NIS-2-Umsetzungsgesetz verstärkt die Security-Pflichten.....	6
2.1.1	Betroffene Unternehmen in Deutschland .....	6
2.1.2	Pflichten für Betreiber und Einrichtungen .....	7
2.1.3	Maßnahmen .....	7
2.1.4	Besondere Verpflichtungen für die Geschäftsleitung.....	8
2.2	Das KRITIS-Dachgesetz rückt physische Resilienz in den Vordergrund.....	9
2.2.1	Betroffene Unternehmen in Deutschland .....	9
2.2.2	Pflichten für Betreiber.....	9
2.2.3	Maßnahmen zur Gewährleistung der Resilienz .....	11
2.2.4	Besondere Verpflichtungen für die Geschäftsleitung.....	11
2.3	Einschätzung der Gesetzeslage und des Umsetzungsaufwands von Unternehmen der Stromwirtschaft.....	12
<b>3</b>	<b>IT-Sicherheitsreferenzarchitektur eines Unternehmens der Stromwirtschaft .....</b>	<b>14</b>
3.1	Einführung der Referenzarchitektur eines Verteilnetzbetreibers .....	14
3.2	Beschreibung der internen und externen Prozesse .....	16
3.3	Beschreibung der Kritikalität der Prozesse.....	17
3.4	Beschreibung implementierbarer IT-Sicherheitsmaßnahmen.....	18
<b>4</b>	<b>Beispielrechnungen zur Rentabilität von IT-Sicherheitsmaßnahmen .....</b>	<b>20</b>
4.1	Ermittlung der Kosten zur Etablierung von IT-Sicherheitsmaßnahmen .....	20
4.2	Erfüllungsaufwand für die Wirtschaft nach NIS2UmsuCG.....	20
4.3	Ermittlung der Schadenskosten.....	24

4.3.1	Identifikation und Analyse bestehender Assets.....	24
4.3.2	Identifizierung von Bedrohungen und Schwachstellen .....	24
4.3.3	Bestimmung der Eintrittswahrscheinlichkeit und der Auswirkungen .....	25
4.4	Schadensabschätzung nach NIS2UmsuCG .....	26
<b>5</b>	<b>Der Return on Security Investment zur Verdeutlichung der Investitionseffekte.....</b>	<b>27</b>
5.1	Definition des RoSI – Return on Security Investment.....	27
5.2	Berechnung des RoSI für wichtige und besonders wichtige Einrichtungen.....	28
	<b>Abbildungsverzeichnis .....</b>	<b>31</b>
	<b>Tabellenverzeichnis.....</b>	<b>32</b>
	<b>Literaturverzeichnis .....</b>	<b>33</b>
	<b>Abkürzungen.....</b>	<b>35</b>
	<b>Glossar .....</b>	<b>36</b>

# 1 Executive Summary

In der Energiewirtschaft hält die Digitalisierung Einzug, um den vielfältigen Herausforderungen der Energiewende zu begegnen. Die Vernetzung einer immer größer werdenden Anzahl von Anlagen schafft eine neue und stärkere Abhängigkeit der Stromversorgungssicherheit von IT- und Kommunikationssystemen. Daher nimmt die Bedeutung der IT-Sicherheit auch im Stromsystem weiter zu. Die Gewährleistung von IT-Sicherheit ist für die betreffenden Unternehmen ein kostenintensiver und hochkomplexer Prozess.

Um fundierte und transparente Entscheidungen in Bezug auf Cybersicherheit zu treffen, widmet sich diese Studie der Frage: „**Wie kann die Rentabilität von IT-Sicherheitsinvestitionen bewertet werden?**“

Das Ziel ist es, Geschäftsleitungen und andere Entscheidungsebenen im Stromsektor dabei zu unterstützen, Kosten, Nutzen und Rentabilität von Cybersicherheitsmaßnahmen zu bewerten. Dabei werden die Herausforderungen der unzureichenden Transparenz hinsichtlich der Kosten von IT-Sicherheitsmaßnahmen und ihren Komponenten sowie des Personalmangels adressiert. Die Studie wurde im Hinblick auf die Investitionsbedarfe erarbeitet, die aus den neuen KRITIS-Gesetzen (Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) und Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz)) resultieren. Einführend in die Thematik werden zunächst die Rolle und die Zuständigkeit der Führungskraft in den neuen KRITIS-Gesetzen vorgestellt, dabei wird besonders auf die sich ergebenden Verpflichtungen für die Geschäftsleitung eingegangen.

Zur Veranschaulichung möglicher Investitionen wird eine IT-Sicherheitsreferenzarchitektur eines Verteilnetzbetreibers vorgestellt. Aus den resultierenden Prozessen werden implementierbare IT-Sicherheitsmaßnahmen abgeleitet, die im Rahmen von Investitionen in IT-Sicherheit umgesetzt werden können. Eine Beispielrechnung zu den finanziellen Auswirkungen von IT-Sicherheitsmaßnahmen und nachfolgenden Investitionseffekten wird anhand des Modells zum Return on Security Investment (RoSI) durchgeführt. Die Berechnung erfolgt auf Basis der im NIS2UmsuCG-Entwurf angegebenen Erfüllungsaufwände zur Implementierung der darin geforderten Maßnahmen sowie der dort abgeschätzten Schadenskosten vor und nach der Implementierung der Maßnahmen.

Die Studie basiert auf den Angaben des Referentenentwurfs vom 24. Juni 2024. Nach Verabschiedung der finalen Gesetzgebung muss erneut geprüft werden, welche Bestimmungen tatsächlich umgesetzt wurden.

## Wesentliche Ergebnisse

- In Interviews mit Unternehmensvertretern der Energiebranche wurde durchgängig die Wichtigkeit der Geschäftsleitung in Bezug auf IT-Sicherheit erkannt. Ebenfalls gibt es bereits eine hohe Sensibilität der Geschäftsleitung für Investitionen in IT-Sicherheitsmaßnahmen. Die Plausibilität des im NIS2UmsuCG angegebenen Erfüllungsaufwands zur Implementierung der Maßnahmen und der abgeschätzten Schadenskosten wurde bestätigt.
- Die Bewertung der Kosten mithilfe des RoSI zeigt, dass für wichtige Einrichtungen die Investitionen bereits im ersten Jahr rentabel sind. Für besonders wichtige Einrichtungen ist dies ab dem zweiten Jahr der Fall.
- Die Beispielrechnung zeigt, dass die Investitionen, die das NIS2UmsuCG fordert, rentabel sind, trotz der für die Stromwirtschaft sehr niedrig angesetzten Kosten im Falle eines IT-Sicherheitsvorfalls.

## 2 Rolle und Zuständigkeiten der Führungskraft in den neuen KRITIS-Gesetzen

Kritische Infrastrukturen (KRITIS) stehen bereits seit einiger Zeit im Fokus von Gesetzgebungen hinsichtlich der Sicherheit und Resilienz. Bei dieser Entwicklung werden für deutsche Unternehmen zunehmend Gesetze und Richtlinien auf europäischer Ebene relevant, woraus sich Ableitungen für national bindendes Recht ergeben. Stand Juli 2024 sind vor allem zwei Richtlinien der Europäischen Union für die Kritischen Infrastrukturen und insbesondere für die Stromwirtschaft von Bedeutung: die EU NIS 2 Directive (EU 2022/2555) und die EU RCE Directive (EU 2022/2557). Beide Richtlinien sind Ende 2022 vom EU-Parlament beschlossen worden und müssen binnen zwei Jahren in nationales Recht überführt werden. Dementsprechend besteht die Anforderung an die deutsche Gesetzgebung, bis zum Oktober 2024 entsprechende Gesetze bzw. Gesetzesänderungen zu beschließen. Zum Zeitpunkt der Erstellung dieser Studie sind Aktivitäten für zwei abgeleitete Gesetze bekannt und werden nachfolgend beschrieben. Es handelt sich um das **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)**, vorliegend im Referentenentwurf vom 24. Juni 2024<sup>1</sup>, und das **Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz)**, vorliegend im Referentenentwurf vom 21. Dezember 2023<sup>2</sup>. Es sei darauf hingewiesen, dass die nachfolgend aufbereiteten Informationen auf den genannten Referentenentwürfen basieren. Potenzielle Änderungen in der finalen Gesetzgebung sind hier dementsprechend nicht berücksichtigt.

Beide europäischen Richtlinien und die abgeleiteten nationalen Gesetze haben gemeinsam, dass zusätzliche Anforderungen in Bezug auf die IT-Sicherheit der betroffenen Unternehmen gestellt werden. Es entsteht eine Verpflichtung zur Ergreifung und Implementierung unterschiedlicher Maßnahmen über verschiedene Unternehmensebenen hinweg. Diese Maßnahmen betreffen sowohl technische als auch organisatorische Aspekte. Im Folgenden wird in beide zu erwartende Gesetze eingeführt und die wichtigsten Maßnahmen werden zusammengefasst.

### 2.1 Das NIS-2-Umsetzungsgesetz verstärkt die Security-Pflichten

Das NIS2UmsuCG ist ein Änderungsgesetz, das bestehende Gesetze ändert – primär die KRITIS-Teile des BSI-Gesetzes (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSI-G). Das NIS-2-Umsetzungsgesetz ändert die deutsche KRITIS-Regulierung deutlich: Neben den Betreibern kritischer Anlagen wird es eine Unterteilung in besonders wichtige Einrichtungen und wichtige Einrichtungen geben. Für etwa 30.000 betroffene Unternehmen (8.250 Unternehmen als besonders wichtige und rund 21.600 Unternehmen als wichtige Einrichtungen) in Deutschland, die über klassische Kritische Infrastrukturen hinausgehen, steigen die Security-Pflichten.

#### 2.1.1 Betroffene Unternehmen in Deutschland

In Deutschland gibt es vier Gruppen von Unternehmen, die von der NIS-2-Richtlinie betroffen sind: die bestehenden Betreiber kritischer Anlagen (KRITIS), besonders wichtige Einrichtungen, wichtige

---

<sup>1</sup> (Referentenentwurf NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, 2024)

<sup>2</sup> (Referentenentwurf KRITIS-Dachgesetz, 2024)

Einrichtungen und einige Bundeseinrichtungen. Nachfolgend werden die Bundeseinrichtungen nicht weiter berücksichtigt. **Tabelle 1** zeigt die drei verbleibenden Arten von Einrichtungen mit den jeweiligen Eigenschaften.

Tabelle 1 Übersicht über die vom NIS2UmsuCG betroffenen Unternehmen in Deutschland

Art der Einrichtung	Eigenschaft (mindestens eine muss erfüllt sein)
<b>Besonders wichtige Einrichtungen</b>	Unternehmen ab 250 Mitarbeiterinnen und Mitarbeitern
	Unternehmen ab 50 Millionen Euro Umsatz und Bilanz ab 43 Millionen Euro
	Sonderfälle, wie beispielsweise kritische Anlagen
<b>Wichtige Einrichtungen</b>	Unternehmen ab 50 Mitarbeiterinnen und Mitarbeitern
	Unternehmen ab 10 Millionen Euro Umsatz und Bilanz ab 10 Millionen Euro
	Vertrauensdienste
<b>Betreiber kritischer Anlagen</b>	KRITIS-Anlage über Schwellenwert, in der Regel $\geq 500.000$ versorgte Personen

## 2.1.2 Pflichten für Betreiber und Einrichtungen

Im NIS2UmsuCG werden verschiedene Pflichten für die drei relevanten Unternehmenstypen definiert, denen betroffene Unternehmen nachkommen müssen.

