Das Kopernikus-Projekt SynErgie

SECURITY GUIDE – SYNERGIE 2.0

KOPERNIKUS PROJEKTE
SynErgie
Die Zukunft unserer Energie

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Autoren:
Fraunhofer-Institut für Integrierte Schaltungen IIS
Andreas Oeder

Software AG
Christian Winter

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Raphael Ahrens

Stand Mai 2022 – Version 1.0

Inhalt

Einleitung **5**

Zusammenfassung **6**

Security Guide **7**

Ziele des Security Guide 7
Anwendungsbereich 7
Umfeldbetrachtungen 10
IT-Sicherheits-Architekturmodell 13
Kryptographische Zertifikate in der ESP 22
SynErgie-PKI – Struktur und Anwendungsmöglichkeiten 23
Vorgehensweise zur Umsetzung der IT-Sicherheit 28
Ermitteln relevanter Assets und Definition von Schutzziele 28
Analyse der Bedrohungen und Schwachstellen 32
Definition der Rollen und Festlegung von Berechtigungen 39
Ermittlung des erforderlichen Sicherheitslevels 44
Prozesse und Anforderungen des Security Life Cycle Managements 58
Beschreibung präventiver Maßnahmen und Empfehlungen 90

Fazit **96**

Literaturverzeichnis **97**

Anhang **102**

Architektur der Energiesynchronisationsplattform 102

Abbildungen

Abbildung 1: Aufbau der SynErgie-PKI 23
Abbildung 2: Schritte zur Umsetzung der IT-Security 28
Abbildung 3: Kategorisierung der Rollen der UP und MP 40
Abbildung 4: Vorgehensmodell zur Bestimmung des Sicherheitslevels 46
Abbildung 5: Schematische Darstellung - Zu evaluierender Service 50
Abbildung 6: Lebensphase im LCM 59
Abbildung 7**:** Phasen des Life Cycle 63
Abbildung 8: Prozesse der Anforderungsphase 66
Abbildung 9: Prozesse der Entwurfsphase 68
Abbildung 10: Prozesse der Entwicklungsphase 72
Abbildung 11: Prozesse der Überprüfungsphase 75
Abbildung 12: Prozesse eines sicheren Deployments 78
Abbildung 13: Prozesse der Betriebs- und Wartungsphase 81
Abbildung 14: Zentrale Rollen zum Betrieb der MP 84
Abbildung 15: Zentrale Rollen zum Betrieb der UP 84
Abbildung 16:Prozesse der Außerbetriebnahme 87
Abbildung 17: Aufbau der MP 102
Abbildung 18: Aufbau der UP 103

Tabellen

Tabelle 1: Einstufung Stromerzeugung und Schwellwerte nach BSI-KritisV 11
Tabelle 2: Empfehlungen zur Rollendefinition 39
Tabelle 3: Sicherheitslevel und resultierende Anforderungen 44
Tabelle 4: Einstufung Erforderliches Sicherheitsniveau 49
Tabelle 5: Risikoklasse resultierend aus Potenzial des Angreifers 54
Tabelle 6: Risikoklasse resultierend aus Wahrscheinlichkeit eines Angriffs 54
Tabelle 7: SL Matrix Festlegungen der Bereiche für Sicherheitslevel 56
Tabelle 8: Legende zu den nachfolgenden Anforderungslisten 63
Tabelle 9: Awarenessprogramm – Schulungen 64
Tabelle 10: Anforderungsphase – Anforderungen 67
Tabelle 11: Entwurfsphase – Sicherheitslevel und Bedrohungsmodellierung 69
Tabelle 12: Entwurfsphase – Security Architecture 69
Tabelle 13: Entwurfsphase – Security Requirements 69
Tabelle 14: Entwicklungsphase – Secure Build 73
Tabelle 15: Entwicklungsphase – Secure Development 73
Tabelle 16: Entwicklungsphase – Präventive Maßnahmen 74

Tabelle 17: Überprüfungsphase – Requirement-driven Testing 76
Tabelle 18: Überprüfungsphase – Security Testing 77
Tabelle 19: Ausbringung – Deployment 79
Tabelle 20: Betrieb und Wartung – Operational Management 82
Tabelle 21: Betrieb und Wartung – Incident Management 83
Tabelle 22: Außerbetriebnahme – Sichere Entsorgung 88

Einleitung

Der Security Guide des Projekts SynErgie 2 bündelt die Ergebnisse aus vorausgegangenen Arbeiten zur IT-Sicherheit. Er soll vorrangig Service- und Plattformentwicklern der Energiesynchronisationsplattform[1] (ESP) als Leitfaden und Handlungshilfe bei der Umsetzung der erforderlichen Maßnahmen zur Erzielung eines erforderlichen Mindeststandards an IT-Sicherheit dienen. Dies gilt für die Unternehmensplattform (UP), die Marktplattform (MP), sowie deren interne als auch externe Services.

Über die reine Entwicklung hinaus betrachtet der Security Guide auch die Sicherheitsaspekte des Deployments, des regulären Betriebs bis hin zur Außerbetriebnahme der Services oder der Plattformen und gibt hierzu Anforderungen und beschreibt Maßnahmen zur Umsetzung.

Ein besonderes Augenmerk gilt dabei dem Bereich der Kritischen Infrastrukturen (KRITIS). Für KRITIS gelten spezielle, gesetzlich verbindliche Vorgaben, wie das IT-Sicherheitsgesetz der Bundesregierung (Bundesrepublik Deutschland 2021a), die Kritisverordnung des Bundesamts für Sicherheit in der Informationstechnik BSI (BSI – Bundesamt für Sicherheit in der Informationstechnik 2021), sowie Vorgaben und Branchenstandards zur Umsetzung der geforderten Maßnahmen. Für den Sektor Energie, Branche Strom ist dies der Bundesverband der Energie- und Wasserwirtschaft (BDEW). Hier ist der Weg zur Umsetzung der IT-Sicherheit verbindlich vorgegeben (bdew 2019).

Für IT-Sicherheit im Umfeld Industrie hingegen zeichnet sich ein anderes Bild, hier legen in der überwiegenden Anzahl die Unternehmen selbst fest, woran sie sich orientieren, um ein ausreichendes Maß an IT-Sicherheit für das Unternehmen umzusetzen. Hierbei können Vorgaben durch die Branche selbst oder aus Kundenbeziehungen entsprechend spezifische Anforderungen gestellt werden. Die Varianten sind hier mannigfaltig.

Im Rahmen der Entwicklung des Sicherheitskonzepts wurde entschieden, dass die ESP sowie deren Komponenten KRITISready umgesetzt werden sollen. Der Begriff KRITISready wurde im Projekt wie folgt definiert: Es bedeutet, dass Anforderungen und Maßnahmen für eine zukünftige Zertifizierung für KRITIS-relevante Systeme konzeptionell definiert und vorgesehen sind, aber aus Kostengründen im Rahmen des Projekts nicht vollständig umgesetzt werden. Zusätzlich ist zu beachten, dass Unternehmen, die bereits Maßnahmen zur IT-Sicherheit ergriffen haben, entsprechende Anforderungen an die IT-Sicherheit der Plattformen stellen, wenn sie die Plattformen ins Unternehmen integrieren sollen oder angebotene Dienste nutzen. Auch diesem Aspekt wird Rechnung getragen.

[1] Die Energiesynchronisationsplattform (ESP) als ganzheitliche, modular erweiterbare IT-Lösung bildet den gesamten Prozess des automatisierten Energieflexibilitätshandels von der Maschine bis zum Energiemarkt ab.

Zusammenfassung

Der Security Guide fasst die Ergebnisse der vorausgegangenen Arbeiten zusammen und dokumentiert als Gesamtwerk Anforderungen und Maßnahmen zur Umsetzung eines angepassten Maßes an IT-Sicherheit für Entwicklung von Services für die ESP und die Komponenten der ESP selbst (UP und MP). Neben der reinen Entwicklung werden auch Anforderungen und Maßnahmen zu Betrieb und Wartung bis hin zur Außerbetriebnahme behandelt.

Der Security Guide bedient sich hierzu zu einem erheblichen Teil der Empfehlungen und Vorgaben aus dem BSI-Grundschutz, relevanter Normen und nationaler, sowie internationaler Behörden und Intuitionen aber auch nicht-behördliche Organisationen zum Thema IT-Sicherheit. Sowohl bei der Definition von Anforderungen, als auch bei der Auswahl und Adaption von Methoden und Verfahren, z.B. bei der Einstufung in Sicherheitsklassen (Sicherheitsklassen, Methoden der Schwachstellenerkennung, Rollendefinitionen, Schutzbedarfsdefinition) werden anerkannte und etablierte Verfahren angewandt oder adaptiert. Ziel ist es, dass im Falle einer späteren Zertifizierung, die Nachvollziehbarkeit der angewandten Verfahren gegeben ist.

Der Security Guide soll es dem Entwickler ermöglichen, ohne sich im Detail in die betrachteten Normen und Richtlinien einzuarbeiten bei der Entwicklung seiner Services einen angemessenen Stand an IT-Sicherheit zu erreichen. Dazu werden im Security Guide einige Methodiken vorgestellt. Für die systematische Erkennung von Schwachstellen und Bedrohungen kommt die Methode des Threat Modelings zur Anwendung. Für eine Klassifikation der erforderlichen IT-Sicherheitsvorgaben sind Sicherheitslevel für die Services definiert. Die Einstufung erfolgt unter Bewertung des erforderlichen Sicherheitsniveaus (dem Schutzbedarf) der von einem Service zu verarbeitenden Daten und Informationen, sowie dem potenziellen Risiko eines Angriffs, dem der Service im Betrieb ausgesetzt ist oder sein kann. Das Life Cycle-Management betrachtet den gesamten Lebenszyklus eines Service und stellt Anforderungen für jede Lebensphase, damit ein festgelegter Sicherheitslevel über die gesamte Lebensphase aufrechterhalten bleibt.

Security Guide

Ziele des Security Guide

Der Security Guide hat das Ziel, Plattform- und Service-Entwicklern und, mit Einschränkungen auch, Betreibern der Marktplattform und der Unternehmensplattform eine Handlungsanleitung an die Hand zu geben, um Service-Entwickler und Betreiber der ESP hinsichtlich der IT-Sicherheit und der Bedrohungen zu sensibilisieren und das notwendige Mindestmaß an IT-Sicherheit für die Services der UP und MP, bei der Entwicklung und beim Betrieb zu erreichen. Zusätzlich soll der Security Guide einen Einblick in die unterschiedlichen Anforderungen und Maßnahmen an die IT-Sicherheit zwischen dem industriellen Umfeld und den Vorgaben zu Kritischen Infrastrukturen vermitteln.

Der Security Guide bündelt die Ergebnisse, die im Projekt SynErgie 2 und dem Vorgänger-Projekt SynErgie 1 zum Thema IT-Security erarbeitet wurden. Der Security Guide kann dabei nicht alle Aspekte vollumfänglich betrachten und verweist an geeigneten Stellen auf zusätzliche Standards, Richtlinien und Empfehlungen.

Anwendungsbereich

Der Leitfaden wendet sich in erster Linie an die Plattform- und Service-Entwickler der ESP. Dabei handelt es sich sowohl um die Entwickler von Services, die direkt auf der Unternehmensplattform ausgeführt werden aber auch Services von externen Servicedienstleistern, zu denen die Unternehmensplattform eine Verbindung aufbaut. Gleiches gilt für Services, die auf der Marktplattform ausgeführt werden.
Die nachfolgend vorgestellten Maßnahmen umfassen in Summe alle Lebensphasen des Life Cycle Managements, der Fokus liegt jedoch bei der Entwicklung und dem regulären Betrieb der Plattformen der ESP und deren Services. Die vorgeschlagenen Vorgehensweisen und Maßnahmen haben zum Ziel, die ESP-Plattform KRITISready zu entwickeln, dies bedeutet, dass der Schritt zu einer Zertifizierung für den Einsatz in Kritischen Infrastrukturen vorbereitet ist und sich an den Vorgaben orientiert, diese aber nicht vollumfänglich aufgreift und beschreiben kann. Auf die IT-Sicherheitsanforderungen auf der Organisationsebene wird nur dort eingegangen, wo es die Betriebsphase betrifft. Ist eine verbindliche Anwendung des Security Guides gewünscht, muss dies durch zusätzliche Maßnahmen erfolgen, die nicht Bestandteil des Leitfadens selbst sind. Die Verbindlichkeit wäre im Rahmen einer Forderung nach einer „SynErgie-Zertifizierung“ für Services durchsetzbar.
Der Security Guide folgt dem Gedanken, dass die IT-Sicherheit für die ESP auf folgenden Säulen beruht:

- **Organisatorische Maßnahmen**: Richtlinien, Mitarbeiterschulung (Awareness schaffen)
- **Hohe Softwarequalität**: Sicherstellung der Funktion und Vermeidung von Schwachstellen
- **Identitäts- und Zugriffsverwaltung**: Rechtemanagement und Zugriffsschutz
- **Kryptographie:** Implementierung kryptographische Verfahren zur Gewährleistung von Manipulationsschutz, Vertraulichkeit, Identitätsschutz, Authentizität sowie Autorisierung
- **Zugangskontrolle:** Schutz gegen unautorisierten physischen Zugang
- **Monitoring und Meldesysteme:** Erkennung von Bedrohung und schnelle Reaktion auf Ereignisse und Umsetzung eines zielgerichteten Schutzes nach Bedrohungslage
- **Angriffsabwehr:** Maßnahmen zur Abwehr von Cyber-Angriffen (Virenscanner, IP-White/Black-Listing)

Der Security Guide beschreibt in den nachfolgenden Kapiteln folgende Themenschwerpunkte:

1. **Umfeldbetrachtungen**
   Betrachtungen allgemeiner Aspekte der IT-Sicherheit für Industrie und Energieflexibilitätsmanagement

2. **IT-Sicherheit im Architekturmodell**
   Betrachtung der IT-Sicherheit auf den verschiedenen Schichten des Architekturmodells

3. **PKI[2] und Kryptographie**
   Beschreibung der Struktur und der Umsetzung der PKI bei SynErgie. Beschreibung der Zertifikate und Anwendung.

4. **Durchführung einer Bedrohungsanalyse**
   Die Umsetzung der Bedrohungsanalyse erfolgt mittels Durchführung eines Threat-Modelings.

5. **Ermittlung eines erforderlichen Sicherheitslevels für Services**
   Der tatsächliche Sicherheitsbedarf und damit die zu ergreifenden Maßnahmen richten sich nach dem Schutzbedarf der Informationen und der Kritikalität, sowie der Risikoeinstufung eines Angriffs.

6. **Rollen und Rechtekonzept**
   Für die Plattformen der ESP wurde ein Rollen- und Rechtekonzept entwickelt. Dabei wird ein rollenbasiertes Zugriffskonzept vorgegeben (engl. Role based Access Control (RBAC)).

7. **(Security) Life Cycle Management**
   Das Security Life Cycle Management beschreibt die Prozesse, sowie die geforderten Maßnahmen, für jede Lebensphase, die aus dem ermittelten Sicherheitslevel resultieren und benennt die verantwortlichen Rollen in der jeweiligen Lebensphase.

8. **Umsetzung der präventiven Maßnahmen und allgemeinen Empfehlungen**
   Dabei handelt es sich einerseits um die Erkenntnisse aus durchgeführten Threat-Modelings die einen allgemeingültigen Stellenwert haben oder um Maßnahmen, auf die noch einmal konkret aufmerksam gemacht werden soll, sowie allgemein Empfehlungen.

[2] PKI – Mit der Public-Key-Infrastruktur bezeichnet man in der Kryptologie ein System, welches digitale Zertifikate ausstellen, verteilen und prüfen kann. Innerhalb einer PKI ausgestellte Zertifikate werden zur Absicherung der rechnergestützten Kommunikation verwendet.

Umfeldbetrachtungen

Die Anforderungen an die IT-Sicherheit der ESP resultieren aus zwei unterschiedlichen Einsatzumgebunden. Einerseits existieren die Sicherheitsanforderungen, die sich aus dem industriellen Umfeld, also der Produktion und somit aus den Anforderungen teilnehmender Unternehmen ergeben und andererseits die Anforderungen, welche aus einer Einstufung der ESP oder Teilen der ESP als Kritische Infrastruktur (KRITIS) resultieren könnten. Die Einstufung als KRITIS kann insbesondere für die UP oder die marktseitigen Services relevant werden, wenn die Schwellenwerte für KRITIS überschritten werden. Anforderungen aus dem industriellen Umfeld resultieren aus Sicherheitsanforderungen der Unternehmen selbst, die diese stellen, wenn sie sich an eine extern betriebene Plattform anbinden sollen oder diese im Unternehmen integrieren. Hierbei steht die Sicherstellung des Produktionsprozesses im Vordergrund und die Vertraulichkeit von Daten. Zusätzlich kommen Anforderungen des Datenschutzes mit hinzu. Auch hier können existierende Zertifizierungen nach entsprechenden Standards weitreichende Anforderungen an die IT-Sicherheit stellen. Bei KRITIS steht im Allgemeinen die Versorgungssicherheit und hier insbesondere die Zuverlässigkeit der Stromversorgung im Vordergrund. Die Vorgaben hierzu sind gesetzlich geregelt (Bundesrepublik Deutschland 2021a; BSI – Bundesamt für Sicherheit in der Informationstechnik 2021).

