

NIS-2 HANDLUNGSLEITFADEN

**Hilfestellung zum Verständnis und zur Umsetzung
der
Anforderungen aus dem NIS-2 Umsetzungsgesetz
für
"wichtige und besonders wichtige
Einrichtungen"**

Version 1.0

Autor: Bernhard Barz, Security-System Engineering

Inhaltsverzeichnis

Vorwort	4
1 Aufbau.....	5
2 Zweck, Zielgruppe und Anwendung.....	6
3 Regulatorischer Ausgangspunkt und zentrale Pflichten	7
4 Security-System Engineering	11
4.1 System Engineering und Security-System	11
4.2 Anwendung im Kontext NIS-2	15
5 Vorgehensmodell zur Umsetzung	17
5.1 Phase 1: Betroffenheit, Scope und Verantwortung	17
5.2 Phase 2: Security-System modellieren	18
5.3 Phase 3: Anforderungen ableiten und priorisieren	19
5.4 Phase 4: Architektur und Maßnahmen gestalten	21
5.5 Phase 5: Nachweise, Wirksamkeit und Assurance planen	23
5.6 Phase 6: Umsetzung, Betrieb und kontinuierliche Verbesserung verstetigen	23
6 Handlungsfelder und Umsetzungshinweise.....	25
6.1 Risikomanagement und Informationssicherheitsstrategie.....	25
6.2 Incident Management.....	27
6.3 BCM/Restore/Recovery	28
6.4 Sicherheit der Lieferkette	29
6.5 Sicherheit bei Beschaffung, Entwicklung und Wartung.....	30
6.6 Bewertung der Wirksamkeit (von Sicherheitsmaßnahmen)	31
6.7 Schulung und Sensibilisierung	31
6.8 Einsatz kryptographischer Verfahren	32
6.9 Personelle Sicherheit, Access- und Asset-Management	32
6.10 Authentifizierung, Kommunikationssicherheit inkl. Notfallkommunikation.....	33
6.11 KRITIS-spezifische Anforderungen und Nachweise	33
7 Road-Map.....	34
8 Vorteile der Anwendung des Security-System Engineering	36

9	Glossar.....	38
10	Literatur.....	42
11	Abkürzungsverzeichnis.....	45
12	Tabellen und Abbildungen.....	46
13	Stichwortverzeichnis	47
	Anhang 1: Resilience im Kontext NIS-2.....	49
	Anhang 1a: Auszug aus KRITIS DachG 16.03.2026.....	52
	Anhang 2: Security-SLA.....	54

Vorwort

Dieser Handlungsleitfaden richtet sich an besonders wichtige und wichtige Einrichtungen sowie an Betreiber kritischer Anlagen, die ihre Pflichten aus dem NIS-2 Umsetzungsgesetz sowie mitgeltende Verordnungen wirksam, nachvollziehbar und dauerhaft in ihre Organisation integrieren wollen. Der Leitfaden gibt einen Überblick über regulatorische Anforderungen und stellt ein Vorgehensmodell zur Umsetzung vor.

Im Mittelpunkt steht die Frage, wie eine Organisation aus regulatorischen Pflichten konkrete Security Anforderungen, Architekturentscheidungen, Prozesse, Nachweise und Managementinformationen ableitet. Dafür werden die Methoden des Security-System Engineering als eigenständiger strukturierender Ansatz genutzt.

Die Grundidee lautet NIS-2 nicht als (Compliance-) Checkliste zu behandeln, sondern einen strukturierten Einstieg in den Sicherheits-Lebenszyklus der eigenen, besonders-wichtigen Dienstleistungen starten. Die NIS-2-Anforderungen sollen hierbei als Bestandteil eines Security-Systems verstanden werden, das Zweck, Scope, kritische Dienste, Stakeholder, Funktionen, Systemelemente, Lieferanten, Schnittstellen, Risiken, Anforderungen, Kontrollen und Evidenzen miteinander verbindet. Dadurch werden Pflichten nicht isoliert dokumentiert, sondern in ein belastbares Sicherheits- und Nachweissystem überführt.

Trotz umfangreicher und sorgfältiger Erfassung und Darstellung, entbindet der Leitfaden nicht von der eigenständigen Prüfung und Referenzierung bestehender rechtlicher Vorgaben.

1 Aufbau

Der vorliegende Handlungsleitfaden folgt drei grundlegenden Handlungssträngen (siehe Abb. 1). Zunächst erfolgt in den Kapiteln 2 und 3 eine Übersicht und Orientierung zu den Anforderungen gemäß NIS-2 Umsetzungsgesetz (nachfolgend NIS2UmsuCG) entsprechend Bundesgesetzblatt Nr. 301 vom 05.12.2025 [1].

Anschließend erfolgt eine kurze Darstellung der Inhalte und Methodik des Security-System Engineering (Kapitel 4).

Im Hauptteil werden ein Vorgehensmodell zur Umsetzung der NIS-2 Anforderungen als Engineering Prozesse (Kapitel 5) sowie konkrete Hinweise zur Umsetzung der Mindestanforderungen gem. NIS-2 Umsetzungsgesetz (Kapitel 6) vorgestellt. Zielsetzung ist die Sichtbarmachung der Zusammenhänge zwischen Anforderungen (Requirements), Funktionen, Architektur, Maßnahmen (Controls) und Nachweisen. Neben der Einbeziehung weitergehender Verordnungen und best-practices-Normen/Standards stellen Sicherheits-Prinzipien (Security-Principles) eine grundlegende Orientierung zu den Umsetzungsarbeiten dar. Dem besonders wichtigen Thema der Nachweisführung und Wirksamkeitsprüfung ist ein eigenes Kapitel gewidmet (Kapitel 7).

In Kapitel 8 erfolgt ein Vorschlag zur zeitlichen Struktur der initialen Umsetzung in Form einer Road-Map.

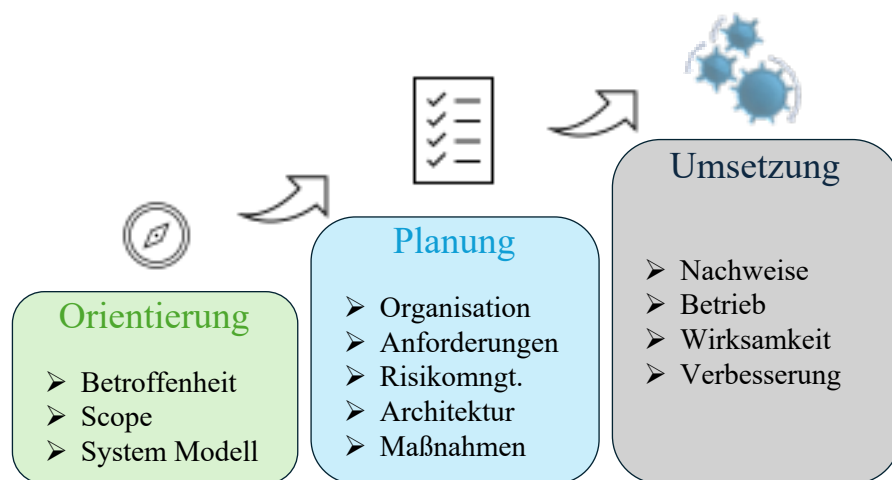


Abb. 1: Handlungsstränge

Eine kurze Zusammenfassung der unterstützenden Ansätze des Security-System Engineering für die komplexen Aufgabenstellungen des NIS-2 (Kapitel 9) sowie ein umfangreiches Glossar (Kapitel 10) runden den Leitfaden ab.

2 Zweck, Zielgruppe und Anwendung

Der Leitfaden unterstützt betroffene Einrichtungen dabei, die NIS-2-Pflichten unter Zuhilfenahme der strukturierten Prozesse und Methoden des Security-System Engineering umzusetzen. Er richtet sich an die im NIS2UmsuCG adressierten Geschäftsleitungen, Compliance- und Datenschutzbeauftragten, die Verantwortlichen für das Informationssicherheitsmanagement sowie die Verantwortlichen für den Betrieb kritischer Anlagen/Systeme und den IT- bzw. OT-Betrieb. Eine erste Übersicht der wesentlichen Aufgaben der verantwortlichen Adressaten ist in Tabelle 1 wiedergegeben.

Adressat	Hauptaufgabe	Referenz NIS2UmsuCG
Geschäftsleitung	- Risikomanagement definieren, umsetzen und überwachen - Teilnahme an Risikomanagement-Schulungen - ISMS-/TOM-/Compliance-Verantwortliche, -Aufgaben und -Ressourcen steuern	§§30, 31 38
Compliance / Datenschutz / Recht	- Betroffenheitsprüfung und Registrierung - Meldepflicht und Dokumentation begleiten	§§28, 32-36, 39,
ISMS-/TOM- Verantwortliche (CISO)	- Prozesse und Maßnahmen definieren (TOM, SzA, Meldepflichten, Nachweise, Audits, Zertifizierungen, etc.) - Umsetzung steuern - Nachweispflichten organisieren und Nachweise sicherstellen.	§§30, 31, 32-36, 39, 41, 52, 61, 62
Operativer Betrieb kritische Anlagen sowie IT- und OT-Betrieb	- Einsatz kritischer Komponenten validieren - SzA-operationalisieren - Technische und organisatorische Maßnahmen umsetzen und testen - Prozesse nachweislich umsetzen	dto.

Tabelle 1: Verantwortliche und Aufgaben

Das NIS2UmsuCG adressiert die Einrichtungen und Betreiber von besonders wichtigen inkl. kritischen Anlagen und Dienstleistungen (nachfolgend "bw-Leistungen"). Hierbei wird gem. §28, Abs. (8) auf die Funktionsherrschaft, d.h. den "bestimmenden rechtlichen, wirtschaftlichen und tatsächlichen Einfluss" abgestellt. Demzufolge liegt die Verantwortung zur Umsetzung der rechtlichen Anforderungen bei den gesetzlichen Vertretern der Einrichtungen (Geschäftsführung, Vorstand). Auf Grund der Auswirkungen und Betroffenheiten unterschiedlicher Organisationseinheiten empfiehlt sich die Etablierung einer operativ koordinierenden Stelle; bspw. CISO.

3 Regulatorischer Ausgangspunkt und zentrale Pflichten

Die EU-Richtlinie (EU) 2022/2555 vom 14.12.2022 (NIS-2 Richtlinie) hat die Zielsetzung, ein EU-weites "hohes gemeinsames Cybersicherheitsniveau sicherzustellen, um so das Funktionieren des Binnenmarkts zu verbessern" [2]. Das Ziel ist es, die Resilienz wichtiger Dienstleistungen und - hierzu erforderliche - Anlagen gegen zunehmende cyber-orientierte Störungen zu stärken und so wirtschaftliche und gesellschaftlichen Beeinflussungen der Digitalisierung entgegenzuwirken.

***Hinweis:** Der in der Informations-/Cybersicherheit neue Begriff "Resilienz" wird in der Richtlinie selbst nicht definiert. Auf Grund der grundlegenden Bedeutung und Auswirkungen auf die Umsetzung der Anforderungen, erfolgt in Anhang 1 eine ausführlichere Erläuterung hierzu.*

Im Folgenden wird Resilienz als Handlungsrahmen verstanden, in dem TOM definiert und umgesetzt werden, um Störungen zu vermeiden sowie Auswirkungen auf die Nutzung wichtigen Dienstleistungen aus Sicht der Leistungsempfänger zu minimieren. Die TOM umfassen wirksam abgestimmte präventive und reaktive technische, organisatorische, personelle und prozessuale (TOPP-) Maßnahmen.

Mit der nationalen Umsetzung der NIS-2 Richtlinie als NIS2UmsuCG wurde der Kreis regulierter Einrichtungen gegenüber den im Vorgängergesetz adressierten Betreibern kritischen Infrastrukturen (KRITIS) deutlich erweitert. Nach allgemeinen Aussagen sind in Deutschland rund 29.500 besonders wichtige, wichtige und kritische Einrichtungen von der neuen Regulierung betroffen [3].

Betreiber kritischer Anlagen bleiben dabei besonders relevant: Sie sind im neuen Regelungsrahmen als besonders wichtige Einrichtungen eingeordnet und müssen neben den allgemeinen NIS-2-Pflichten auch KRITIS-spezifische Anforderungen beachten. Stand 06.07.2026 existiert ein Referentenentwurf vom 26.05.2026 des Bundesministeriums des Inneren zur Bestimmung kritischer Anlagen [4].

Die Zuordnung zum Kreis der betroffenen Unternehmen erfolgt auf Basis der Art und des Umfangs gesellschaftlich relevanter digitaler und nicht digitaler Dienstleistungen. Unterscheidungen in wichtige Einrichtungen (wE) und besonders wichtiger Einrichtungen (bwE) erfolgen anhand von Unternehmensgrößen sowie der Zuordnung zu Sektoren (NIS2UmsuCG, Anlage 1 und 2).

Für Betreiber kritischer Anlagen, bwE und wE besteht eine Registrierungspflicht. Hierzu hat das BSI Online-Hilfsmittel zur Betroffenheitsprüfung sowie zur Registrierung bereitgestellt [5]. Stand Juni 2026 haben sich 17.729 der ca. 29.500 verpflichteten Einrichtung registriert, also ca. 60%.

Zu den zentralen Pflichten gehören (siehe Abb. 2)

- die Registrierung beim BSI,
- die zeitlich definierte Meldung erheblicher Sicherheitsvorfälle,
- die dokumentierte Umsetzung geeigneter, verhältnismäßiger und wirksamer technischer und organisatorischer Risikomanagementmaßnahmen,

- der Einsatz von Systemen zur Angriffserkennung (SzA; explizit für KIRITS-Einrichtungen)
- Umsetzungs-, Überwachungs- und Schulungspflichten für Geschäftsleitungen,
- die regelmäßige Teilnahme an Schulungen zum Risikomanagement durch die Geschäftsleitung sowie
- für wichtige und besonders wichtige Einrichtungen die Dokumentation und Sicherstellung der Nachweisfähigkeit aller Pflichten gegenüber der Aufsichtsbehörde (BSI) sowie - bei KRITIS-Einrichtungen - die regelmäßige Nachweispflicht.

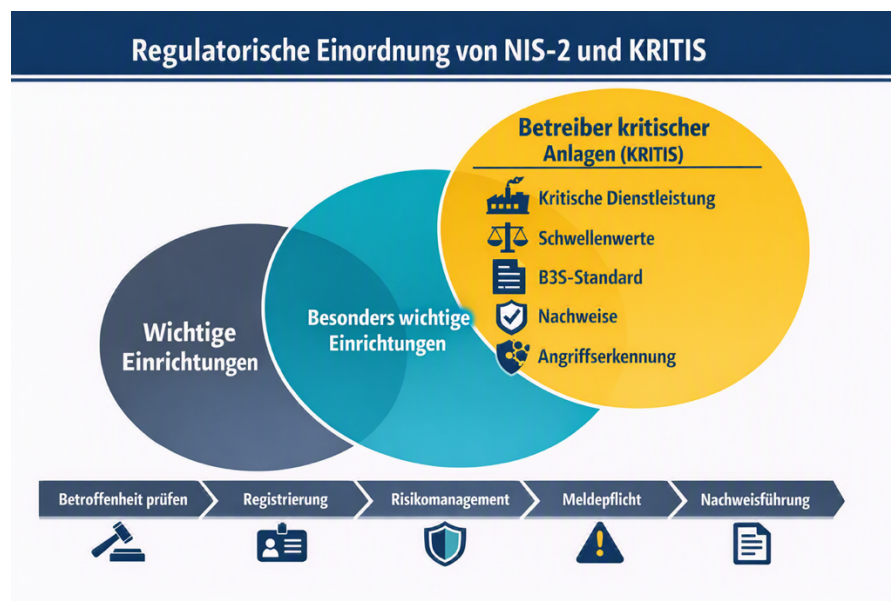


Abb. 2: NIS2-Betroffene

Technische und organisatorische Risikomaßnahmen müssen in Bezug auf Auswirkungen von Sicherheitsvorfällen auf die Dienstleistung und Dienstnutzer geeignet, verhältnismäßig und wirksam sein und einen "gefahrenübergreifenden Ansatz (All-Gefahrenansatz)" anwenden (NIS2UmsuCG, §30, Abs. (2)). Dieser umfasst die "Zielsetzung, sowohl Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen" [2, Art. 21, (2)]. Die Begriffe "geeignet, verhältnismäßig und wirksam" sind für KRITIS, bWE und wE mit unterschiedlichen Ausprägungen belegt; sie müssen als Teil des Risikomanagements durch die Geschäftsleitungen ausgeprägt werden.