Tabelle 2 Übersicht über die Pflichten für die drei relevanten Unternehmenstypen nach NIS2UmsuCG

Pflicht	Betreiber kritischer Anlagen	Besonders wichtige Einrichtung	Wichtige Einrichtung
<b>Maßnahmen Risikomanagement</b>	X	X	x
<b>Besondere Maßnahmen SZA</b>	X		
<b>Meldepflichten</b>	X		
<b>Registrierung</b>	X	X	X
<b>Unterrichtungspflicht (Kunden)</b>	X	X	X
<b>Leitungsorgane</b>	X	X	X
<b>Nachweise</b>	X	X	X

## 2.1.3 Maßnahmen

Die von Betreibern und Einrichtungen umzusetzenden Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen und sollen europäische und internationale Normen berücksichtigen. Die Maßnahmen sollen den Stand der Technik einhalten und müssen mindestens die folgenden Themen umfassen:

- Risikoanalyse und Sicherheit für Informationssysteme\*
- Bewältigung von Sicherheitsvorfällen\*
- Aufrechterhaltung und Wiederherstellung\*, Backup-Management\*, Krisenmanagement
- Sicherheit der Lieferkette\*, Sicherheit zwischen Einrichtungen\*, Dienstleistersicherheit\*
- Sicherheit in der Entwicklung\*, Beschaffung und Wartung\*
- Management von Schwachstellen\*
- Bewertung der Effektivität von Cybersicherheits- und Risikomanagement\*
- Schulungen zu Cybersicherheit und Cyberhygiene\*
- Kryptografie und Verschlüsselung\*
- Personalsicherheit\*, Zugriffskontrolle\* und Anlagenmanagement\*
- Multi-Faktor-Authentisierung und kontinuierliche Authentisierung\*
- Sichere Kommunikation (Sprache, Video und Text)\*
- Sichere Notfallkommunikation\*

Viele der genannten Maßnahmen sind bereits für aktuelle KRITIS-Betreiber durch das IT-Sicherheitsgesetz 2.0 und das BSI-Gesetz relevant und innerhalb des Informations-Sicherheits-Managements nach ISO 27001 verpflichtend. Sie sind in der Aufzählung mit einem Sternchen gekennzeichnet.

Besonders die Ausweitung der Regelungen auf **Prozessinfrastruktur**, beispielsweise im Zuge eines Business Continuity Management (BCM), die Verpflichtung zur **Etablierung eines Krisenmanagements** und eine gegebenenfalls zusätzliche **Verpflichtung zur Registrierung nach der NIS-2-Eingruppierung** sind explizite Erweiterungen der aktuellen Verpflichtungen von KRITIS-Betreibern.

#### 2.1.4 Besondere Verpflichtungen für die Geschäftsleitung

Die Geschäftsleitung von besonders wichtigen oder wichtigen Einrichtungen trägt eine große Verantwortung in Bezug auf die IT-Sicherheit. Sie muss sicherstellen, dass angemessene Maßnahmen ergriffen werden, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu minimieren. Es ist wichtig, dass die Geschäftsleitung diese Maßnahmen nicht nur genehmigt, sondern auch **ihre Umsetzung und Überwachung sicherstellt**. Sie muss aktiv daran arbeiten, dass die Einrichtung ausreichend gegen Cyberrisiken geschützt ist.

Um sicherzustellen, dass die Geschäftsleitung über das erforderliche Wissen und die Fähigkeiten verfügt, muss sie **regelmäßig an Schulungen teilnehmen**. Diese Schulungen sollen dabei helfen, Risiken zu erkennen und zu bewerten sowie bewährte Praktiken im Risikomanagement zu verstehen. Die Geschäftsleitung soll auch die Auswirkungen von Risiken auf die Dienstleistungen der Einrichtung verstehen, damit sie effektive Maßnahmen zur IT-Sicherheit ergreifen kann.

Darüber hinaus gibt es auch eine weitere Vorgabe bezüglich der IT-Sicherheit. Diese Vorgabe fordert **ein Mindestniveau an IT-Sicherheit** für besonders wichtige und wichtige Einrichtungen. Das bedeutet, dass alle Einrichtungen angemessene technische und organisatorische Maßnahmen ergreifen müssen, um die Risiken für ihre Netz- und Informationssysteme zu beherrschen. Die konkrete Ausgestaltung dieser Maßnahmen rich-

tet sich nach etablierten IT-Standards, den Kosten und den bestehenden Risiken. Es ist wichtig, dass diese Maßnahmen angemessen und verhältnismäßig sind, um sicherzustellen, dass die Einrichtungen adäquat geschützt sind, ohne dabei übermäßige Kosten zu verursachen.

Die Geschäftsleitung hat auch hier die Verantwortung, die **Risikomaßnahmen zu billigen und zu überwachen**. Das bedeutet, dass sie sicherstellen muss, dass die Einrichtung die Vorschriften einhält und die erforderlichen Maßnahmen zur IT-Sicherheit umsetzt und somit angemessen gegen Cyberrisiken geschützt ist.

## 2.2 Das KRITIS-Dachgesetz rückt physische Resilienz in den Vordergrund

Neben der NIS-2-Richtlinie spielt vor allem das KRITIS-Dachgesetz eine wichtige Rolle. Sein Fokus liegt auf Resilienz und physischer Sicherheit. Das KRITIS-Dachgesetz soll ebenfalls ab Oktober 2024 auf nationaler Ebene in Kraft treten und adressiert vor allem Pflichten für Betreiber. Nachfolgend sind wiederum zunächst die betroffenen Unternehmen und anschließend die Pflichten für die Betreiber sowie erwartbare Maßnahmen im Sinne der Resilienz aufgeführt. Abschließend wird auch hier die Rolle der Geschäftsleitung besonders hervorgehoben.

### 2.2.1 Betroffene Unternehmen in Deutschland

Betroffene Unternehmen in Deutschland sind vor allem Betreiber kritischer Anlagen in den (bisherigen) KRITIS-Sektoren, aber auch der Bund. **Tabelle 3** fasst dies zusammen. Im Weiteren werden die speziell adressierten Aspekte für den Bund und für behördliche Einrichtungen jedoch vernachlässigt.

Tabelle 3 Übersicht über die vom KRITIS-Dachgesetz betroffenen Unternehmen in Deutschland

Art der Einrichtung	Eigenschaft
<b>Betreiber kritischer Anlage</b>	Anlagen mit bisherigem KRITIS-Schwellenwert
<b>Bund</b>	Einrichtungen: Bundesministerien, Bundeskanzleramt

### 2.2.2 Pflichten für Betreiber

Innerhalb des KRITIS-Dachgesetzes werden eine Reihe von Pflichten und Maßnahmen für die Betreiber definiert, um die Resilienz insgesamt zu erhöhen. Zunächst fasst **Tabelle 4** die genannten Pflichten für die Betreiber zusammen.

Tabelle 4 Übersicht über die Pflichten für Betreiber nach KRITIS-Dachgesetz

Pflicht	Beschreibung
<b>Registrierung</b>	Die Betreiber sind verpflichtet, <b>spätestens drei Monate</b> nach Erklärung als Betreiber kritischer Anlagen dem BBK und dem BSI Registrierungsinformationen zu übermitteln. Die zuständigen Behörden stellen eine Registrierungsmöglichkeit zur Verfügung.

<b>Risikoanalyse und Risikobewertung</b>	Durchführung einer Risikoanalyse und Risikobewertung auf Grundlage der vom BBK vorgegebenen Vorlagen und Muster. Die Analyse und die Bewertung haben mindestens <b>alle 4 Jahre</b> zu erfolgen.
<b>Resilienzmaßnahmen, Resilienzplan</b>	<b>Nach Ablauf von 10 Monaten</b> nach Registrierung sind die Betreiber verpflichtet, geeignete Maßnahmen zur Gewährleistung der Resilienz zu ergreifen. Mindestanforderungen für diese Maßnahmen werden vom BBK und BSI aufgestellt. Die Maßnahmen sind in einem Resilienzplan darzustellen. Er muss die den Maßnahmen zugrunde liegenden Erwägungen inklusive der Risikoanalyse enthalten.
<b>Nachweise</b>	Das BBK und das BSI können Nachweise zum Zweck der Überprüfung der Einhaltung der Vorschriften und der Umsetzung von Maßnahmen verlangen. Dieser Nachweis kann durch Audits erfolgen und die Auditergebnisse müssen den Behörden übermittelt werden.
<b>Meldewesen für Vorfälle</b>	Die Betreiber sind verpflichtet, Vorfälle, die die Erbringung der kritischen Dienstleistung erheblich stören oder erheblich stören könnten, dem BBK und dem BSI gemeinsam zu melden. Eine erste Meldung muss <b>binnen 24 Stunden nach Kenntnis des Vorfalls</b> übermittelt werden.
<b>Geschäftsleitungspflichten</b>	Die Geschäftsleitung ist verpflichtet, die Einhaltung der Vorschriften und die ergriffenen Maßnahmen zu billigen und ihre Umsetzung zu überwachen. Weiter muss die Geschäftsleitung regelmäßig an Schulungen teilnehmen, um ausreichend aktuelle Kenntnisse zur Erkennung und Bewertung von Risiken zu besitzen.

## 2.2.3 Maßnahmen zur Gewährleistung der Resilienz

Abgeleitet aus den Pflichten werden im KRITIS-Dachgesetz vor allem Maßnahmen zur Gewährleistung der Resilienz definiert. Diese Maßnahmen basieren auf den jeweiligen Risikobewertungen und sollen dem aktuellen Stand der Technik entsprechend von den Betreibern umgesetzt werden. Nachfolgend werden die adressierten Maßnahmen aufgeführt.



Maßnahmen zur expliziten Sicherstellung der Resilienz sind bisher besonders im Rahmen des für KRITIS-Betreiber verpflichtenden Informations-Sicherheits-Managements adressiert. Das KRITIS-Dachgesetz legt vor allem einen Fokus auf das Notfall- und Krisenmanagement. Die Einbeziehung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) soll über eine noch zu installierende Registrierungsstelle erfolgen, wodurch neben dem BSI nun auch dem BBK eine feste Ansprechperson oder Kontaktstelle genannt werden muss.

## 2.2.4 Besondere Verpflichtungen für die Geschäftsleitung

Die Geschäftsleitung von Unternehmen, die kritische Anlagen betreiben, hat bestimmte Verpflichtungen. Sie muss die Maßnahmen unterstützen, um die Vorschriften einzuhalten, und sicherstellen, dass diese Maßnahmen umgesetzt werden. Es ist wichtig, zu beachten, dass ein Verzicht auf oder eine Vereinbarung über mögliche **Schadensersatzansprüche unwirksam sind, wenn die Geschäftsleitung ihre Verpflichtungen nicht erfüllt hat.**

Außerdem muss die Geschäftsleitung regelmäßig an Schulungen im Sinne der fundierten Etablierung von Resilienzmaßnahmen teilnehmen. Die zuständige Aufsichtsbehörde kann einen **Nachweis über die Teilnahme an Schulungen** verlangen.