Kritische Infrastrukturen

Im Sinne der Europäischen Union (EU-Richtlinie 2008/114/EG) ist eine „Kritische Infrastruktur“ eine Anlage, ein System oder ein Teil davon, welches von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung ist und deren Störung oder Zerstörung erhebliche Auswirkungen hätte, da ihre Funktionen nicht aufrechterhalten werden könnte.

In Deutschland existieren hierzu Regelungen und Vorgaben wie die BSI Kritisverordnung (BSI – Bundesamt für Sicherheit in der Informationstechnik 2021) (BSI-KritisV), das IT-Sicherheitsgesetz (Bundesrepublik Deutschland 2021a), sowie das Energiewirtschaftsgesetz EnWG (Bundesrepublik Deutschland 2005). Diese sind bei der Entscheidung, ob ein System als KRITIS einzustufen ist und welche grundsätzlichen Regelung gelten, heranzuziehen.

In Tabelle 1 sind die zum Zeitpunkt Mai 2022 gültigen Schwellwerte für Strom aufgeführt, ab dem eine Anlage oder ein System als KRITIS[3] eingestuft wird .

Tabelle 1: Einstufung Stromerzeugung und Schwellwerte nach BSI-KritisV

Anlagenkategorie	Bemessungskriterium	Schwellwert
Erzeugungsanlage[4]	Installierte Nettonennleistung (elektrisch oder direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil) in MW	104
	Installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses der Bundesnetzagentur vom 20. Mai 2020, Aktenzeichen BK6-18-249 (Bundesnetzagentur) kontrahiert ist	0
	Installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV (Bundesministerium der Justiz und für Verbraucherschutz 31.05.2022) präqualifiziert ist	36
Anlage oder System zur Steuerung/Bündelung elektrischer Leistung[5]	Installierte Nettonennleistung (elektrisch) in MW	104
	Installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses BK6-18-249 kontrahiert ist	0
	Installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert ist	36
Zentrale Anlage oder System für den Stromhandel	Abgewickeltes Handelsvolumen in TWh/Jahr	3,7

Erfolgt eine Einstufung als Kritische Infrastruktur anhand der vorgegebenen Bemessungskriterien und Schwellwerte, sind die Vorgaben des IT-Sicherheitskatalogs gemäß § 11 Absatz 1b Energiewirtschaftsgesetz (Bundesnetzagentur 2018) einzuhalten und es ist ein Informationssicherheitsmangementsystem (ISMS) zu implementieren, welches den Anforderungen der DIN ISO/IEC 27001 (Deutsches Institut für Normung e.V.) und den dort referenzierten Normen und Standards in der jeweils geltenden Fassung genügt. Die

[3] https://www.gesetze-im-internet.de/bsi-kritisv/index.html

[4] Diese Kategorie umfasst auch Anlagen zur Speicherung von elektrischer Energie sowie dezentrale Energieerzeugungsanlagen im Sinne des § 3 Nummer 11 des Energiewirtschaftsgesetzes.

[5] eine Anlage oder ein System zur Bündelung elektrischer Leistung und Steuerung von Erzeugungsanlagen oder dezentraler Energieerzeugungsanlagen, insbesondere zur Anwendung bei Direktvermarktungsunternehmen im Sinne des § 3 Nummer 17 des Erneuerbare-Energien-Gesetzes. Unter den Begriff der Steuerung fallen auch die die Anlagen betreffenden Schalthandlungen

Implementierung und Konformität eines ISMS ist durch ein Zertifikat bei einer, durch die Deutsche Akkreditierungsstelle (DAkkS) akkreditierten, unabhängigen Zertifizierungsstelle, zu belegen. Dies können beispielsweise die Einrichtungen des TÜVs sein. Eine detaillierte Übersicht liefert die Internetseite der DAkkS[6].

Ob die ESP insgesamt oder Teile hiervon als Kritische Infrastruktur einzustufen ist, muss im Einzelfall anhand der Bemessungskriterien entschieden werden.

IT-Sicherheitsmaßnahmen aus dem Umfeld Industrie 4.0

Aus Gründen der Produktionssicherheit, Einhaltung von Lieferfristen, Schutz von Know-how, Schutz von Kundendaten und weiteren Aspekten ist im industriellen Umfeld ein angemessenes Maß an IT-Sicherheit gefordert. Ein weiterer Aspekt sind allgemeine Haftungsfragen, die Funktionen der ESP und der Teilkomponenten UP und MP betreffend. Auch im industriellen Umfeld werden Anforderungen an die Funktionssicherheit und die IT-Sicherheit gestellt, da bei Ausfällen die Produktion betroffen sein kann. Eine der maßgeblichen Normen zur IT-Sicherheit ist die internationale Norm ISA/IEC 62443 Industrial communication networks – Network and System Security (DIN EN 62443-3-2:2018-10 - Entwurf) (DIN EN IEC 62443-4-2:2019-12). Bei der ICE 62443 zeigt sich, dass sich die Norm immer mehr der ISO/IEC 27000 Normenreihe annähert und alternativ auch diese in Teilbereichen angewendet werden kann. Je nach Branche existieren aber auch weitere Standards oder Richtlinien, die zur Umsetzung eines angemessenen Sicherheitsniveaus angewandt werden können, wie beispielsweise die VDS Richtlinie 3473 (speziell für KMU) (VDS Richtlinie 3473), sowie die VDI/VDE2182 (VDI/VDE 2182 Blatt 1) Normreihe und weitere. Eine vollumfängliche Auflistung ist hier aufgrund des Umfangs nicht umsetzbar.

[6] https://www.dakks.de/de/akkreditierte-stellen-suchergebnis.html

IT-Sicherheits-Architekturmodell

IT-Sicherheit ist eine wesentliche Voraussetzung für den erfolgreichen Betrieb von IT-Systemen. Daher ist die Perspektive der IT-Sicherzeit ein zentrales Querschnittsthema im Architekturmodell. Das Referenzarchitekturmodell wird im Detailpapier „Referenzarchitektur der Energiesynchronisationsplattform“ als Teil des Diskussionspapiers (Menci et al. 2021) beschrieben.

Sicherheitsperspektive im Architekturmodell

IT-Sicherheit muss bei allen Konzeptions- und Umsetzungsschritten eines Systems in adäquatem Maß bedacht werden und bei allen logischen und physischen Bestandteilen des Systems entsprechend implementiert und im operativen Betrieb aufrechterhalten werden. Daher muss IT-Sicherheit in allen Schichten des Architekturmodells und bei allen darin befindlichen Elementen beachtet werden – dies gilt für die ESP konkret für alle Elemente, die nachfolgend in den einzelnen Schichten aufgeführt sind.

Um IT-Sicherheit bestmöglich gewährleisten zu können und bei allen Architekturelementen angemessen zu berücksichtigen, ist eine systematische Herangehensweise notwendig, für die es bewährte Methoden gibt. Zusätzlich gibt es etablierte Sicherheitsfunktionalitäten, welche die Architektur eines Systems ergänzen. Durch diese beiden Gesichtspunkte bringt die Perspektive der IT-Sicherheit zusätzliche Elemente in alle Schichten des Architekturmodells ein. Diese Elemente bringen beim Planen, Implementieren, Aufsetzen und Betreiben eines Systems entsprechende Aufgaben mit sich.

Insgesamt gibt es aus der Perspektive der IT-Sicherheit nach vorigen Überlegungen zwei Querschnitte durch das Architekturmodell. Zum einen den Querschnitt der Absicherung der operativen Architekturelemente und zum anderen den Querschnitt der sicherheitsspezifischen Architekturelemente. Ersteres wird mit letzterem systematisch umgesetzt. Die sicherheitsspezifischen Architekturelemente werden im Folgenden erläutert. An ausgewählten Stellen wird eine Konkretisierung hin zur ESP vorgenommen. Dabei wird teilweise auch auf die Absicherung der operativen Architekturelemente eingegangen, d. h. es werden spezifische Sicherheitsaspekte für die operativen Architekturelemente erörtert.

Aus den Anforderungen können die **Sicherheitsziele**[7] für ein bestimmtes System abgeleitet werden. Ganz allgemein gibt es die grundlegenden Schutzziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*. Diese werden oft durch die Schutzziele *Authentizität*, *Nichtabstreitbarkeit* und

[7] Unter dem Begriff **Sicherheitsziele** versteht man im Allgemeinen die Anforderungen an ein System, die zum Schutz von schützenswerten Gütern erfüllt werden muss. Schutzziele sind notwendig, um den abstrakten Begriff der Sicherheit im Kontext der Informationstechnologie greifbar und so vor allem auch messbar bzw.

ggf. weitere Ziele ergänzt. Basierend auf den grundlegenden Schutzzielen und den Sicherheitsanforderungen werden konkrete Sicherheitsziele festgelegt. Die Bedeutung der grundlegenden Schutzziele für die ESP wird nachfolgend noch detaillierter dargestellt und darüber hinaus werden konkrete Schutzziele für die Plattformen der ESP eingeführt.

Strategic Requirements

Für das Erreichen der Schutz- bzw. Sicherheitsziele ist es ein erheblicher Vorteil, nach dem Prinzip **Security by Design** vorzugehen. Dies bedeutet, dass man schon bei Entwurf eines Systems Sicherheitsaspekte bedenkt und diese bei der Implementierung und Installation konsequent umsetzt. Integraler Bestandteil der Entwurfsphase ist die Erarbeitung eines **Sicherheitskonzepts**. Das finale Sicherheitskonzept enthält eine Zuordnung von allen Teilsystemen oder Systemkomponenten zu Sicherheitsprofilen bzw. -stufen (s. nachfolgend „Functional Layer“) und legt die konkret umzusetzenden Sicherheitsmaßnahmen in Bezug auf alle Elemente in allen Schichten der Architektur fest.

Der Weg von der Anforderungsanalyse über die Definition der konkreten Sicherheitsziele und Sicherheitsprofile bis hin zum ausgearbeiteten Sicherheitskonzept mit konkreten Sicherheitsmaßnahmen für einzelne Architekturelemente ist ein Prozess, der konsequenterweise im Process Layer einzuordnen ist. Die Sicherheitsanforderungen, die Sicherheitsziele und das Sicherheitskonzept sind jedoch aufgrund ihrer grundlegenden Relevanz als Elemente der Strategic Requirements eingeordnet. Die adäquate Erfüllung der Sicherheitsanforderungen sollte ein originäres Unternehmensinteresse sein und daher sollten von der Unternehmensführung Strukturen geschaffen werden, mit denen dies zielgerichtet angegangen werden kann. Das Werkzeug hierfür ist ein ISMS. Ein ISMS wird genutzt, um auf organisatorischer Ebene Verantwortlichkeiten und Prozesse zur Bestimmung, Umsetzung und Aufrechterhaltung von Sicherheitsmaßnahmen zu definieren und die Durchführung zu koordinieren und zu dokumentieren. Dies ist die Grundlage für eine zielgerichtete und ganzheitliche Absicherung von Systemen.

Business Layer

Im Business Layer werden die an der ESP beteiligten Rollen identifiziert und deren Tätigkeiten bzw. Aufgaben beschrieben. Hieraus lässt sich aus der Sicherheitsperspektive heraus ein **Berechtigungsmodell** ableiten und mit Berechtigungen für die existierenden Rollen befüllen. Naheliegend ist hier ein Modell zur *rollenbasierten Zugriffskontrolle* (RBAC – engl. „role-based access control“). Evtl. ist es sinnvoll, dieses Modell durch *attributbasierte Zugriffsregeln* (ABAC bzw. RuBAC – engl. „attribute-based access control“ bzw. „rule-based access control“) zu verfeinern und zu stärken. Hiermit ließe sich beispielsweise festlegen, dass eine bestimmte Rolle eine bestimmte Handlung nur durchführen darf, wenn sie sich an einem bestimmten Ort befindet (etwa im Unternehmen bzw. im Intranet des Unternehmens, dessen

Unternehmensplattform bedient werden soll), oder dass eine bestimmte Aktion nur in einem bestimmten Zeitraum zulässig ist (etwa die Buchung einer Flexibilitätsmaßnahme nur innerhalb einer bestimmten Frist). Je nach Einsatzzweck kann es auch nötig sein, dass das Berechtigungsmodell *mandantenfähig* ist, d. h., dass es möglich ist, mehrere sog. Mandanten zu definieren, die voneinander unabhängige Institutionen darstellen und in Bezug auf die Zugriffsmöglichkeiten voneinander getrennt sind.
Abbilden lässt sich ein rollenbasiertes Berechtigungsmodell mit einer **Zugriffsmatrix**, in der die Rollen den zulässigen Aktionen gegenübergestellt werden. Bei komplexen Systemen wie der ESP ist es sinnvoll, die Zugriffsmatrix durch zwei ineinandergreifende Matrizen zu ersetzen. In der ersten Matrix werden die Rollen den abstrakten Aktionen zugeordnet und in der zweiten Matrix werden diese Aktionen spezifischen Berechtigungen im System zugeordnet. Für die erste Matrix genügt die abstrakte Sicht des Business Layers, für die zweite Matrix ist darüber hinaus zusätzliches Wissen aus den tieferliegenden Ebenen über die konkrete Systemausgestaltung nötig.

Die gewährten Rechte sollten sich stets nach dem **Principle of least Privilege** richten, d. h. ein Nutzer sollte stets nur die Rechte haben, die für die Erfüllung seiner Aufgaben notwendig sind. Bei der Festlegung von Rollen und deren Berechtigungen sind nicht nur *menschliche Systemnutzer* zu berücksichtigen, sondern auch die verschiedenen Teilsysteme, Komponenten und Zusatzdienste (zu nennen sind hier insbesondere die Services der Markt- und Unternehmensplattform) als Akteure im Gesamtsystem. Auch für solche *technischen Nutzer* muss festgelegt werden, welche Aktionen diese durchführen dürfen.

Functional Layer
Im Functional Layer befinden sich zunächst die operativen Funktionalitäten der ESP, welche gemäß Sicherheitskonzept (s. oben unter „Strategic Requirements“) abgesichert werden müssen. Aus der Sicherheitsperspektive heraus werden im Functional Layer zusätzlich alle benötigten Sicherheitsfunktionalitäten erfasst. Diese werden im Folgenden aufgeführt:

- **Sicherheitsprofile/-stufen:** In Sicherheitsprofilen bzw. -stufen wird festgelegt, welche Anforderungen zu erfüllen sind, um einen bestimmten Grad an Sicherheit zu erlangen. Dies wird genutzt, um ein System als Ganzes oder verschiedene Systemelemente gemäß dem konkreten Schutzbedarf, welcher aus dem Einsatzzweck resultiert, einzuordnen. Es hilft auf diese Weise, das System mit angemessenen Schutzmaßnahmen zu versehen. Eine Anforderungsanalyse (s. oben unter „Strategic Requirements“) ist Voraussetzung für diese Einordnung von Systemen oder Systemelementen zu Sicherheitsprofilen bzw. -stufen. In SynErgie werden Systemelemente hinsichtlich ihres Sicherheitsbedarfs hauptsächlich aus Sicht des Stromnetzes und Strommarkts bewertet. Insbesondere bei der Unternehmensplattform muss der Sicherheitsbedarf für den Praxisbetrieb aufgrund unternehmensspezifischer

Besonderheiten gesondert und individuell bewertet werden. Dies bedeutet die Bewertung darf nicht nur im Hinblick auf eine ungestörte allgemeine Stromversorgung erfolgen, sondern muss auch Anforderungen aus dem eigentlichen Wertschöpfungsprozess des Unternehmens betrachten. Die kann dazu führen, dass verschiedene Elemente ggf. einer höheren Sicherheitsstufe zugewiesen werden.

- **Identitätenverwaltung**: Alle Entitäten im System, d. h. alle menschlichen Nutzer sowie – wie bereits oben unter „Business Layer“ erwähnt – alle aktiven Systemkomponenten, müssen erfasst werden und eindeutig sowie möglichst täuschungsresistent identifizierbar sein. Vor der Registrierung zum System ist dementsprechend eine physische Identifizierung in einem vertrauenswürdigen Rahmen nötig. Danach kann eine Identität im Verwaltungssystem hinterlegt und mit technischen Identifizierungsmerkmalen ausgestattet werden.

- **Public Key Infrastructure** (**PKI**): Eine PKI ist ein Konzept zum Verknüpfen kryptographischer Schlüssel mit Identitäten und zum Beglaubigen dieser Verknüpfungen in Form von sog. digitalen Zertifikaten. Ebenso wird eine konkrete Umsetzung des Konzepts in IT-Systemen als PKI bezeichnet. Die kryptographischen Schlüssel und die digitalen Zertifikate können als Sicherheitsanker für vielfältige Anwendungen genutzt werden.