Weiterhin sollen der "Stand der Technik" sowie - sofern sinnvoll - einschlägige europäischen und internationale Normen einhalten werden. Die technischen und organisatorischen Maßnahmen müssen mindestens die in Tabelle 2 definierten Handlungsfelder umfassen.

Nr.	Handlungsfeld	Anmerkung
1	Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssystem	gemeint sind übergreifende "policies"
2	Bewältigung von Sicherheitsvorfällen	inkl. Meldeprozesse
3	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	implizit sind Resilienzmaßnahmen und ein BCM gemeint
4	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	- Fokus: Dienstleistung und Dienstnutzer - Umfasst sind somit auch die direkten Anbieter (supplier) und Dienstleister (service provider) aller involvierten Entitäten (Vor- und Nachlieferanten) - Umfasst auch die Beachtung der Ergebnisse gemeinsamer (EU-weiter) Assessments zu Lieferketten
5	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen	Umfasst ist auch die Umsetzung regulatorischer Vorgaben zum Einsatz "kritischer Anlagen, Komponenten oder Dienstleistungen"
6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	
7	Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit der IT-Technik	
8	Konzepte und Verfahren für den Einsatz kryptographischer Verfahren	
9	Konzepte für Sicherheit des Personals, Zugriffskontrolle und die Verwaltung von IKT-Systemen, -Produkten und -Prozessen	Zugriffskontrolle = Access-Mngt = Zutritt-, Zugriff- und Zugangskontrolle
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	

Tabelle 2: Übersicht Mindest-Handlungsfelder

Es ist zu beachten, dass Mindest-Handlungsfelder angegeben werden. Dies bedeutet, dass in Abhängigkeit der Risikoanalyse sowohl weitere Felder hinzukommen können als auch die Ausprägung der Maßnahmen und Prozesse individuell zu definieren ist.

Es ist weiterhin zu beachten, dass die Umsetzung der Maßnahmen und Prozesse von jeder betroffenen, verantwortlichen Einrichtung umzusetzen und nachzuweisen sind. Dies gilt unabhängig davon, ob der Betrieb der Netzwerk- und Informationssysteme in Eigenregie- oder als Outsourcingleistung erfolgt.

Die Meldepflicht betrifft erhebliche Sicherheitsvorfälle. Darunter fallen solche, die schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht haben oder verursachen können sowie solche, die andere natürliche und juristische Personen durch erhebliche materielle und immaterielle Schäden beeinträchtigt haben oder beeinträchtigen können (NIS2UmsuCG, §2, 11.).

4 Security-System Engineering

4.1 System Engineering und Security-System

Die geschäftliche Vernetzung und Digitalisierung, die damit zusammenhängenden internen und externen Gefährdungs- und Beeinflussungsmöglichkeiten (inkl. Supply Chain Probleme), sowie die zunehmenden regulatorischen Anforderungen stellen eine komplexe Aufgabenstellung dar. Das bestehende Arbeits-Modell der "additiven Implementation" von Sicherheitsmaßnahmen in (bestehende) Geschäftssysteme auf der Basis von Maßnahmenkatalogen stößt hier an Grenzen der Beherrschbarkeit. Diese Grenzen werden durch die beiden gegenüberstehenden Perspektiven und teilweise Dilemmata gebildet:

- a) Aus Sicht der Geschäfts-Verantwortlichen bildet sich einerseits eine Fremdbestimmung zur Gestaltung der Businessprozesse durch immer umfangreichere Sicherheitsmaßnahmen. Andererseits ist der Nutzen und die Wirksamkeit von Sicherheitsmaßnahmen nicht ex-ante zu beurteilen. Es bleibt somit oftmals "ein Gefühl" von Unsicherheit.
- b) Aus Sicht der Sicherheitsverantwortlichen ist die reaktive Umsetzung von Sicherheitsmaßnahmen mit der Unübersichtlichkeit der Systemstruktur/-architektur und ggf. Mehrfachimplementierung einzelner Maßnahmen verbunden. Die Darstellung der technischen und wirtschaftlichen Effektivität und Effizienz der Gesamtheit aller Sicherheitsmaßnahmen für die Geschäfts-Prozesse ist schwierig.

Beide Perspektiven führen darüber hinaus zu einer gegensätzlichen Sicht auf die Gesamtverantwortung der Sicherheit aller Geschäfts-Prozesse.

Security-System Engineering (folgend auch SSE) ist ein methodischer Ansatz, mit dem Informations- und Cybersicherheit als gestaltbares System verstanden, beschrieben, umgesetzt und überprüft wird. Der Ansatz überträgt Grundprinzipien des Systems Engineering und des Security Engineering auf Sicherheitsaufgaben. Im Mittelpunkt steht die Anwendung definierter Life-Cycle-Prozessschritte zur Planung, zum Design, zum Betrieb und zur Verbesserung eines Security-Systems. Als Security-System wird hierbei ein strukturelles und funktionales System verstanden, welches die Gesamtheit aller Sicherheitsmaßnahmen zusammenhängend und zielorientiert umfasst. Sicherheit wird also nicht als Add-on zu den Systemen und Prozessen der Geschäftsprozesse definiert, sondern als eigenständige (isolierte) Funktionsebene in Abhängigkeit der Geschäftsanforderungen (siehe Abb. 3).

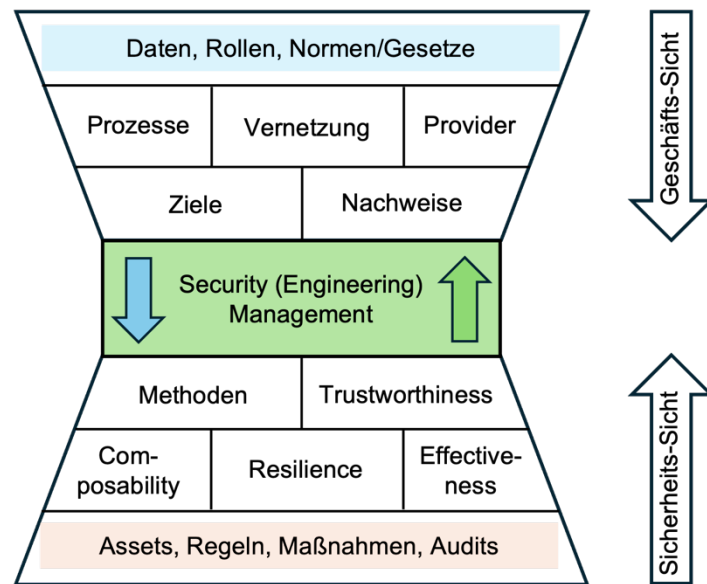


Abb. 3: Neue Sicht auf das Security-Management

Handlungsleitend ist mithin nicht die einzelne Maßnahme, sondern die prozessorientierte Umsetzung der Schritte: Zweck, Anforderungen, Funktionen, Architektur, Controls-Management, Betrieb, Verifizierung und Verbesserungen.

Für das Grundverständnis der Aktivitäten, Methoden und Prozesse des SSE ist ein klares Verständnis einzelner Begriffsbestandteile erforderlich.

Mit **System** sind nicht technische Komponenten wie ein IT-System oder eine Firewall verstanden. Gemäß dem ursprünglichen Wortsinn ist **System** ein Konstrukt aus einzelnen Teilen, die so verknüpft sind bspw. zusammenwirken, dass sie einen (Gesamt-) Zweck erfüllen. Die Verknüpfung bzw. das Zusammenwirken kann hierbei sowohl technisch als auch logisch/funktional definiert sein.

Im technischen Kontext wie auch in der Software-Entwicklung ist der Begriff **Engineering** als methodische und strukturierte Vorgehensweise bereits etabliert (Ergebnis-Orientierung). Sicherheitstechnisch ist der Begriff "**Social-Engineering**" gebräuchlich, wenn Vorgehensweisen zur Evozierung von unerwünschten Verhaltensweisen von Benutzern gemeint sind (Ziel-Orientierung).

In äquivalenter Weise wird mit **Security-System Engineering** die strukturierte Entwicklung von Security-Systemen verstanden, die die Summe aller Sicherheitsanforderungen logisch/funktional umfassen und erfüllen. Zur Anwendung kommen Konzepte, Prinzipien und technische-wissenschaftliche Methoden [6].

Mit der geänderten Perspektive eröffnet sich die Möglichkeit der klareren Zuordnung von Aufgaben, Verantwortungsbereich und -umfang und Handlungsfelder.

Die Trennung auf die jeweiligen (Teil-) Systeme ermöglicht die Entzerrung und Definition der Verantwortungsbereiche für Wirtschaftlichkeit, Performance und Effizienz der jeweiligen Teilsysteme.

Eine Definition der Sicherheitsanforderungen erfolgt aus dem jeweiligen Kontext heraus. Insbesondere für die Geschäfts-Seite ist eine Definition in Form von sog. "loss of ...-Bedingungen" möglich. Gemeint sind im Geschäfts-Kontext die Vermeidung von Störungen, die Sicherstellung der Nutzbarkeit und Kontrollierbarkeit der Betriebsabläufe, die Verhinderung von Daten- oder Ressourcenverluste und weitere. Ein inhärenter Bestandteil der Engineering-Prozesse ist die Übersetzung (Transformation) derart definierter Business-Anforderungen in den Sicherheits-Kontext.

Die Effizienz und Effektivität des Security-System ist an der Schnittstelle durch geschäfts-orientierte Nachweise darzulegen, was mit dem Konzept des Trustworthiness (siehe unten) einhergeht.

Die Definition und das Management des Security-System ist grundlegend zunächst nicht an Maßnahmen (controls) und best-practices gebunden (quasi "control-agnostic"). Als Basis der einzelnen Engineering-Schritte sind definierte und ggf. anzupassende (Security-) Axiome und Prinzipien handlungsleitend.

Die strukturierten Prozesse des Security-System Engineering können aus Engineering Frameworks wie NIST SP 800-160 [7] als sog. System-Life-Cycle-Prozesse bestimmt werden. Dieses umfasst die drei interagierenden Felder **Problem**, **Solution** und **Trustworthiness** sowie das unterlagerte Feld des **Systems Security Analysis** (Abb. 4).

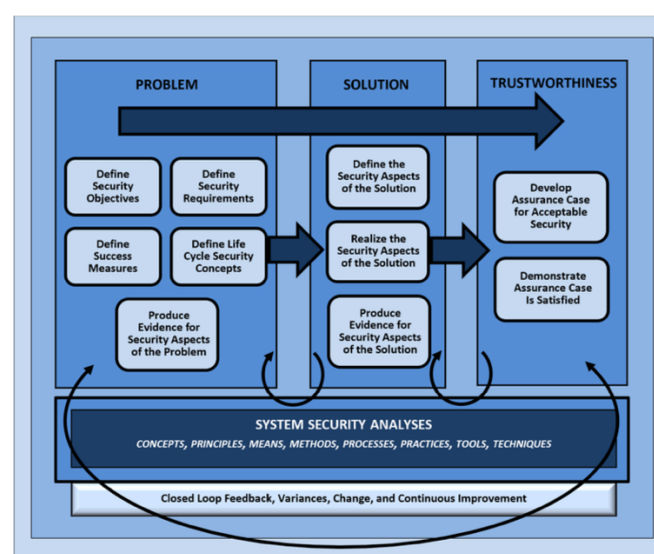


Abb. 4: Engineering-Framework nach NIST SP 800-160 [7]

Mit Bezug auf die o.g. Definition des Security-System Engineering erfolgt die Interpretation der Felder als Bestandteil der SSE-Prozesse wie folgt.

Inhalt des **Problem**-Feldes ist die Definition der Sicherheitsanforderungen aus Sicht der Geschäftsprozesse. Handlungsleitend ist das Ziel eines angemessenen sicheren Systems (adequately secure), welches die Ziele und Sicherheitstoleranzen der Geschäftsverantwortlichen und den Umfang und die Stärke von Sicherheitsmaßnahmen mit Performance- und Nutzungseinschränkungen (constraints) in Einklang bringt. Neben den bereits erwähnten "loss of - Bedingungen" umfasst dies auch die Bereiche Betriebsbedingungen (operational capabilities) und Performance. Darüber hinaus werden hier zu erfassende und nachzuweisende Parameter definiert, die eine Bewertung der Effektivität und Effizienz ermöglichen.

Das Problem-Feld adressiert somit WAS und in WELCHEM Umfang sicherzustellen ist.

Das **Solution**-Feld umfasst die Übersetzung der Sicherheitsanforderungen der Geschäftsverantwortlichen in die Anforderungen des Security-System, der System-Komponenten sowie Vorgaben zur Definition der Architektur. Auch hier werden ergänzend die Parameter definiert und umgesetzt, die die Bewertung des Systems gegenüber den Anforderungen (des Problem-Feldes) sicherstellen.

Das Solution-Feld definiert somit den Lösungsraum, mithin das WIE der Umsetzung der Anforderungen.

Während Problem und Solution überwiegend als Standard-Engineering Methoden bezeichnet werden können, umfasst das Security-System Engineering zusätzlich das **Trustworthiness**-Feld. Hier werden die Nachweise definiert, implementiert/erhoben und bewertet die das Security-System gegenüber den Geschäfts-Verantwortlichen erbringen muss. Aus Sicht der Geschäfts-Verantwortlichen wird hierdurch nachgewiesen (evidence-based), dass das Security-System die Anforderungen erfüllt; es mithin des Vertrauens würdig ist ("The security-system is worth of being trusted").

Den drei Feldern unterlagert sind die Grundlagen der **Security-System Prozesse**. Diese umfassen sowohl

- definitorische Aufgaben, wie einzuhaltende Prinzipien und anzuwendende Risiko-Bedingungen,
- analytische Aufgaben, wie die Bestimmung der System-Kritikalitäten, Effektivitäts- und Resilience-Prüfungen, Risiko-Management, etc. sowie Prüfung von Beeinflussungen von Maßnahmen
- methodische/prozessuale Aufgaben, wie die Definition von Verifikations- und Validierungskriterien.

Alle Aktivitäten der definierten Felder stellen den Kern der Engineering Prozesse eines Security-System dar. Eine Gesamtsicht relevanter Engineering-Prozesse ist in Abb. 5 wiedergegeben. Hierbei sind ebenfalls - wie im Kernmodell nach NIST (Abb. 4) - durch die diversen Rückkopplungsschleifen die Zusammenhänge (Interaktionen) der einzelnen (Teil-)Prozesse, sowie die Rückkopplungen auf Grund von Änderungen/Anpassungen an neue Anforderungen bzw. Verbesserungsschleifen ersichtlich.