Diese Regelungen entsprechen den Bestimmungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und die Sicherheit der Informationstechnik von Einrichtungen. Die Geschäftsleitung von

Unternehmen mit kritischen Anlagen hat eine spezielle **Überwachungspflicht** und ist dafür verantwortlich, dass die Maßnahmen zur Einhaltung der Vorschriften umgesetzt werden. Selbst wenn Hilfspersonen eingesetzt werden, bleibt das Leitungsorgan verantwortlich. **Die Verantwortung kann nicht vollständig delegiert werden.**

Der Unterschied im Vergleich zum NIS2UmsuCG besteht in den zu betrachtenden Ebenen. Das NIS2UmsuCG fokussiert vor allem Aspekte der IT-Sicherheit und Informationstechnik, wohingegen das KRITIS-Dachgesetz den Fokus auf die physische Ebene und Resilienz legt. Beide Gesetze ergänzen sich in einer möglichst gesamtheitlichen Betrachtung, die besonders für die Rolle der Geschäftsleitung notwendig ist.

## 2.3 Einschätzung der Gesetzeslage und des Umsetzungsaufwands von Unternehmen der Stromwirtschaft

Um die unterschiedlichen Perspektiven und Erfahrungen verschiedener Unternehmen der Stromwirtschaft zu erfassen, wurden im Rahmen der Studie Interviews mit Experten<sup>3</sup> aus den Bereichen Netzbetreiber, Anlagenbetreiber und Hersteller durchgeführt. Ziel dieser Interviews war es, tiefgehende Einblicke in das Wissen, die Sensibilität und die Entscheidungsprozesse in Bezug auf IT-Sicherheit und die kommenden Gesetzgebungen zu erhalten. Außerdem sollten subjektive Einschätzungen des monetären Aufwands zur Etablierung der geforderten IT-Sicherheitsmaßnahmen erfragt werden, um ein Stimmungsbild in der Studie zu erarbeiten.

Innerhalb der Studiererstellung wurde hierfür eine qualitative Umfrage in Form von sechs Experteninterviews durchgeführt. Die teilnehmenden Unternehmen sind von unterschiedlicher Größe und Komplexität – von einem kleinstädtischen Stadtwerk bis zum Verteilnetzbetreiber in einem komplexen Stadtwerks-Verbund. Den Teilnehmern können aufgrund der Zusage zum Interview eine Grundsensibilität und Offenheit für das Thema IT-Sicherheit zugeschrieben werden, insbesondere da sie bereits in früheren Projekten zu Aspekten der IT-Sicherheit tätig waren. Demnach sind die Ergebnisse nicht vollständig repräsentativ für die Branche, geben aber dennoch Anhaltspunkte für die Studie.

Im Rahmen der Interviews wurden Fragen zu dem grundlegenden Kenntnisstand zur kommenden Gesetzgebung, zur subjektiv eingeschätzten Sensibilität für das Thema IT-Sicherheit, zum Umgang mit Investitionsentscheidungen und zu einer Einschätzung der Investitionsaufwände zur Erfüllung der dargestellten Pflichten nach NIS2UmsuCG und KRITIS-Dachgesetz diskutiert.

In Bezug auf den Kenntnisstand zu den neuen Gesetzgebungen und die Sensibilität für das Thema IT-Sicherheit wurde deutlich, dass allen Teilnehmern die angespannte Gefahrenlage sowie die Notwendigkeit von IT-Sicherheitsmaßnahmen bewusst sind. Außerdem besteht bereits ein großes Wissen zu den geplanten Gesetzgebungen, insbesondere durch aktive Mitarbeit in Branchenverbänden und den Austausch mit anderen Unternehmen der Energieversorgung.

Durchgängig wurde die Wichtigkeit der Geschäftsleitung in Bezug auf die IT-Sicherheit formuliert. Notwendige Investitionsentscheidungen werden von der Geschäftsleitung getragen, weshalb eine hohe Sensibilität, aber auch ein Wissen zur Effektivität von zu etablierenden Maßnahmen vorhanden sein muss. Wie sich im weiteren Verlauf der Studie zeigen wird, ist die bereits bestehende Informationssicherheits-Zertifizierungspflicht von KRITIS-Betreibern ein wichtiger Punkt. Die Umsetzung der Maßnahmen und eine abgeschlossene

---

<sup>3</sup> Bei den Interviewten handelte es sich ausschließlich um männliche Personen.

Zertifizierung haben seit 2017 bereits zu einem Umdenken in Bezug auf die Notwendigkeit von IT-Sicherheit geführt. Dennoch zeigen die Ergebnisse der durchgeführten Interviews, dass Maßnahmen zur IT-Sicherheit besonders für (Verteil-) Netzbetreiber zumeist noch als Kostenfaktor gesehen werden, da sie zwar gesetzlich vorgeschrieben sind, aber keinen bezifferbaren Wettbewerbsvorteil bringen und die Gefahrenlage durch Cyberangriffe oftmals noch immer zu abstrakt ist.

Um eine Argumentation für die Etablierung von IT-Sicherheitsmaßnahmen zu führen, ist also die Einschätzung zum einen der Kosten, zum anderen aber auch der Größe des Nutzens der Maßnahmen nötig. Um das Verhältnis von Kosten zu Nutzen von Maßnahmen bewerten zu können, wird die Einschätzung zu möglicherweise notwendigen Investitionen der befragten Unternehmen in den nachfolgenden Kapiteln und Abschnitten näher erläutert.

## 3 IT-Sicherheitsreferenzarchitektur eines Unternehmens der Stromwirtschaft

Um ein gemeinsames Verständnis zu schaffen, die relevanten Prozesse der Wertschöpfung zu erfassen und eine mögliche Sicherheitsarchitektur zu beschreiben, wird hier eine Referenzarchitektur eines Verteilnetzbetreibers dargestellt. Die Prozesse inklusive der Kritikalität und eine Einführung möglicher Sicherheitsmaßnahmen sind nachfolgend dargestellt. Nähere Erläuterungen zu den verwendeten Begriffen in der Referenzarchitektur finden sich im Glossar der Studie.

### 3.1 Einführung der Referenzarchitektur eines Verteilnetzbetreibers

Im Rahmen der Studie wird ein beispielhaftes Unternehmen der Stromwirtschaft anhand der verschiedenen Unternehmensbereiche skizziert. Die Struktur entspricht der Vereinfachung der Bereiche eines Verteilnetzbetreibers, unterteilt in eine Geschäftsebene sowie eine zusätzliche Leitsystem- und eine Stationsebene. Damit sollen neben der Betrachtung geschäftsrelevanter Prozesse auch ihre Verknüpfung mit betriebsrelevanten Prozessen und den damit verbundenen technischen Bereichen verdeutlicht werden. Das Zusammenspiel der Prozesse in den Geschäfts- und Betriebsbereichen ist essenziell, um Risiken und Auswirkungen von IT-Angriffen in Unternehmen der Stromwirtschaft zu bewerten. Der Grundansatz basiert auf der Norm IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“.<sup>4</sup> Dabei werden logisch oder physisch zusammenhängende Komponenten mit gemeinsamen Sicherheitsanforderungen in Zonen oder Bereiche gruppiert. Die Kommunikation zwischen den Zonen erfolgt über abgesicherte Netzwerkübergänge, auch bekannt als „Conduits“. Der schematische Aufbau ist in **Abbildung 1** dargestellt.

---

<sup>4</sup> (Internationale Normenreihe für Cybersecurity in der Industrieautomatisierung, IEC 62443, 2020)

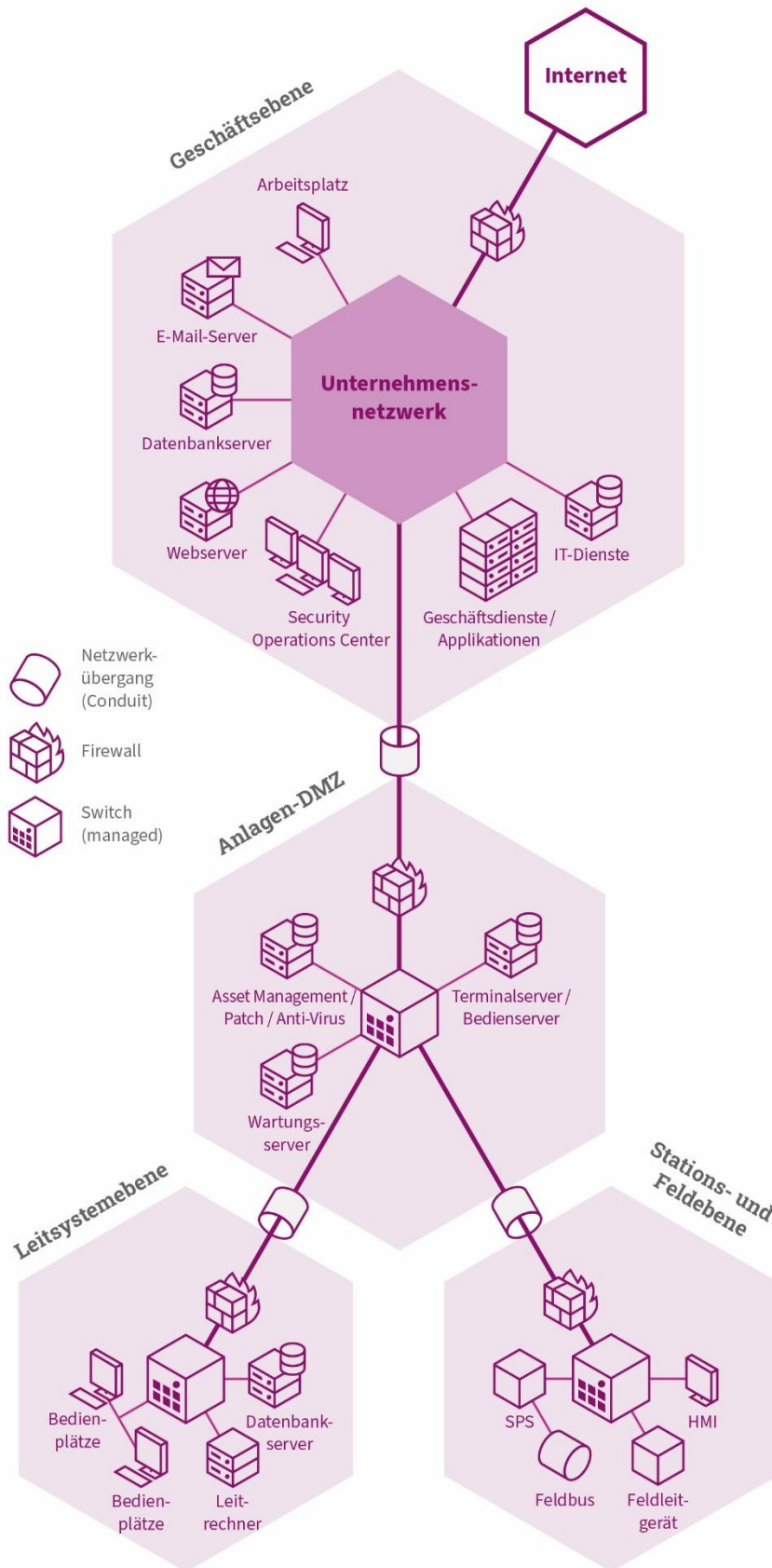


Abbildung 1 IT-Referenzarchitektur eines beispielhaften Verteilnetzbetreibers mit Unterscheidung der Unternehmensebenen in Anlehnung an IEC 62443

Die Einhaltung einer sicheren und effizienten Energieversorgung erfordert das Zusammenspiel verschiedener Planungs- und Betriebsprozesse. Dies betrifft im Wesentlichen die marktorientierte und vorausschauende Beschaffung von Energieprodukten in der Geschäftsebene sowie die Überwachung und Steuerung des elektrischen Netzes in der Leitsystemebene. Hierfür werden über zentrale IT-Dienste Hard- und Softwareanwendungen bereitgestellt und aktualisiert (z. B. Patches) sowie betriebsrelevante Anlagen in einer gesonderten DMZ (Demilitarisierte Zone) verwaltet. Die Aktualisierung von Firmware zur Beseitigung von Schwachstellen (Patch Management) und die Überwachung der IT-Infrastruktur bezüglich möglicher Sicherheitsvorfälle in einem Security Operations Center (SOC) spielen hierbei eine wichtige Rolle zur Erhöhung der IT-Sicherheit. Häufig stellen **Web- oder E-Mail-Dienste in der Geschäftsebene erste Einfallstore** für gezielt geplante IT-Angriffe dar, die sich ohne frühzeitige Entdeckung in weitere Unternehmensbereiche wie die Leitsystemebene ausbreiten und die oben beschriebenen Prozesse der Energieversorgung signifikant beeinträchtigen können.