- **Berechtigungsverwaltung**: Das Berechtigungsmodell aus dem Business Layer muss durch ein System abgebildet werden. In diesem System werden die Identitäten aus der Identitätenverwaltung ihren Berechtigungen zugeordnet, d. h. die Berechtigungen der Identitäten werden verwaltet. Dabei muss es möglich sein, neuen Identitäten Berechtigungen zu geben, bei bestehenden Identitäten im Falle von Aufgabenänderungen Berechtigungen anzupassen und bei ausscheidenden Identitäten alle Berechtigungen zu entziehen. Im Falle eines RBAC-Modells werden die Berechtigungen über eine Zuordnung von Identitäten zu Rollen gesetzt und bei den Rollen sind die entsprechenden Rechte hinterlegt (s. auch oben unter „Business Layer“).

- **Zugriffskontrolle**: IT-Systeme müssen dafür sorgen, dass die in der Berechtigungsverwaltung gesetzten Berechtigungen nicht überschritten werden, d. h., dass Identitäten nur Aktionen durchführen können, zu denen sie berechtigt sind.

- **Physische Zugangsbeschränkung**: Auch der physische Zugang zu IT-Systemen muss je nach Sicherheitsstufe mit angemessenen Maßnahmen auf berechtigte Personen und ggf. bestimmte Zeitfenster beschränkt werden, um das Risiko für schadhafte Handlungen an den Systemen zu minimieren.

- **Netzwerksicherheit**: Ziel der Netzwerksicherheit ist eine möglichst gute Abschottung des Unternehmensnetzwerks und die Kontrolle darüber. Dies beginnt mit der Perimetersicherung, ist damit aber nicht abgeschlossen. Vielmehr ist es auch erforderlich, das interne Netzwerk in physische und logische Zonen zu unterteilen und die Zugriffs- und Kommunikationsmöglichkeiten an den Übergängen zwischen den Zonen und innerhalb der Zonen auf das Erforderliche einzuschränken**.**

- **Kapselung**: Der Gedanke der Kapselung lässt sich nicht nur auf der Netzwerkebene anwenden, sondern auch auf der Anwendungsebene auf die einzelnen Komponenten eines Systems. Die Teilsysteme, Dienste bzw. Komponenten sollen nur im erforderlichen Umfang aufeinander zugreifen können, um bei Kompromittierung eines Teils des Systems nicht alle Daten preiszugeben oder gar zu verlieren, damit auch dann möglichst ein eingeschränkter Weiterbetrieb aufrechterhalten werden und damit die Wiederherstellung der Systemkontrolle und des Normalbetriebs möglichst zügig ablaufen kann.

- **Kommunikationssicherheit**: Bei der Kommunikation über Netzwerkverbindungen sind Maßnahmen zum Schutz der Kommunikationsinhalte erforderlich. Dies gilt insbesondere bei der Kommunikation über externe Netzwerke, sollte vorzugsweise aber auch bei internen Netzwerken beachtet werden. In manchen Anwendungsfällen, bei denen eine Kommunikation über eine Kette von Verbindungen mit zwischengeschalteten Diensten hinweg stattfindet, kann es notwendig sein Ende-zu-Ende-Sicherheit in Bezug auf Integrität, Echtheit oder Vertraulichkeit herzustellen.

- **Eingabevalidierung**: Keine Komponente sollte Eingaben ungeprüft übernehmen, da Eingaben technisch invalide oder unplausibel oder im schlimmsten Fall schadhaften Code injizieren können. Um dies zu verhindern, sind Validierungsfunktionen nötig und bei Freitexteingaben ggf. auch Transformationsfunktionen, die im Hinblick auf das verarbeitende System syntaktisch kritische Eingaben durch Escape-Sequenzen ersetzen.

- **Minimierung der Angriffsfläche**: Ein System sollte nur die tatsächlich benötigten und genutzten operativen Funktionalitäten bieten. Dies betrifft sowohl die Zugangsmöglichkeiten zu Funktionalitäten als auch das tatsächliche Vorhalten von Funktionalitäten. Jede unnötige Erweiterung von Zugriffsmöglichkeiten und installierten Funktionalitäten vergrößert die potenziellen Angriffsmöglichkeiten. Zudem werden installierte, aber nicht genutzte Komponenten oft nicht aktualisiert, so dass ggf. bekannt gewordene Sicherheitslücken im System bestehen bleiben.

- **Logging** und **Monitoring**: Im laufenden Betrieb eines Systems müssen sicherheitsrelevante Ereignisse geloggt, d. h. aufgezeichnet werden. Die Logging-Funktion selbst muss derart abgesichert sein, dass keine Log-Einträge unterdrückt, gelöscht, verändert oder auf betrügerische Weise eingefügt werden können – kurz gesagt, das Logging-System muss manipulationssicher sein. Komplementär zur Logging-Funktion sind auch Monitoringfunktionen nötig, welche die Aufzeichnungen auswerten und visualisieren und bei kritischen Ereignissen einen Alarm auslösen. Logging und Monitoring sollte auf Netzwerkebene, Systemebene und Anwendungsebene betrieben werden.

Process Layer

Im Process Layer werden die Prozesse zum Erfüllen der funktionalen Aufgaben beschrieben. Hier existieren zunächst die operativen Prozesse. Die Sicherheitsperspektive ergänzt diese Prozesse um Sicherheitsaspekte und führt auch zusätzliche, sicherheitsspezifische Prozesse ein. Aus der Sicherheitsperspektive sind insbesondere folgende Prozesse zu nennen:

- **Erarbeitung des Sicherheitskonzepts**: Wie bei den Strategic Requirements oben erwähnt, ist die Erarbeitung des Sicherheitskonzepts ein Prozess in der Entwurfsphase des Systems. Dieser beginnt mit der Feststellung der Sicherheitsanforderungen, erstreckt sich über die Bestimmung der Sicherheitsziele und die Festlegung von Sicherheitsstufen (mit ihren jeweiligen konkreten Anforderungen) und mündet in einem Sicherheitskonzept mit konkreten Sicherheitsmaßnahmen.

- **Qualitätskontrolle** (**Sicherheitsaudit** und **Zertifizierung**): Bevor ein System für den Produktivbetrieb freigegeben wird, sollte das System in einem Audit auf seine Sicherheit überprüft werden. Dies kann je nach Anforderungen von einer Prüfung der Architektur über eine Prüfung der Funktionalitäten bis hin zu einem intensiven Penetration-Testing und einer Quellcodebegutachtung reichen. Idealerweise wird das System auch während des Betriebs in regelmäßigen Zeitabständen (etwa alle zwei Jahre) sowie nach Systemänderungen im Rahmen des Releasemanagements überprüft. Von einer Zertifizierung spricht man, wenn die Anforderungen an ein System standardisiert sind und die Kriterien für den Audit festgelegt sind. Trotz begrifflicher Nähe sind Zertifizierungen und digitale Zertifikate (s. oben bei PKI unter „Functional Layer“) unabhängige Konzepte. Audits und Zertifizierungen kann man für Gesamtsysteme wie Unternehmensplattformen oder auch für Systembausteine wie Services und Apps durchführen.

- **Sichere Teilnehmerregistrierung**: Grundlage für ein sicheres „Onboarding“ ist eine sichere Teilnehmeridentifizierung. In den nachfolgenden Schritten finden Interaktionen

mit der Identitätenverwaltung und der Berechtigungsverwaltung statt, um Authentifizierungsmerkmale mit dem Teilnehmer zu vereinbaren und um seine Berechtigungen zu konfigurieren. Ein Registrierungsprozess muss jeweils für Personen, für institutionelle Nutzer (z. B. für Unternehmen, die eine Unternehmensplattform an die Marktplattform anschließen wollen) und für technische Komponenten (z. B. für Unternehmensplattformen oder Services bzw. Apps) existieren.

- **Authentifizierung** und **Autorisierung**: Die zusammenspielenden Prozesse „Authentifizierung“ und „Autorisierung“ setzen die Zugriffskontrolle (s. oben unter „Functional Layer“) um. In einem Authentifizierungsprozess weist ein registrierter Teilnehmer sich mit zuvor vereinbarten Merkmalen, z. B. einem Passwort, einem kryptographischen Schlüssel oder per Fingerabdruckscan, aus. Zur Erhöhung der Sicherheit kann man eine Zweifaktorauthentifizierung anwenden, bei der zwei verschiedene Merkmale abgefragt werden. Der Authentifizierung nachgelagert sind Autorisierungsprozesse, die vor jedem Zugriff auf Systemressourcen durchgeführt werden.

- **Aufsetzen einer PKI**: Eine PKI (s. oben unter „Functional Layer“) dient als Grundlage für viele weitere Sicherheitsfunktionalitäten. Dabei kommt dem Wurzelzertifikat der PKI eine besondere Rolle als Vertrauensanker zu. Deshalb müssen bei der Erstellung desselben und beim Aufbau der PKI die Schritte einer sicheren Vorgehensweise genau eingehalten werden (Bundesdruckerei 2022; Akram et al. 2020).

- **Zertifikatsausstellung** und **Zertifikatsrückruf**: Kernaufgabe einer PKI ist es, digitale Zertifikate für Teilnehmer auszustellen. Daneben gibt es auch Situationen, wo ein Zertifikatsrückruf nötig ist, etwa bei Ausscheiden eines Teilnehmers oder bei Kompromittierung eines Zertifikats. Eine PKI muss daher sowohl einen Prozess zur Zertifikatsausstellung als auch für den Zertifikatsrückruf bereitstellen.

- **Sichere Kommunikationsprozesse**: Bei Kommunikationsprozessen sind Schritte zur Sicherung der Kommunikationsinhalte nötig, insb. hinsichtlich Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit. Das erste Schutzziel ist insbesondere dann relevant, wenn die Kommunikation über externe Netzwerke läuft. Hierfür werden Schritte zur Ver- und Entschlüsselung in den Kommunikationsprozess eingefügt (Bundesamt für Sicherheit in der Informationstechnik - Verschlüsselung 2021). Die anderen Schutzziele sind je nach Kommunikationsinhalt und Konstellation der Kommunikationspartner relevant und können durch Schritte zur digitalen Signatur und Signaturverifikation abgesichert werden.

Information Layer
Im Information Layer werden die relevanten Informationsobjekte erfasst und die Repräsentation von Informationen wird spezifiziert. Bei diesen Objekten und deren Repräsentation (Datenformate, Protokolle) sind stets auch die Sicherheitsrisiken zu analysieren, etwa das Risiko von Schadcode in Datenobjekten oder das Risiko von Informationslecks, und entsprechende Maßnahmen – idealerweise direkt durch die Wahl vorteilhafter Formate und Protokolle oder in Form von Schutzmechanismen auf dem System Layer (s. unten) – im Sicherheitskonzept festzulegen.

Die IT-Sicherheitsperspektive führt zusätzliche Informationsobjekte ein. Hier sind zunächst für die Entwurfsphase **Notationen** und **Datenstrukturen** zum Abbilden von *Berechtigungsschemata* (s. oben unter „Business Layer“) und von *Sicherheitsprofilen* (s. oben unter „Functional Layer“) nötig. Im operativen Betrieb der ESP fallen verschiedene **Datenobjekte** zur Gewährleistung von Sicherheit an, insbesondere *digitale Zertifikate* (s. oben bei PKI unter „Functional Layer“) und *digitale Signaturen* auf Basis digitaler Zertifikate zum Schützen von anderen Datenobjekten und von Kommunikationsvorgängen. Ebenso sind für den Betrieb **Verschlüsselungsprotokolle** nötig.

Component Layer
Im Component Layer werden die konkreten physischen und digitalen Systemkomponenten erfasst. Die Elemente des Component Layers setzen die Funktionalitäten aus dem Functional Layer und die Prozesse aus dem Process Layer technisch um und verarbeiten die Elemente des Information Layers. In der weiteren Beschreibung dieser Schicht wird zur Erhöhung des Leseflusses auf die Querverweise zu den höheren Schichten verzichtet, da diese sehr zahlreich wären auch im Component Layer werden aus der Sicherheitsperspektive Maßnahmen zur Absicherung der operativen Komponenten dieses Layers definiert. Die konkret zu treffenden Maßnahmen werden basierend auf der Anforderungs- bzw. Risikoanalyse im Sicherheitskonzept festgelegt. An erster Stelle steht die Integration und Konfiguration der **Zugriffskontrolle**. Hier muss der Teilaspekt der Autorisierung inhärent in der Implementierung der einzelnen Komponenten verankert werden, wobei sowohl die Berechtigungen von menschlichen Nutzern als auch von technischen Komponenten kontrolliert werden müssen. Ggf. muss auch Mandantenfähigkeit vorhanden sein. Hinzu kommen Maßnahmen zur **Härtung** von Anwendungen und Betriebssystemen. Beispiele für solche Maßnahmen in Bezug auf Anwendungen sind das Ausführen von logischen Komponenten in separaten Prozessen zur *Kapselung* dieser Komponenten sowie die *Validierung von Eingangsdaten* zur Verhinderung von Unplausibilitäten, Inkompatibilitäten, Verarbeitungsfehlern und Codeinjektionsangriffen. Beispiele für Härtungsmaßnahmen an Betriebssystemen sind restriktive Prozessberechtigungen und ggf. zusätzlich Sandboxing bzw. Containering zur *Kapselung* von Komponenten sowie das Deaktivieren bzw. vollständige Entfernen von ungenutzten

Systemdiensten zur *Minimierung der Angriffsfläche*. Bei vielen Komponenten fallen zudem Maßnahmen zur **sicheren Konfiguration** von Zugängen, etwa mit sicheren Passwörtern, und von sicherheitsspezifischen Parametern, etwa in Bezug auf Verschlüsselungsprotokolle, an. Die Sicherheitsperspektive führt zudem zusätzliche Elemente im Component Layer ein:

- Es werden Softwaremodule für die **Identitätenverwaltung**, die **Berechtigungsverwaltung** und für die **Zugriffskontrolle** mit ihren Teilaspekten Authentifizierung und Autorisierung benötigt. Die Authentifizierungskomponente ist eine zentrale Anlaufstelle für alle weiteren Komponenten. Für die Autorisierung kann es je nach Systemarchitektur und Komplexität des Berechtigungsmodells auch dedizierte Komponenten zusätzlich zu den integrierten Autorisierungsfunktionalitäten in den Anwendungskomponenten geben, etwa ein Modul zur Evaluierung attributbasierter Zugriffsregeln oder Module zum Erzeugen und Auswerten von Objekten, die delegierte Berechtigungen repräsentieren.

- Eine **PKI** benötigt für ihren Betrieb verschiedene Komponenten, insbesondere eine *Zertifizierungsstelle* (engl. „certificate authority“, CA), die mit dem Wurzelzertifikat Zwischenzertifkate erstellt und je Zwischenzertifikat eine Zertifizierungsstelle, die weitere Zwischenzertifikate oder Nutzerzertifikate ausstellt. Die privaten Schlüssel zu den Zertifikaten, insbesondere der private Schlüssel zum Wurzelzertifikat, benötigen Schutzvorkehrungen gegen Kompromittierung, etwa ein Software- oder Hardwaremodul zur sicheren Speicherung. Zusätzlich werden Komponenten zur Entgegennahme und Veröffentlichung von *Zertifikatsrückrufen* benötigt (Anmerkung: Bei der ESP ist die zentrale Zertifizierungsstelle Teil der Marktplattform).

- Auf dem Gebiet der **Netzwerksicherheit** sind wesentliche Komponenten *Firewalls*, *demilitarisierte Zonen* (DMZ) sowie Komponenten zum *Security Information and Event Management* (SIEM), wobei letzteres auf das *Monitoring* in Bezug auf Netzwerke abzielt.

- Spezielle **Hardwarekomponenten** bieten bestimmte Möglichkeiten zur Erhöhung der Sicherheit. Ein *Trusted Platform Module* (TPM) ermöglicht einen Schutz vor der Manipulation der Systemsoftware. *Smartcards* können als sicherer Speicher für private kryptographische Schlüssel vor der Kompromittierung dieser Schlüssel schützen.

- Auch die Umsetzung der **physischen Absicherung** der ESP ist auf dem System Layer einzuordnen. Die Absicherung wird über bauliche (z. B. abschließbare Türen) und organisatorische Maßnahmen (z. B. manuelle Einlasskontrolle) zur *Beschränkung des Zugangs* zu den Gebäuden und den konkreten Räumen, in denen sich die Hardware der ESP befindet, realisiert. Auch eine bauliche *Robustheit* gegen *Unwetter* und, soweit möglich, gegen *Naturkatastrophen* muss zum Schutz der IT-Infrastruktur gewährleistet

sein. Bei den physischen Sicherheitsmaßnahmen sind auch die Stromversorgung der Systemkomponenten und die Kommunikationsanbindungen zu berücksichtigen.