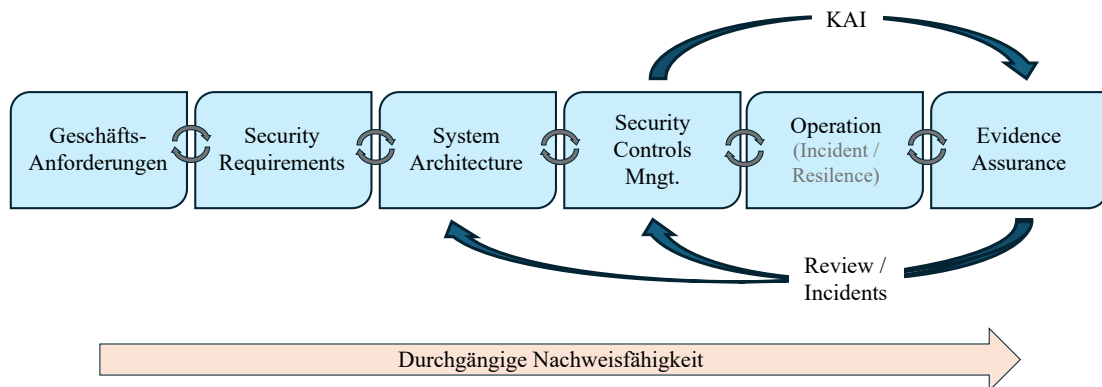


Abb. 5: Engineering-Prozess

4.2 Anwendung im Kontext NIS-2

Zur Transformation der SSE-Prozesse auf die Umsetzung der NIS-2 Anforderungen wird das allgemeine Security-Engineering Modell ([6]; siehe Abb. 6) verwendet. Hierbei ist zu beachten, dass die Aktionen/Aufgaben aus dem Feld "System Security Analysis" als integraler Bestandteil der Felder behandelt werden.

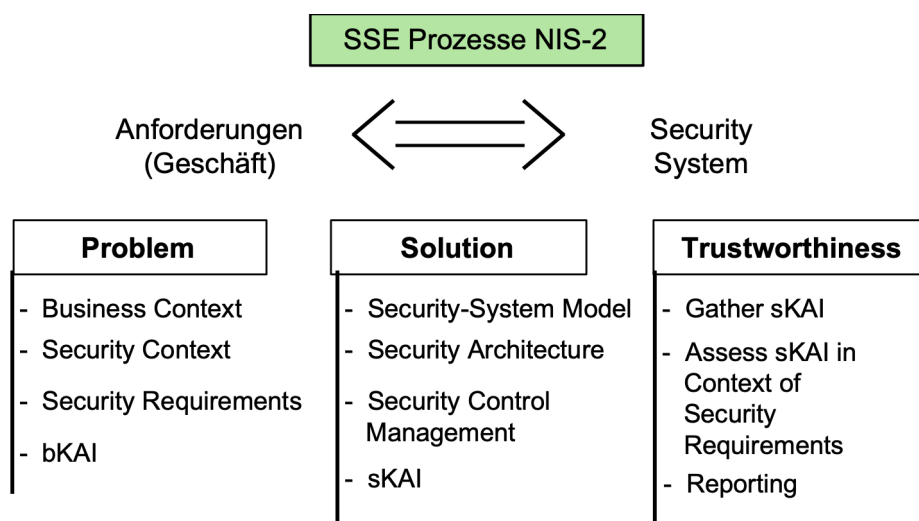


Abb. 6: SSE Prozesse im NIS-2 Kontext

Die Anforderungen des NIS2UmsuCG können initial wie folgt, den einzelnen Feldern zugeordnet werden.

Grundbestandteil des Geschäfts-Kontextes ist die Prüfung der Betroffenheit gem. NIS2UmsuCG. Da es sich i.d.R. um bestehende Infrastrukturen handelt, ist es erforderlich, die betroffenen, NIS2-relevanten Geschäftssysteme und -Prozesse als "System-of-Interest" logisch zu separieren und zu dokumentieren. Dies umfasst insbesondere auch die Supply Chain im rechtlichen Sinne (Empfänger- bzw. Betroffenen-Sicht). Weiterhin ist die Sicherstellung der Schulungspflicht der Geschäftsleitungen, die Überwachung der Risikomanagementaufgaben sowie die Melde- und Nachweispflichten zu managen.

In Praxi wird die Umsetzung der Risikomanagementaufgaben (gem. abgestimmter Vorgaben) dem Security Context zugeordnet, da insbesondere der gefahrenübergreifende Ansatz umfangreiche technische Kenntnisse erfordert. Grundlegend ist hierbei Positionierung aus (Dienste-) Nutzer-Sicht, so dass alle Supply Chain Akteure erfasst werden. Als Zielsetzung für das Security-System wird die Vermeidung von Störungen und die Begrenzung der Auswirkungen (der Dienste) gefordert, wodurch die Stärkung der Resilienz sowie ein BCM-Business Continuity Management impliziert ist.

Die Umsetzung der Anforderungen ist für bwE nach Aufforderung sowie für KRITIS-Einrichtungen zu einem vom BSI definierten Zeitpunkt durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen.

Die Anforderung des NIS2UmsuCG begründen primär ein Security-System Modell, welches auf Dienste-/Funktionserhalt ausgerichtet werden soll.

In Bezug auf die Sicherheitsarchitektur bzw. Sicherheitselemente sind zumindest für KRITIS-Einrichtungen mögliche Vorgaben zu kritischen Komponenten in den Prozessen sowie der Umsetzung zu integrieren.

Als Anforderungen und Vorgaben zum Security Control Management, d.h. der Auswahl und Steuerung der Sicherheitsmaßnahmen sind die Einhaltung des Stands der Technik, die Mindestmaßnahmen gemäß §30, Abs. (2) sowie - für KRITIS-Einrichtungen - der Einsatz von Systemen zur Angriffserkennung (SzA) relevant.

Nach derzeitigem Kenntnisstand sind keine weiteren direkt zuordbaren Anforderungen zu verzeichnen.

5 Vorgehensmodell zur Umsetzung

Das Vorgehensmodell dient der phasenorientierten Strukturierung der technischen, organisationalen, personellen und prozessualen Arbeiten von der initialen Betroffenheitsprüfung bis zum ordnungsgemäßen Regelbetrieb (managed NIS-2-Betrieb). Im Folgenden wird davon ausgegangen, dass alle Geschäftsprozesse etabliert sind und somit der Teil der vorhandenen Infrastruktur und Betriebsprozesse der Einrichtung mit NIS-2-Relevanz integriert ist. Zielsetzung der Arbeiten gem. Vorgehensmodell ist die Schaffung der erforderlichen Transparenz und Nachweismöglichkeit zur Fokussierung und Steuerung der NIS2-relevanten Arbeiten innerhalb der Organisation.

Das vorgestellte Vorgehensmodell umfasst sechs Phasen, deren Abarbeitung linear erfolgen kann, wobei jedoch inhaltlich ggf. Rückkopplungen auf vorherige Phasen zur Anpassung von Entscheidungen erfolgen.

5.1 Phase 1: Betroffenheit, Scope und Verantwortung

Zu Beginn muss die Organisation feststellen, ob sie als wichtige oder besonders wichtige Einrichtung einzustufen ist und ob sie zusätzlich Betreiber kritischer Anlagen ist. Dafür sind die rechtlichen Kriterien Sektor, kritische Anlagen/Dienste und Unternehmensgröße sowie die leistungserbringenden Organisationseinheiten zu erfassen (siehe Tab. 3). Wichtig ist im ersten Schritt ausschließlich auf die kritische Anlage bzw. den kritischen Dienst (§28 NIS2UmsuCG), auf die tatsächliche Funktionsherrschaft über den Betrieb derselben (§2 KRITIS DachG) sowie auf die rechtliche Selbständigkeit der leistungserbringenden Organisationseinheit (§28, Abs. (4) NIS2UmsuCG) zu fokussieren.

Diese Prüfung ist zu dokumentieren, auch wenn das Ergebnis lautet, dass keine Betroffenheit vorliegt.

Prüffeld	Leitfrage	Ergebnis / Inhaltsvorschlag	Verantwortung
Rechtliche Einheit	Welche Gesellschaft ist betroffen?	Registerdaten, Standorte, zentrale Ansprechpartner	Recht/Compliance
Sektor und Einrichtungsart	In welchem regulierten Sektor wird die Leistung erbracht?	Sektor, Branche, Einrichtungsart, Sondertatbestand	Compliance/CISO
Kritischer Dienst	Welche Dienste sind für Kunden, Gesellschaft oder Betrieb wesentlich?	Dienstbeschreibung, Nutzergruppen, Abhängigkeiten	ISMS/BCM
Schwellenwert	Wird ein relevanter Schwellenwert erreicht oder überschritten?	Berechnung, Datenquelle, Bewertungsdatum	Fachbereich/Controlling
Entscheidung	Wer bestätigt Betroffenheit und Scope?	Managementfreigabe, offene Klärungspunkte, nächste Prüfung	Geschäftsleitung

Tabelle 3: Steckbrief Betroffenheit und Scope

Tabelle 3 dient als Grundlage zur initialen Prüfung. Eine erneute Prüfung sollte nach jeder wesentlichen Organisations- oder Architekturänderung erfolgen.

Mit der Festlegung der Betroffenheit bzw. des Betroffenheitsumfangs ist auch definiert, dass die Geschäftsführung bzw. der Vorstand der jeweiligen Einrichtung als Geschäftsleitung die Verantwortung zu den Anforderungen nach §38 NIS2UmsuCG persönlich trägt.

Mit Security-System Engineering wird diese Aufgabe nicht nur als juristische Einordnung, sondern als Scope- bzw. Analyse der Systemgrenzen bearbeitet. Zunächst wird somit festgelegt, welches organisatorische System betrachtet wird: rechtliche Einheit, Geschäftsbereich, kritischer Dienst, Plattform, Standortverbund oder Lieferkettenverbund. Auf dieser Grundlage kann die Organisation nachvollziehbar bestimmen, welche Dienste in den NIS-2-Scope fallen, welche Stellen registrierungs- oder meldebezogen relevant sind und welche Abgrenzungsfragen noch entschieden werden müssen.

Ergebnis der Phase 1:

- E1) Ein Betroffenheits- und Scope-Steckbrief mit kritischer Anlage/Dienstleistung und Organisationseinheit/Betreiber
- E2) Verantwortliche Geschäftsleitung

5.2 Phase 2: Security-System modellieren

Die Phase 2 dient der Präzisierung und der vollständigen Transparenz zu den Grenzen des NIS2-relevanten (Teil-) Systems. Handlungsleitend ist die Erfassung aller Assets und Ressourcen, die einen Anteil an der kritischen Dienstleistung beitragen. Hierbei empfiehlt sich eine zwei-stufige Vorgehensweise.

Im ersten Schritt sind **alle** für die NIS2-relevanten Dienste erforderlichen technischen Assets auf Basis der dienstrelevanten Workflows der einzelnen Funktionen der kritischen Dienstleistung zu erfassen und dokumentieren. Dies umfasst alle IT- und OT-Prozess-Tools, IT-/OT-Systeme, Daten-Systeme, Netzwerke und Dienstleister, die an den geschäftlichen Datenflüssen mittelbar und unmittelbar beteiligt sind. Mittelbar und unmittelbar dient hierbei im Besonderen der Erfassung von Abhängigkeiten, etwa zwischen bzw. zu Fachverfahren, Identitätsdiensten, Cloud-Plattformen, Backup, Netzwerksegmenten (inkl. administrativen Netzen) und externen Administratoren. Sofern interne und externe Systeme und Dienstleister als "shared-services" genutzt werden, sind die übergeordneten Systeme und die Abhängigkeiten hierzu zu kennzeichnen (bspw. Virtualisierungs-, Patch- und Automatisierungssysteme sowie Zugangssysteme).

Als Ergebnis des ersten Schritts existiert eine Darstellung der horizontalen und vertikalen Struktur (Wertschöpfungs-/Funktionskette und beteiligte Services und Funktionen von Dienstleistern) sowie eine Übersichtsdokumentation welche mittelbaren und unmittelbaren (Sub-) Dienste und (Sub-) Dienstleister in die funktionale Erbringung der kritischen Dienstleistung involviert sind. Dies kann als "initiale Architektur der kritischen Dienstleistung" bezeichnet werden.

Im zweiten Schritt erfolgen erste grundsätzliche Entscheidungen ob und welche internen bzw. shared technischen und prozessualen Services für die kritische Dienstleistung separiert, d.h. ggf. redundant installiert bzw. betrieben werden oder integrativ im Gesamtverbund verbleiben. Handlungsleitend sind organisatorische, technische und prozessuale Prinzipien sowie die grundsätzliche Betrachtung der operativen bzw. geschäftlichen Anteils der kritischen Dienstleistung am "Gesamt-Geschäft" der Organisation. Diese Entscheidungen sind pro Funktion zu treffen und für die Validierung in weiteren Schritten - insb. zur Minimierung der Einflüsse und Abhängigkeiten von Sicherheitsmaßnahmen im Sinne der Resilienz - zu dokumentieren

Auf Grund der expliziten Anforderungen an die Lieferkette sind die beteiligten Dienstleister sinnvollerweise separat mit ihrem jeweiligen funktionalen Leistungsanteil zu erfassen. Auf Grund der Definition und des Bezugs der kritischen Dienstleistung bis zum jeweiligen Empfänger/Nutzer sind sowohl vorgelagerte als auch nachgelagerte Dienstleister aufzunehmen. Eine Übertragung von Leistungen und Risiken auf Externe ist gesetzlich nicht vorgesehen.

Ergebnis der Phase 2:

- E3) Initiale Dokumentation zur Architektur der kritischen Dienstleistung
- E4) Dokumentation der "shared Services", die Bestandteil der initialen Architektur sind
- E5) Übersicht aller Dienstleister mit ihrem jeweiligen Leistungsanteil.

5.3 Phase 3: Anforderungen ableiten und priorisieren

Die Phase 3 des Vorgehensmodells dient der Konkretisierung aller Anforderungen und Vorgaben an die weiteren Aktionen zur Bestimmung und Ausprägung der Sicherheitsmaßnahmen der NIS2-relevanten Dienstleistung. Stichworte und Zielsetzung dieser Phase sind die Themen Compliance, Resilience und Transparenz. Die Aufgaben können grob anhand der Themenfelder Vorgaben, Organisation und Nachweise strukturiert werden.

Zu den wesentlichen Vorgabethemen zählen die Methoden zur Ermittlung der Gefährdungen sowie die Kategorisierungen zur Risikobestimmung. Da als übergeordnete Zielsetzung die Vermeidung von Ausfällen bzw. Minimierung der Ausfall-Einflüssen gilt, sind Gefährdungen entsprechend fokussiert

aus geeigneten Gefährdungskatalogen gemäß All-Gefahrenansatz auszuwählen. Dies umfasst insbesondere die Art und der Umfang der Risikoexposition sowie physische, technische und nicht-technische Gefährdungen. Gleichmaßen sind bei der Definition der Risiken neben der (klassischen) Kategorisierung für Eintrittswahrscheinlichkeit und Schadenshöhe auch Ausfalldauern bei Eintritt einer Störung ins Kalkül zu ziehen. Bei der Schadenshöhe ist darüber hinaus der Einfluss (Impact) aus Sicht der Dienstempfänger relevant. Mit Anwendung des Sicherheitsprinzips "assume breach" ist zu entscheiden, ob und in welchem Umfang eine vorgelagerte Kompromittierungs-/Auswirkungsanalyse zur Anwendung kommt. Hierdurch können sowohl die Kritikalität einzelner Komponenten als auch mögliche Exposure-Pfade erfasst werden, so dass dies die Bestimmung von Sicherheitsmaßnahmen fokussiert.