### 3.2 Beschreibung der internen und externen Prozesse

Nach der Referenzarchitektur aus **Abbildung 1** lassen sich unterschiedliche Prozesse bei Verteilnetzbetreibern identifizieren. Die nachfolgend dargestellten Prozesse sollen möglichst allgemeingültig für Verteilnetzbetreiber sein. Dabei wird in interne und externe Prozesse unterschieden – also Prozesse, die in einem definierten Bereich ohne Interaktion zu äußeren Ebenen ablaufen, und Prozesse, die über die verschiedenen Unternehmensebenen hinweg stattfinden und mit externen Schnittstellen versehen sind. Je nach konkreter Infrastruktur der unterschiedlichen Netzbetreiber gibt es Variationen in den Prozessen. Die nachfolgende Aufzählung zeigt grundlegende Prozesse in den unterschiedlichen Unternehmensebenen nach **Abbildung 1**, hat jedoch keinen Anspruch auf Vollständigkeit.

Tabelle 5 Grundlegende Prozesse nach den Unternehmensebenen aus Abbildung 1

Unternehmensebene	Intern / Extern	Grundlegende Prozesse
<b>Geschäftsebene</b>	Intern	Unternehmensinterne Kommunikation und Nutzung verschiedener IT- und Webdienste, Überwachungsprozesse der internen Systeme im Security Operations Center
	Extern	Unternehmensexterne Kommunikation zum Beispiel über E-Mail, Nutzung von unternehmensexternen Diensten und generelle Verbindung zum Internet, Energiemarktprozesse mit anderen Marktteilnehmern
<b>Anlagen-DMZ</b>	Intern	–
	Extern	Zugriff von unternehmensinternen und -externen Quellen zur Verbindung mit der Leitsystem- oder Feldebene, Abruf von unternehmensexternen Update- und Softwarequellen
<b>Leitsystemebene</b>	Intern	Bedienung des Leitsystems mittels abgesetzter Bedienplätze, Abruf und Speicherung von Daten von Datenbanksystemen

Unternehmensebene	Intern / Extern	Grundlegende Prozesse
	Extern	Fernwartung und -bedienung mittels DMZ-Durchgriff durch interne Beschäftigte oder externe Unternehmen (z. B. Hersteller)
<b>Feld- und Stationsebene</b>	Intern	Automatisierungsprozesse (Schutz und Regelung), Steuerung durch Nahbediensysteme (HMI)
	Extern	Steuerung durch die Leitsystemebene, Fernwartung und -bedienung mittels DMZ-Durchgriff durch interne Beschäftigte oder externe Unternehmen (z. B. Hersteller), Überwachung des Netzwerks und Auswertung in anderen Unternehmensebenen

### 3.3 Beschreibung der Kritikalität der Prozesse

Für die Netzbetreiber steht vor allem die kritische Dienstleistung der Energieversorgung in Form des Netzbetriebs im Mittelpunkt. Diese Dienstleistung ist maßgeblich von der **Feld- und Stationsebene** abhängig, auf der sich der Versorgungsprozess abspielt. Die Grundfunktionen des Netzbetriebs werden in den Automatisierungsfunktionen dieser Ebene erfüllt und sind in erster Linie nicht abhängig von überlagerten Unternehmensebenen. Beispielhafte Prozesse stellen, analog zu **Tabelle 5**, Funktionen des Schutzes auf der Feldebene dar. Eine Schutzfunktion erfolgt autark auf der Feldebene und hat keine äußerliche Abhängigkeit. Die Funktionsfähigkeit wird demnach rein lokal sichergestellt. Jedoch besteht die Möglichkeit, dass Prozesse von außen, insbesondere von der Leitsystemebene, angesteuert oder über einen separaten Zugang von externen Unternehmen gewartet werden.

Sämtliche Prozesse und möglichen Risikofaktoren müssen vom Betreiber überwacht und ihre Kritikalität, besonders für die kritische Dienstleistung, muss eingeschätzt werden. Nach heutigem Stand und nach den dargestellten gesetzlichen Änderungen im Rahmen von NIS2UmsuCG und KRITIS-Dachgesetz ist ein **Risikomanagement** essenziell. Innerhalb des Risikomanagements werden die unterschiedlichen Prozesse aufgezählt und das Risiko wird mittels Einschätzung der Kritikalität und Wahrscheinlichkeit der Verwundbarkeit bewertet. Ein geeignetes Risikomanagement kann beispielsweise nach BSI 200-3 oder E VDE-AR-N 4143-2 von Verteilnetzbetreibern umgesetzt werden.<sup>5,6</sup>

In Bezug auf die grundlegenden Prozesse nach **Tabelle 5** sind vor allem solche kritisch, die externe Schnittstellen nutzen. Besonders maßgeblich sind sie für die **Geschäftsebene**, wohingegen die Wahrscheinlichkeit der Beeinträchtigung der kritischen Dienstleistung aus der Geschäftsebene heraus gering ist. Dementsprechend stellen grundlegend die **externen Schnittstellen der Leitsystem- und besonders der Feldebene mögliche Gefahren für den Versorgungsprozess** dar. Ein fehlgeleiteter Zugriff von außen auf die Leitsystem- und Feldebene muss zwingend verhindert und notfalls früh erkannt werden. Möglichkeiten, um schadhafte Eingriff zu verhindern und ihm entgegenzuwirken, werden nachfolgend anhand von technischen und organisatorischen Maßnahmen beschrieben.

<sup>5</sup> (BSI-Standard 200-3, o.D.)

<sup>6</sup> (E VDE-AR-N 4143-2, 2023)

### 3.4 Beschreibung implementierbarer IT-Sicherheitsmaßnahmen

Aus der Beschreibung der essenziellen Prozesse der Unternehmensebenen beim Verteilnetzbetreiber wird ersichtlich, dass unterschiedliche Maßnahmen zur Wahrung der IT-Sicherheit notwendig sind. Neben den eingeführten Gesetzesänderungen durch das NIS2UmsuCG und das KRITIS-Dachgesetz werden Maßnahmen beispielsweise nach IEC 62443 in einem Schichtenmodell definiert und anwendungsbezogen standardisiert. Das Modell wird als Defense-in-Depth bezeichnet, bezieht sich auf eine möglichst gesamtheitliche Sicherheitsbetrachtung und ist in **Abbildung 12** dargestellt. Der Standard IEC 62443<sup>7</sup> kann demnach als Grundlage genutzt werden, um die jeweiligen Maßnahmen im Unternehmen zu implementieren.

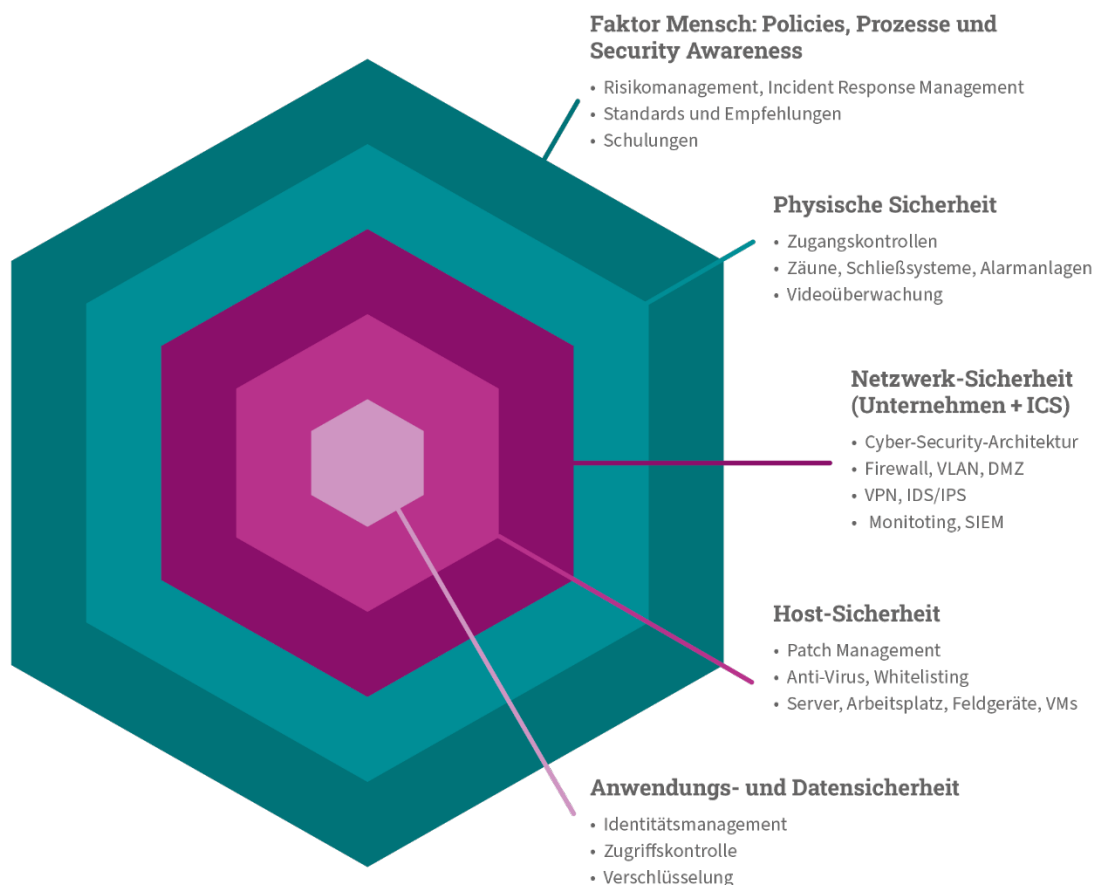


Abbildung 2 Darstellung des Defense-in-Depth-Modells nach IEC 62443

Die Idee dieses Modells ist, dass es nicht ausreichend ist, *eine* große Sicherheitsmaßnahme umzusetzen, sondern viele unterschiedliche Maßnahmen auf den verschiedenen Anwendungsebenen zu implementieren und zu koordinieren. Mit der Beachtung von Defense-in-Depth soll erreicht werden, dass einem potenziellen Angreifer in jeder Ebene Maßnahmen entgegenstehen. Eine Vielzahl von bekannten Angriffen und Schadensereignissen basieren auf einem initialen Eintritt der Angreifer durch Ausnutzen des „Faktors Mensch“, also dem gezielten Ausnutzen von unachtsamem Handeln der Beschäftigten im Unternehmen. Nach **Abbildung 2** betrifft dies primär die **Geschäftsebene**. Effektiv kann dem besonders durch Sensibilisierung und flächen-

<sup>7</sup> (Internationale Normenreihe für Cybersecurity in der Industrieautomatisierung, IEC 62443, 2020)

deckende **Awareness** für das Thema IT-Sicherheit begegnet werden. Zusätzlich lassen sich weitere organisatorische Maßnahmen wie das Risikomanagement und auch Incident Response oder Notfallmanagement nennen.