Kryptographische Zertifikate in der ESP

Kryptographische Zertifikate beruhen auf asymmetrischer Kryptographie. Daher wird kurz auf deren Grundlagen eingegangen. Asymmetrische Kryptographie ermöglicht eine Vielzahl von Anwendungen, insbesondere Verschlüsselung und Signatur von Daten sowie Authentifizierung von Personen und Systemen (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2021b). Diese Art von Kryptographie beruht auf Schlüsselpaaren, wovon stets ein Schlüssel geheim ist, d.h. nur der besitzenden Entität bekannt ist, und der zugehörige öffentliche Schlüssel einem beliebig großen Kreis interessierter Entitäten bekannt gemacht werden kann. Je nach Anwendungsfall reicht dieser Kreis von einzelnen Personen und Systemen bis hin zur Weltöffentlichkeit.

Da öffentliche Schlüssel per se nicht die Information beinhalten, wem diese gehören, gibt es kryptographische Zertifikate zu öffentlichen Schlüsseln. Diese nennen die besitzende Instanz in Verbindung mit dem öffentlichen Schlüssel und beglaubigen dies mit einer kryptographischen Signatur. Die Signatur hängt wiederum vom Schlüsselpaar der beglaubigenden Instanz ab. Das Problem der nachweisbaren Schlüsselzuordnung scheint damit zunächst nur verlagert zu sein, wird mit Zertifikaten aber gelöst, wie nachfolgend dargestellt.

Im Kontext von Zertifikaten spielen Zertifizierungsstellen (engl. „Certificate Authority“, CA), die kryptographische Zertifikate ausstellen, eine zentrale Rolle. Beim Erstellen von Zertifikaten nutzt die CA ein CA-Zertifikat, um Signaturen für die auszugebenden Zertifikate zu erzeugen. CA-Zertifikate sind hierarchisch organisiert und Ausgangspunkt einer Hierarchie ist jeweils ein sogenanntes Wurzelzertifikat, das nicht von einem anderen Zertifikat, sondern mit seinem zugehörigen privaten Schlüssel signiert wurde. In der Hierarchie unter einem Wurzelzertifikat (bzw., wenn man bei der Baummetapher bleibt, *über* einem Wurzelzertifikat) befinden sich meist auf mehreren Ebenen weitere CA-Zertifikate, sogenannte Zwischenzertifikate. Am Ende der Hierarchie stehen die Anwendungszertifikate, sogenannte Blattzertifikate, welche keine CA-Funktionalität besitzen. Letztendlich werden somit über eine solche Hierarchie auf Basis eines einzigen Wurzelzertifikats viele Schlüssel nachweisbar der jeweiligen besitzenden Instanz zugeordnet.

In Anwendungssystemen sind typischerweise einige Wurzelzertifikate als Vertrauensanker hinterlegt, so dass sämtliche, sich „darunter“ befindenden, gültigen Zertifikate für die angegebenen Zwecke wie z.B. Signaturen oder Authentifizierung akzeptieren werden. Ein

Zertifikat ist gültig, wenn der momentane Zeitpunkt, wie er über die Systemuhr bestimmt wird, in dem im Zertifikat angegebenen Gültigkeitszeitraum liegt und das Zertifikat nicht widerrufen wurde. Für die Bekanntgabe widerrufener Zertifikate gibt es etablierte technische Mechanismen, nämlich Zertifikatswiderrufslisten (engl. „Certificate Revocation List“, CRL) und das Online Certificate Status Protocol (OCSP).

Eine Zertifikatshierarchie und die weiteren hier genannten Technologien und Systeme bilden eine sogenannte Public-Key-Infrastruktur (PKI). Als technischer Standard für eine PKI und insbesondere für die Struktur von Zertifikaten hat sich die ITU Recommendation X.509 (ITU-T) durchgesetzt.

SynErgie-PKI – Struktur und Anwendungsmöglichkeiten

Die ESP von SynErgie hat eine eigene PKI. Die zentrale Zertifizierungsstelle mit dem Wurzelzertifikat wird auf der Marktplattform (MP) betrieben. Direkt unter dem Wurzelzertifikat befinden sich zwei Zwischenzertifikate. Mit dem einen Zwischenzertifikat stellt die CA weitere Zwischenzertifikate für an der ESP teilnehmende energieflexible Unternehmen aus. Ebenso unter dem Wurzelzertifikat befindet sich ein Zwischenzertifikat, womit die MP wiederum Zwischenzertifikate für an der MP teilnehmende Services ausstellt. Sowohl die Unternehmen als auch die marktseitigen Services können mit ihren Zwischenzertifikaten eine eigene CA betreiben. Die Struktur der SynErgie-PKI ist in Abbildung 1 dargestellt. Gezeigt werden in der Abbildung auch die Zertifikate der sogenannten OCSP-Responder auf Seiten der Marktplattform, womit die OCSP-Funktionalität zum Prüfen des Widerrufsstatus von Zertifikaten umgesetzt wird.

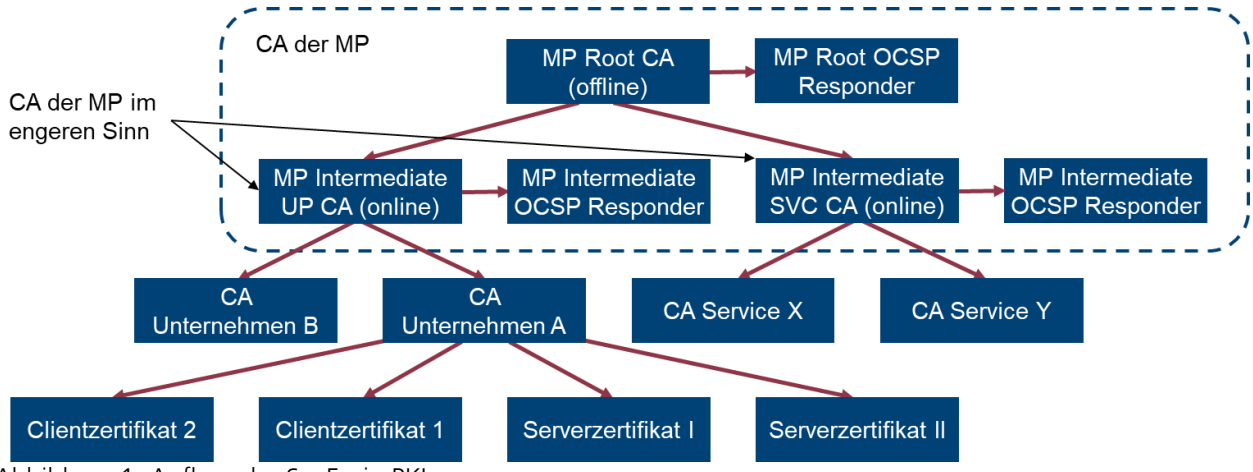


Abbildung 1: Aufbau der SynErgie-PKI

Marktseitige Services können auf die Zertifikatshierarchie, die von der Marktplattform bereitgestellt wird, zurückgreifen, müssen dies aber nicht. Da jeder Service ein Zwischenzertifikat erhält, kann dieser für verschiedene Zwecke davon abgeleitete Blattzertifikate erzeugen. Hier gibt es mindestens drei Anwendungsmöglichkeiten:

- Der Service kann sich mit einem abgeleiteten Blattzertifikat gegenüber den Nutzern ausweisen.
- Der Service kann Nutzern dedizierte Anwendungszertifikate zum Authentifizieren ausstellen.
- Der Service kann Nutzern dedizierte Anwendungszertifikate zum Signieren von Daten ausstellen.

Außerdem, bzw. genauer gesagt als Ergänzung oder Alternative zu den zwei letztgenannten Punkten, kann der Service Nutzer und Daten auf Basis von Zertifikaten akzeptieren, die von einem Unternehmens-Zwischenzertifikat abgeleitet sind. Hierfür ist es nicht nötig, dass der Service eine Zertifizierungsstelle betreibt, jedoch aber, dass das Unternehmen eine Zertifizierungsstelle betreibt.

Auf Unternehmensseite gibt es ebenfalls verschiedene Anwendungsmöglichkeiten zum Betrieb einer Zertifizierungsstelle innerhalb der SynErgie-PKI, basierend auf dem Zwischenzertifikat, welches sie von der Marktplattform erhalten. Hierbei ist die marktseitige Nutzung von Zertifikaten und die unternehmensinterne Nutzung von Zertifikaten zu unterscheiden. Wie im vorigen Absatz bereits angedeutet, können marktseitige Services die folgenden Möglichkeiten anbieten oder auch vorschreiben:

- Je nach Vorgabe der marktseitigen Services müssen Unternehmen sich mit einem Zertifikat ausweisen. Dazu können oder müssen sie je nach Vorgabe ein Zertifikat nutzen, das von ihrem Unternehmens-Zwischenzertifikat abgeleitet ist.
- Evtl. müssen Unternehmen Daten, die sie an einen Service schicken, wie z.B. Energieflexibilitätsdatenmodell-Objekte[8] (EFDM-Objekte), digital signieren, wozu sie je nach Vorgabe des Service ein Zertifikat nutzen können oder müssen, das von ihrem Unternehmens-Zwischenzertifikat abgeleitet ist.

Services haben auch die Möglichkeit, Unternehmen für die zwei genannten Zwecke, wie oben dargestellt, mit Zertifikaten zu versorgen, die vom Service-Zwischenzertifikat abgeleitet sind.

Unternehmensintern kann ebenfalls die SynErgie-PKI verwendet werden. Hier ist es den Unternehmen generell freigestellt, ob und wie Zertifikate für welche Zwecke eingesetzt werden.

[8] Ein Energieflexibilitätsdatenmodell (kurz EFDM) beschreibt generisch mit Hilfe von Kennzahlen und technischen Parametern die potentiellen Möglichkeiten eines energieflexiblen Systems, seine Leistung vom Referenzbetrieb zu variieren.

Hinsichtlich der Referenzarchitektur der Unternehmensplattform (UP) sind aktuell folgende Aussagen zum Einsatz von Zertifikaten möglich:

- Für die Authentifizierung von Services und Personen innerhalb der UP wird aktuell LDAP verwendet und ein Wechsel zu OpenID Connect ist geplant. Zertifikate sind daher nicht für die Authentifizierung innerhalb der UP vorgesehen.
- Es werden derzeit Umsetzungsvarianten zum Signieren von EFDM-Objekten innerhalb der UP diskutiert. Hierfür könnten Zertifikate genutzt werden, die vom SynErgie-Zwischenzertifikat des Unternehmens abgeleitet sind.

Ausrollen von Zertifikaten

Bei der Erzeugung von Schlüsseln und Zertifikaten sind eine Reihe von Sicherheitsmaßnahmen zu beachten, die direkten Einfluss auf die Systemarchitektur, die Betriebsprozesse und die Implementierung der nötigen Services haben. Dies wurde bei der Implementierung der Zertifizierungsstelle für die Marktplattform und bei der Implementierung des CA-Service für Unternehmensplattformen berücksichtigt.

Generell sollten private Schlüssel direkt auf dem System, auf dem sie verwendet werden sollen, erzeugt und sicher verwahrt werden. Eine Ausnahme bilden eingebettete Systeme mit geringem Funktionsumfang, wo eine Erzeugung von Schlüsseln nicht möglich ist. Hier können Schlüssel auf einem anderen Gerät erzeugt und in einer geschützten Umgebung auf das Zielgerät aufgespielt werden.

Hervorzuheben ist auch, dass beim Ausstellen eines Zertifikats durch eine Zertifizierungsstelle nicht der private Schlüssel des zu erstellenden Zertifikats benötigt wird. Stattdessen wird der private Schlüssel des signierenden Zertifikats benötigt, worüber die Zertifizierungsstelle bereits verfügt. Von außen werden nur die Informationen benötigt, die im Zertifikat zu beglaubigen sind, d.h. insbesondere der öffentliche Schlüssel, Angaben zur besitzenden Entität, der Verwendungszweck des Zertifikats und der Gültigkeitszeitraum (siehe nachfolgend die Beschreibung der Attribute). Dementsprechend wird der private Schlüssel des zu erstellenden Zertifikats nicht übertragen und auch nicht von der Zertifizierungsstelle erzeugt, sondern vorab von der Stelle, die das Zertifikat beantragen möchte. Der eigentliche Antrag geschieht mit einem sogenannten Certificate Signing Request (CSR), der im Wesentlichen den öffentlichen Schlüssel und die Angaben zur besitzenden Entität enthält und mit dem zugehörigen privaten Schlüssel signiert ist. Die Signatur stellt sicher, dass der CSR nur von der Stelle erzeugt werden kann, die tatsächlich über den privaten Schlüssel verfügt und dass die Inhaltsdaten des CSR gegen Manipulation geschützt sind. Die Signatur stellt jedoch nicht sicher, dass die Inhaltsdaten korrekt sind, insbesondere, dass die beantragende Stelle diejenige ist, die sie vorgibt zu sein.

Den vorhergehenden Erläuterungen entsprechend sind die Zertifizierungsdienste von MP und UP so implementiert, dass sie CSRs entgegennehmen und basierend darauf Zertifikate erstellen. Zudem sind die Dienste durch Authentifizierungsmechanismen geschützt, sodass nur berechtigte Stellen Zertifikate beantragen können, wobei Zertifikate nur auf den Namen der jeweiligen Stellen ausgestellt werden.

Die Erzeugung eines CSR obliegt der beantragenden Stelle. Möchte beispielsweise ein Unternehmen an der SynErgie-PKI teilnehmen, muss es dafür ein Zwischenzertifikat von der Zertifizierungsstelle der Marktplattform beziehen. Hierzu führt es die folgenden Schritte aus:

1. Zunächst erstellt das Unternehmen einen privaten Schlüssel und den dazugehörigen öffentlichen Schlüssel.
2. Den öffentlichen Schlüssel und weitere Informationen fügt das Unternehmen in einen CSR ein und signiert diesen mit dem privaten Schlüssel.
3. Für die Zertifikatsanfrage muss das Unternehmen neben dem CSR auch ein Zertifikatsprofil angeben, welches den Verwendungszweck des Zertifikats festlegt. Nach aktueller Architektur ist hier der Zweck Zwischenzertifizierungsstelle fest vorgesehen.
4. Zur Authentifizierung der Zertifikatsanfrage nutzt das Unternehmen den Aktivierungscode, den es bei der Registrierung auf der Marktplattform per Post erhalten hat. Mit diesem Aktivierungscode berechnet es einen sogenannten HMAC über die Zertifikatsanfrage und verknüpft die Anfrage damit nachweislich mit der eigenen Identität.
5. Das Unternehmen schickt die Zertifikatsanfrage bestehend aus CSR und Profilwahl zusammen mit dem HMAC[9] an die Zertifizierungsstelle der MP.
6. Während das Unternehmen auf die Antwort wartet, validiert die Zertifizierungsstelle den HMAC, prüft die Signatur des CSR und überprüft, ob der im CSR angegebene Unternehmensname mit dem Unternehmensnamen übereinstimmt, welcher zu dem verwendeten Aktivierungscode gehört. Falls alle Prüfungen positiv verlaufen, erstellt die CA der MP ein Zertifikat für das Unternehmen.
7. Das Unternehmen empfängt das neue Zertifikat von der Marktplattform.

Da das genutzte Profil vorgibt, dass das Zertifikat für eine Zwischenzertifizierungsstelle gedacht ist, kann das Unternehmen mit dem Zertifikat und dem zugehörigen privaten Schlüssel nun eine eigene Zertifizierungsstelle betreiben und damit selbst Zertifikate für verschiedene Anwendungszwecke in internen Systemen, sowie für die Kommunikation mit weiteren ESP-Diensten ausstellen.

[9] Ein HMAC ist ein Message Authentication Code (MAC), dessen Konstruktion auf einer kryptografischen Hash-Funktion, wie beispielsweise dem Secure Hash Algorithm (SHA), und einem geheimen Schlüssel basiert.