Weitere Vorgabethemen umfassen Festlegungen zu Management-, Betriebs- und Störungs-Management-Maßnahmen und -Prozessen. Grundlegend sind hierbei zunächst Festlegungen zur Anwendung des Stands der Technik bzw. anzuwendender Normen, Standards und best-practices. Hier können Normen wie ENISA-Guidelines, BSI-Grundschutz oder ISO 27001, aber auch ISO 22301 Business continuity management systems [8], die Handreichung "Stand der Technik" Bundesverbands TeleTrust [9] oder auch die Standards der NIST SP800-16 Vol. 1 und Vol. 2 unterstützen.

Weitere organisatorische Anforderungen und Festlegungen umfassen prozessuale Festlegungen zu internen und externen Meldeprozessen zu meldepflichtigen Störungen (Incidents). Auf Grund der engen Meldepflichten sind interne und externe Meldewege sowie Kommunikations- und Dokumentationsfestlegungen vorzuplanen.

Mit der Anforderung zur Eignung, Verhältnismäßigkeit und Wirksamkeit sind insbesondere auch Vorgaben zur Nachweismöglichkeit der Sicherheit zu definieren. Hierzu sind primär Anforderungen in Bezug auf die Definition, Erhebungs- und Bewertungsprozesse zu definieren. Darüber hinaus ist die Definition passender Indikatoren und Nachweise als Randbedingung zur Festlegung von Sicherheitsmaßnahmen erforderlich. Zur Darstellung, Präzisierung und Fokussierung auf die Wirksamkeit der Maßnahmen ist ergänzend zu reinen Sicherheits-Management-Indikatoren die Verwendung der Bezeichnung "KAI - Key Assurance Indicator" angezeigt.

Ergebnis der Phase 3:

- E6) Dokumentation zu Vorgaben hinsichtlich Inhalte und Umsetzungs-Prozesse der regulatorischen Anforderungen (Sicherheits-Policy).
- E7) Definition geeigneter Wirksamkeits-Indikatoren ("KAI - Key Assurance Indicator")

5.4 Phase 4: Architektur und Maßnahmen gestalten

In Phase 4 erfolgt die Ableitung der Sicherheits-Architektur sowie die Definition und Ausprägung der Sicherheitsmaßnahmen. Als Architektur wird in Anlehnung an [7] das Vorhandensein und das funktionale Zusammenwirken aller Maßnahmen zur (Cyber-) Sicherheit der kritischen Dienstleistungen verstanden.

Die Aufgaben der Phase 4 gliedern sich wie folgt:

Ausgehend von den Anforderungsdefinitionen der Phase 3 erfolgt zunächst die Durchführung einer Kompromittierungs-Ausbreitungs-Analyse. Mit den hier als Ergänzung/Präzisierung gefundenen kritischen Komponenten bzw. Gefährdungen erfolgt anschließend die Durchführung der Risikoanalyse und die Bestimmung angemessener/erforderlicher Maßnahmen.

Die Auswahl der Maßnahmen erfolgt unter dem TOPP-Aspekt, d.h. Maßnahmen werden vollständig in dem Sinne definiert, als dass alle verknüpften technischen, organisationalen, personellen und prozessualen Aspekte einer Maßnahme betrachtet und definiert werden. Dies ermöglicht die Erfassung von Wirkzusammenhängen als auch die Struktur und Dokumentation zur Bewertung und Optimierung der Maßnahmenwirksamkeit. Im NIS2UmsuCG wird in §30 (1) auf "Störung(en) der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die für die Erbringung ihrer Dienste genutzt " werden, abgehoben. Hierzu ist zu unterstreichen, dass eben nicht primär auf Daten und Informationen fokussiert wird, sondern im Sinne der Resilienz auf die technische und prozessuale Organisation, welches prinzipiell einer "BIA-business impact analysis" entspricht. Dies ist dann auch handlungsleitend für die Maßnahmenbestimmung. Ein weiterer Aspekt der Anwendung des TOPP-Prinzips ist die Bewertung/Umsetzung der Vorgaben zu Eignung, Verhältnismäßigkeit und Wirksamkeit einer Maßnahme.

Einen besonderen Fokus - ggf. in einer separaten Risikoanalyse - ist auf die mit Vor- und Nachlieferanten verbundene Gefährdungslage gegeben. Die Gefährdungen sind hierbei direkter (bspw. Wegfall der Leistung) als auch indirekter Natur (Vergrößerung der Exposure-Surface).

Eng verbunden mit den Vor- und Nachlieferanten ist die Transparenz und Risikobewertung von Schnittstellen zu internen/externen Netzen und Systemen. Dies dient in Bezug auf shared-Services ggf. zu einer Präzisierung und Neubewertung von Entscheidungen zur Separierung der für shared-Services erforderlichen Assets.

Mit der ersten Übersicht erforderlicher Sicherheitsmaßnahmen inkl. der Wirkzusammenhänge erfolgt ein Abgleich zu Rahmenwerken des "Stand(s) der Technik". Neben den im vorigen Kapitel genannten Standards und best-practices sei hierzu nochmal explizit auf das "Technical Implementation Guidance" der ENISA verwiesen [10].

Mit der Übersicht aller erforderlichen Sicherheitsmaßnahmen erfolgt in der Regel hier eine Priorisierung/Koordination der Steuerung der Umsetzung der Maßnahmen.

Sofern die Organisation über eine bestehende Zertifizierung (BSI-Grundschutz oder ISO 27001) verfügt ist vorab zunächst eine GAP-Analyse als Zwischenschritt angezeigt. Dies hilft der Organisation u.U. bei der Optimierung der Aufwende für Maßnahmen. Es wird hierzu jedoch ausdrücklich darauf hingewiesen, dass die NIS-2-Konformität spezifische Anforderungen enthält, die mit einer bestehenden Zertifizierung in der Regel nicht/nicht umfänglich erfüllt sind. Maßgebliche Themen sind hierbei der scope der NIS-2 Tätigkeiten, die unterschiedliche/fokussierte Interpretation von Sicherheitszielen auf die Resilienz der Dienstleistung, die damit zusammenhängende unterschiedliche Ausrichtung der Risikoanalyse, die Definition von Maßnahmen gem. techn./wirtschaftlicher Angemessenheitsnachweise sowie der damit zusammenhängenden Klarstellung, dass eine Akzeptanz von Risiken an die Angemessenheitsnachweise geknüpft ist; eine Übertragung von Risiken ist normativ gänzlich nicht vorgesehen. Weitere Details und Erläuterungen sind den BSI-Informationsseiten zu entnehmen [11].

Die Kompromittierungs-Ausbreitungs-Analyse sowie die Risiko-Analyse unterliegen einer regelmäßigen Verifizierung und Validierung. So steht für kritische Dienstleistungen eine Regel-Überprüfung alle 4 Jahre an. Darüber hinaus ist ein Review im Sinne der Gesetzes-Konformität nach jedem (mindestens meldepflichtigem) Incident sowie nach Änderungen der Dienstleistungsarchitektur durchzuführen.

Die für KRITIS-Betreiber definierten besonderen Anforderungen (Einsatzvorgaben für kritische Komponenten und SzA-Systeme zur Angriffserkennung) stellen zusätzliche Rahmenbedingungen und Ausprägungen der Sicherheitsprozesse und -maßnahmen dar. Es sei an dieser Stelle darauf hingewiesen, dass durch das NIS2UmsuCG keine Einrichtung/Nutzung eines SOC-Security Operation Center gefordert wird. Weitere Detail werden in Kapitel 6.2 behandelt.

Ergebnis der Phase 4:

- E8) Kompromittierungs-Ausbreitungs-Analyse und Risikoanalyse mit spezifischem Fokus auf Resilienz
- E9) Initiale und bereinigte Übersicht der als angemessen und erforderlich definierten Maßnahmen
- E10) ggf. GAP-Analyse und Auswirkungen auf Maßnahmen bei bestehender Zertifizierung
- E11) Nachweis der Ermittlung/Begründung zu dem Erfordernis und Angemessenheit
- E12) Umsetzungs-Prioritäten-Plan

5.5 Phase 5: Nachweise, Wirksamkeit und Assurance planen

Im fünften Schritt wird definiert und bearbeitet, wie die Organisation nachweist, dass die Anforderungen des NIS2UmsuCG erfüllt sind. Hierzu ist zunächst festzuhalten, dass alle Betreiber kritischer Dienstleistungen zur Vorlage der aller Dokumente verpflichtet sind (KRITIS, §39) bzw. werden können (w-, bw-Betreiber, §61 ff.). Umfasst sind alle Dokumente in Zusammenhang mit der Umsetzung aller Anforderungen, d.h. betroffen sind Vorgabe-, Organisations-, Nachweis- und Betriebsdokumente.

Ein besonderes Augenmerk der Dokumentation besteht hinsichtlich

- der vollständigen Absicherung der Leistungen und Verbindungen zu Vor- und Nachlieferanten,
- der Nachvollziehbarkeit von Entscheidungen zur Angemessenheit von Maßnahmen,
- der Dokumentation von Störungen der kritischen Dienstleistungen inklusive der Bewertung und Ableitung/Umsetzung von Verbesserungsmaßnahmen sowie
- auf die Erfassung, Prüfung und Bewertung der Wirksamkeit der Maßnahmen mit der Geschäftsleitung

Weitere Informationen/Details zu den Themen Nachweisführung, etc. ist Kapitel 7 zu entnehmen.

Ergebnis der Phase 5:

- E13) Vollständige und nachvollziehbare Vorgabe-, Organisations-, Nachweis- und Betriebsdokumente.

5.6 Phase 6: Umsetzung, Betrieb und kontinuierliche Verbesserung verstetigen

Die Umsetzung der NIS-2-Anforderungen ist kein einmaliges Projekt. Anforderungen, Risiken, Lieferanten, Systeme und Bedrohungen ändern sich laufend. Deshalb müssen die Aktivitäten der Phasen 1-5 in regelmäßige Steuerungs- bzw. Managementprozesse integriert werden: ISMS (sofern vorhanden), Risikomanagement, Projekt- und Architekturprozesse, Change Management, Incident Response, BCM, Lieferantenmanagement, Auditplanung und Managementberichterstattung.

Mit Security-System Engineering wird die Verstetigung über geregelte Rückkopplungen gesteuert. Erkenntnisse aus Sicherheitsvorfällen, Übungen, Audits, Schwachstellen, Lieferantenmeldungen, Architekturänderungen, neuen regulatorischen Anforderungen und Managemententscheidungen werden nicht nur als einzelne Maßnahmen verfolgt, sondern auf ihre Wirkung im Security-System geprüft. Die Organisation bewertet dazu, ob Systemzweck, Scope, Requirements, Sicherheitsfunktionen, Architektur, Nachweise oder Restrisiken angepasst werden müssen. Eine Schwachstellenmeldung kann beispielsweise ein neues Requirement, eine Architekturänderung, einen zusätzlichen Test und eine Aktualisierung des Lieferantenmodells auslösen.

Das Ergebnis ist ein kontinuierlicher Verbesserungsprozess, der nicht nur Maßnahmenstatus kontrolliert, sondern das Security-System als Ganzes lernfähig hält.

Ergebnis der Phase 6:

- E14) Interne und externe Auditnachweise zur Wirksamkeit der NIS-2-Maßnahmen
- E15) Nachweis der Modifikation von Sicherheitsmaßnahmen aufgrund definierter Verbesserungsmaßnahmen

6 Handlungsfelder und Umsetzungshinweise

Dieses Kapitel ist als ergänzende Information aufgebaut, welche sich an den Mindesthandlungsfeldern gemäß §30 NIS2UmsuCG orientiert. Zu den einzelnen Handlungsfeldern werden ergänzend zu den Informationen aus Kapitel 5 Umsetzungshinweise in prägnanter Art ausgegeben. Diese gehen ausschließlich auf die spezifischen Anforderungen des NIS2UmsuCG ein, d.h. ein grundlegendes ISMS (nach BSI/ISO 27001) wird als gegeben angenommen. Auf Grund fehlender Erläuterungen im NIS2UmsuCG wird zur Interpretation und inhaltlichen Ausprägung der Handlungsfelder soweit möglich auf die EU-Richtlinie [2] referenziert. Verantwortlich für die Umsetzung der Anforderungen aus dem NIS2UmsuCG sind die Geschäftsleitungen der Organisationen. Auf Grund der Spezifität und des organisationsweiten Charakters erforderlicher Sicherheitsmaßnahmen ist eine übergreifende Koordination über eine zentrale Organisationseinheit sinnvoll und zu definieren; bspw. durch einen CISO

6.1 Risikomanagement und Informationssicherheitsstrategie

Das Risikomanagement des NIS2UmsuCG ist ggü. Standard-Werken wie BSI Grundschutz oder ISO 27001 deutlich unterschiedlich auszuprägen.

Wesentliche spezifische Aspekte der Sicherheitsstrategie umfassen:

S1) Die Ausrichtung auf die Vermeidung von Beeinträchtigungen sowie eine ergänzende Fokussierung auf die Resilienz der Organisation.

In diesem Zusammenhang sind die bisherigen Definitionen der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit deutlich erweitert auszuprägen, da von einer daten-/informationszentrierte Definition zu einer leistungs- und resilienzzentrierten Definition gewechselt wird.

In gleichem Maße gilt das auch für das (in Teilen des NIS2UmsuCG) Schutzziel der Authentizität. (Letzteres umfasst u.a. Schwellen zur minimalen Leistungserbringung/Betriebsfähigkeit.

S2) Die Erfassung und Regulierung von vor- und nachgelagerten Dienstleistern (supply-chain). Ergänzende Hinweise sind in der BSI-Information zu C-SCRM (Cyber-Supply Chain Risk Management) zu finden (siehe auch Kap. 6.4).

S3) Die Definition standardisierter Rechen- und Entscheidungsverfahren und Kriterien zur Bestimmung der "Angemessenheit" von Sicherheitsmaßnahmen (auf Grund des Wegfalls der Risiko-Behandlungsoptionen Akzeptanz und Übertragung).

- a. Zur Betrachtung der Angemessenheit sind in Bezug auf einzelne Gefährdungen die Summe aller relevanten Sicherheitsmaßnahmen für den Gefährdungskontext heranzuziehen.
- b. Konsequenterweise sind bei der Bestimmung von Sicherheitsmaßnahmen auch Änderungen der Systemarchitektur und Validierungen von shared-services zu erfassen und zu bewerten.

S4) Definitionen und Festlegungen zur Sicherstellung der Wirksamkeit von Sicherheitsmaßnahmen.

Dies umfasst mindestens die beiden Dimensionen Berücksichtigung der Rahmenbedingungen für die wirksame Operationalisierung der Maßnahmen (personelle und prozessuale Rahmenbedingungen, Wirkmaß) als auch geeignete Kriterien zur ex-ante Bewertung im Rahmen interner/externer Audits (Vulnerabilities, Penetrationstests, Hygienemaßnahmen, etc.).

S5) Die besondere Ausprägung des Incident-Managements zur Sicherstellung der Meldepflichten durch Festlegung von Ressourcen, Verantwortlichen und Meldekettten.

S6) Die kritische Prüfung und ggf. Anpassung der Kriterien, Festlegungen und Prozessen zur Business Impact Analyse im Kontext der Maßnahmen zur "Cyber Hygiene" als Baseline der sicheren, resilienten Leistungserbringung.