Für die **Leitsystem- und Feldebene** sind dementsprechend vor allem die nachgelagerten Schichten des Defense-in-Depth-Modells relevant, nach denen ein initialer Eintritt bereits erfolgt ist. Unter einem Eintritt kann man hier auch verstehen, dass beispielsweise Informationen zu physischen Einrichtungen des ausgewählten Opfers erlangt oder ausfindig gemacht wurden. Geht man von einer physischen Bedrohung oder einem Angriffsschritt aus, bei dem beispielsweise Rechentechnik eines Angreifers in einem Umspannwerk platziert wird, ist die Etablierung von Maßnahmen der **physischen Sicherheit** sinnvoll. Demnach soll ein physischer Zugriff von unbefugten Personen durch physische Sicherheitsbarrieren wie Zäune und Mauern verhindert werden.

Die nächste Ebene des Modells nach **Abbildung 2** beschreibt Maßnahmen für die **Netzwerk-Sicherheit**. Die netzwerkseitige Separation der unterschiedlichen Unternehmensebenen nach **Abbildung 1** ist ein Beispiel dafür. Darüber hinaus zählen auch Maßnahmen zur **sicheren Konfiguration und Überwachung** der Übergänge zwischen den Ebenen sowie die komplette netzwerktechnische Überwachung des Datenverkehrs oder von Netzwerkgeräten durch Systeme zur Angriffserkennung (SZA) oder auch Intrusion Detection Systems (IDS) dazu.

Der Schutz der einzelnen Endgeräte innerhalb der Netzwerke wird in der Ebene der **Host-Sicherheit** adressiert. Hier kann das **Patch Management** als organisatorische wie auch technische Maßnahme genannt werden. Besonders beim Patch Management tritt die Leitsystem- und Feldebene zunehmend in den Vordergrund und muss zwingend bei der Digitalisierung und Vernetzung der einzelnen Systeme mitgedacht werden.

Als innerste Schicht ist nach **Abbildung 2** die **Anwendungs- und Datensicherheit** anzusehen. Hier werden Maßnahmen adressiert, die auszutauschende Informationen, also Daten, und die Anwendungen auf den Host-Systemen schützen sollen. Ein naheliegendes Beispiel für den Schutz der übertragenen Daten stellt die **Verschlüsselung** dar, die auch zunehmend für Industrieprotokolle wie IEC 61850 oder IEC 60870-5-104 angewandt wird.<sup>8,9</sup> Das Thema **Identitätsmanagement** bei Anwendungen ist hingegen für die Leitsystem- und Feldebene eines Verteilnetzbetreibers oftmals nur schwierig in die Praxis zu überführen, bietet jedoch zusätzliches Potenzial für den Schutz vor einer Infiltration der Endgeräte und Anwendungen.

---

<sup>8</sup> (IEC 61850:2024 SER, 2024)

<sup>9</sup> (IEC 60870-5-104, 2016)

## 4 Beispielrechnungen zur Rentabilität von IT-Sicherheitsmaßnahmen

Für das Ziel der Kosten-Nutzen-Abschätzung geht es in diesem Kapitel um die Ermittlung der relevanten Größen der Investitionskosten für die Etablierung von IT-Sicherheitsmaßnahmen und der möglichen Schadenskosten. Als Grundlage für eine Beispielrechnung zur Rentabilität dient in dieser Studie in erster Linie eine belastbare Abschätzung der anfallenden Investitionskosten für die adressierten Maßnahmen aufgrund der Gesetzesänderungen. Hierzu wird zunächst grundlegend auf die Ermittlung von Kosten zur Etablierung von IT-Sicherheitsmaßnahmen und auf eine Aufstellung des Erfüllungsaufwands für die Wirtschaft nach NIS2UmsuCG eingegangen. Um anschließend die ermittelten Kosten in Relation setzen zu können, wird eine Möglichkeit der monetären Bewertung von Schäden durch Sicherheitsvorfälle dargestellt und die genannten Größen aus NIS2UmsuCG werden eingeführt.

### 4.1 Ermittlung der Kosten zur Etablierung von IT-Sicherheitsmaßnahmen

Für die Umsetzung des NIS2UmsuCG sind neue Maßnahmen zu treffen und in Unternehmen einzuführen, beispielsweise die Etablierung von Meldekettens bei Sicherheitsvorfällen oder die regelmäßige Durchführung von Schulungen.

Aus betriebswirtschaftlicher Sicht sollte für jede Maßnahme eine Wirtschaftlichkeitsbetrachtung durchgeführt werden. Die Kostenstruktur ist dabei von der jeweils zu betrachtenden Maßnahme abhängig.

In jedem Fall sind für eine Umsetzung Personalkosten zu veranschlagen, die durch interne und externe Ressourcen anfallen, beispielsweise für die Projektierung der Anschaffung und Inbetriebnahme oder auch für die Begleitung eines fortwährenden Prozesses. Diese Personalkosten berechnen sich aus den Stundensätzen der Beschäftigten und der veranschlagten Arbeitszeit für die Umsetzung.

Ist für eine Maßnahme eine Anschaffung notwendig, so fallen Investitionskosten an. Dies kann zum Beispiel der Fall sein, wenn ein Monitoringsystem zur Überwachung von kritischen Prozessen, etwa ein System zur Angriffserkennung (SzA), angeschafft wird oder Sicherheitsprodukte wie Firewalls modernisiert werden, um einen erweiterten Funktionsumfang zu erhalten. Außerdem müssen die Betriebskosten für solche Systeme berücksichtigt werden.

Bei dem Beispiel eines SzA fallen vereinfacht die Kostenpositionen der Projektierung (inklusive Konzeptionierung, Marktstudie, Angebotsphase etc.), der reinen Beschaffung und des Personaleinsatzes zur Inbetriebnahme sowie die laufenden Kosten des Personaleinsatzes zum Betrieb (z. B. 24/7-Schichtdienste zur Betreuung der Systeme) und Betriebskosten wie Lizenzkosten an. Eine detaillierte und korrekte Einschätzung der Kosten zur Etablierung von IT-Sicherheitsmaßnahmen ist demnach mitunter sehr komplex und bedarf eines gesamtheitlichen Blicks auf die spezifische Maßnahme.

### 4.2 Erfüllungsaufwand für die Wirtschaft nach NIS2UmsuCG

Aus dem NIS2UmsuCG geht eine Abschätzung des Gesetzgebers des wirtschaftlichen Investitionsbedarfs hervor, die bei jährlich rund 2,2 Milliarden Euro und einem einmaligen Aufwand von rund 2 Milliarden Euro liegt. Diese Summen gelten als Gesamtsummen für die deutsche Wirtschaft. In der Begründung innerhalb des

vorliegenden Referentenentwurf wird eine Aufstellung des Erfüllungsaufwands für die Wirtschaft vorgelegt, um den genannten Investitionsbedarf auf die einzelnen Maßnahmen zu verteilen.

Nachfolgend werden die Gesamtkosten unter Nennung der Anzahl betroffener Unternehmen der wichtigen und besonders wichtigen Einrichtungen auf die einzelnen Unternehmen heruntergerechnet. Es wird von **zukünftig 8.250 besonders wichtigen und 21.600 wichtigen Einrichtungen** ausgegangen. Diese Abschätzung wurde ebenfalls direkt aus der Erklärung des Erfüllungsaufwands entnommen. **Tabelle 6** stellt die Kosten je Unternehmen der Kategorie besonders wichtige Einrichtungen und **Tabelle 7** die Kosten für wichtige Einrichtungen dar.

Tabelle 6 Kosten für besonders wichtige Einrichtungen

Kategorie	Maßnahme	Kosten in Euro
<b>Einhaltung eines Mindestniveaus an IT-Sicherheit</b>	Einführung bzw. Anpassung digitaler Prozessabläufe (einmaliger Aufwand)	203.816,40
	Bürokratiekosten (für einmaligen Aufwand)	183,60
	Der einmalige Aufwand zur Einhaltung eines Mindestniveaus an IT-Sicherheit soll gleich dem jährlichen Aufwand zur Einhaltung eines Mindestniveaus an IT-Sicherheit sein.  Des Weiteren betragen die Bürokratiekosten für den einmaligen Aufwand 0,09 Prozent und die Kosten für die Einführung digitaler Prozessabläufe 99,91 Prozent der Gesamtkosten. (Dies ergibt sich daraus, dass im NIS2UmsCG von jährlichen Kosten in Höhe von 2,2 Milliarden Euro ausgegangen wird und davon 1,9 Millionen Euro auf Bürokratiekosten entfallen.)	
	Personalkosten (Einhaltung eines Mindestniveaus an IT-Sicherheit) (2.752 Stunden, 52,30 Euro Lohnsatz)	143.929,60
	Sachkosten (Einhaltung eines Mindestniveaus an IT-Sicherheit)	60.000,00
<b>Nachweis der Einhaltung eines Mindestniveaus an IT-Sicherheit</b>	Personalkosten für Erbringung der Nachweispflicht (inklusive notwendiger Dokumentationen und Prüfungen) (Zeitaufwand: 282 Stunden, 56,90 Euro Lohnsatz)	16.045,80
	Sachkosten für Erbringung der Nachweispflicht (inklusive notwendiger Dokumentationen und Prüfungen)	19.291,67
<b>Meldung erheblicher Sicherheitsvorfälle</b>	Personalkosten für Meldung (Zeitaufwand: 6,75 Stunden je Sicherheitsvorfall, Vorfälle pro Jahr und Unternehmen: 0,095, 58,40 Euro Lohnsatz)	37,45
<b>Registrierungspflichten</b>	Personalkosten für erstmalige Übermittlung der Informationen (einmaliger Erfüllungsaufwand) (Zeitaufwand: 0,42 Stunden, 36,30 Euro Lohnsatz)	15,25
	Personalkosten für Meldung von Änderungen der registerpflichtigen Angaben (jährlicher Erfüllungsaufwand)	2,02

Kategorie	Maßnahme	Kosten in Euro
	(Zeitaufwand: 0,167 Stunden, 1/3 Änderungen pro Jahr, 36,30 Euro Lohnsatz)	
<b>Regelmäßige Schulungen</b>	Personalkosten für Schulungen der Geschäftsleitung (Zeitaufwand: 4 Stunden, 10 Beschäftigte je Unternehmen, 58,40 Euro Lohnsatz)	2.336,00
	Sachkosten für Schulungen der Geschäftsleitung (100 Euro Schulungskosten, 10 Beschäftigte je Unternehmen)	1.000,00
	Personalkosten für Schulungen der Beschäftigten (Zeitaufwand: 1 Stunde, 200 Beschäftigte je Unternehmen, 36,30 Euro Lohnsatz)	7.260,00
	Sachkosten für Schulungen der Beschäftigten (0 Euro wegen kostenlosen Schulungsangebots, 200 Beschäftigte je Unternehmen)	0,00