Besonders wichtig ist der Schutz des privaten Schlüssels des Wurzelzertifikats einer PKI. Daher wurden hierfür bereits beim Aufbau der SynErgie-PKI besondere Maßnahmen ergriffen. Die wesentliche Anforderung hier ist, dass der private Schlüssel des Wurzelzertifikats „offline“ ist, d. h. nicht auf einem mit dem Internet verbundenen System vorgehalten wird. Daher wurden ganz zu Beginn des Aufbaus der SynErgie-PKI dieser Schlüssel und das zugehörige Wurzelzertifikat nicht auf der Marktplattform, sondern auf einem dedizierten System erstellt. Die Marktplattform hat im weiteren Verlauf lediglich die privaten Schlüssel für ihre beiden Zwischenzertifikate sowie die zugehörigen CSRs erzeugt. Diese CSRs wurden manuell auf das dedizierte System der Wurzel-CA übertragen. Dort wurden im nächsten Schritt die Zwischenzertifikate für die Marktplattform erstellt. Diese Zwischenzertifikate und das Wurzelzertifikat (natürlich ohne den privaten Schlüssel) wurden anschließend für die weitere Nutzung und Veröffentlichung auf die Marktplattform übertragen. Damit hatte die Wurzelzertifizierungsstelle ihre Aufgaben bis auf Weiteres, d.h. bis in mehreren Jahren die Erneuerung der Zwischenzertifikate nötig wird, erfüllt. Daher wurde ihr privater Schlüssel in einem verschlüsselten Offline-Speicher archiviert und das System wurde außer Betrieb genommen

Attribute

Die von der Marktplattform erstellten Zertifikate enthalten zunächst die Standardattribute von X.509-Zertifikaten (Network Working Group 2022). Dies sind im Wesentlichen Identitätsattribute, kryptographische Parameter, Angaben zum Verwendungszweck der Zertifikate (etwa Authentifizierung oder Signatur) und der Gültigkeitszeitraum. Damit wird die Zertifizierungsstelle der MP dem Zweck gerecht, Identitäten zu beglaubigen. Darüber hinaus kennzeichnen die Zwischenzertifikate der MP durch ihre Namen, ob ein darunter ausgestelltes Zertifikat einem Serviceanbieter oder einem Servicenutzer (d.h. einem energieflexiblen Unternehmen) gehört. Weitere Attribute hingegen, die über die Standard-Attribute von X.509-Zertifikaten hinausgehen, werden von der CA der MP nicht in den ausgestellten Zertifikaten hinterlegt.

Die MP ist serviceagnostisch und wird daher nicht dafür genutzt, servicespezifische Attribute, etwa ein servicespezifisches Berechtigungsmanagement, zu implementieren. Andernfalls müsste eine enge architektonische und operative Verzahnung der MP mit den Services umgesetzt werden und die Services wären an die MP gebunden. Bei einer Implementierung des Berechtigungsmanagements über die Zertifizierungsstelle der MP müssten die Services zudem Konfigurationsmöglichkeiten direkt in der CA erhalten oder es müssten andere Prozesse zum Festlegen der Attribute etabliert werden. Zudem müssten Zertifikate bei jeder Attributsänderung, also ggf. häufig, widerrufen werden. Auf Unternehmensseite ist es den Unternehmen generell freigestellt, ob und wie Zertifikate für welche Zwecke eingesetzt werden und welche Attribute dazu ggf. in Zertifikaten hinterlegt werden.

Vorgehensweise zur Umsetzung der IT-Sicherheit

Für die ESP und die Services der ESP wurde, basierend auf Empfehlungen und Vorgaben seitens der bereits erwähnten Standards und Richtlinien eine Vorgehensweise erarbeitet, die im Folgenden vorgestellt werden soll.

Diese beinhaltet folgenden Schritte, die den aktuellen Projektstand widerspiegeln und als Basis für die weitere Entwicklung dienen sollen. Sofern sich Anforderungen, gesetzliche Rahmenbedingen oder Ziele ändern, ist immer auch eine Überprüfung und gegebenenfalls eine Anpassung erforderlich.

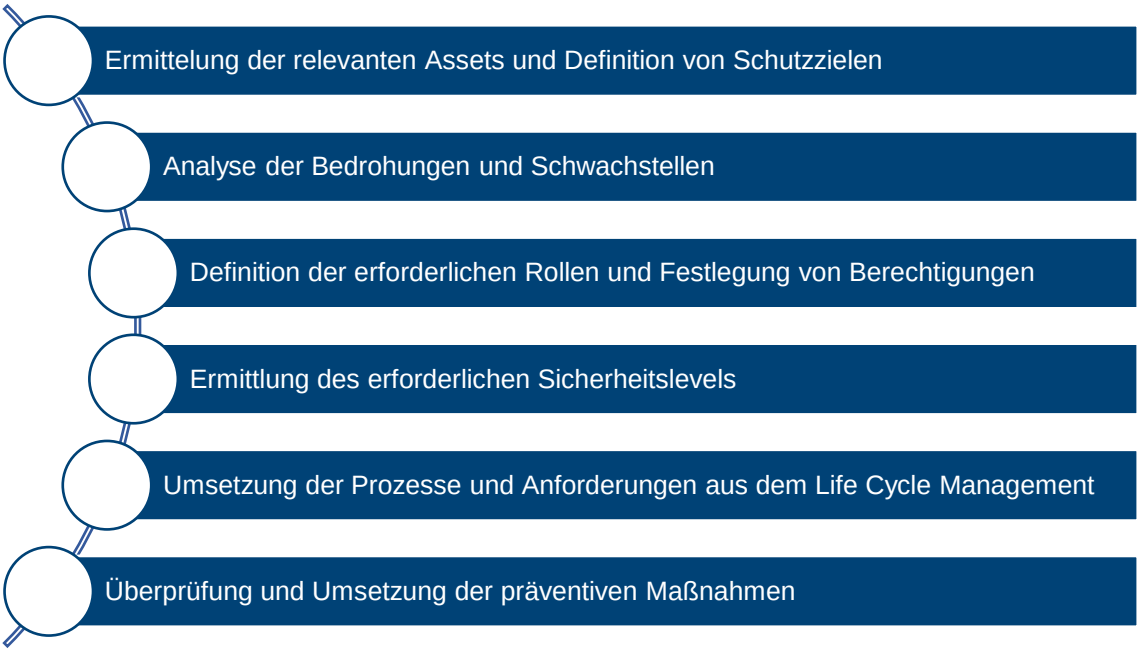


Abbildung 2: Schritte zur Umsetzung der IT-Security

Ermitteln relevanter Assets und Definition von Schutzziele

Zu Beginn ist es notwendig die Assets zu ermitteln, die es zu schützen gilt und die erforderlichen Schutzziele zu definieren. Für die UP und die MP wurden diese Schutzziele bereits in einer allgemeinen Form definiert. Diese können sich im Rahmen einer Entwicklung und beim Einsatz jedoch ändern und sind generell wiederkehrend auf deren Gültigkeit zu überprüfen und gegebenenfalls anzupassen:

Schutzziele der UP

1. Die Produktionsprozesse der Unternehmen dürfen durch jegliches Handeln der Plattform nicht ungewollt beeinflusst, verzögert oder behindert werden.
2. Die Verfügbarkeit der Plattform muss innerhalb eines definierten Service Level Agreements (SLA) gewährleistet sein.
3. Die Plattform muss vor unberechtigtem Zugriff geschützt werden.
4. Informationen, die Rückschlüsse auf die Produktion eines Unternehmens erlauben, dürfen nur nach dem "need to know"-Prinzip weitergegeben werden.
5. Die Informationen der Plattform dürfen nicht unerlaubt verändert werden.
6. Die Informationen der Plattform müssen vor Verlust geschützt werden (Backups, Checksums, USV).
7. Beim Austausch von sensiblen Informationen muss die Identität aller Kommunikationspartner (dies meint sowohl Benutzer als auch Systeme) sichergestellt werden.
8. Jegliche Aktion einzelner Stakeholder und der Plattform selbst müssen sicher protokolliert werden. Insbesondere bei Maßnahmen, die einen Einfluss auf die Produktion oder den Handel haben.
9. Jegliche Aktion muss einem Stakeholder oder einer Plattform-Komponenten zugeordnet werden können und diese Zuordnung darf nicht anfechtbar sein. So, dass diese Informationen gegebenenfalls vor Gericht als Beweis verwendet werden können.
10. Umsetzung eines Notfallmanagements: Die Plattform muss im Notfall deaktiviert werden können, so dass die Produktion durch einen Fehler der Plattform nicht unterbrochen wird bzw. die Produktion wiederaufgenommen werden kann.

Schutzziele der MP

1. Das Marktmodell und die dazugehörigen Marktmechanismen zeichnen sich durch eine angemessene Robustheit aus
2. Die Verfügbarkeit der Plattform muss innerhalb eines definierten SLAs gewährleistet sein.
3. Im Routinebetrieb auftauchende Fehler müssen erkennbar sein und dürfen die Stabilität der Marktplattform nicht gefährden
4. Glaubhafte Nachweisbarkeit der Identität eines einzelnen Marktteilnehmers gegenüber den anderen Marktteilnehmern muss gewährleistet werden.
5. Informationen müssen eindeutig ihrer Informationsquelle zugeordnet sein.

6. Rechtlich relevante elektronische Informationen dürfen nur von autorisierten Stakeholdern erstellt und verändert werden. Jede Modifikation muss nachvollziehbar und zurückverfolgbar sein.
7. Informationen dürfen für unberechtigte Dritte nicht einsehbar sein.
8. Zugriffe auf die Marktplattform und deren angebotene Dienste sowie die Einigung und der Abschluss eines Handels müssen sicher protokolliert werden.
9. Bereitstellung von Informationen, die ggf. vor Gericht als Beweis verwendet werden können, wobei eine Manipulation eben dieser ausgeschlossen werden muss.
10. Die Verfügbarkeit der Daten muss sichergestellt sein (z. B. durch Backups).

Schutzziele resultierend aus KRITIS

Mit der Richtlinie zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen (EU-Richtlinie 2008/114/EG) hat die Europäische Kommission die Grundlage für die Ermittlung und Ausweisung von Kritischen Infrastrukturen (EKI bzw. EPSKI),) geschaffen, um damit die Bewertung der Notwendigkeit ihres Schutzes zu verbessern. Die Richtlinie konzentriert sich auf die Sektoren Energie und Verkehr. Die nationale Umsetzung der Richtlinie unterliegt den Mitgliedsstaaten.

In Deutschland regeln dies für die Kritischen Infrastrukturen (KRITIS) das IT-Sicherheitsgesetz IT-Sig 2.0 (Bundesrepublik Deutschland 2021a) und die BSI-Kritis Verordnung (BSI – Bundesamt für Sicherheit in der Informationstechnik 2021) Für die jeweiligen Sektoren werden die Details zur Umsetzung dann in aller Regel durch die Verbände geregelt. So legt der BDEW im Standard B3S (bdew 2019) weitere Anforderungen und Schutzziele für Aggregatoren im Sektor Energie fest, die aus den Sicherheitsanforderungen zur Einhaltung der Stabilität der Stromnetze resultieren, die nachfolgend als Schutzziele aus der Netzsicht für KRITIS bezeichnet werden:

- Es muss sichergestellt werden, dass Informationen, deren Offenlegung die zugesagte Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung oder die Einhaltung anderer relevanter Anforderungen in Bezug auf den sicheren Netzbetrieb in relevantem Umfang gefährden würde, Unberechtigten nicht bekannt werden.
- Es muss die Integrität, Authentizität und korrekte Verarbeitung von Informationen sichergestellt werden, deren fehlerhafte, manipulierte oder unvollständige Übertragung, Speicherung oder Verarbeitung die planmäßige Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung in relevantem Umfang beeinträchtigen oder die Einhaltung anderer Anforderungen in Bezug auf den sicheren Netzbetrieb gefährden würde.
- Es muss sichergestellt werden, dass Informationen, Systeme, Komponenten oder Prozesse, die für die planmäßige Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung oder die Einhaltung anderer relevanter

Anforderungen in Bezug auf den sicheren Netzbetrieb notwendig sind, im benötigten Umfang zur Verfügung stehen.

- Die durch den Aggregator zugesicherten Beiträge, z. B die Bereitstellung/Einspeisung elektrischer Leistung, darf nicht durch informationstechnische Vorfälle gestört oder unterbrochen werden.
- Die planmäßige Erzeugung und der planmäßige Verbrauch von Strom zur Gewährleistung der Versorgungssicherheit muss eingehalten werden.
- Informationstechnische Systeme, Komponenten und Prozesse in KRITIS (IT-Systeme der Prozessdatenverarbeitung zur Messung, Steuerung und Regelung), die für die Funktionsfähigkeit kritischer Dienstleistungen zur Steuerung und Bündelung elektrischer Leistung maßgeblich sind, sind in unterschiedlichen Lagen zu schützen.
- Von besonderer branchenspezifischer Relevanz sind somit die Bestandteile der Systemlandschaft und Prozesskette, die der Bündelung und Steuerung zahlreicher verteilter Erzeugungs- oder Verbrauchsanlagen an einer zentralen Stelle dienen und dadurch ein hohes Gefährdungspotenzial bei unplanmäßigen, fahrlässigen oder vorsätzlichen Ein- bzw. Zugriffen sowie Störungen beinhalten. D. h. besonders relevant sind Komponenten, die von einer Stelle ausgehend eine hohe duplizierende Wirkung im Gesamtsystem zulassen (i. d. R. zentrale Systeme und Prozesse mit verteilender Wirkungskette von innen nach außen).

Analyse der Bedrohungen und Schwachstellen

Bei der Software-Entwicklung geht es zuallererst darum, eine Software zu entwerfen, welche die vorgegebenen Aufgaben erfüllt. Was die Aufgaben einer Software sind, wird in den Anforderungen festgehalten, die mit verschiedensten Requirements-Engineering-Prozessen ermittelt werden. Threat-Modeling ist ein Prozess zur Bestimmung der Sicherheitsanforderungen.

Das *Threat modeling manifesto* definiert Threat-Modeling folgendermaßen (Threat Modeling Manifesto 2020)

> *Bei der Bedrohungsmodellierung (Threat-Modeling) werden Darstellungen eines Systems analysiert, um Bedenken hinsichtlich der Sicherheits- und Datenschutzmerkmale aufzuzeigen.*
> *Wenn wir ein Bedrohungsmodell (Threat-Model) erstellen, stellen wir vier Schlüsselfragen auf höchster Ebene:*
> *Woran arbeiten wir? Was kann schiefgehen? Was werden wir dagegen tun? Haben wir unsere Arbeit gut genug gemacht?*

Im Gegensatz zu anderen Methoden der Anforderungsermittlung liegt der Fokus des Threat-Modelings auf der Fragestellung, welche Gefahren bei der Verwendung der Software auftreten können. Als Gefahr versteht man dabei alle ungewollten Ereignisse und Interaktionen, welche eine negative Auswirkung haben können. Erst mit dem Wissen über die möglichen Gefahren, befasst man sich mit den verbundenen Risiken und den Gegenmaßnahmen, welche die Risiken reduzieren und die potenziellen Schäden mindern.
Um die Gefahren zu ermitteln, benötigt man ein solides Verständnis über die Funktionsweise der Software und über das Umfeld, in dem diese eingesetzt wird. Hierzu reicht es nicht aus den Quellcode zu betrachten, sondern es muss zusätzlich geklärt werden:

- Wer mit dem System interagiert? Das bezieht sowohl die Benutzer als auch andere Software-Systeme mit ein.
- Wie die Software ausgeführt wird? Handelt es sich um eine Desktop-Anwendung, einen Betriebssystem-Dienst oder eine Server-Anwendung?
- Wie die Software angebunden ist? Kann die Software mit anderen Prozessen, Betriebssystem-Diensten, Server im LAN oder WAN kommunizieren?
- Wie und wer kann mit der Software interagieren? Öffnet die Software einen Netzwerk-Port, einen IPC-Endpunkt oder eine manuelle Eingabe?

- Wie sensible sind die Informationen, die durch die Software verarbeitet werden?

Die Beantwortung dieser Fragen lässt sich alleine mit der Funktionsbeschreibung der Software nicht beantworten, sondern es müssen zusätzliche Betrachtungen erfolgen. Die Gründe dafür sind unter anderem, dass

- eine Software meist mehr Funktionen anbietet als in einer Installation genutzt werden
- die Anbindung und Interaktionsmöglichkeit beschränkt werden kann (z.B. durch eine Firewall, ein VPN, das Betriebssystem, die Konfiguration der Software)
- die Benutzer der Software nicht bestimmt werden können und
- die zu verarbeitenden Informationen nicht bekannt sind.

Zur Beantwortung dieser Fragen ist es hilfreich, ein Modell der Software zu erstellen, in dem nicht nur die Interna der Software repräsentiert werden, sondern auch das Umfeld, in dem die Software ausgeführt wird. Zur Modellierung der Software können verschiedene Beschreibungen angewendet werden, solange die Interaktionen mit den Akteuren und die Interna der Software modelliert werden können. Die geläufigen Beschreibungssprachen sind UML-Sequenz-Diagramme und Datenflussdiagramme (DFD), aber auch Zustandsdiagramme, Message Sequence Charts und Business Process Model and Notation (BPMN) können verwendet werden. Dabei hängt es von der Software und dem Umfeld ab, welche Beschreibungssprache den Sachverhalt am besten beschreibt. Bei einer Software mit vielen Funktionen oder einem komplexen Umfeld empfiehlt es sich, mehrere Modelle zu erstellen, wobei auch verschiedene Beschreibungssprachen verwendet werden können.