Zur Umsetzung und regelmäßigen Aktualisierung des Risikomanagements stehen mindestens folgende (Teil-) Aktivitäten an:

R1) Ermittlung und Festlegung der zu betrachtenden Gefährdungen gem. "All-Gefahren-Ansatz". Dies umfasst physische, personelle, it-technische, prozessuale und organisationale Gefahren, die zu einer Beeinträchtigung der Leistungserbringung - aus Sicht der Leistungsempfänger - führen können.

R2) Der Asset-Begriff umfasst im Sinne des "All-Gefahren-Ansatzes" sowohl kritische Dienste, Abhängigkeiten, Lieferanten und Leistungsempfänger als auch Schnittstellen, (kritische) Betriebszustände und mögliche gesellschaftliche Auswirkungen.

R3) Insbesondere zur Erfassung von Gefährdungen durch Dienstleister empfiehlt sich die Orientierung an den Workflows der IT-Leistungsprozesse sowie der OT-Betriebsprozesse (bspw. Patchmanagement).

R4) Mit Anwendung des Prinzips "assume breach" ist eine Kompromittierungsanalyse zur Erfassung kritischer Assets sowie zur Ausprägung von System-, Netzwerk- und Kommuniionsmaßnahmen (Access-Management) sinnvoll.

R5) Eine Kategorisierung der Risiken nach Eintrittswahrscheinlichkeit und Schadenshöhe ist sinnvollerweise an den Dimensionen der Erkennung und des Impacts für die Leistungsempfänger auszurichten

R6) Zur Ermittlung der Sicherheitsmaßnahmen sind sowohl Kataloge wie "Stand der Technik" [9] als auch die Anwendung grundlegender Resilienzprinzipien [12] als auch referenzieren. Die EU-Richtlinie benennt explizit auch die Umsetzung von Sicherheitsmaßnahmen zum "Schutz der Systeme/Assets vor Systemfehlern und Benutzerfehlern (human errors).

6.2 Incident Management

Neben den geforderten Meldepflichten umfasst das NIS2UmsuCG in Bezug auf Sicherheitsvorfälle die Anforderungen "Störungen ... der Erbringung der Dienste ... zu vermeiden" und "Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten". Die EU-RiLi präzisiert das "Incident-Handling" als Maßnahmen und Prozeduren, die dem Ziel der Vorbeugung, Detektion, Analyse und Begrenzung bzw. Reaktion und Wiederherstellung von Incidents dienen. Somit werden folgende spezifische Umsetzungsthemen adressiert.

- I1) Zum Incident-Management ist ein (angemessenes) Monitoring aller Zustände der für kritische Leistungen erforderlichen Assets erforderlich (Lagebild). Dies umfasst mindestens
 - a. ein Management aller erforderlichen Assets (Systeme/Komponenten, Netzwerke, Schnittstellen, Kommunikationsverbindungen, personelle und prozessuale Assets)
 - b. ein Monitoring der Assetstatus (Betrieb, Störung, Ausfall, etc.) mit passenden Alarmierungsschwellen
 - c. ein Monitoring sicherheitsspezifischer Störungen/Ereignisse; bei KRITIS-Organisationen darüber hinaus als SzA - Systeme zur Angriffserkennung verpflichtend.
(weitere Hinweise zum Monitoring sind in [7, 13] zu finden).
 - d. Alarmierungsprozeduren
- I2) Definition von Verantwortlichen und Prozeduren zur Bewertung von Störereignissen.
Die Optimierung der Ressourceneinsätze stellt hierbei eine permanente Rückkopplung zur Konfiguration/Auslösung von Alarmen bzw. deren systemtechnisch zugeordnete Kritikalität dar.
- I3) Zur Begrenzung der Auswirkungen sind präventive technische Aspekte der Systemarchitektur, ggf. automatisierte Maßnahmen zur Begrenzung der Ausbreitung von Störungen (responsive Maßnahmen) und Incident/Notfallprozeduren (Recovery) in Einklang zu bringen.
- I4) Definition und Umsetzung interner und externer Meldeprozeduren. Diese sind im Rahmen von Awarenessmaßnahmen zu simulieren/prüfen.
- I5) Prozessuale Kopplung der Respond/Recover-Prozeduren mit den zeitlich definierten Meldepflichten ggü. dem BSI
- I6) Umfassende Dokumentation des Störfalls; Beachtung
- I7) Im Rahmen der Incident-Behandlung ist sicherzustellen, dass
 - a. mit der Bearbeitung (Respond, Recover) die Sicherheit des Gesamtsystems nicht zusätzlich geschwächt wird
 - b. das Monitoring des Systems sowie die Bewertung weiterer Alarme weiterhin uneingeschränkt erfolgt um Schein-/Ablenkungseffekten entgegenzuwirken.

- I8) Post-Mortem-Analyse in Bezug auf die Angemessenheit und Wirksamkeit etablierter Sicherheitsmaßnahmen; ggf. Initiierung von Anpassungen/Ergänzungen. Die Analyse umfasst hierzu mindestens die Ursache und Ausbreitung, das Vermeidungspotential, die Behebungseffektivität und die Beeinflussung während der Behebung.
- I9) Das NIS2UmsuCG fordert für KRITIS-Einrichtungen in §31 den Einsatz von "Systemen zur Angriffserkennung (SzA)" für die maßgeblichen kritischen Anlagen. Der Aufwand hierfür soll in einem angemessenen Verhältnis zu den Folgen eines Ausfalls/einer Beeinträchtigung stehen. Dazu MÜSSEN " geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfasst und ausgewertet" werden. Weiterhin SOLLTEN die SzA geeignet sein, " fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen". Die Etablierung eines SOC-Security Operation Center wird durch das NIS2UmsuCG nicht explizit gefordert und ist insbesondere in Bezug auf die Ressourcenbindung eines 24/7-Betriebs resp. Auslagerung umfangreicher Protokolldaten bei SOC-as-a-Service mit einem erheblichen Aufwand verbunden.
- Demgegenüber ist abzuwägen, dass die Kritikalität geeigneter Parameter und Merkmale im Prinzip eine kontinuierliche Erfassung aktueller Angriffsvektoren sowie Bewertung und Implementierung voraussetzt. Dies kann und muss konsequenterweise automatisiert erfolgen.

6.3 BCM/Restore/Recovery

Im Kontext des NIS2UmsuCG wird Business Continuity Management als Resilienz Management verstanden. Somit sind folgende wesentliche Aspekte hervorzuheben

- B1) Resilienz hat zum Ziel auch im Störfall eine Mindest-Dienstleistung an die Empfänger zu liefern (die Verfügbarkeit ist immer "größer als Null"). Das Minimum ist durch die Strategie zu definieren und ist damit Anforderung und Maßstab der System-Architektur sowie der operativen Leistungs-Prozesse (siehe auch Anlage 1)
- B2) Die Anforderung "Minimierung der Auswirkungen einer Störung" haben sowohl eine leistungs/(system-)technische als auch zeitliche Dimension. Zu beiden Dimensionen sind sowohl angemessene präventive, detektive als auch reaktive Vorarbeiten zu leisten und - im Sinne von Notfallübungen - zu testen.
- B3) Der Resilience-Lifecycle umfasst im Minimum die Phasen antizipieren, widerstehen, wiederherstellen und anpassen, so dass eine direkte Verknüpfung mit den Monitoring-Maßnahmen des Incident-Managements gegeben ist. Weitere Informationen hierzu sind insbesondere in [14] gegeben.
- B4) Als erwartbarer Nachweis der anforderungsgerechten Umsetzung wären BCM-Unterlagen, Wiederanlaufzielen, Backup- und Restore-Testprotokollen, Krisenstabsübungen, Freigaben des

Fachbereichs und einem Assurance Case zur Wiederanlauffähigkeit kritischer Dienste zu dokumentieren

6.4 Sicherheit der Lieferkette

Die Sicherheit der Lieferkette (supply chain security) ist eine der hervorgehobenen Anforderungen des NIS2UmsuCG. Das Themenfeld umfasst aus System Engineering Sicht drei Bereiche zur Beeinflussung der Sicherheit der kritischen Leistung

- a) Einfluss auf Grund der direkten Beteiligung an der Erbringung der kritischen Leistung (Funktions-sicht)
- b) Beteiligung an/Einfluss auf operative Sicherheit des internen Leistungssystems (System-/Asset-Sicht)
- c) Logische Erweiterung der Grenzen des internen Leistungssystems auf Grund der Kopplung mit dem Supplier Netz (Netz-/System-Sicht)

Insbesondere zu den Punkten a) und c) sind folgende Umsetzungsaspekte hervorzuheben

C1) Das Risikomanagement muss die mit den Aspekten der Beeinflussungsbereichen verbundenen Gefährdungen erfassen.

Die EU Richtlinie adressiert dies als umfassend zu betrachtende Themen in Bezug auf die übergreifende Qualität und Resilienz der kritischen Leistung sowie die Sicherheitsmaßnahmen/das Sicherheitsmanagement der Dienstleister. Zu nennen sind bspw.

- a. Der Funktionsanteil im Workflow der kritischen Leistung
- b. Art und Umfang der Zugänge und Zugriffe auf die Assets des Leistungssystems
- c. Funktionale und unterstützende Datenflüsse
- d. Nachweise zum Sicherheitssystem

C2) Des Weiteren verweist die EU Richtlinie auf die Verankerung der Sicherheitsmaßnahmen in vertragliche Vereinbarungen. Hierzu sind in Anlage 2 ausführliche Hinweise zur Gestaltung eines Security-SLA mit Lieferketten-Dienstleistern aufgeführt.

C3) In Abhängigkeit der Integrationstiefe der Leistungen des Dienstleisters sind das - gegenseitige - Monitoring von Systemstatus, Alarmierungen und Meldekettens zur Einhaltung der gesetzlichen Meldefristen zu gestalten.

C4) Protokollierung der Schnittstellen (permanente und nicht-permanente Zugänge und Zugriffe aller Entitäten).

C5) Definition von initialen Freigabeprozessen für personelle Zugänge/Zugriffe des Dienstleisters sowie zentral kontrollierte, protokollierte und kurzfristig deaktivierbare Zugriffspfade.

- C6) Regelmäßige, nachzuweisende Prüfungen der systemischen und personellen Zugangs- und Zugriffsberechtigungen (Entität, Art und Umfang)
- C7) Protokollierung des Datenverkehrs (insb. in Bezug auf Anomalieerkennungen bei KRITIS-Organisationen)
- C8) Der erwartete Nachweis besteht aus Lieferantenregister, Zugriffsmatrix, vertraglichen Sicherheitsanforderungen, (Re-) Zertifizierungsnachweisen/Auditierungen, Protokollen privilegierter Zugriffe, Schwachstellenkommunikation und Tests von Notfall-Management-Maßnahmen.
- C9) Abschließend ist auch die Relevanz des EU-Cybersecurity-Act zu prüfen/beachten, da hiermit die grundlegenden Prämissen einer EU-weiten Cybersecurity geschaffen wurden. Insofern hat der EU-CSA eine steuernde Funktion auch für die EU NIS-2-Richtlinie. Mit Datum 20.01.2026 hat die EU den Revisionsentwurf CSA-2 veröffentlicht [15]. Mit diesem sollen insbesondere
 - a. der Komplexität und Vielfalt der Cybersicherheitsstrategien sowie
 - b. der Erhöhung der Sicherheitsrisiken in IKT-Lieferketten

begegnet werden. Ein besonderer Fokus wird hierbei auf nicht-technische Kriterien und Maßnahmen gelegt.

6.5 Sicherheit bei Beschaffung, Entwicklung und Wartung

Besonders hervorzuhebende Hinweise ergeben sich insbesondere aus den Anforderungen des §41 NIS2UmsuCG

- D1) Etablierung eines permanenten Prüfprozesses zu Untersagungen des Einsatzes kritischer Komponenten
- D2) ggf. Etablierung einer besonderen Freigabe-/Risikoprüfung für umfangreiche Beschaffungen spezifischer Komponenten/Systemassets
- D3) Sicherstellung der Etablierung kontrollierter operativer Prozesse hinsichtlich Patch- und Update-Implementationen (Quellenidentifizierung, Integrität der Patch-/Updatedateien)
- D4) Darüber hinaus ist zu prüfen, ob für die Sicherheitsfunktionen kritischen Komponenten ein Prüf- und Freigabeprozess resp. eine unabhängige (CC-) Zertifizierung vor Inbetriebnahme umgesetzt/geprüft wird.

6.6 Bewertung der Wirksamkeit (von Sicherheitsmaßnahmen)

Das NIS2UmsuCG stellt die Wirksamkeit von Sicherheitsmaßnahmen prominent heraus. Damit verbunden sind Definitionen und Umsetzungsaufgaben über den "Life-Cycle" der Sicherheitsmaßnahmen (siehe auch Strategiehinweis S4). Zusätzliche Hinweise sind

- T1) In Abhängigkeit der Kritikalität einer Sicherheitsmaßnahme sind bereits mit der Definition und Operationalisierung Evidence-Kriterien für eine Erfassung und Bewertung zu definieren und umzusetzen. Der Fokus ist hierbei auf die Resilienz der Leistungserbringung auszurichten.
- T2) Wirksamkeitsprüfungen sind sowohl an Incidents als auch an Vulnerability-Prüfungen, Penetrationstests und Hygienemaßnahmen auszurichten.
- T3) Die Nutzung von "Assurance-Cases" als Review-Methode sollte geprüft werden; hierdurch kann die Nachweisfähigkeit der Wirksamkeit von Maßnahmen gestärkt werden. (Assurance-Cases können bspw. Restore-Tests, Tabletop-Übungen oder SIEM-Use-Case-Tests sein).
- T4) Die Priorisierung des Anpassungsbedarfs an Sicherheitsmaßnahmen sowie die Etablierung zusätzlicher Maßnahmen ist sowohl an die Ergebnisse der Bewertung von Incidents (post-mortem Analyse) als auch regelmäßige Reviews/interne Audits zu orientieren.
- T5) Die Erfassung, Bewertung und Priorisierung von Anpassungen an Sicherheitsmaßnahmen ist zu Nachweiszwecken strukturiert und vollständig zu dokumentieren.
- T6) Die BSI Vorgaben zu Grundsätzlichen Anforderungen im Nachweisverfahren (GAiN, [16]) sowie das Schema zur Reife- und Umsetzungsgradbewertung (RUN, [17]) sollten zur Strukturierung interner Audits angewandt werden (verpflichtend für KRITIS-Organisationen).

6.7 Schulung und Sensibilisierung

Zu den Schulungen im Bereich der Sicherheit der Informationstechnik sind folgende Hinweise zu beachten.

- H1) Schulungen umfassen sowohl externe (Aus-/Weiterbildung) als auch interne Schulungen.
- H2) Der Inhalt der Schulungen umfasst alle operativen Arbeitsaspekte; eine Strukturierung entsprechend organisatorischen Rollen und Aufgaben (Administration, Risikomanagement, Security-Prinzipien, Architektur, Netzwerk, etc.) ist sinnvoll.
- H3) Als Sensibilisierungen sind Awarenessschulungen für alle organisatorische Rollen sowie insbesondere Schulungen zur Detektion von Mustern und Auffälligkeiten/Anomalien im Incident-Life-cycle umzusetzen.
- H4) Nachweise zu Schulungen sollten sowohl Schulungsplan und Teilnahmebescheinigungen als auch Kompetenzmatrizen zu sicherheitsrelevanten Aufgaben organisatorischer Rollen umfassen.