Tabelle 7 Kosten für wichtige Einrichtungen

Kategorie	Maßnahme	Kosten in Euro
<b>Einhaltung eines Mindestniveaus an IT-Sicherheit</b>	Einführung bzw. Anpassung digitaler Prozessabläufe (einmaliger Aufwand)	81.456,00
	Bürokratiekosten (für einmaligen Aufwand)	74,00
	Der einmalige Aufwand zur Einhaltung eines Mindestniveaus an IT-Sicherheit soll gleich dem jährlichen Aufwand zur Einhaltung eines Mindestniveaus an IT-Sicherheit sein. Des Weiteren betragen die Bürokratiekosten für den einmaligen Aufwand 0,09 Prozent und die Kosten für die Einführung digitaler Prozessabläufe 99,91 Prozent der Gesamtkosten. (Dies ergibt sich daraus, dass im NIS2UmsuCG von jährlichen Kosten in Höhe von 2,2 Milliarden Euro ausgegangen wird und davon 1,9 Millionen Euro auf Bürokratiekosten entfallen.	
	Personalaufwand (Einhaltung eines Mindestniveaus an IT-Sicherheit) (1.100 Stunden, 52,30 Euro Lohnsatz)	57.530,00
	Sachkosten (Einhaltung eines Mindestniveaus an IT-Sicherheit)	24.000,00
<b>Meldung erheblicher Sicherheitsvorfälle</b>	Personalkosten für Meldung (Zeitaufwand: 6,75 Stunden je Sicherheitsvorfall, Vorfälle pro Jahr und Unternehmen: 0,095, 58,40 Euro Lohnsatz)	37,45

<b>Registrierungspflichten</b>	Personalkosten für erstmalige Übermittlung der Informationen (einmaliger Erfüllungsaufwand) (Zeitaufwand: 0,42 Stunden, 36,30 Euro Lohnsatz)	15,25
	Personalkosten für Meldung von Änderungen der registerpflichtigen Angaben (jährlicher Erfüllungsaufwand) (Zeitaufwand: 0,167 Stunden, 1/3 Änderungen pro Jahr, 36,30 Euro Lohnsatz)	2,02
<b>Regelmäßige Schulungen</b>	Personalkosten für Schulungen der Geschäftsleitung (Zeitaufwand: 4 Stunden, 10 Beschäftigte je Unternehmen, 58,40 Euro Lohnsatz)	2.336,00
	Sachkosten für Schulungen der Geschäftsleitung (100 Euro Schulungskosten, 10 Beschäftigte je Unternehmen)	1.000,00
	Personalkosten für Schulungen der Beschäftigten (Zeitaufwand: 1 Stunde, 200 Beschäftigte je Unternehmen, 36,30 Euro Lohnsatz)	7.260,00
	Sachkosten für Schulungen der Beschäftigten (0 Euro wegen kostenlosen Schulungsangebots, 200 Beschäftigte je Unternehmen)	0,00

Im Rahmen der durchgeführten Interviews wurden die einzelnen Kostenkategorien, Maßnahmen und konkreten Kosten diskutiert und von den Teilnehmern subjektiv eingeschätzt. Als allgemeiner Tenor konnte festgestellt werden, dass die Kategorien in den Tabellen sehr grob, aber dennoch grundlegend zutreffend sind. Besonders die Maßnahme der Einführung bzw. Anpassung digitaler Prozessabläufe ist dabei sehr unspezifisch und kann je nach Ausgangslage des jeweiligen Unternehmens und konkreter Umsetzung stark variieren. Je nach Komplexität und Größe des Unternehmens kann ein Prozessablauf für die Etablierung einer spezifischen IT-Sicherheitsmaßnahme sehr unterschiedlich aussehen und die Kosten können stark divergieren.

Am Beispiel der im Jahr 2023 zu etablierenden Systeme zur Angriffserkennung zeigt sich dies vor allem im Umfang der zu betreibenden Lösung und der daraus abgeleitet notwendigen Unternehmensprozesse. Wird ein SzA komplett vom Netzbetreiber betrieben und mit eigenen Ressourcen überwacht, können sowohl der Aufwand für die einmalige Einführung der Prozesse als auch der laufende Aufwand im 24/7-Schichtbetrieb erheblich höher sein als bei einem Netzbetreiber, der sein SzA outsourct und kein eigenes Personal aktiv bereitstellen muss. Eine Bereitschaft des eigenen Personals muss dennoch für Notfälle sichergestellt werden.

Weiterhin wird aus dem Erfüllungsaufwand deutlich, dass unterschiedliche Ausgangssituationen unbeachtet bleiben. Die interviewten Netzbetreiber, die nach BSI-Gesetz bereits als KRITIS eingestuft wurden und schon seit 2017 ein Information Security Management System (ISMS) eingeführt und bereits mehrfach rezertifiziert haben, rechnen mit einem deutlich geringeren Erfüllungsaufwand als Betreiber, die gegebenenfalls bisher noch nicht erfasst sind und viele strukturelle, organisatorische und technische Maßnahmen ergreifen müssen.

Jedoch wurde die Aufstellung des Erfüllungsaufwands im Rahmen der Interviews als grundlegend valide eingestuft, wenngleich aus den genannten Gründen nicht direkt anwendbar für ein einzelnes Unternehmen.

### **4.3 Ermittlung der Schadenskosten**

Die Aufstellung des Erfüllungsaufwands und der Kosten zur Etablierung von IT-Sicherheitsmaßnahmen muss objektiv einschätzbar gemacht werden. Als mögliche Größe zur Bewertung der Investitionskosten wird im späteren Verlauf über den Return on Security Investment (RoSI) auf mögliche Schadenskosten eingegangen. Demnach wird nachfolgend beschrieben, wie diese Schadenskosten abgeschätzt werden können. Als Grundlage zur Abschätzung eines möglichen Schadens ist eine **Risikoanalyse** im Rahmen des Risikomanagements notwendig. Ein mögliches Vorgehen ist den im Folgenden erläuterten Schritten zu entnehmen.

#### **4.3.1 Identifikation und Analyse bestehender Assets**

Zunächst werden alle Assets identifiziert, die in die Ausführung der Geschäftsprozesse involviert sind. Zur Identifikation, Charakterisierung und Priorisierung können beispielsweise die Vorgaben der ISO 27001 verwendet werden.<sup>10</sup>

##### **Erstellen eines Asset-Inventars**

Eine Liste der Assets sollte bei Unternehmen bereits grundlegend vorhanden sein. Andernfalls muss sie erstellt oder gegebenenfalls aktualisiert werden. Die Liste sollte alle Assets umfassen, die an der Erbringung der kritischen Dienstleistung beteiligt sind.

##### **Priorisierung der Assets**

Für jedes Asset muss anschließend die Kritikalität bewertet werden. Dafür kann man beispielsweise eine Bewertung nach den drei Schutzziele Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) durchführen. Dabei wird jedem Asset für jedes dieser drei Sicherheitsziele ein Wert zwischen 1 und 5 zugeordnet, abhängig davon, wie wichtig dieses Sicherheitsziel für das Asset ist. Die drei Werte werden anschließend addiert, sodass sich ein Wert für die Kritikalität zwischen 3 und 15 ergibt. Die Assets können nun nach ihrer Kritikalität sortiert werden.

##### **Quantifizierung des Wertes eines Assets**

Die Zuweisung eines monetären Wertes auf Basis der Kritikalität zu jedem Asset ergibt sich aus dessen physischem monetären Wert (oftmals dem Anschaffungswert) zusammen mit der Kritikalität. Dabei erhält jedes Asset den Wert der physischen Kosten multipliziert mit der Kritikalität. Damit wird jedoch lediglich der Wert der Assets und weniger eine monetäre Beschreibung der Geschäftsprozesse und der kritischen Dienstleistung ausgedrückt.

#### **4.3.2 Identifizierung von Bedrohungen und Schwachstellen**

Es ist nun bekannt, welche Assets vorliegen und welche Kritikalität sie haben. Im nächsten Schritt muss festgestellt werden, welchen Bedrohungen diese Assets ausgesetzt sind.

---

<sup>10</sup> (ISO/IEC 27001:2022, 2022)

## Modellierung von Bedrohungen

Die Assets können einer Reihe von Bedrohungen ausgesetzt sein, die identifiziert werden müssen. Dafür können jedoch Bedrohungslisten aus Veröffentlichungen bekannter Institutionen (z. B. NIST (National Institute of Standards and Technology) oder BSI) herangezogen werden. Beispielsweise hat das BSI im **IT-Grundschutz-Kompendium** eine Reihe elementarer Gefährdungen aufgelistet.<sup>11</sup> Sie können genutzt werden, um die Bedrohungen der Assets zu modellieren. Für jedes Asset bzw. jeden Informationsverbund kann nun überprüft werden, ob Maßnahmen existieren, die den Bedrohungen (Gefährdungen) begegnen. Für die Modellierung und Analyse sind nicht nur die einzelnen Assets zu betrachten, sondern auch ihre Wechselwirkung im Informationsverbund. Daher muss beispielsweise auch die gesamte Netzwerkstruktur betrachtet werden.

1. Bestimmung möglicher Bedrohungen, zum Beispiel elementare Gefährdungen des IT-Grundschutzes oder nach NIST 800-30<sup>12</sup>
2. Bestimmung der wichtigen Schutzziele eines Assets, zum Beispiel die Verfügbarkeit, die bei der Bestimmung der Kritikalität festgelegt wurde
3. Identifikation von Gegenmaßnahmen, die eine Verletzung der Schutzziele verhindern. Sie können in einer Kreuzreferenztafel den Bedrohungen gegenübergestellt werden.

## Scannen auf Schwachstellen

Neben den Bedrohungen können auch Schwachstellen im System existieren, die von einem Angreifer ausgenutzt werden können. Bekannte Schwachstellen können durch **Schwachstellenscanner** identifiziert werden. Eine regelmäßige Überprüfung der eigenen Informationssysteme mit diesen Scannern ist eine sinnvolle Ergänzung zur Bedrohungsmodellierung.

### 4.3.3 Bestimmung der Eintrittswahrscheinlichkeit und der Auswirkungen

Für das Risikomanagement ist es des Weiteren wichtig, die Eintrittswahrscheinlichkeit und die potenziellen Auswirkungen eines Schadensfalls abzuschätzen.

#### Bestimmung der Eintrittswahrscheinlichkeit

Bei der Bestimmung der Eintrittswahrscheinlichkeit müssen zwei Werte bestimmt werden: zunächst einmal die Eintrittswahrscheinlichkeit für ein Ereignis, ohne dass (zusätzliche) Sicherheitsmaßnahmen umgesetzt wurden, zum anderen die Senkung der Eintrittswahrscheinlichkeit durch eine spezifische Maßnahme oder eine Kombination aus unterschiedlichen Maßnahmen.

#### Bestimmung der Auswirkungen

Bei der Ermittlung der Auswirkungen geht es um die Identifizierung potenzieller Verluste aufgrund der erfolgreichen Durchführung eines Angriffs für ein Asset.

Hierbei sind verschiedene Kostenpunkte zu berücksichtigen. Zum einen sind dies die Kosten für die Wiederherstellung. Sie beinhalten – falls nötig – die Wiederbeschaffung oder Reparatur sowie die Inbetriebnahme.

<sup>11</sup> (IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit, 2023)

<sup>12</sup> (NIST SP 800-30, 2020)

Darüber hinaus können auch ein Ausfall an Einnahmen entstehen sowie, abhängig von der Art des Schadens, ein Reputationsverlust.

Zusammen mit der (jährlichen) Ausfallwahrscheinlichkeit kann dann ein jährlicher Verlust durch Angriffe berechnet werden.