Nachdem ein Modell der Software erstellt wurde, beginnt die Analysephase des Threat-Modelings. Ziel dieser Phase ist es Fehlverhalten der Software zu finden, welche beim Betrieb der Software auftreten können. Was ein Fehlverhalten ist, hängt von der Software und des Umfeldes ab, in dem die Software eingesetzt wird. Sobald ein Fehlverhalten eine negative Auswirkung haben könnte, wird sie als Bedrohung[10] klassifiziert. Am Ende der Analysephase hat man eine Liste der Bedrohungen für die analysierte Software.
Die einfachste Form der Analyse ist ein einfaches Brainstorming mit den Stakeholdern, bei dem die Beteiligten ihre Bedenken gegenüber der Software einbringen können. Dieser einfache Ansatz hat aber das Problem, dass zum einen nicht immer alle Stakeholder zur Verfügung stehen. Zum anderen liegt der Fokus der Stakeholder eher auf den Aufgaben, welche die Software erledigen soll, weniger auf dem was nicht passieren darf. Um dem entgegenzuwirken, wurden verschiedene formalere Methodiken entwickelt, welche in der Analysephase eingesetzt werden können, wie STRIDE (Kohnfelder und Garg 1999; Shostack 2014), PASTA (UcedaVelez und Morana 2015), TRARA (Wynn et al. 2011) und Trike (Larcom und Eddington

[10] aus dem englischen Threat übersetzt

2005) und viele andere mehr (Shevchenko et al. 2018). Für das Projekt SynErgie kamen STRIDE und PASTA in die engere Auswahl.

Die älteste dieser Methodiken ist STRIDE und ihre Spezialisierungen STRIDE-per-Element und STRIDE-per-Interaction (Kohnfelder und Garg 1999; Shostack 2014). STRIDE steht für die sechs möglichen Fehlerklassen (Kohnfelder und Garg 1999; Shostack 2014)

- **S**poofing - Vortäuschen einer fremden Identität
- **T**ampering - Manipulation von Daten auf der Festplatte, dem Netzwerk oder wo anders
- **R**epudiation - Abstreitbarkeit einer Handlung
- **I**nformation disclosure - Einsicht in Informationen durch unautorisierte Dritte
- **D**enial of service - Herbeigeführter Ausfall einer Funktion der Software
- **E**levation of privilege - Erlauben von Handlungen durch unautorisierte Dritte

Bei der Anwendung von STRIDE werden alle Elemente des Modells betrachtet und je Element wird die Frage gestellt, ist eine diese Fehlerklassen hier anwendbar? Sobald ein Fehler gefunden wurde und dieser als Bedrohung eingestuft werden kann, wird dieser in die Liste der Bedrohungen aufgenommen. Häufig muss bei STRIDE die Liste der Bedrohungen am Ende der Analysephase nochmal auf Duplikate hin überprüft werden, da viele Fehler über mehrere Fehlerklassen gefunden werden können. Die Liste wird im Anschluss nach dem potentiellen Schaden sortiert, welchen die Bedrohungen verursachen könnten.
Eine neuere Methodik ist PASTA (Process for Attack Simulation and Threat Analysis), deren Fokus auf einem deutlich formelleren Vorgehen liegt und dabei die Modellierung miteinschließt. PASTA ist in sieben Schritte unterteilt (UcedaVelez und Morana 2015)

1. Define Objectives - Festlegen der Ziele der Software, sowie der gesetzlichen Vorgaben
2. Define Technical Scope - Beschreibung des technischen Umfeldes
3. Application Decomposition - Modellierung des Systems
4. Threat Analysis - Ermittlung von Bedrohungen aus vergangenen internen und externen Ereignissen und Angriffsbibliotheken
5. Vulnarability & Weakness Analysis - Sammlung von Schwachstellen im Design und in den verwendeten Komponenten
6. Attack Modeling - Beschreibung von möglichen Angriffen auf Basis der gefundenen Bedrohungen und Schwachstellen
7. Risk & Impact Analysis - Bewertung der gefundenen Angriffe nach ihrem Risiko und dem möglichen Schaden

PASTA hat den Vorteil, dass in den Schritten 1, 2, 4 und 5 die potenziellen Angriffsflächen der Software, die möglichen Angreifer und deren Ziele dokumentiert werden. Aber den Nachteil, dass es schwierig anzuwenden ist, wenn die Umsetzung der Software, das Umfeld, in dem sie

ausgeführt wird oder die möglichen Angreifer und deren Ziele nicht klar definiert werden kann. Zusätzlich hat PASTA einen höheren Arbeitsaufwand im Vergleich zu STRIDE (Shevchenko et al. 2018).

Nach der Analysephase beginnt die Abwehrphase, in der die Bedrohungsliste beginnend mit der größten Bedrohung bearbeitet wird und für jede Bedrohung die möglichen Gegenmaßnahmen betrachtet werden. Dabei muss der Aufwand, welcher durch die Umsetzung der Gegenmaßnahmen entsteht, gegen die Risiken und den Schaden der Bedrohung abgewogen werden. Eine Gegenmaßnahme kann dabei sowohl eine Veränderung der Software bedeuten (z.B. Verbesserung der Zugriffskontrolle) als auch eine Veränderung in der Umgebung (Zugang zur Software ist nur noch aus einem internen Netz möglich.). Sollte der zu erwartende Schaden oder das Risiko sehr gering sein, ist es auch durchaus möglich, keine Gegenmaßnahme zu treffen. Sobald die Gegenmaßnahmen umgesetzt sind, beginnt die Introspektionsphase, in der das Modell, die Bedrohungen und die Gegenmaßnahmen nochmal betrachtet werden. Dabei wird überprüft, ob und wie die Gegenmaßnahmen die Software oder das Umfeld beeinflussen, wodurch sich wiederum die Bedrohungen verändern. An dieser Stelle könnte man wieder bei der Modellierung anfangen. Die Introspektionsphase gibt aber auch die Gelegenheit das Vorgehen zu evaluieren.

Die Durchführung eines Threat-Models hat für jede Komponente zu erfolgen. Jede Komponente ist entweder Teil der UP, der MP oder ein Service, welcher auf einer der beiden Plattformen ausgeführt wird. Für die Threat-Models wird von allen Entwicklungsteams STRIDE empfohlen. Für die Modellierung können Datenflussdiagramme verwendet werden. Der Fokus liegt bei der Durchführung auf STRIDE in Verbindung mit Datenflussdiagrammen, da STRIDE weniger formell und daher schneller zu erlernen ist und Datenflussdiagramme, im Gegensatz zu anderen Beschreibungssprachen, nur aus fünf Elementen bestehen[11]. Dies erleichterte die Einarbeitung für die Teams.

Um die Durchführung zu beschleunigen, können existierende Diagramme wiederverwendet werden. Es ist ratsam, dass Entwicklungsteams neben der Durchführung mit einem IT-Sicherheitsexperten auch selbständig eine Analysephase durchführen, was folgende Gründe hat: Zum einen werden die Teams dazu gebracht, darüber nachzudenken wie das Umfeld ihrer Komponente aussehen wird. Zum zweiten müssen sich die Teams mit möglichen Fehlern und Bedrohungen, denen ihre Komponente standhalten muss, auseinandersetzen. Zum dritten, die Teams sind diejenigen, welche ihre Software am besten verstehen und daher bessere Modelle erstellen und bei der Fehlersuche besser mit den Details vertraut sind.

[11] Datenflussdiagramme sind nicht wie UML und BPMN standardisiert, daher variiert die Zahl der Elemente je nach Autor und der Art zu zählen zwischen vier und zwölf.

Die Threat-Models der Teams sollten dann zentral nach der Analyse der Teams gesammelt und vereinheitlicht und nochmal analysiert werden, wenn es die gesamte Plattform betrifft, um dann in die Abwehrphase überzugehen. In der Abwehrphase werden Gegenmaßnahmen gefunden, von denen möglichst viele Teams gleichzeitig profitieren. Auf diese Maßnahmen wird im folgenden Abschnitt eingegangen.

Im Rahmen des im Projektverlaufs durchgeführten Threat Models mit den Service-Erstellern und den zusammengeführten Threat Models zeigten sich Bedrohungen, die Maßnahmen erfordern. Im weiteren Projektverlauf ist das Threat Modeling zyklisch durchzuführen und neu zu bewerten.
Als Beispiele sollen folgende ermittelte Bedrohungen nun einmal exemplarisch benannt werden:

Fehlendes Logging
Um einen Angriff frühzeitig zu erkennen und diesen im Nachhinein zu analysiert, benötigt man Informationen über die sicherheitsrelevanten Aktivitäten im System an einer zentralen Stelle. Diese Aktivitäten müssen von allen Komponenten der ESP erkannt und als Log-Event an einen zentralen Log-Server übertragen werden

Unzureichende Datenvalidierung
Eine ausführliche Datenvalidierung ist ein entscheidender Beitrag zum Härten einer Software. Eine unzulässige Eingabe muss sicher erkannt, abgelehnt und ein entsprechendes Log-Event erzeugt werden. Was eine unzulässige Eingabe ist, hängt von der Software und ihren Anforderungen ab.

Fehlende Autorisierung in der UP
Innerhalb der UP führen die Services keine Autorisierung durch, sondern bauen darauf, dass alle Nachrichten, welche diese empfangen, bereits vom Manufacturing Service Bus[12] (MSB) autorisiert wurden.
Der Grund hierfür war eine frühe Designentscheidung für die UP.
Allerdings verhindert diese Entscheidung eine „Defense-in-Depth“-Strategie, bei der auf mehreren Ebenen Sicherheitsüberprüfungen durchgeführt werden

Unbekannte Quelle über den MSB
Innerhalb der UP können die Services den Erzeuger einer Nachricht nicht bestimmen. Dies hängt damit zusammen, dass einige Komponenten als Proxy/Broker fungieren und Nachrichten von einem Service empfangen und an andere Services unverändert weiterleiten. Beispiele für solche Komponenten sind der MSB und der Energieflexibilitätsmanagementservice[13] (EFMS).

[12] Der MSB ist eine im Projekt verwendeten Middleware des Fraunhofer IPA zum standardisierten Datenaustausch
[13] Das übergeordnete Ziel des EFMS ist es, die im Unternehmen vorhandene Energieflexibilität zu verwalten und zu orchestrieren.

Da innerhalb der UP alle Nachrichten über den MSB gehen, sind alle Services der UP von diesem Problem betroffen.

(Svc_A → MSB → Svc_B)
(Svc_C → MSB → Svc_B)

Der MSB ist zwar in der Lage via TLS-Client-Authentication die direkten Kommunikationspartner zu identifizieren. Allerdings kann der MSB diese Information nicht verlässlich weiterleiten. Weiterhin gibt es auch andere Proxy-Services, wie den EFMS, welche die Überprüfung der Quelle erschweren.
(Svc_A → MSB → EFMS → MSB → Svc_B)

Manipulierbare Nachrichten in der UP
Nachrichten, welche über den MSB und andere Proxyserver versendet werden, können von diesen Komponenten manipuliert werden, ohne dass der Sender oder der Empfänger dies feststellen kann.

Versand in der UP ist abstreitbar
Dadurch, dass eine Nachricht auf dem Weg zwischen den Services manipuliert werden kann, ist es möglich den Inhalt einer Nachricht abzustreiten.
Dadurch, dass ein Empfänger nicht bestimmen kann, wer eine Nachricht verfasst hat, ist es dem Sender möglich den Versand abzustreiten.
Dies ist ein Problem, sobald es für den Sender von Vorteil ist den Versand oder den Inhalt abzustreiten. Bisher ist noch kein Szenario bekannt, wo dies innerhalb der UP vorkommt.

Uneinheitliche Konfigurationsschnittstellen
Manche Services bieten eine Schnittstelle an, mit der im laufenden Betrieb der Service umkonfiguriert werden kann. Eine solche Schnittstelle muss besonders abgesichert werden. Besonders wenn dies in Form einer Web-UI geschieht, ist dies ein weiteres Problem, da damit alle Sicherheitsprobleme aus dem Bereich der Web-Anwendungen (CSRF, Session-Stealing, ...) zu den bereits existierenden hinzukommen. Zieht man zusätzlich noch in Betracht, dass viele dieser Einstellungen einmalig oder nur selten angepasst werden müssen, sollte abgewogen werden, wie hoch der Nutzen einer solchen Schnittstelle hinsichtlich Aufwand und Risiko ist.

Schwachstelle selbst-entwickelte Benutzerverwaltung
Beim Erstellen der Threat-Models zeigt sich häufig, dass viele Services einen Benutzer identifizieren und autorisieren müssen. (z.B. für die Web-Konfigurations-Schnittstellen) Hierfür wurden Benutzerdatenbanken und Log-in-Mechanismen in die Services integriert. Zum einen müssen diese Log-In-Mechanismen auf Ihre Sicherheit hin geprüft werden.

Zum anderen müssen die Benutzerdatenbanken vor einem unberechtigten Zugriff geschützt werden. Besonders in der UP ist dies nicht notwendig und führt zu einem höheren administrativen Aufwand.

1. Es müssten die Benutzer und deren Rechte auf jedem Service separat verwaltet werden.
2. Es besteht die Gefahr, dass die Benutzerdatenbank eines Service von einem Angreifer ausgelesen wird und die darin enthaltenen Login-Informationen bei anderen Services wiederverwendet werden können.

Bedrohung: Denial-of-Service via Ressourcenerschöpfung
Jedes Programm verwendet Ressourcen (CPU, RAM, Festspeicher, Bandbreite, …) und ein Programm kann seine Aufgabe nicht ausführen, wenn nicht die ausreichenden Ressourcen zur Verfügung stehen. Dies kann gezielt ausgenutzt werden, um die Ausführung des Programms selbst, alle seine Benutzer und alle verbunden Programme zu stören.
Besonders Angriffsziele sind Ressourcen wie (Fest-)Speicher oder Kommunikationsbandbreite welche leicht von außen erschöpft (in hohem Maße ausgelastet) werden können.

Definition der Rollen und Festlegung von Berechtigungen

Ein weiteres Sicherheitsmerkmal ist die Umsetzung eines geeigneten Rechte- und Zugriffsmanagement. Für die ESP und ihre Teilplattformen wurde ein rollenbasiertes Rechtekonzept gewählt.

Basis eines rollenbasierten Rechtekonzepts ist die Definition von Rollen, denen ganz spezifische Aufgaben übertragen werden und die hierfür erforderlichen Rechte eingeräumt werden. Je feingranularer die Definition der Rollen erfolgt, desto übersichtlicher ist die Vergabe der notwendigen Rechte. Die Besetzung der Rolle erfolgt dann durch die Zuweisung der Rolle zu einer Stelle, also letztendlich einem Mitarbeiter. Ein Rollenkonzept ermöglicht, dass eine Person mehrere Rollen in einem Unternehmen übernimmt. Dabei gilt es abzuwägen, ob bestimmte Kombinationen von Rollen ein potenzielles Risiko darstellen können. Ein Anwendungsentwickler sollte bspw. nicht gleichzeitig der Test Manager sein. Ebenso kann eine Rolle aber auch mehreren Mitarbeitern zugeordnet werden.

Tabelle 2: Empfehlungen zur Rollendefinition[14]

Empfehlungen zu Rollendefinitionen
Rollen sollen dem Need-to-Know-Prinzip entsprechen
Anwendung des Least-Privileg Prinzips – Die Rolle soll nur die für seine Aufgabe notwendigen Rechte erhalten
Nutzer, Geräte und Anwendungen werden den Rollen zugeordnet
Rollenkonflikte werden bei der Rollenzuordnung geprüft und aufgelöst
Rollenzuordnungen zu Stellen werden zeitlich befristet
Ausscheidende Mitarbeiter, Altgeräte und zu löschende Anwendungen werden von ihren Rollen getrennt, d.h. die Zuordnung wird aufgelöst.
Bei den Rollen sollen System- und Fachaufgaben getrennt werden
Rollen werden nach dem 4-Augen Prinzip definiert
Die Rollenzuordnung wird regelmäßig geprüft und aktualisiert
Es gibt einen Freigabe-Workflow für Benutzer, Geräte, Anwendungen, Clouds, Rollen und Privilegien
Für tragende Rollen erfolgt eine angemessene Sicherheitsüberprüfung
Die Besetzung von Rollen erfordert eine Beurteilung der Vertrauenswürdigkeit und der Befähigung

Aus der Aufgabenbeschreibung der Rolle resultieren die notwendigen Berechtigungen. Für SynErgie wurden bereits in der Vergangenheit Stakeholder oder Akteure benannt, die nun als Basis für die Rollen dienen. Zusätzlich wurden diese durch Rollen ergänzt, die sich aus dem Security Life Cycle Management als notwendig ergeben. Bei der Definition von Rollen und der Vergabe von Rechten gilt es einige Regeln zu beachten. In Tabelle 2 werden einige grundlegenden Empfehlungen aufgeführt, die bei der Definition von Rollen beachtet werden

[14] (BSI-Standard 200.2), (Bundesamt für Sicherheit in der Informationstechnik 2021), (Datenschutz PRAXIS für Datenschutzbeauftragte 2019).

sollten (BSI-Standard 200.2), (Bundesamt für Sicherheit in der Informationstechnik 2021), (Datenschutz PRAXIS für Datenschutzbeauftragte 2019).