6.8 Einsatz kryptographischer Verfahren

Anforderungen zu kryptographischen Verfahren und Verschlüsselung umfassen den Einsatz in Authentisierungs- und Kommunikationsverfahren sowie zum Datenschutz. Besondere Hinweise sind

- K1) Prüfung/Bewertung des Risikos zur Schlüsselgenerierung und -speicherung durch Dienstleister (Exklusivität der Schlüssel)
- K2) Einsatz sicherer und zukunftsfähiger Verschlüsselungsverfahren
- K3) Sichere Generierung und Aufbewahrung von Schlüsselmaterial
- K4) Nachweis der regelmäßigen Prüfung kryptographischer Verfahren hinsichtlich Verfahren und Schlüssellängen
- K5) Weitere relevante Hilfestellungen sind den Technischen Richtlinien des BSI (BSI TR-02102-1, [18]) zu entnehmen.

6.9 Personelle Sicherheit, Access- und Asset-Management

Die Präzisierung dieser Anforderung gemäß der RU-Richtlinie führt zu einer differenzierteren Sicht auf §30, Abs. (2) lit 9 NIS2UmsuCG. Wesentliche Elemente hierzu sind

- A1) Die personelle Sicherheit umfasst eine Konzeptionierung von Maßnahmen entsprechend der Kritikalität der personellen Rollen und Aufgaben (Rollenkonzept). Hierzu gehören bspw. auch die Abfrage polizeilicher Führungszeugnisse, etc. sofern nicht im Widerspruch zu weiteren gesetzlichen Regelungen
- A2) Access-Management umfasst die Steuerung von Zutritts-, Zugangs- und Zugriffsberechtigungen (Gebäude/Räume, Systeme, Daten). Zugangs- und Zugriffsberechtigungen sind hierbei nicht auf personelle Berechtigungen beschränkt; maßgeblich sind auch alle technischen und "prozessualen" Berechtigungen wie bspw.
 - a. Ausführungen von Programmen, .exe-Dateien, Makros
 - b. Ausführung von Patch- und Updateprozeduren
 - c. Ausführung von Systemtools (PowerShell, rdp, etc.)
- A3) Asset-Management umfasst alle Assets, zur Erbringung der (kritischen) Dienstleistung erforderlich sind (technische, personelle und prozessuale Assets). Mit Bezug auf den Incident-LifeCycle sind auch Informationsquellen zu Schwachstellen, Kompromittierungskriterien, etc. den erforderlichen Assets zuzuordnen (Threat Intelligence Assets).

A4) Zu den Nachweisen dieser Anforderungen sind sowohl die Konzepte als auch die wirksame Umsetzung vorzuhalten (FreigabeprozEDUREN, regelmäßige Audits, Anpassungen von Maßnahmen).

6.10 Authentifizierung, Kommunikationssicherheit inkl. Notfallkommunikation

Diese Anforderungen fokussieren auf die Absicherung der organisationalen und operativen Kommunikationsverfahren und -strukturen (interne und externe Kommunikation). Hierzu sind folgende besondere Hinweise zu vermerken

- M1) Die Anwendung sicherer Authentifizierungsverfahren sollte sowohl personen- als auch systemzentrierte Mechanismen umfassen (MFA, Passkeys, TPM, etc.)
- M2) Anwendung von Zero-Trust-Prinzipien, o.ä. zum Schutz vor Privilege Escalation und Kommunikationspfaden.
- M3) Art und Umfang der Anwendung sicherer Kommunikationsverfahren (inkl. Notfallkommunikation) sind im Einklang mit dem All-Gefahren-Ansatz im Risikomanagement zu definieren (siehe auch R1/R2).

6.11 KRITIS-spezifische Anforderungen und Nachweise

Spezifische Anforderungen und Regelungen für Betreiber kritischer Anlagen sind über die in den vorangegangenen Feldern in den §§ 30, 31, 32, 39, 40, 41 und 56 NIS2UmsuCG definiert. Wesentlich ist, dass die Betreiber von Anlagen regelmäßig die Erreichung der Schwellwerte zur Definition des Status "Betreiber kritischer Anlagen" prüfen.

Auf die Darstellung weiterer besonderer Hinweise wird hier zu Gunsten des Verweises auf die Informationen des BSI [11] verzichtet.

7 Road-Map

Das NIS2UmsuCG geht von einer direkten Umsetzung der Anforderungen aus. Dies bedeutet, dass nach der Registrierung mit dem Aufbau oder der Überarbeitung eines NIS2-ISMS begonnen werden muss. Nachfolgend ist hierzu ein strukturierter Umsetzungsplan dargestellt, der die erforderliche Transparenz über Scope, Anforderungen, Architekturabhängigkeiten und Nachweise zum Ziel hat.

Tag 1 bis 30: Orientierung, Betroffenheit, KRITIS-Status und Scope. In den ersten 30 Tagen sollte die Organisation die NIS-2-Betroffenheit und einen möglichen KRITIS-Status prüfen, Verantwortlichkeiten klären, eine NIS-2- beziehungsweise KRITIS-Kontaktstelle bestimmen, kritische Dienste und kritische Dienstleistungen erfassen, Anlagen- und Schwellenwertinformationen zusammentragen, Registrierungsdaten vorbereiten und einen ersten Security-System-Plan erstellen. Das Ziel ist ein dokumentierter Scope, der von Geschäftsleitung, ISMS-Verantwortlichen und technischen Verantwortlichen verstanden und bestätigt ist.

Tag 31 bis 60: Requirements und Architektur. In dieser Phase werden priorisierte NIS-2-Anforderungen in Security Requirements übersetzt. Für kritische Dienste werden Lieferanten- und Zugriffsschnittstellen sowie eine erste Security-Architekturskizze erstellt. Das Ziel ist, aus regulatorischen Pflichten konkrete, prüfbare Anforderungen und umsetzbare Architekturentscheidungen abzuleiten.

Tag 61 bis 90: Nachweise, Übungen, KRITIS-Prüfvorbereitung und Managemententscheidung. In der dritten Phase werden ausgewählte Anforderungen geprüft. Geeignete Maßnahmen können ein Melde-Prozess, ein Restore-Test, ein Test des Lieferanten-Notfallentzugs oder eine Zugriffsstichprobe umfassen. Für KRITIS-Unternehmen sollte zusätzlich ein Anlagensteckbrief, eine vorläufige Prüfgrundlage, ein Mängel- und Evidenzregister sowie ein Nachweisplan für die kritische Anlage erstellt werden. Für mindestens einen kritischen Dienst oder eine kritische Dienstleistung sollte ein Assurance Case erstellt werden. Das Ziel ist eine Managemententscheidung über Verstetigung, Ressourcen und weitere Umsetzungsprioritäten.

Dieser 90-Tage-Plan ist bewusst minimal gehalten. Er ersetzt keine vollständige NIS-2-Umsetzung, schafft aber eine belastbare Grundlage. Die Organisation gewinnt Klarheit über Betroffenheit, Scope, zentrale Anforderungen, Architekturabhängigkeiten, Nachweise und Managemententscheidungen. Tabelle 4 fasst die Phasen kompakt zusammen.

Zeit- raum	Ziel	Aufgaben	Ergebnis	Verant- wortlich	Sta- tus
Tag 1 bis 30	Betroffenheit, KRITIS-Status und Scope klä- ren	Betroffenheitsprüfung, Kontaktstelle, kritische Dienste, KRITIS-Anlagen, Schwellenwerte, Registrie- rungsdaten erfassen	Bestätigter Scope, offene Klärungs- punkte, erster Security-System- Plan	Geschäfts- leitung / CISO / Compliance	of- fen
Tag 31 bis 60	Requirements und Architektur ableiten	Priorisierte Requirements, Lieferanten- und Zugriffs- schnittstellen, erste Archi- tekturentscheidungen er- stellen	Priorisierte Anfor- derungen, Archi- tekturübersicht, Maßnahmenplan	CISO / IT- Architektur / Betrieb	of- fen
Tag 61 bis 90	Nachweise, Übungen und Managemen- tentscheidung vorbereiten	Tabletop, Restore-Test, Zu- griffsstichprobe, KRITIS- Anlagensteckbrief, Evi- denzregister, Mängelliste, Assurance Case erstellen	Nachweisplan, ge- prüfte Kernanfor- derungen, Manage- mententscheidung	ISMS / Au- dit / Anla- genverant- wortliche	of- fen

Tabelle 4: Initiale Road-Map

8 Vorteile der Anwendung des Security-System Engineering

Die Anwendung von Security-System Engineering bietet bei der Bearbeitung von NIS2-Aufgaben einen erheblichen praktischen Nutzen. Der wichtigste Vorteil besteht darin, dass Anforderungen nicht isoliert betrachtet werden. Jede Pflicht wird in Beziehung zu kritischen Diensten, Stakeholdern, Sicherheitsfunktionen, Architektur, Betrieb, Lieferanten, Nachweisen und Managemententscheidungen gesetzt. Dadurch entsteht ein vollständigeres Verständnis der tatsächlichen Sicherheitswirkung.

Ein zweiter Vorteil liegt in der besseren Beherrschung von Komplexität. NIS-2 betrifft nicht nur einzelne technische Maßnahmen, sondern ganze sozio-technische Systeme aus Menschen, Prozessen, Technologien und Lieferketten. Security-System Engineering macht Abhängigkeiten, Schnittstellen, Vertrauensgrenzen, Betriebszustände und Zielkonflikte sichtbar. Dadurch können Organisationen früher erkennen, wo Risiken entstehen und welche Entscheidungen systemweite Auswirkungen haben. Ein dritter Vorteil ist die bessere Nachweisfähigkeit. Maßnahmen werden nicht erst nachträglich dokumentiert, sondern aus Requirements, Akzeptanzkriterien und Wirksamkeitsannahmen abgeleitet. Verifikation, Validierung und Assurance schaffen eine nachvollziehbare Argumentation, warum eine Maßnahme geeignet ist und worauf sich die Organisation bei Managemententscheidungen, Audits oder Aufsichtsfragen stützen kann.

Ein vierter Vorteil betrifft die Steuerungsfähigkeit der Geschäftsleitung. Durch Lagebild, Assurance Cases und Roadmaps können Risiken, Restrisiken, fehlende Evidenzen und Entscheidungsoptionen verständlicher dargestellt werden. Die Geschäftsleitung erhält damit nicht nur Statusmeldungen, sondern belastbare Entscheidungsgrundlagen.

Schließlich unterstützt Security-System Engineering die dauerhafte Weiterentwicklung. Vorfälle, Schwachstellen, Lieferantenmeldungen, Übungen, Audits und regulatorische Änderungen werden nicht als Einzelfälle behandelt, sondern als Rückkopplungen in ein bestehendes Security-System. Dadurch kann die Organisation Anforderungen, Architektur, Prozesse, Nachweise und Verbesserungsmaßnahmen kontinuierlich anpassen.

Tabelle 5 unterstützt die Kommunikation des Leitfadens gegenüber Management, Fachbereichen und Prüffunktionen.

Stakeholder	Praktischer Nutzen	Beispielhafte Entscheidung	Relevantes Artefakt
Geschäftsleitung	Erhält verständliche Entscheidungsgrundlagen zu Risiken, Ressourcen und Restrisiken	Welche Maßnahmen übersteigen die Angemessenheitsgrenze und welche Maßnahmen werden finanziert?	Managementbericht, Assurance Case, 90-Tage-Plan
CISO / ISMS	Kann Anforderungen, Maßnahmen und Nachweise systematisch steuern	Welche Requirements haben höchste Priorität?	Evidenzregister

IT-/OT-Betrieb	Erkennt, welche technischen Maßnahmen für kritische Dienste wirksam sein müssen	Welche Systeme müssen für Wiederanlauf und Angriffserkennung zuerst abgesichert werden?	Architekturskizze, Anlagensteckbrief
Audit / Compliance	Kann Nachweise früh planen und aufsichtsfähig strukturieren	Welche Evidenz reicht für eine belastbare Prüfung?	Nachweisregister, Prüfplan, Mängel-liste

Tabelle 5: Vorteile Security-System Engineering

9 Glossar

Dieses Glossar erläutert zentrale Begriffe des Schulungskonzepts, des Security-System Engineering und des NIS-2-Handlungsleitfadens. Die Erläuterungen sind praxisorientiert formuliert und verweisen auf einschlägige Standards, Normen und Leitlinien, insbesondere ISO/IEC/IEEE 15288, ISO/IEC/IEEE 24765, NIST SP 800-160, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, BSI IT-Grundschutz und BSI-Standards.

Begriff	Erläuterung	Referenzierte Standards und Normen
Akzeptanzkriterium	Legt fest, wann eine Anforderung als erfüllt gilt. Es verbindet Requirements mit überprüfbaren Ergebnissen, Tests oder Evidenzen.	ISO/IEC/IEEE 15288; NIST SP 800-160.
Architektur	Beschreibt Struktur, Elemente, Beziehungen, Schnittstellen, Verantwortlichkeiten und Prinzipien eines Systems oder Security-Systems.	ISO/IEC/IEEE 15288; NIST SP 800-160; ISO/IEC 27002.
Assurance	Begründetes Vertrauen, dass ein System, eine Funktion oder Maßnahme bestimmte Sicherheitsziele erfüllt.	NIST SP 800-160; ISO/IEC/IEEE 15288.
Assurance Case	Strukturierte Argumentation aus Claim, Argument und Evidence, die eine Sicherheitsbehauptung nachvollziehbar stützt.	NIST SP 800-160; ISO/IEC/IEEE 15288.
Bedrohung	Möglicher Umstand oder Akteur, der ein unerwünschtes Ereignis auslösen kann, zum Beispiel Ransomware oder Lieferantenschwachstelle.	ISO/IEC 27000; BSI IT-Grundschutz; NIST SP 800-160.
Besonders wichtige Einrichtung	Nach NIS-2 beziehungsweise nationalem Recht besonders regulierte Organisation, etwa aufgrund Größe, Sektor, Kritikalität oder besonderer Dienstleistung.	NIS-2-Richtlinie; BSI-Gesetz.
Control	Maßnahme oder Regelung, die Risiken verändert oder reduziert. Controls können organisatorisch, technisch, personell oder prozessual sein.	ISO/IEC 27000; ISO/IEC 27001; ISO/IEC 27002; BSI IT-Grundschutz.
Cyber Hygiene	Cyber Hygiene ist die kontinuierliche, organisationsweit verbindliche Anwendung grundlegender Sicherheitsroutinen durch Menschen, Prozesse und Technik, um alltägliche Cyberrisiken zu vermeiden, Schwachstellen zu begrenzen und die Funktionsfähigkeit der Informationssysteme zu sichern.	EU RiLi 2022/2555 (NIS-2)

Cyber Resilience	Fähigkeit, Cyberangriffe und Störungen so zu bewältigen, dass kritische Dienste aufrechterhalten, wiederhergestellt und verbessert werden können.	NIST SP 800-160 Vol. 2; NIS-2-Richtlinie; BSI-Standard 200-4.
Cybersecurity	Schutz von Systemen, Netzen, Diensten, Anwendungen und Daten vor Cyberbedrohungen.	NIS-2-Richtlinie; NIST SP 800-160; ISO/IEC 27001.
Evidenz	Nachweis, der eine Aussage, Anforderung oder Wirksamkeitsbehauptung stützt, etwa Testprotokoll, Log oder Freigabe.	ISO/IEC 27001; ISO/IEC/IEEE 15288; NIST SP 800-160.
Geschäftsleitungspflichten	Verantwortung, Billigung, Überwachung und Schulung im Hinblick auf Cybersicherheitsrisiken und Risikomanagementmaßnahmen.	NIS-2-Richtlinie; BSI-Gesetz; ISO/IEC 27001.
Incident Handling	Erkennung, Bewertung, Behandlung, Eskalation, Kommunikation und Nachbereitung von Sicherheitsvorfällen.	NIS-2-Richtlinie; ISO/IEC 27035; ISO/IEC 27001; BSI IT-Grundschutz.
ISMS	Managementsystem zur Steuerung der Informationssicherheit mit Politik, Zielen, Rollen, Prozessen, Risikomanagement und Verbesserung.	ISO/IEC 27001; ISO/IEC 27000; BSI-Standard 200-1.
IT-/OT-Technik	Systeme, Komponenten und Prozesse für die Erbringung von Diensten sowie - bei kritischen Anlagen - zur Funktionsfähigkeit derselben erforderlich sind.	BSI-Gesetz
Kontinuierliche Verbesserung	Fortlaufende Anpassung von Anforderungen, Maßnahmen, Architektur, Nachweisen und Prozessen auf Basis neuer Erkenntnisse.	ISO/IEC 27001; ISO/IEC/IEEE 15288; BSI-Standard 200-1.
Lebenszyklus	Phasen eines Systems von Bedarf, Entwicklung, Beschaffung, Integration, Betrieb und Wartung bis zur Außerbetriebnahme.	ISO/IEC/IEEE 15288; NIST SP 800-160.
Lieferkettensicherheit (supply chain security)	Steuerung von Sicherheitsrisiken durch Produkte, Dienste, Dienstleister, Entwicklungsprozesse, Remote-Zugriffe oder Abhängigkeiten Dritter.	NIS-2-Richtlinie; ISO/IEC 27036; ISO/IEC 27001; BSI IT-Grundschutz.
Meldepflicht	Verpflichtung, erhebliche Sicherheitsvorfälle innerhalb vorgegebener Fristen an zuständige Stellen zu melden.	NIS-2-Richtlinie; BSI-Gesetz.
Requirement	Dokumentierte Anforderung an ein System, eine Funktion, einen Prozess oder eine Leistung. Gute Requirements sind eindeutig und prüfbar.	ISO/IEC/IEEE 15288; ISO/IEC/IEEE 24765; NIST SP 800-160.