#### **4.4 Schadensabschätzung nach NIS2UmsuCG**

Im Referentenentwurf des NIS2UmsuCG wird eine Abschätzung der Kosten angegeben, die auf die betroffenen Unternehmen zukommen. Laut dieser Schätzung verursachen in Deutschland Cyberangriffe bei Unternehmen mit mindestens zehn Beschäftigten jährlich einen Schaden von 210 Milliarden Euro. Laut Statistischem Bundesamt gibt es in Deutschland 444.055 dieser Unternehmen, was je Unternehmen einen Schaden von rund 500.000 Euro ergibt.<sup>13</sup>

Mit der neuen Gesetzgebung werden eine Reihe von Maßnahmen vorgeschrieben, die von Unternehmen umzusetzen sind. Diese Maßnahmen werden voraussichtlich dazu führen, dass der Schaden, der durch Cyberangriffe entsteht, sinken wird. Der Referentenentwurf geht davon aus, dass der Schaden um die Hälfte sinkt, sodass 250.000 Euro Schaden je Unternehmen abgewehrt werden.<sup>14</sup> Vom NIS2UmsuCG sind schätzungsweise 14.500 Unternehmen betroffen. Daraus ergibt sich ein abgewehrter Gesamtschaden von rund 3,6 Milliarden Euro.

Der hier zur Berechnung verwendete Schaden gibt einen mit einer Schadenswahrscheinlichkeit bewerteten Durchschnitt, gemittelt auf alle Unternehmen, die vom NIS2UmsuCG betroffen sind, wieder. Im Falle eines Cyberangriffs auf ein Energieversorgungsunternehmen kann der Schaden schnell weitaus größer werden, falls die sichere Energieversorgung nicht mehr gewährleistet werden kann und in einem Dominoeffekt weitere kritische Einrichtungen anderer Sektoren nicht mehr operieren können. Die daraus resultierenden Folgeschäden im Falle eines Stromausfalls können sehr groß sein und sind schwer abschätzbar. Deshalb wurde für die Berechnung im Folgenden auf den Schadensbetrag des Referentenentwurfs des NIS2UmsuCG zurückgegriffen.

---

<sup>13</sup> (Referentenentwurf NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, 2024)

<sup>14</sup> Ebd.

## 5 Der Return on Security Investment zur Verdeutlichung der Investitionseffekte

Die zuvor beschriebenen Ermittlungen und Beispiele nach NIS2UmsuCG zu möglichen Kosten der Etablierung von IT-Sicherheitsmaßnahmen sowie zu möglichen Ausfallkosten können über das Modell des Return on Security Investment (RoSI) direkt miteinander in Beziehung gesetzt werden.<sup>15</sup> Daraus ergibt sich die Möglichkeit, das finanzielle Potenzial einer bestimmten Maßnahme in Bezug auf die Senkung der zu erwartenden Schadens- oder Verlustkosten als Folge eines Cyberangriffs zu bewerten. Im Sinne des Return on Investment (RoI) lässt sich als Ergebnis ausdrücken, ob und wann sich die Etablierung einer Maßnahme finanziell für das jeweilige Unternehmen lohnt.<sup>16</sup>

In den durchgeführten Interviews wurde dieses Modell als bereits bekannt, jedoch selten verwendet bewertet. Die Interviewpartner erachteten aber das Ergebnis des Modells als eine sinnvolle Basis zur Entscheidungsfindung für die Geschäftsführung. Des Weiteren erleichtert eine quantitative Bewertung der Investitionen in IT-Sicherheit die Kommunikation der Relevanz und kann ein gemeinsames Verständnis der beteiligten Abteilungen im Entscheidungsprozess schaffen. Über den Ansatz wird IT-Sicherheit nicht weiter als ein reiner Kostenfaktor angesehen, sondern über die Bewertung mit sinkenden Schadenskosten kann ein positiver Effekt der Maßnahmen dargestellt werden.

### 5.1 Definition des RoSI – Return on Security Investment

Der RoSI basiert auf der betriebswirtschaftlichen Kennzahl des Return on Investment (RoI). Dieser bewertet den Gewinn, der aus investiertem Kapital erwirtschaftet wird und somit, ob Investitionen rentabel sind. Angelehnt ist das nachfolgend dargestellte Modell an die Veröffentlichung von Yaqoob et al. (2019)<sup>17</sup>.

Zur Bewertung von Investitionen in die IT-Sicherheit können keine erwirtschafteten Gewinne als Maß für die Rentabilität herangezogen werden. Deshalb bewertet der RoSI die Risikominderung und Schadensverhütung durch Sicherheitsinvestitionen.

Zur Berechnung des RoSI ist eine **Kosten-Nutzen-Analyse** durchzuführen. Sie bewertet die Wirksamkeit von Investitionen in Gegenmaßnahmen durch den Vergleich des jährlichen Verlusts vor und nach der Investition in Gegenmaßnahmen.

Hierzu wird die **Eintrittswahrscheinlichkeit von Angriff x** vor und nach der Implementierung von Gegenmaßnahmen bestimmt. Daraus berechnet sich der **jährliche Verlust durch Angriff x** vor und nach der Implementierung der Gegenmaßnahmen. Durch Kumulation der jährlichen Verluste pro Angriff kann der **gesamte jährliche Verlust durch Angriffe** berechnet werden.

<sup>15</sup> (Yaqoob, Arshad, Haider, Amjad, & Shafqat, 2019)

<sup>16</sup> (Friedlob & Plewa Jr., 1996)

<sup>17</sup> (Yaqoob, Arshad, Haider, Amjad, & Shafqat, 2019)

Der RoSI wird folgendermaßen berechnet:

$$RoSI = \sum_{i,j,k=1}^n \frac{\text{Jährlicher Verlust}(i,k) - \text{Veränderter jährlicher Verlust}(i,k,j) - \text{Kosten}(j)}{\text{Kosten}(j)}$$

Wobei:

**Jährlicher Verlust (i,k):** Gesamter jährlicher Verlust durch erfolgreiche Angriffe *k* auf *i* kritische Assets

**Veränderter jährlicher Verlust (i,k,j):** Gesamter jährlicher Verlust durch erfolgreiche Angriffe *k* auf *i* kritische Assets nach der Implementierung von *j* Gegenmaßnahmen

**Kosten (j):** Gesamtinvestitionskosten für *j* Gegenmaßnahmen

## 5.2 Berechnung des RoSI für wichtige und besonders wichtige Einrichtungen

Im Folgenden wird beispielhaft die Berechnung des RoSI für Investitionen, die sich aus dem NIS2UmsuCG ergeben, durchgeführt. Dabei wird der Erfüllungsaufwand des NIS2UmsuCG verwendet, wonach der Durchschnitt aller vom NIS2UmsuCG betroffenen Unternehmen definiert wird.

Der jährliche Verlust kann Kapitel 4.4 entnommen werden:

Jährlicher Verlust (gesamt) = 500.000 Euro

Veränderter jährlicher Verlust (gesamt) = 250.000 Euro

Die Kosten, sowohl jährlich als auch einmalig (nur im ersten Jahr anzusetzen), können Kapitel 4.2 entnommen werden:

Einmalige Kosten (besonders wichtige Einrichtungen) = 204.015,25 Euro

Jährliche Kosten (besonders wichtige Einrichtungen) = 249.973,10 Euro

Einmalige Kosten (wichtige Einrichtungen) = 81.545,25 Euro

Jährliche Kosten (wichtige Einrichtungen) = 92.165,63 Euro

Im Folgenden wird eine Beispielrechnung der Entwicklung des RoSI für besonders wichtige Einrichtungen in den ersten drei Jahren durchgeführt.

Tabelle 8 Beispielrechnung der Entwicklung des RoSI für besonders wichtige Einrichtungen

Jahr	Berechnung	RoSI
1.	$\frac{500.000\text{€} - 250.000\text{€} - 204.015,25\text{€} - 249.973,10\text{€}}{204.015,25\text{€} + 249.973,10\text{€}}$	-0,45
2.	$\frac{500.000\text{€} - 250.000\text{€} - 249.973,10\text{€}}{249.973,10\text{€}}$	0,0001
3.	$\frac{500.000\text{€} - 250.000\text{€} - 249.973,10\text{€}}{249.973,10\text{€}}$	0,0001

In **Tabelle 9** ist eine Beispielrechnung der Entwicklung des RoSI für wichtige Einrichtungen in den ersten drei Jahren dargestellt:

Tabelle 9 Beispielrechnung der Entwicklung des RoSI für wichtige Einrichtungen

Jahr	Berechnung	RoSI
1.	$\frac{500.000\text{€} - 250.000\text{€} - 81.545,25\text{€} - 92.165,63\text{€}}{81.545,25\text{€} + 92.165,63\text{€}}$	0,44
2.	$\frac{500.000\text{€} - 250.000\text{€} - 92.165,63\text{€}}{92.165,63\text{€}}$	1,71
3.	$\frac{500.000\text{€} - 250.000\text{€} - 92.165,63\text{€}}{92.165,63\text{€}}$	1,71

Der RoSI gibt an, ob eine Investition für eine Organisation vorteilhaft ist oder nicht. Eine positive Rendite zeigt, dass ein Unternehmen die Investition tätigen sollte, da sie für das Unternehmen in der Zukunft von Nutzen sein wird. Eine negative Rendite zeigt, dass die Investition nicht vorteilhaft sein wird. Eine Nullrendite hingegen zeigt, dass die Investition weder gewinnbringend ist noch zu einem Verlust führen wird.

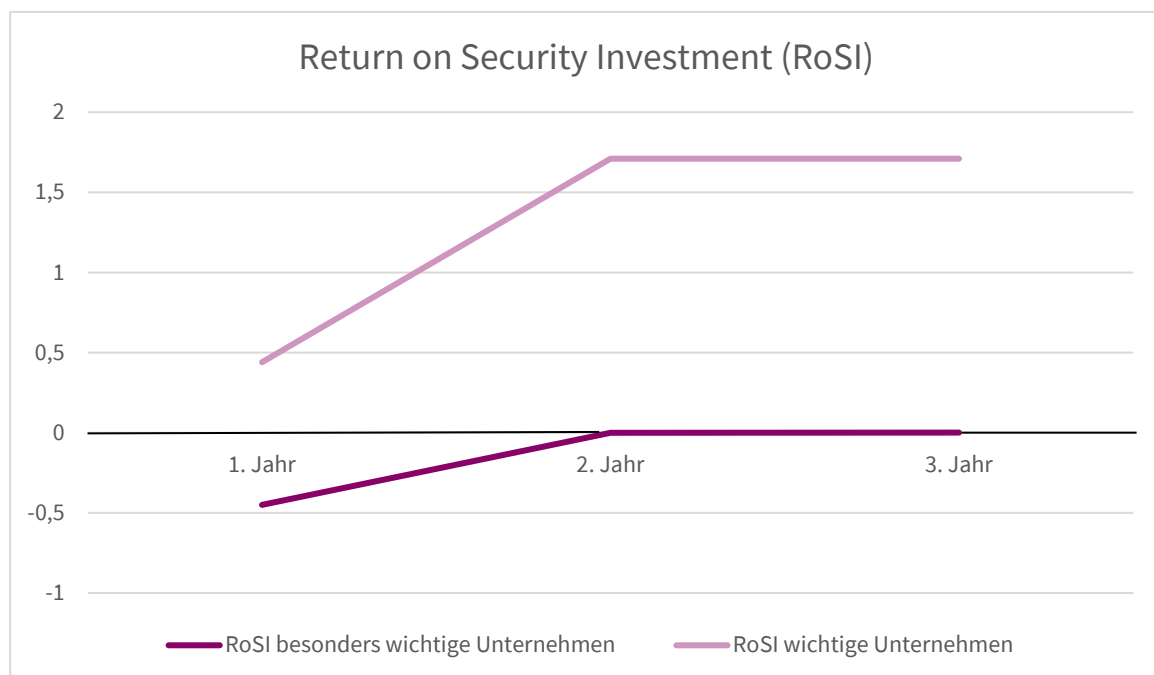


Abbildung 3 Darstellung der Entwicklung des RoSI für beide Unternehmenskategorien unter den Annahmen aus NIS2UmsuCG

Die Berechnungsbeispiele mit den Annahmen aus NIS2UmsuCG zeigen, dass sich für **besonders wichtige Einrichtungen** die Investitionen, die aus dem NIS2UmsuCG hervorgehen, unter den genannten groben Abschätzungen schon im zweiten Jahr rentieren. Dies liegt an den hohen einmaligen Investitionen vor allem für die Einführung bzw. Anpassung digitaler Prozessabläufe. Die Rentabilität für besonders wichtige Einrichtungen ist demnach sehr von der genauen Höhe der einzelnen Kosten abhängig und kann unter Umständen

auch nach individueller Berechnung negativ ausfallen. Für **wichtige Einrichtungen** hingegen rentieren sich die Investitionen bereits im ersten Jahr.