Zusätzlich sind bei der Besetzung von Rollen bei Kritischen Infrastrukturen die Anforderungen aus dem internationalen Standard ISO/IEC 27001 Anhang A (Deutsches Institut für Normung e.V.) zu beachten, die sich speziell auch mit dem Thema der Sicherheitsüberprüfung und Beurteilung der Befähigung beschäftigen.

Nachfolgend werden einige ausgewählte Rollen der Marktplattform und der Unternehmensplattform beschrieben, die für das Deployment und den Betrieb zuständig sind. Die Rollen werden dabei, wie in Abbildung 3 dargestellt, in sechs Kategorien unterteilt. In Kapitel **Prozesse und Anforderungen des Security Life Cycle Managements** werden zu den jeweiligen Lebensphasen weitere Rollen benannt, die sich je nach Organisation und Unternehmen unterscheiden können und deren Beschreibung sich nicht aus der ESP heraus ergibt.

Abbildung 3: Kategorisierung der Rollen der UP und MP

Infrastrukturbetreiber
Der Infrastrukturbetreiber stellt die Infrastruktur und Umgebung (Server, Cloud) für den sicheren Betrieb der Plattform bereit. Die Rolle ist optional. Sofern der Plattformbetreiber die Plattform auf seiner eigenen Infrastruktur betreibt, übernimmt der Plattformbetreiber die Funktion des Infrastrukturbetreibers. Zu den Pflichten des Infrastrukturbetreibers gehört der sichere und zuverlässige Betrieb, der Schutz der Infrastruktur gegen Cyberangriffe, die Verfügbarkeit der Infrastruktur entsprechend vereinbarter SLAs.

Plattformbetreiber
Der Plattformbetreiber ist verantwortlich für den operativen (inhaltlichen) Betrieb der jeweiligen Plattform (MP oder UP). Für den operativen Betrieb sind weitere, hierarchisch untergeordnete Rollen erforderlich. Die für die IT-Sicherheit relevanten Rollen sind administrative Rollen wie Administratoren und Identitätsmanager.

Administratoren
Die Rollen der Administratoren gelten beim Deployment und Betrieb als tragende Rollen. Ihnen obliegt die Verantwortung Services zu installieren, einen eingebundenen Service zu administrieren, erforderliche Zugriffsrechte einzuräumen und den Datenaustausch zu konfigurieren. Aus diesem Grunde lautet die Empfehlung, die Administratorenrollen zu untergliedern, um einen möglichen Schaden im Falles eines erfolgreichen Spoofing- oder Elevation of Privilege-Angriffs oder durch einen korrumpierten Administrator zu begrenzen.

Administratorrollen der MP:

- Root CA Admin: verantwortlich für die Administration der Root-CA
- Sys Admin: Administration der IT-Infrastruktur und der Betriebssysteme
- Operativer Admin: Administration und Wartung der Marktplattform und der Services der Marktplattform
- User Manager: Administrator, dem die Verwaltung der Nutzer (Service-Nutzer und Service Anbieter) obliegt

Administratorrollen der UP:

- Sys Admin: Administration der IT-Infrastruktur und der Betriebssysteme
- Service Kurator: Buchung von Services am Marketplace und Aufnahme in das Repository der UP
- Service Integrator: Installation der Services aus dem Repository und Konfiguration der Datenflüsse zwischen den Services der UP über den Data Integration Flow des MSB
- Service Admin: Konfiguration der spezifischen Services der UP über das Konfigurations-Interface der Services
- IAM Manager: Legt Nutzer im System der UP an, erteilt die erforderlichen Berechtigungen und hält diese aktuell

Nutzer – Anwenderrollen
Als Nutzer sind die Anwender der UP benannt, die im Rahmen ihrer betrieblichen Aufgabenbeschreibungen die UP und die Services zur Unterstützung ihrer Tätigkeiten nutzen. In den Diskussionen und Workshops zeigte sich, dass eine Beschreibung der einzelnen Anwenderrollen nur exemplarisch erfolgen kann, da diese sehr unternehmensspezifisch sind.

Allgemein können dies Energie Manager, Produktionsplaner, Maschinen Operatoren, Flex Händler, Energie Einkäufer, Energie Verkäufer usw. sein. Aus Sicht der IT-Security und des Rechtekonzepts lässt sich zum aktuellen Zeitpunkt festhalten, dass diese Rollen nur auf die für den Aufgabenbereich relevanten Services und Informationen Zugriff erhalten sollten. Wichtig für die IT-Security ist, dass die Zugriffsrechte und Ausführungsrechte, die den Anwendern eingeräumt werden, so eingerichtet werden, dass das Least-Privilege-Prinzip und das Need-to-Know-Prinzip eingehalten werden. Eine Rolle soll jedoch herausgegriffen werden, da diese aktuell die Entscheidung darüber trifft, welche Inserate auf welchem Markt angeboten werden sollen:

- Flex Manager: Ist als Entscheider bei der UP dafür verantwortlich, ob ein Flexibilitätsinserat das Unternehmen „verlässt“ und somit am Strommarkt angeboten wird.
- Marktrollen und Netze: Für die Beschreibung der Marktrollen und der Rollen des Netzbetriebs wird derzeit auf die Rollenbeschreibungen des BDEW (Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) 2019) und der ENTSO-E (ENTSO-E 2020) verwiesen. Ob es im Rahmen eines lokalen Strommarktes zu weiteren Rollendefinitionen kommen wird, muss dann geklärt werden, wenn dieser Strommarkt weiter spezifiziert ist. Aktuell erfolgt die Kommunikation zu externen Rollen der Flexibilitätsvermarktung über die Vermarktungskomponente der UP.

IT-Sicherheitsteam (Resilienz und Angriffsabwehr)
Damit den Anforderungen des neu verabschiedeten IT-Sicherheitsgesetztes IT-Sig 2.0 (Bundesrepublik Deutschland 2021b) und der heraus resultierenden BSI-KritisV (BSI – Bundesamt für Sicherheit in der Informationstechnik 2021) für KRITIS entsprochen wird, ist es zukünftig erforderlich, beim Einsatz der ESP (in der Hauptsache der UP) im Bereich KRITIS Maßnahmen zur Früherkennung von Cyber-Angriffen und zur Angriffsabwehr zu ergreifen. Im Falle erfolgreicher erheblicher Sicherheitsvorfälle muss eine Meldung an die Meldestelle des BSI erfolgen. Aber auch aus betrieblicher Sicht ist es sinnvoll sich mit der Angriffsabwehr und Notfallplänen und einer schnellen Wiederherstellung von Systemen, im Falles eines erfolgreichen Cyber-Angriffs, auseinanderzusetzen. Für diese Aufgaben wurden aktuell drei Rollen definiert, die exemplarisch sind und im Unternehmen konkretisiert werden sollten. Diese Rollen gehören dem Computer Security Incident Response Team, oder abgekürzt CSIRT, an.

- **IT SicherheitsOperator**: Überwacht die ordnungsgemäße Funktion der Plattform und der Services, ist für die Erkennung von ungewöhnlichem Verhalten zur Früherkennung von Cyber-Attacken verantwortlich und übernimmt die Aufgaben, die aus den Anforderungen des IT-Sicherheitsgesetzes 2.0 zur frühzeitigen Angriffserkennung und Abwehr für KRITIS erforderlich sind. Er übernimmt bei KRITIS die Meldung erheblicher Sicherheitsvorfälle an die Meldestelle des BSI.

- **Incident Manager:** Ist verantwortlich für die Aufrechterhaltung des Betriebs und die effektive Durchführung des Incident-Management-Prozesses
- **Backup Manager:** Ist verantwortlich für die Planung und Durchführung regelmäßiger Backups und für die Festlegung der Intervalle. Zusammen mit dem Incident Manager sorgt er dafür, dass nach einem Ausfall der Plattformen die Aufnahme des Betriebs schnellstmöglich wieder erfolgen kann.

Ermittlung des erforderlichen Sicherheitslevels

Der Sicherheitslevel (SL) unterscheidet fünf diskrete Stufen und dient der Klassifikation und Spezifizierung von IT-Sicherheitsanforderungen, die einer Anwendung (Service) oder einer Komponente oder einem System zugeordnet werden. Dabei hat SL-0 die niedrigste Sicherheitsstufe und SL-4 die höchste Sicherheitsstufe.

Insgesamt werden für die ESP, sowie die Services und Komponenten fünf Sicherheitslevel (SL-0, SL-1, SL-2, SL-3 und SL-4) festgelegt (siehe hierzuTabelle 3), die sich aus dem erforderlichen Schutzbedarf (im Folgenden erforderliches Sicherheitsniveau genannt) und der Risikostufe (also dem Risiko, welche die jeweilige Komponente ausgesetzt sein wird) ergeben. Dabei nehmen die Anforderungen an die IT-Sicherheit und die hieraus abzuleitenden Maßnahmen bei höheren SLs zu.

Es soll sowohl den Anforderungen an die IT-Sicherheit, als auch den funktionalen Anforderungen Rechnung getragen werden. Die Anforderungen an die IT-Sicherheit fokussieren hierbei auf die Fähigkeiten und die Motivation eines potenziellen Angreifers. Die funktionalen Anforderungen legen Anforderungen an die Vertraulichkeit, die Integrität und an die Verfügbarkeit und das Erkennen und Behandeln von Fehlfunktionen fest.

Tabelle 3: Sicherheitslevel und resultierende Anforderungen

SL	Anforderungen an IT-Sicherheit	Funktionale Anforderungen
SL-0	Es sind keine Maßnahmen zum Schutz gegen Angriffe notwendig	Ein Schutz von Informationen ist nicht notwendig. Es bestehen geringe Anforderungen an die ordnungsgemäße Funktion. Ein Ausfall oder eine Fehlfunktion haben keine nennenswerten Auswirkungen
SL-1	Schutz gegen gelegentliche und zufällige Verstöße durch Angreifer mit geringen Fähigkeiten	Der Schutz von vertraulichen Informationen muss geringen Anforderungen genügen. Informationen sollten korrekt sein. Kleinere Fehler können toleriert werden. Fehler, welche die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkennbar oder vermeidbar sein. Längere Ausfallzeiten, sind zu vermeiden. Der Schutz personenbezogener Daten muss gewährleistet sein.
SL-2	Schutz gegen vorsätzliche Verstöße durch einfache Mittel mit geringem Ressourcenaufwand, generischen Security-Kenntnissen und geringer Motivation	Der Schutz vertraulicher Informationen muss mittleren Anforderungen genügen und in kritischen Bereichen stärker ausgeprägt sein. Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein. Längere Ausfallzeiten sind

		nicht akzeptabel. Der Schutz von vertraulichen Daten muss gewährleistet sein.
SL-3	Schutz gegen vorsätzliche Verstöße durch hochentwickelte Mittel mit moderatem Ressourcenaufwand und Expertenwissen, die mit klar definierten Zielen effektive, aber kostenorientierte Angriffsszenarien entwickeln und mit moderater Motivation vorgehen	Der Schutz vertraulicher und systemrelevanter Informationen muss hohen Anforderungen genügen. Die verarbeiteten Informationen müssen in hohem Maße korrekt sein, auftretende Fehler müssen erkennbar sein und es müssen Maßnahmen ergriffen werden bei Fehlfunktionen den Betrieb aufrecht zu erhalten oder Ausfallzeiten kurz zu halten.
SL-4	Schutz gegen vorsätzliche Verstöße durch hochentwickelte Mittel mit erweitertem Ressourcenaufwand, höchsten Fähigkeiten, die gegen ein spezifisch ausgewähltes Ziel vorgehen und über nahezu unbegrenzte finanzielle Mittel verfügen (Staatliche Organisationen)	Der Schutz vertraulicher und systemrelevanter Informationen muss höchsten Anforderungen genügen und in höchsten Maß korrekt sein. Die verarbeiteten Informationen müssen in höchstem Maß korrekt sein. Ausfallzeiten sind nicht akzeptabel.

Die Festlegung des Sicherheitslevels für eine Komponente erfolgt hierbei in drei Schritten.

In Schritt 1 wird der notwendige Schutzbedarf von Daten oder Informationen, mit denen ein Service oder eine Komponente arbeitet, festgelegt. In diesem Schritt steht der Schutzbedarf der Daten, die konsumiert, verarbeitet und erzeugt werden im Vordergrund.

Im zweiten Schritt erfolgt eine Betrachtung des potenziellen Risikos, die der Service oder die Komponenten ausgesetzt sind. Das Risiko kann dabei von unterschiedlichen Einflussfaktoren abhängen und ist gegebenenfalls branchen- aber auch unternehmensabhängig. Nicht jede Branche und jedes Unternehmen unterliegt identischen Risiken.

Im letzten, dritten Schritt wird dann aus den Ergebnissen aus Schritt 1 und Schritt 2 der erforderliche Sicherheitslevel bestimmt.

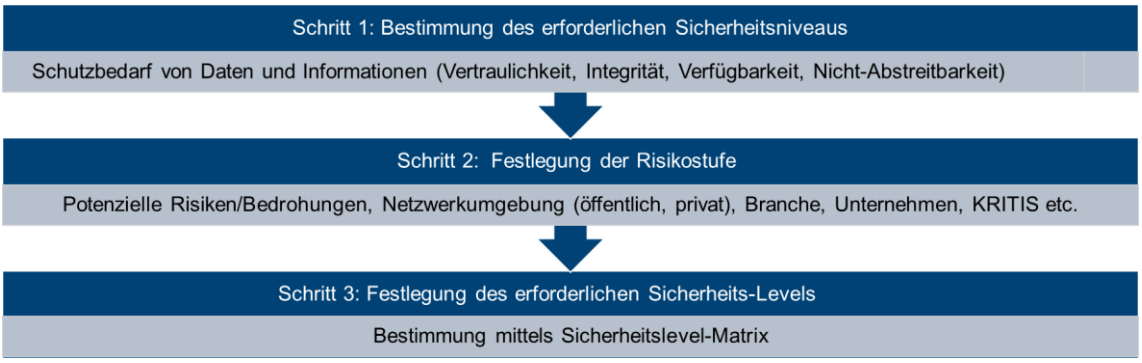


Abbildung 4: Vorgehensmodell zur Bestimmung des Sicherheitslevels

Eine detaillierte Beschreibung der erarbeiteten Vorgehensweise zur Ermittlung des notwendigen Sicherheitslevels wird nachfolgend beschrieben.

Bestimmung des erforderlichen Sicherheitsniveaus

Im ersten Arbeitsschritt soll das erforderliche Sicherheitsniveau bestimmt werden. Dieses resultiert aus dem Schutzbedarf, dem empfangene, verarbeitete oder zur Verfügung gestellte Daten unterliegen. Dabei werden diese in die INPUT, LOGIC und OUTPUT-Daten unterteilt. Damit eine belastbare Aussage über den Schutzbedarf getroffen werden kann, ist es erforderlich alle Kommunikationsbeziehungen eines Service zu benennen. Zur Erklärung: der Schutzbedarf eines Service resultiert aus den Informationen oder Daten mit den höchsten Anforderungen an den Schutzbedarf.

Die Vorgehensweise ist eine Zusammenführung und Adaption der Empfehlungen des NIST zu „Standards for Security“ (NIST (CDC) FIPS 199) und „Minimum Security Requirements FIPS-PUBS 200 (NIST (CDC) FIPS 200) und des BSI IT-Grundschutz (BSI-Standard 200.2).
Bei der Modellierung müssen die Kommunikationsbeziehungen eines Service mit anderen Services/Diensten oder Ressourcen benannt werden und es ist für jeden Datenaustausch eine Bewertung nach den Kategorien:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Nicht-Abstreitbarkeit

vorzunehmen. In der Literatur (Bundesamt für Sicherheit in der Informationstechnik 2022) werden diese oftmals auch als Grundwerte oder Schutzziele (BSI) benannt.

Vertraulichkeit
Eine Einschätzung wie schwerwiegend es wäre, wenn Informationen, welche von der Komponente verarbeitet, gespeichert und kommuniziert werden, unberechtigt veröffentlicht werden.

Integrität
Eine Einschätzung wie wichtig es für die Komponente ist, dass die von der Komponente verarbeiten gespeicherten und empfangenen Informationen nicht manipuliert wurden. Sowie, wie wichtig es ist, dass die Funktionsweise der Komponente korrekt ist.

Verfügbarkeit
Eine Einschätzung wie wichtig es ist, dass der Betrieb der Komponente stets aufrecht gehalten werden kann.

Nichtabstreitbarkeit (Verbindlichkeit)
Eine Einschätzung darüber wie wichtig es ist, dass die von der Komponente empfangen und versendeten Informationen verbindlich auf den Versender zurückzuführen sind.