Resilience	Fähigkeit, Störungen oder Angriffe zu antizipieren, ihnen zu widerstehen, sich zu erholen und sich anzupassen.	NIST SP 800-160 Vol. 2; BSI-Standard 200-4.
Risiko	Wirkung von Unsicherheit auf Ziele; in der Informationssicherheit geprägt durch Bedrohungen, Verwundbarkeiten und Auswirkungen.	ISO/IEC 27000; ISO/IEC 27005; BSI-Standard 200-3.
Schutzbedarf	Beschreibt, wie stark Informationen, Prozesse oder Zielobjekte geschützt werden müssen.	BSI-Standard 200-2; BSI IT-Grundschutz.
Security Requirement	Sicherheitsanforderung aus Schutzbedarf, Risiken, regulatorischen Pflichten, Stakeholder Needs oder Architekturentscheidungen.	NIST SP 800-160; ISO/IEC/IEEE 15288; ISO/IEC 27001.
Security-System	Logisches und funktionales System, mit dem eine Organisation Informations- und Cybersicherheit gestaltet, betreibt, überwacht und nachweist.	NIST SP 800-160; ISO/IEC/IEEE 15288; ISO/IEC 27001.
Security-System Engineering	Anwendung von Systems Engineering und Security-Systems Engineering auf Informations- und Cybersicherheit.	ISO/IEC/IEEE 15288; NIST SP 800-160; BSI-Standards 200-1 bis 200-4.
Sicherheitsfunktion	Fähigkeit des Security-Systems, die zur Erreichung von Sicherheitszielen beiträgt, etwa Erkennen, Reagieren oder Wiederherstellen.	NIST SP 800-160; ISO/IEC 27002; BSI IT-Grundschutz.
System	Kombination zusammenwirkender Elemente, die für einen bestimmten Zweck organisiert sind.	ISO/IEC/IEEE 15288; ISO/IEC/IEEE 24765; NIST SP 800-160.
Systemelement	Bestandteil eines Systems, der eine Funktion oder Teilfunktion erfüllt, etwa Komponente, Prozess, Rolle, Richtlinie oder Dienstleister.	ISO/IEC/IEEE 15288; NIST SP 800-160.
Systemgrenze	Beschreibt, was zum betrachteten System gehört und was als externe Schnittstelle oder Umgebung behandelt wird.	ISO/IEC/IEEE 15288; NIST SP 800-160; BSI-Standards 200-1 und 200-2.
System-of-Systems	Verbund eigenständiger Systeme, die zusammen eine übergeordnete Fähigkeit bereitstellen.	ISO/IEC/IEEE 15288; NIST SP 800-160.
Systems Engineering	Interdisziplinärer, lebenszyklusorientierter Ansatz zur Entwicklung, Realisierung, Nutzung und Außerbetriebnahme von Systemen.	ISO/IEC/IEEE 15288; ISO/IEC/IEEE 24765; INCOSE

		Systems Engineering Handbook.
Validierung	Prüft, ob ein System oder eine Maßnahme den tatsächlichen Bedarf und vorgesehenen Einsatzzweck erfüllt.	ISO/IEC/IEEE 15288; NIST SP 800-160.
Verifikation	Prüft, ob ein System, eine Komponente, ein Prozess oder eine Maßnahme gemäß Spezifikation richtig umgesetzt wurde.	ISO/IEC/IEEE 15288; NIST SP 800-160.
Verwundbarkeit	Schwäche, die durch eine Bedrohung ausgenutzt werden kann; technisch, organisatorisch, prozessual oder personell.	ISO/IEC 27000; NIST SP 800-160; BSI IT-Grundschutz.
Wichtige Einrichtung	Unter NIS-2 beziehungsweise nationalem Umsetzungsrecht regulierte Organisation, die bestimmte Sektor-, Größen- oder Dienstkriterien erfüllt.	NIS-2-Richtlinie; BSI-Gesetz.

10 Literatur

- [1] Bundesgesetzblatt Teil I, Gesetz zur Umsetzung der NIS-2 Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 05.12.2025, Nr. 30, 2025
- [2] RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie); <https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=de>; letzter Abruf 06.07.2026
- [3] Bundesamt für Sicherheit in der Informationstechnik: Zweiter Schritt zur NIS-2-Registrierung: BSI-Portal ab sofort freigeschaltet; https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/regulierte-wirtschaft_node.html; letzter Abruf 03.07.2026
- [4] (beispielhaft) Informationen der AG KRITIS; <https://ag.kritis.info/2026/05/28/referentenentwurf-des-bmi-verordnung-zur-bestimmung-kritischer-anlagen-nach-dem-kritis-dachgesetz-kritisverordnung-kritisv/>; letzter Abruf 06.07.2026
- [5] Bundesamt für Sicherheit in der Informationstechnik: Informationen für regulierte Unternehmen; https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/regulierte-wirtschaft_node.html; letzter Abruf 07.06.2026
- [6] Barz B.; Security-System Engineering Ein Ansatz zu den Grundlagen der Informationssicherheit; Springer Verlag; 2025
- [7] NIST Special Publication NIST SP 800-160v1r1, Engineering Trustworthy Secure Systems, Volume 1, November 2022
- [8] ISO 22301, Security and Resilience - Business continuity management systems - Requirements, Ausgabe 2019
- [9] TeleTrust, Handreichung Stand der Technik in der IT-Sicherheit, <https://www.teletrust.de/publikationen/broschueren/stand-der-technik/>, letzter Abruf 14.09.2026
- [10] ENISA, Technical implementation guidance, Version 1.0, June 2025, https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cyber-security_risk_management_measures_version_1.0.pdf, letzter Abruf 10.09.2026
- [11] BSI, #nis2know-Infopakete, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/infopakete_node.html, letzter Abruf 14.09.2026

- [12] NIST Special Publication NIST SP 800-160v2r1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Volume 2, Dezember 2021
- [13] Barz, Observability, Monitoring aus Systemsicht?!, <https://www.kes-informationssicherheit.de/print/titelthema-die-zeitschrift-fuer-informations-sicherheit/observability-monitoring-aus-systemsicht/>, letzter Abruf 29.09.2026
- [14] Richards M.G, Hastings D.E. et al, Design for Survivability: Concept Generation and Evaluation in Dynamic Tradespace Exploration, Second International Symposium on Engineering Systems, MIT, Cambridge, Massachusetts, June 15-17, 2009
- [15] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2); <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0011>; letzter Abruf 14.08.2026
- [16] BSI, Grundsätzliche Anforderungen im Nachweisverfahren, Version 2.2, Stand 09.07.2026, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/anforderungen_gain_22.pdf?__blob=publicationFile&v=4 , letzter Abruf 01.10.2026
- [17] BSI, Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung (RUN), Version 1.0, Stand 02.01.2025, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/run.pdf?__blob=publicationFile&v=10 , letzter Abruf 01.10.2026
- [18] BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html , letzter Abruf 01.10.2026
- [19] BMI-Bundesministerium des Innern, Schutz kritischer Infrastrukturen, <https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html>, letzter Abruf 13.08.2026
- [20] Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG), Bundesgesetzblatt Teil I, Nr. 66, 16.03.2026
- [21] EU Joint Research Centre, https://joint-research-centre.ec.europa.eu/projects-and-activities/resilience_en, letzter Abruf 13.08.2026
- [22] Manca, A.R., Benczur, P., and Giovannini, E., 2017, Building a scientific narrative towards a more resilient EU society
- [23] Vogel E., Dyka Z., Klann D, Langendörfer P., Resilience in the Cyberworld: Definitions, Features and Models

- [24] MITRE, Cyber Resiliency Framework and Cyber Survivability Attributes, MTR210700R1, <https://www.mitre.org/sites/default/files/2024-01/PR-22-0359-Mapping-Cyber-Resiliency-to-the-CSEIG-CSA-Revision-1.pdf>, letzter Abruf 10.09.2026
- [25] EVB-IT, https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/evb-it-und-bvb/aktuelle_evb-it-node.html, letzter Abruf 13.08.2026
- [26] UP KRITIS, Beispiel für ein Security Level Agreement zum Einsatz in Kritischen Infrastrukturen, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-beispiel-secla.html>, letzter Abruf 13.08.2026

11 Abkürzungsverzeichnis

BCM	Business Continuity Management (Notfallmanagement)
BSI	Bundesamt für Sicherheit in der Informationstechnik
bwE	besonders wichtige Einrichtung
bw-Leistung	besonders wichtige Leistung
CC	Common Criteria
CISO	Chief Information Security Officer
CSA	CyberSecurity Act
C-SCRM	Cyber-Supply Chain Risk Management
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen
GAiN	Grundsätzlichen Anforderungen im Nachweisverfahren
ggü.	gegenüber
IKT	Informations- und Kommunikationstechnik
ISMS	InformationenSicherheitsManagementSystem
IT/OT	Information and Operation Technology (Informationstechnik/Betriebstechnik)
KRITIS	Kritische Infrastrukturen
MFA	Multi Faktor Authentifizierung
NIS	Netz- und Informationssicherheit
NIS2UmsuCG	NIS-2 Umsetzungsgesetz
NIST	National Institute of Standards and Technology
RiLi	Richtlinie
RUN	Reife- und Umsetzungsgradbewertung
Security-SLA	Security Service Level Agreement
SOC	Security Operation Center
SSE	Security-System Engineering
SzA	System zur Angriffserkennung
TOM	Technische und Organisatorische Maßnahmen
TOPP	Technische, Organisatorische, Prozessuale und Personelle Maßnahmen
TPM	Trusted Platform Module
TR	Technische Richtlinie
wE	wichtige Einrichtung

12 Tabellen und Abbildungen

Tabelle 1: Verantwortliche und Aufgaben	6
Tabelle 2: Übersicht Mindest-Handlungsfelder	9
Tabelle 3: Steckbrief Betroffenheit und Scope	17
Tabelle 4: Initiale Road-Map	35
Tabelle 5: Vorteile Security-System Engineering.....	37
Tabelle 6: Resilienz-Definitionen	50
Abb. 1: Handlungsstränge.....	5
Abb. 2: NIS2-Betroffene.....	8
Abb. 3: Neue Sicht auf das Security-Management	12
Abb. 4: Engineering-Framework nach NIST SP 800-160 [7].....	13
Abb. 5: Engineering-Prozess.....	15
Abb. 6: SSE Prozesse im NIS-2 Kontext.....	15

13 Stichwortverzeichnis

Begriff	Kapitel
Access-Management	6.9
All-Gefahrenansatz	3; 5.3; 6.1
Angemessenheit	3; 5.4; 6.1
Architektur	4.1; 5.2; 5.4
Assurance	4.1; 5.5; 6.6
Assurance Case	5.5; 6.6; 7
Asset-Management	5.2; 6.9
Authentifizierung	6.10
BCM	5.3; 6.3
Besonders wichtige Einrichtung (bwE)	2; 3; 5.1
Betroffenheitsprüfung	2; 3; 5.1
CISO	2; 6
Compliance	2; 5.3
Controls	4.1; 5.4
Cyber Hygiene	6.1; 6.6
Cyber-Resilienz	3; 6.3; Anhang 1
Evidenz	4.1; 5.5; 6.6
Geschäftsleitung	2; 3; 5.1; 8
Incident Management	3; 5.6; 6.2
Informationssicherheitsstrategie	6.1
ISMS	2; 5.6; 6
Key Assurance Indicator (KAI)	5.3
Kompromittierungsanalyse	5.3; 5.4; 6.1
Kontinuierliche Verbesserung	4.1; 5.6; 8
Kritische Anlage	2; 3; 5.1; 6.11
KRITIS	2; 3; 6.11; Anhang 1a
Kryptographie	6.8
Lieferkettensicherheit	3; 5.2; 6.4; Anhang 2
Meldepflicht	2; 3; 6.2
Nachweisfähigkeit	3; 5.5; 6.6
NIS-2	1–8
NIS2UmsuCG	1–8
Notfallkommunikation	6.10

Resilienz	3; 5.3–5.4; 6.1; 6.3; Anhang 1
Risikoanalyse	3; 5.3–5.4; 6.1
Risikomanagement	2; 3; 5.6; 6.1
Road-Map	7
Scope	4.2; 5.1; 7
Security-Architektur	5.4
Security Requirement	4.1; 5.3; 7
Security-SLA	6.4; Anhang 2
Security-System	4; 5.2; 8
Security-System Engineering (SSE)	4; 5; 8
Sicherheitsfunktion	4.1; 5.4
Sicherheitsvorfall	3; 6.2
Stand der Technik	3; 5.3–5.4; 6.1
Supply Chain	4.1; 5.2; 6.4
Systeme zur Angriffserkennung (SzA)	3; 6.2; 6.11
Technische und organisatorische Maßnahmen (TOM)	3; 6.1
TOPP-Maßnahmen	3; 5.4; Anhang 1
Trustworthiness	4.1
Validierung	4.1; 5.4
Verhältnismäßigkeit	3; 5.4; 6.1
Verifikation	4.1; 5.4
Wirksamkeit	3; 5.3; 5.5; 6.6
Zero Trust	6.10
Zugriffskontrolle	3; 6.4; 6.9

Anhang 1: Resilience im Kontext NIS-2

Der Begriff Resilience wird im Kontext von Krisen und massiven Störungen auf technischen Systemen durchaus different verstanden. Hierzu ist auch eine Unterscheidung von Resilienz und Cyber-Resilience zu beachten. Im Folgenden werden zunächst einige Definitionen wiedergegeben, bevor eine Arbeitsdefinition zum vorliegenden Kontext dargestellt wird.