Bei der Interpretation der Ergebnisse sei darauf hingewiesen, dass die Annahmen auf starken Mittelungen über verschiedenste Unternehmenstypen und Ausgangssituationen basieren. Demensprechend ist die Einschätzung der Kosten für IT-Sicherheitsmaßnahmen sehr individuell zu treffen und unterliegt großen Streuungen. Weiterhin sind auch die Verlustkosten sehr verallgemeinernd zusammengefasst. Sie sind nicht explizit auf Versorgungsunternehmen der Stromwirtschaft bezogen, in denen eine Störung der Stromversorgung als mögliche Angriffsauswirkung weitreichende monetäre, aber auch gesellschaftliche Folgen haben kann. Dies kann über eine Verlustabschätzung nur sehr schwer abgebildet werden. Auch unterscheiden sich die Annahmen zu den Verlustkosten nicht bei den beiden Kategorien der besonders wichtigen und wichtigen Einrichtungen. Den dargestellten Ergebnissen liegen die gleichen Verlustkosten zugrunde, wohingegen der Erfüllungsaufwand unterschiedlich ist.

Die Ergebnisse zeigen jedoch eine mögliche Anwendung des RoSI-Modells unter den ausgeführten stark einschränkenden Annahmen. Das Modell kann auf Basis konkreter zutreffender Ermittlungen angewandt werden und die Beschreibungen innerhalb der Studie können als Grundlagen dafür dienen. Über diesen Weg lassen sich für von den eingeführten Gesetzesänderungen betroffene Unternehmen die notwendigen Investitionen direkt in Relation zu den vermiedenen Schadenskosten setzen. Hieraus kann zusätzlich ein Bewusstsein für die Etablierung von IT-Sicherheitsmaßnahmen geschaffen werden, da oftmals eine konkrete Abschätzung von Schadenskosten nicht durchgeführt wird, ohnehin nicht bei der Betrachtung von neu zu etablierenden Maßnahmen.

# Abbildungsverzeichnis

Abbildung 1	IT-Referenzarchitektur eines beispielhaften Verteilnetzbetreibers mit Unterscheidung der Unternehmensebenen in Anlehnung an IEC 62443 .....	15
Abbildung 2	Darstellung des Defense-in-Depth-Modells nach IEC 62443 .....	18
Abbildung 3	Darstellung der Entwicklung des RoSI für beide Unternehmenskategorien unter den Annahmen aus NIS2UmsuCG .....	29

# Tabellenverzeichnis

Tabelle 1	Übersicht über die vom NIS2UmsuCG betroffenen Unternehmen in Deutschland.....	7
Tabelle 2	Übersicht über die Pflichten für die drei relevanten Unternehmenstypen nach NIS2UmsuCG.....	7
Tabelle 3	Übersicht über die vom KRITIS-Dachgesetz betroffenen Unternehmen in Deutschland.....	9
Tabelle 4	Übersicht über die Pflichten für Betreiber nach KRITIS-Dachgesetz.....	9
Tabelle 5	Grundlegende Prozesse nach den Unternehmensebenen aus Abbildung 1 .....	16
Tabelle 6	Kosten für besonders wichtige Einrichtungen.....	21
Tabelle 7	Kosten für wichtige Einrichtungen.....	22
Tabelle 8	Beispielrechnung der Entwicklung des RoSI für besonders wichtige Einrichtungen .....	28
Tabelle 9	Beispielrechnung der Entwicklung des RoSI für wichtige Einrichtungen.....	29

# Literaturverzeichnis

- IEC 60870-5-104. (06 2016). *Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles*. Von <https://www.vde-verlag.de/iec-normen/223604/iec-60870-5-104-2006-amd1-2016-csv.html> abgerufen
- BSI-Standard 200-3. (o.D.). *Bundesamt für Sicherheit in der Informationstechnik*. Von <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement.html> abgerufen
- E VDE-AR-N 4143-2. (09 2023). *VDE V*. Von <https://www.vde-verlag.de/normen/1100814/e-vde-ar-n-4143-2-anwendungsregel-2023-09.html> abgerufen
- Friedlob, G., & Plewa Jr., F. (1996). *Understanding Return on Investment*. ISBN: 978-0-471-10372-1.
- Heimat, B. d. (07. Mai 2024). Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationsmanagements in der Bundesverwaltung. *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz*.
- IEC 61850:2024 SER. (05 2024). *IEC 61850:2024 SER Communication networks and systems for power utility automation*. Von <https://www.vde-verlag.de/iec-normen/211712/iec-61850-2024-ser.html> abgerufen
- Internationale Normenreihe für Cybersecurity in der Industrieautomatisierung, IEC 62443. (15. 06 2020). *Internationale Normenreihe für Cybersecurity in der Industrieautomatisierung, IEC 62443*. Von <https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung> abgerufen
- ISO/IEC 27001:2022. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Von <https://www.iso.org/standard/27001> abgerufen
- IT-Grundschutz-Kompodium – Werkzeug für Informationssicherheit. (2023). *Bundesamt für Sicherheit in der Informationstechnik*. Von [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html) abgerufen
- NIST SP 800-30. (16. 01 2020). *NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments*. Von National Institute of Standards and Technology (NIST): <https://www.nist.gov/privacy-framework/nist-sp-800-30> abgerufen
- Referentenentwurf KRITIS-Dachgesetz. (10. 04 2024). *Referentenentwurf des Bundesministeriums des Innern und für Heimat „Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen*. Von <https://ag.kritis.info/2023/07/18/referentenentwurf-des-bmi-kritis-dachgesetz-kritis-dachg/> abgerufen
- Referentenentwurf NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz. (24. 06 2024). *Referentenentwurf des Bundesministeriums des Innern und für Heimat „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des*

*Informationssicherheitsmanagements in der Bundesverwaltung*. Von <https://ag.kritis.info/wp-content/uploads/2024/06/NIS2-Referentenentwurf-Bearbeitungsstand-24.06.2024-16-13.pdf> abgerufen

Yaqoob, T., Arshad, A., Haider, A., Amjad, M. F., & Shafqat, N. (2019). *Framework für Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations*,. <https://www.sciencedirect.com/science/article/abs/pii/S0167739X18312081?via%3Dihub>. Von <https://doi.org/10.1016/j.future.2018.12.033> abgerufen

# Abkürzungen

<b>BBK</b>	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
<b>BCM</b>	Business Continuity Management
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik
<b>BSIG</b>	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
<b>DMZ</b>	Demilitarisierte Zone
<b>HMI</b>	Human-Machine Interface
<b>ICS</b>	Internet Connection Sharing
<b>IDS</b>	Intrusion Detection System
<b>IEC</b>	International Electrotechnical Commission
<b>IPS</b>	Intrusion Prevention System
<b>ISO</b>	International Organization for Standardization
<b>KPI</b>	Key Performance Indicator
<b>KRITIS</b>	Kritische Infrastrukturen
<b>KRITIS-Dachgesetz</b>	Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen
<b>NIS</b>	Network and Information Security
<b>NIS2UmsuCG</b>	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
<b>NIST</b>	National Institute of Standards and Technology
<b>RCE</b>	Resilience of Critical Entities
<b>RoI</b>	Return on Investment
<b>RoSI</b>	Return on Security Investment
<b>SIEM</b>	Security Information and Event Management
<b>SOC</b>	Security Operations Center
<b>SPS</b>	Speicherprogrammierbare Steuerung
<b>SzA</b>	System zur Angriffserkennung
<b>VLAN</b>	Virtual Local Area Network
<b>VM</b>	Virtual Machine
<b>VPN</b>	Virtual Private Network

# Glossar

Begriff	Definition
BSI 200-3	Der BSI-Standard 200-3 „Risikoanalyse auf Basis von IT-Grundschutz“ beschreibt ein Vorgehensmodell zur Erstellung und Durchführung von Risikoanalysen aufbauend auf einer IT-Grundschutzerhebung.
Conduit	Nach IEC 62443 ein gesicherter Übergang bzw. eine gesicherte Verbindung zwischen zwei Netzwerken
DMZ	Demilitarisierte Zone als speziell gesichertes und überwachtetes Netzwerk, das in der Regel zwischen öffentlichen und privaten Netzwerken verortet ist
E VDE-AR-N 4143-2	Die VDE-Anwendungsregel „Sicherheit im Stromnetz – Risikomanagement des Netzbetreibers“ (E VDE-AR-N 4143-2) dient dazu, Gefährdungen in den betrieblichen Abläufen des Netzbetriebs zu identifizieren und zu bewerten und die daraus resultierenden Risiken zu minimieren.
Feldbus	Kommunikationsbus (allgemein Datenübertragungssystem) zur Kopplung von Messsensoren oder Stellgliedern (z. B. Schaltern) mit Leitgeräten
Feldleitgerät	Geräte zur Erfassung von Messdaten oder zur Ausführung von Steuersignalen bzw. Befehlen im Feld
HMI	Mensch-Maschine-Schnittstelle, englisch: Human-Machine Interface (z. B. Konfigurationsoberfläche für Geräte)
IEC 62443	Die Normenreihe IEC 62443 behandelt Aspekte der IT-Sicherheit von „Industrial Automation and Control Systems“ (IACS) und beschreibt einen ganzheitlichen Ansatz für Betreiber, Integratoren und Hersteller.
ISO 27001	Die internationale Norm ISO/IEC 27001 legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines dokumentierten Informations-Sicherheits-Management-Systems im Kontext einer Organisation fest.
Leitsystem	System zur Überwachung und Steuerung elektrischer Netze unter Erfüllung verschiedener Betriebsführungsaufgaben (z. B. Leistungs-Frequenz-Regelung)
NIS2UmsucG	Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)
Patch	Ein Patch ist eine Software-Aktualisierung, die Fehler behebt, Sicherheitslücken schließt oder Funktionen verbessert.

Begriff	Definition
SOC	Security Operations Center, umfasst alle organisatorischen und technischen Maßnahmen zum Schutz eines Unternehmens vor internen und externen IT-Angriffen
SPS	Speicherprogrammierbare Steuerung, enthält Programme zur Steuerung oder Regelung von Geräten (z. B. Schutzgeräte)
Terminalserver	Zentrale Bereitstellung und Verwaltung von Software für Endgeräte (Clients)