In Bezug auf den Schutz kritischer Infrastrukturen definiert das BMI Resilienz als die *"Fähigkeit eines Systems, Ereignissen zu widerstehen oder sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder schnell wiederzuerlangen"* [19]. Dies wird im KRITIS-Dachgesetz umfassender ausgeprägt und "ist „Resilienz“ (als) die Fähigkeit einer kritischen Anlage (verstanden), einen Vorfall zu verhindern, sich vor einem Vorfall zu schützen, einen Vorfall abzuwehren, auf einen Vorfall zu reagieren, die Folgen eines Vorfalls zu begrenzen, einen Vorfall aufzufangen und zu bewältigen und sich von einem Vorfall zu erholen" [20].

Interessanterweise gibt sowohl das NIS-2-Umsetzungsgesetz [1] als auch die zugrundeliegende EU Directive (EU) 2022/2555 sowie die abgelöste EU Directive (EU) 2016/1148 keine eigenständige Definition des Begriffes Resilienz an. Als Grundlage der EU Directive stehen "nur" eine allg. Definition des EU-Joint Research Centre als "Resilience is defined as the ability not only to withstand and cope with challenges but also to undergo transitions, in a sustainable, fair, and democratic manner [21]. Diese Definition basiert auf einem konzeptionellen Rahmenwerk für eine resiliente Gesellschaft der EU (EU JRC Science for policy report), mit der Definition "A resilient society is able to cope with and react to shocks or persistent structural changes by either resisting to it (absorptive capacity) or by adopting a degree of flexibility and making small changes to the system (adaptive capacity) [22].

Auch der Begriff Cyber-Resilienz ist weder im KRITIS-Dachgesetz (Auszug im Anhang 1a) noch im NIS2UmsuCG definiert. Dies unterstreicht, dass der im NIS2UmsuCG definierte All-Gefahren-Ansatz umfassend ist und somit sowohl physische, system-technische, organisationale, personelle und prozessuale Gefahren umfasst (siehe hierzu auch BSI-FAQ zu NIS-2).

Die genannten Definitionen sind in Tab. 6 einmal zusammengefasst, wobei ein Schema von E. Vogel et al. [23] mit folgenden Definitionen (freie Übersetzung) verwendet wird:

Anticipation: Prozess, der darauf abzielt, ein System auf eine Unterbrechung oder einen Angriff vorzubereiten.

Resistance: Fähigkeit, den Auswirkungen einer Unterbrechung oder eines Angriffs zu widerstehen und ein definiertes Maß an Funktionalität aufrecht zu erhalten.

Recovery: Fähigkeit des Systems die verlorene Funktionalität wiederherzustellen.

Adaptation: Fähigkeit eines Systems auf künftige Unterbrechungen/Angriffe effektiver zu reagieren, d.h. mit geringerem Funktionalitätsverlust und geringerer Wiederherstellungszeit.

Detection: Das System ist in der Lage Unterbrechungen oder Angriffe zu erkennen, um angemessene Gegenmaßnahmen zu initiieren.

Quelle	Verhinderung	Schutz	Anticipation (Vorbereitung)	Resistance (abwehren, be- grenzen)	Recovery (auffangen, be- wältigen, erho- len)	Adaption (anpassen, opti- mieren)	Detection (erkennen)
BMI [1]				x	x	x	
KRITIS- DachG [2]	x	x	x	x	x		1)
EU JRC							
EU JRC Sci ²⁾			cope	absorb	react	adapt, transform	

Tabelle 6: Resilienz-Definitionen

1) Die Erkennung von Störungen/Angriffen ist nicht Bestandteil der Definition; sehr wohl jedoch eine Anforderung, die als "Systeme zu Angriffserkennung" für KRITIS-Einrichtungen unmittelbar gilt und für bw-Einrichtungen inhärent aus den Anforderungen zum Vorfallmanagement ersichtlich sind (siehe hierzu auch die Incident-definition aus (EU) 2022/2555, Article 6, (8) [2]).

2) Die vom JRC definierten drei Fähigkeiten (Absorption, Adaption, Transformation) werden hierbei chronologisch in Bezug auf unmittelbare, mittelbare und langfristige Reaktionen auf eine Krise bzw. Maßnahmen zur Minderung künftiger Krisen verstanden.

Zusammenfassend lässt sich feststellen, dass mit dem Begriff und der Zielsetzung der Erhöhung der Resilienz ein vollständiger Lebens-Zyklus-Managementprozess verstanden werden muss. Zu betrachten sind alle physischen, system-technischen, organisationalen, personellen und prozessualen Aspekte, die Einfluss auf die Erbringung kritischer oder besonders wichtiger (Dienst-) Leistungen haben können. Eine Behandlung als Ausprägung des (IT-) Schutzziels "Verfügbarkeit" in Risikoanalysen und Maßnahmenumsetzungen greift deutlich zu kurz.

Im Folgenden wird Resilienz-Definition somit eher als Handlungsrahmen verstanden, in dem Sicherheitsmaßnahmen (TOM) definiert und umgesetzt werden, um Störungen zu vermeiden sowie

Auswirkungen auf die Nutzung wichtigen Dienstleistungen aus Sicht der Leistungsempfänger zu minimieren. Die TOM umfassen wirksam abgestimmte präventive und reaktive technische, organisatorische, personelle und prozessuale (TOPP-) Maßnahmen. Kriterien zur Maßnahmenauswahl und Maßnahmenausprägung ist die Verhältnismäßigkeit in Bezug auf die Auswirkungen und Gefährdungen für die Empfänger und Nutzer der kritischen Dienstleistungen. Das Maßnahmen geeignet sein müssen ist trivial, jedoch im Kontext der Wirksamkeitsprüfungen zu validieren.

Unterstützung zur Auswahl von Maßnahmen und Techniken in Bezug auf die Organisation und Stärkung der Resilienz bieten u.a. die Normen und Frameworks NIST SP 800-160 Vol.2 [12] und MITRE Cyber Resiliency Engineering Framework [24]

Anhang 1a: Auszug aus KRITIS DachG 16.03.2026

§ 13

Resilienzplichten der Betreiber kritischer Anlagen; Resilienzplan

(1) Der Betreiber kritischer Anlagen ist verpflichtet, nach Maßgabe der Absätze 2 und 3 Maßnahmen zur Gewährleistung seiner Resilienz zu treffen, um

1. das Auftreten von Vorfällen zu verhindern,
2. einen angemessenen physischen Schutz von Liegenschaften und kritischen Anlagen zu gewährleisten,
3. auf Vorfälle zu reagieren, sie abzuwehren und die negativen Auswirkungen solcher Vorfälle zu begrenzen und
4. nach Vorfällen die zügige Wiederherstellung der kritischen Dienstleistung zu gewährleisten.

(2) Für die Erreichung der Ziele sind auf Grundlage der nationalen Risikoanalysen und Risikobewertungen sowie der Risikoanalyse und Risikobewertung des Betreibers kritischer Anlagen verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zu treffen. Der Stand der Technik soll eingehalten werden. Insgesamt ist ein Verhältnismäßigkeitsmaßstab anzuwenden. Dabei ist eine Zweck-Mittel-Relation vorzunehmen, bei der insbesondere der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls gegen das Risiko eines Vorfalls abzuwägen ist. Wirtschaftliche Aspekte, darunter die Leistungsfähigkeit des Betreibers, sind zu berücksichtigen.

(3) Zu den Maßnahmen zur Erreichung der Ziele nach Absatz 1 können die folgenden zählen, soweit ihnen nicht bereits bestehende spezialgesetzliche Regelungen in den jeweiligen Branchen vorgehen:

1. zum Zweck der Zielerreichung nach Absatz 1 Nummer 1 zählen Maßnahmen der Notfallvorsorge,
2. zum Zweck der Zielerreichung nach Absatz 1 Nummer 2 zählen:

- a) Maßnahmen der baulichen und technischen Sicherung und des organisatorischen Schutzes (Objektschutz) wie Liegenschaftsabgrenzungen und hemmende Fassadenelemente,
- b) Instrumente und Verfahren für die Überwachung der Umgebung,
- c) der Einsatz von Detektionsgeräten und
- d) Zugangskontrollen,

3. zum Zweck der Zielerreichung nach Absatz 1 Nummer 3 zählen:

- a) Risiko- und Krisenmanagementverfahren und -protokolle und
- b) vorgegebene Abläufe im Alarmfall,

4. zum Zweck der Zielerreichung nach Absatz 1 Nummer 4 zählen:

- a) Maßnahmen zur Aufrechterhaltung des Betriebs, darunter die Notstromversorgung und
- b) die Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wieder aufzunehmen,

5. ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeitenden zu gewährleisten, einschließlich des Personals externer Dienstleister, und

6. das Personal für die unter den in Absatz 1 Nummer 1 bis 4 sowie in Nummer 5 genannten Maßnahmen durch Informationsmaterialien, Schulungen und Übungen vertraut zu machen.

(4) Der Betreiber kritischer Anlagen muss die Maßnahmen nach Absatz 1 in einem Resilienzplan darstellen und diesen anwenden. Aus dem Resilienzplan müssen die den Maßnahmen zugrunde liegenden Erwägungen hervorgehen. Auf die Risikoanalyse und Risikobewertung des Betreibers ist Bezug zu nehmen. Der Resilienzplan ist bei Bedarf sowie nach Durchführung einer Risikoanalyse und Risikobewertung des Betreibers kritischer Anlagen zu aktualisieren.

(5) Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe stellt bis einschließlich 17. Januar 2026 Vorlagen und Muster für die Erstellung von Resilienzplänen auf seiner Internetseite bereit.

Anhang 2: Security-SLA

Zu den Resilienz-Anforderungen betroffener Einrichtungen stehen die (möglichst) kontinuierliche Nutzung der "bw-Leistungen" für den Endkunden im Vordergrund. Als explizite Anforderung nach §30, Abs. (2) NIS-2-UmsuG ist hierbei auch die Sicherheit der Lieferkette ein besonders zu berücksichtigendes Handlungsfeld. Um hier einen konsistenten Sicherheitsprozess zu schaffen, muss die Abhängigkeit von einbezogenen, unmittelbaren und mittelbaren Supplier auch vertraglich an den eigenen Verpflichtungen ausgerichtet werden. Hierzu hat sich der Begriff Security-SLA etabliert, womit eine verbindliche und nachweisbare Vereinbarung über sicherheits- und resilienzrelevante Leistungen, Reaktionszeiten, Mitwirkungspflichten, Nachweise und Eskalationswege gemeint ist.

NIS2 verlangt die Etablierung eines risikobasiertes Sicherheitsniveau für die eigenen bw-Leistungen. Dazu ist zu vergegenwärtigen, dass die Nutzung der "bw-Leistungen" für den Endkunden, eben die gesamte Kette der beteiligten Supplier umfasst, d.h. alle Cloud- und Hosting-Anbieter, Softwarelieferanten, Wartungs- und Fernzugriffsdienstleister, Managed-Service-Provider, Logistikpartner oder sonstige Betreiber. Darüber hinaus und als wichtige Ergänzung zum Fokus auf den Endkunden, sind eben sowohl **Vor- als auch Nachlieferanten** der eigenen Leistung einzubeziehen, d.h. eine End-zu-Ende-Leistungskette. Wenn ein Glied dieser Kette ausfällt, kompromittiert wird oder zu spät informiert, kann die Inanspruchnahme durch den Endkunden gefährdet sein. Security-SLAs machen daher auch sichtbar, welche Beiträge jede Partei zur Absicherung der Endnutzerleistung leistet.

Security-SLAs müssen entlang kritischer Leistungs-, Angriffs- und Verteidigungsketten betrachtet werden. Je stärker ein Supplier an der Erbringung der eigenen "bw-Leistung" beteiligt ist, desto klarer müssen Sicherheitsanforderungen, Mitwirkungspflichten und Nachweisrechte ausfallen.

Auf Grund der Zielsetzung ist deutlich, dass ein Security-SLA auch von einem datenschutzrechtlichen Vertrag zur Auftragsdatenverarbeitung klar abgegrenzt ist. Letzteres regelt den Umgang mit personenbezogenen Daten, während das Security-SLA die operative Sicherheit, Resilienz und Mitwirkung bei Cybervorfällen steuert. Beide Regelwerke müssen zusammenpassen, ersetzen einander aber nicht.

Was in ein Security-SLA gehört

Am Anfang steht die Übersicht über Systeme, Daten, Schnittstellen und Leistungen für die "bw-Leistung". Sinnvoll ist, dies anhand der Wertschöpfungskette einerseits (horizontale Kette) sowie an beteiligten Services und Funktionen der Supplier (vertikale Kette) darzustellen.

Daraufhin können dann Rollen und Verantwortlichkeiten identifiziert werden, mit denen ein Security-SLA entsprechend des Umfangs und Anteils eines jeden Beteiligten festgelegt wird.

Der Kern sind mess- und nachweisbare Details zu Sicherheits- und Resilienzanforderungen für den jeweiligen Anteil zu regeln. Basis hierzu muss eine Risikoanalyse zu möglichen Einflüssen und Auswirkungen im Gesamt-Kontext sein. Geeignete, mit Kennzahlen belegbare Inhalte sind etwa maximale Erstreaktionszeiten je Schweregrad, Fristen für Sicherheitsupdates, Zeitfenster für Schwachstellenbehebung, Verfügbarkeit sicherheitsrelevanter Dienste, Wiederanlaufziele, Protokollaufbewahrung, Meldewege sowie Regelungen zu Sicherheitsberichten, Audits und Nachweisen wie Zertifizierungen oder unabhängigen Prüfungen.

Besondere Aufmerksamkeit erfordert das Incident-Management. Das Security-SLA muss festlegen, ab wann ein Ereignis als sicherheitsrelevant gilt, welche Frühinformationen unverzüglich durch den Supplier bereitzustellen sind und wie laufende Updates erfolgen. Durch den Security-SLA müssen die eigenen Pflichten durch den Supplier optimal unterstützt werden. Dazu gehören mindestens Zeitpunkt und Art des Vorfalls, betroffene Leistungen, erste Bewertung der Auswirkungen, getroffene Sofortmaßnahmen, bekannte Indikatoren, Ansprechpartner, erwartete nächste Schritte und eine Mitwirkung zum Abschlussbericht mit Ursachenanalyse und Verbesserungsmaßnahmen.

Der Supplier muss hierzu qualifizierte Ressourcen bereitstellen, Zugänge zu relevanten Informationen ermöglichen, Logs sichern, forensische Untersuchungen unterstützen und mit Behörden oder Ermittlungsstellen abgestimmt kooperieren. Für kritische Abhängigkeiten sollten ggf. Test- und Notfallübungen geregelt werden.

Schließlich ist je nach Kritikalität eine Ausweitung der Verpflichtungen auf Sub-Dienstleister zu definieren.

Pragmatische Umsetzung

Es empfiehlt sich eine risikobasierte Lieferantenklassifizierung: Standardlieferanten benötigen schlanke Mindestanforderungen, kritische Betriebs- oder IT-Dienstleister dagegen detaillierte Security-SLAs mit klaren Fristen, Berichtspflichten, Auditmöglichkeiten und Eskalationen.

Hilfestellungen und Ausgangspunkt können etwa die aktualisierten EVB-IT-Regelungen [25] oder auch das von UP KRITIS erstellte "Beispiel für ein Security Level Agreement" [26] geben.

Bewährt hat sich ein modularer Ansatz: Ein allgemeiner Sicherheitsanhang definiert Mindeststandards für alle Lieferanten; besondere Anlagen regeln höhere Anforderungen für Cloud, Managed Services, Softwareentwicklung, Fernwartung oder Incident Response. Die Vereinbarungen sollten regelmäßig - längstens jedoch nach meldepflichtigen Ereignissen überprüft und ggf. angepasst werden. Als wichtiger Bestandteil der eigenen Pflichten ist ein Security-SLAs als laufendes Steuerungsinstrument zu verstehen.