Für die Einstufung der Grundwerte werden vier Stufen definiert (niedrig, normal, hoch und sehr hoch). Eine Beschreibung, die bei der Bestimmung dient, ist in Tabelle 4 verfügbar.
Die Betrachtung kann oder sollte nicht völlig isoliert für den Service selbst erfolgen, da dieser im Zusammenhang mit anderen Services als Gesamtheit für einen Geschäftsprozess eine mehr oder weniger hohe Relevanz hat. Diese übergreifende Betrachtung kann der Entwickler selbst möglicherweise nicht tätigen, so dass ein Systemintegrator oder der Systemarchitekt zu gewissen Zeitpunkten mit in die Festlegung einbezogen werden sollte. Andernfalls müssen Annahmen getroffen werden. Im Laufe des Projektfortschritts und auch im Rahmen des Life Cycle Managements müssen diese Einstufung zyklisch hinterfragt und hinsichtlich ihrer Richtigkeit immer wieder neu bewertet werden.

Der somit festgestellte Schutzbedarf und ein hieraus abgeleitetes, erforderliches Sicherheitsniveau unterliegen somit einer zyklischen Überprüfung und erfordern gegebenenfalls einer Anpassung, wenn sie Änderungen bei der Bewertung ergeben. Dies kann beispielsweise dann der Fall sein, wenn sich die Verfügbarkeitsanforderungen ändern oder die Vertraulichkeit der Informationen an Bedeutung gewinnt.

Bei der Einstufung des **erforderlichen Sicherheitsniveaus** sollen folgende Aspekte mit einfließen:

- Möglicher, resultierender Schaden (Schadenshöhe) bei Verletzung der Grundwerte (Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Abstreitbarkeit)
- Regulatorische Vorgaben (bspw. DSGVO. KRITIS, IT-Sicherheitsgesetz)
- Vorgaben aus (Branchen-)Standards oder Anforderungen aus relevanten Normen und für das Unternehmen erforderlichen Zertifizierungen
- Auswirkungen auf das Stromnetz im (abhängig von der gemanagten Energiemenge/Leistung – Überschreitung der Bemessungsgrenze für KRITIS)

Tabelle 4: Einstufung Erforderliches Sicherheitsniveau

Erforderliches Sicherheitsniveau	Beschreibung
Niedrig	Der Verlust der Vertraulichkeit, Integrität, Verfügbarkeit oder Nicht-Abstreitbarkeit hat **vernachlässigbare Auswirkungen** auf die Funktion der ESP (UP oder MP), den organisatorischen Betrieb, das Organisationsvermögen oder das System
Normal	Der Verlust der Vertraulichkeit, Integrität, Verfügbarkeit oder Nicht-Abstreitbarkeit kann **begrenzte nachteilige Auswirkungen** auf die Funktion der ESP (UP oder MP), den organisatorischen Betrieb, das Organisationsvermögen oder das System haben.
Hoch	Der Verlust der Vertraulichkeit, Integrität, Verfügbarkeit oder Nicht-Abstreitbarkeit kann **schwerwiegende nachteilige Auswirkungen** auf die Funktion der ESP (UP oder MP), den organisatorischen Betrieb, das Organisationsvermögen oder das System haben.
Sehr hoch	Der Verlust der Vertraulichkeit, Integrität, Verfügbarkeit oder Nicht-Abstreitbarkeit kann **schwerwiegende oder katastrophale nachteilige Auswirkungen** auf die Funktion der ESP (UP oder MP), den organisatorischen Betrieb, das Organisationsvermögen oder das System oder die Infrastruktur haben.

Methodisches Vorgehen:
Zur Bestimmung des erforderlichen Sicherheitsniveaus wird der Schutzbedarf der konsumierten Daten (INPUT), der verarbeiteten (LOGIC) und der generierten und zur Verfügung gestellten Daten (OUTPUT) in den Kategorien Vertraulichkeit, Integrität, Verfügbarkeit und Nicht-Abstreitbarkeit ermittelt. Dabei ist es notwendig für jede Kommunikationsbeziehung die jeweils übertragenen Daten einzeln zu betrachten und eine Einstufung nach Tabelle 4 vorzunehmen (Stufen niedrig bis sehr hoch).

Die folgende Vorgehensweise stützt sich auf die seitens NIST (NIST (CDC) FIPS 199) und BSI (Grundschutz) vorgeschlagenen Verfahren. Der Service wird hinsichtlich seiner Kommunikationsbeziehungen und der internen Datenverarbeitung betrachtet. Dabei ist jede Kommunikationsbeziehung eines Service zu betrachten und ebenso jeder Nachrichtentyp zu bewerten. NIST legt hierzu einen Vektor **S**ecurity_**C**ategorie fest, der für jeden Informationstyp (Datum) zu bestimmen ist.

$$\textbf{\textit{Security Category}}_{\textit{information type}} \textbf{\textit{= \{(confidentiality, impact), (integrity, impact), (availability, impact), (non-repudiation, impact)\}}}$$

Values for impact: {LOW, NORMAL, HIGH, VERY HIGH, NOT APPLICABLE}

Dabei ergibt sich die Security Category für jeden Nachrichtentyp aus der Einstufungen der Grundwerte Vertraulichkeit (confidentiality), Integrität (integrity), Verfügbarkeit (availability) und Nicht-Abstreitbarkeit (non-repudiation). Die Beurteilung erfolgt nach „Wichtigkeit“, bzw. der (Aus-)wirkungen (Impact) beim Verlust infolge eines Angriffes oder Fehlers des jeweiligen Grundwertes. Die Bewertung ist für jeden Nachrichtentyp, den ein Service empfängt, verarbeitet und zur Verfügung stellt, durchzuführen.

Die Adaption für SynErgie stellt sich wie folgt dar:

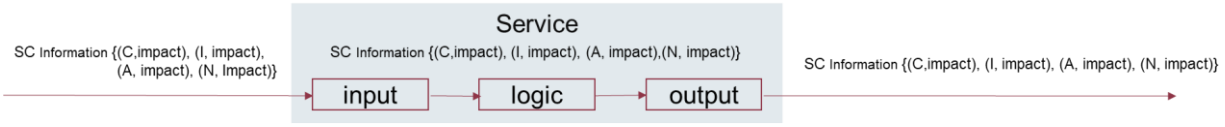


Abbildung 5: Schematische Darstellung - Zu evaluierender Service

Hilfestellung für die Bestimmung des Schutzbedarfs:

- Welche Inputdaten gibt es, wer liefert diese?
- Welche Daten werden im Service verarbeitet und erzeugt?
- Welche Outputdaten werden generiert und wer ist der Adressat?
- Welches erforderliche Schutzniveau muss für jeden Datentyp festgelegt werden.

Dabei sollte mit betrachtet werden, ob durch Maßnahmen wie Datensparsamkeit gegebenenfalls eine Vereinfachung erzielt werden kann (need-to-know-Prinzip). Erhält ein Service beispielsweise hochvertrauliche Daten, die er für seine korrekte Funktion (eigentlich) nicht benötigt, muss möglicherweise eine wesentlich höhere Einstufung des Schutzbedarfs erfolgen, als dies eigentlich notwendig wäre. Letztendlich macht dies IT-Sicherheitsanforderungen und abgeleitete Maßnahmen erforderlich, die letztendlich für die korrekte Funktion nicht zwingend erforderlich wären. Hier könnte beispielsweise eine Anonymisierung von Daten eine Vereinfachung ermöglichen. Ähnliche Überlegungen können auch für die anderen Grundwerte erfolgen.

Für die Festlegung des gesamten Schutzbedarfs eines Service und somit des erforderlichen Schutzniveaus wurde, wie bereits erwähnt, ein Verfahren nach NIST (NIST (CDC) FIPS 199), sowie die Vorgehensweise nach BSI-Grundschutz (BSI-Standard 200.2) adaptiert. NIST schlägt eine Betrachtung und Bewertung der Grundwerte für jeden einzelnen Informationstyp vor und wendet dann für jeden Grundwert das Maximalprinzip an, d.h. die jeweils höchste Einstufung je Grundwert gilt als maßgeblich für den Schutz dieses Grundwerts für den Service insgesamt. Dazu ist es notwendig die Bewertung für jeden Informationstyp getrennt vorzunehmen. Anschließend wird die jeweils höchste Einstufung eines Grundwertes (Vertraulichkeit, Integrität, usw.) herangezogen und in die Gesamtbewertung (SC_overall) übernommen.

Beispiel:

Es wird für jeden Nachrichtentyp eine Einstufung der Grundwerte hinsichtlich des Schutzbedarfs vorgenommen und die jeweils höchste vorkommende Bewertungsstufe je Nachrichtentyp markiert.

SC *public information* = {(confidentiality, low), (integrity, **normal**), (availability, **normal),** (non-repudiation, low)}.

SC investigative information = {(confidentiality, **high**), (integrity, normal), (availability, normal), (non-repudiation, low)}

SC *administrative information* = {(confidentiality, low), (integrity, low), (availability, low), (non-repudiation, low)}

Bestimmung der Gesamtbewertung nach NIST/FIPS 199:

Folgt man dem Bewertungsschema nach NIST/FIPS 199, dann wird für die Bestimmung der Security Category (SC) die jeweils höchste vorkommende Stufe bei der Gesamtbewertung eines Grundwertes herangezogen. Es gilt also der höchste vorkommende Wert. Für die Vertraulichkeit ist dies im Beispiel der Wert „high“, der bei der Bestimmung der „investigative information“ vergeben wurde. Für Integrität und Verfügbarkeit war die höchste Einstufung „normal“ und für Nicht-Abstreitbarkeit war die höchste Einstufung „low“. Diese werden nun in den Vektor für SC overall eingetragen.

NIST: SC overall = {(confidentiality, high), (integrity, normal), (availability, normal), (non-repudiation, low)}

Das Gesamtresultat gibt nun Auskunft darüber, welche Anforderungen an eine Komponente hinsichtlich der Anforderungen und Maßnahmen zu stellen ist, um die Grundwerte zu garantieren.

Bestimmung der Gesamtbewertung nach BSI Grundschutz:

Das Bewertungsschema nach BSI Grundschutz verfolgt hier einen anderen Ansatz und bewertet nach der höchsten, vorgekommenen Einstufung. Im genannten Beispiel wäre das die Stufe „high“. Damit wird BSI die Security Category insgesamt „high“, also hoch.

BSI: SC overall = high!!

Für die weitere Vorgehensweise zur Ermittlung des Sicherheitslevels soll das Verfahren des BSI herangezogen werden. Erstens ist damit das Ziel wenige Sicherheitslevel zu definieren

besser umzusetzen und näher an den Vorgaben zum IT-Grundschutz und den Vorgaben des BSI, die für KRITIS relevant sind. Die Ermittlung nach NIST dient als vorangeschalteter Prozess und dient später dabei bei der Umsetzung von Maßnahmen, die für einen Sicherheitslevel vorzunehmen sind.

Bestimmung der Risikostufe

Der zweite Parameter, der zur Einstufung in einen Sicherheitslevel betrachtet werden muss, ist das potenzielle Risiko, welchem ein Service oder eine Komponente ausgesetzt ist. Die Festlegung der Risikostufe erfordert eigentlich eine vollumfassende Risikoanalyse, die jedoch unternehmensspezifisch erfolgen müsste. So wie dies beispielweise bei der Umsetzung des BSI Grundschutz oder der Implementierung eines ISMS nach ISO/IEC 2700x (DIN EN ISO/IEC 27001:2017-06), bzw. der Umsetzung der Maßnahmen nach IEC 62443 (DIN EN 62443-3-2:2018-10 - Entwurf; DIN EN IEC 62443-4-2:2019-12) vorgesehen ist. In diese Analyse fließen beispielsweise bereits implementierte Sicherheitsmaßnahmen mit ein, die ein Risiko minimieren, sofern diese vorhanden sind. Sind keinerlei Maßnahmen getroffen, ergibt sich für diese Unternehmen eine andere Risikobewertung als für ein Unternehmen mit einem hohen Maß an umgesetzter IT-Sicherheit (Separierte Netze, Firewalls, Zugangskontrollen, usw.). Ebenso kann ein potenzielles Risiko eines Cyber-Angriffs von der Branche abhängig sein. Zusätzlich ist die Wahrscheinlichkeit eines Cyber-Angriffs für einen Service, der über ein öffentliches Kommunikationsnetz kommuniziert, höher anzusetzen, als bei einem Service, der sich hinter ein einer Firewall befindet oder in einem abgetrennten Netzsegment und keine direkte Verbindung über ein öffentliches Netz aufbauen kann.

Eine unternehmensspezifische Risikoanalyse kann somit nur durch die Unternehmen selbst erfolgen, da die Randbedingungen für die Unternehmen nicht verfügbar sind. Stattdessen kann nur eine vorläufige Einstufung unter gewissen getroffenen Annahmen erfolgen.

Die Vorgabe eines Sicherheitslevels ohne eine Risikobetrachtung ist aber nicht sinnvoll. Deshalb wird ein mittleres Risiko als Standardwert angenommen. Im Rahmen einer späteren Analyse kann diese Risikostufe bei einem Service jedoch hiervon abweichen. Die Abweichung muss dann begründet werden. Kommuniziert der Service über ein öffentliches Kommunikationsnetz (Internet) ist beispielsweise die Risikostufe „hoch“ anzunehmen. Agiert ein Service in einer abgekapselten Umgebung kann gegebenenfalls eine niedrigere Risikostufe gewählt werden, sofern dies begründet werden kann.

Für die Ermittlung der Risikostufe wird im Allgemeinen der potenzielle Angreifer (Fähigkeiten, Ressourcen, potenzielle finanzielle Mittel) und die Häufigkeit von Angriffen in der Branche oder einer ähnlichen Plattform herangezogen. Als Informationsquelle können hier die Lageberichte

des BSI (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2021a), sowie der Branchenverbände, wie beispielsweise der BDEW für die Energiewirtschaft (Kuhn et al.), dienen. Die Einschätzung des eigenen Risikos, Opfer einer Cyberattacke zu werden ist jedoch eine Aufgabe, die eine ständige Beobachtung von Angriffsversuchen und erfolgreichen Angriffen im eigenen Unternehmen erfordert, ebenso wie die Zuhilfenahme von Informationenquelle oder Plattformen, die Auskunft über aktuelle Cyberangriffe geben (Dreißigacker et al. 2021; Kondruss 2022; Mccandless 2013).

Bei der Bestimmung des eigenen Risikos geben Tabelle 5 und Tabelle 6 eine Orientierung.

Tabelle 5: Risikoklasse resultierend aus Potenzial des Angreifers

Risikoklasse	Beschreibung (Angreifer)
Niedrig	Kein unmittelbarer Angriff auf das System
mittel	Angreifer ist normaler Internet-User bis hin zu interessierten Einzelpersonen und Firmen mit generischen Security-Kenntnissen. Es ist mit zufälligen oder vorsätzlichen Verstößen durch einfache Mittel mit geringem Ressourcenaufwand, allgemeinen Fähigkeiten und geringer Motivation zu rechnen.
Hoch	Experten und Firmen, die mit klaren Zielen effektive, jedoch kostenorientierte Angriffsszenarien entwickeln und einsetzen. Es ist mit vorsätzlichen Verstößen durch hochentwickelte Mittel mit moderatem Ressourcenaufwand, fachspezifischen Fähigkeiten und Kenntnissen (IACS, Energieversorgung, etc.) und moderater Motivation zu rechnen.
Sehr hoch	Staatliche Organisationen, bei denen die Erreichung des spezifisch ausgewählten Angriffsziels um fast jeden Preis im Vordergrund steht (APT). Es ist mit vorsätzlichen und ausführlich geplanten Verstößen durch hochentwickelte Mittel mit erweitertem Ressourcenaufwand, fachspezifischen Fähigkeiten (Spezialwissen im Einsatzfeld des Systems) und hoher Motivation zu rechnen.

Tabelle 6: Risikoklasse resultierend aus Wahrscheinlichkeit eines Angriffs

Risikoklasse	Beschreibung (Wahrscheinlichkeit)
Niedrig	Unwahrscheinlich, aber in der Branche generell schon einmal vorgekommen Alternative Betrachtung: alle 10 Jahre oder seltener
mittel	Möglich – im eigenen Land schon vorgekommen Alternative: mindestens einmal im Jahr
Hoch	Wahrscheinlich – in der eigenen Stadt schon mehrfach vorgekommen Alternative: mindestens einmal im Monat
Sehr hoch	Häufig – kommt ständig vor Alternative: mindestens einmal pro Woche

In die **Risikostufe** sollen folgende Betrachtungen mit einfließen:

- Potenzial der möglichen Bedrohungen durch Angriffe oder sonstige Ereignisse
- Potenzial eines Angreifers und damit Stärke eines möglichen Angriffs. Hierbei gilt es spezifische Eigenschaften des Unternehmens mit einzubeziehen.
- Wahrscheinlichkeit und Häufigkeit von Angriffen (kann für jede Branche oder Unternehmen sehr unterschiedlich ausfallen)
- Einsatzumgebung (Firmennetz, Cloud-Service, Domäne oder Zone)
- Softwarequalität (Implementierungsschwächen, Fehlkonfiguration, Fehlfunktion)

Festlegung des Sicherheitslevels

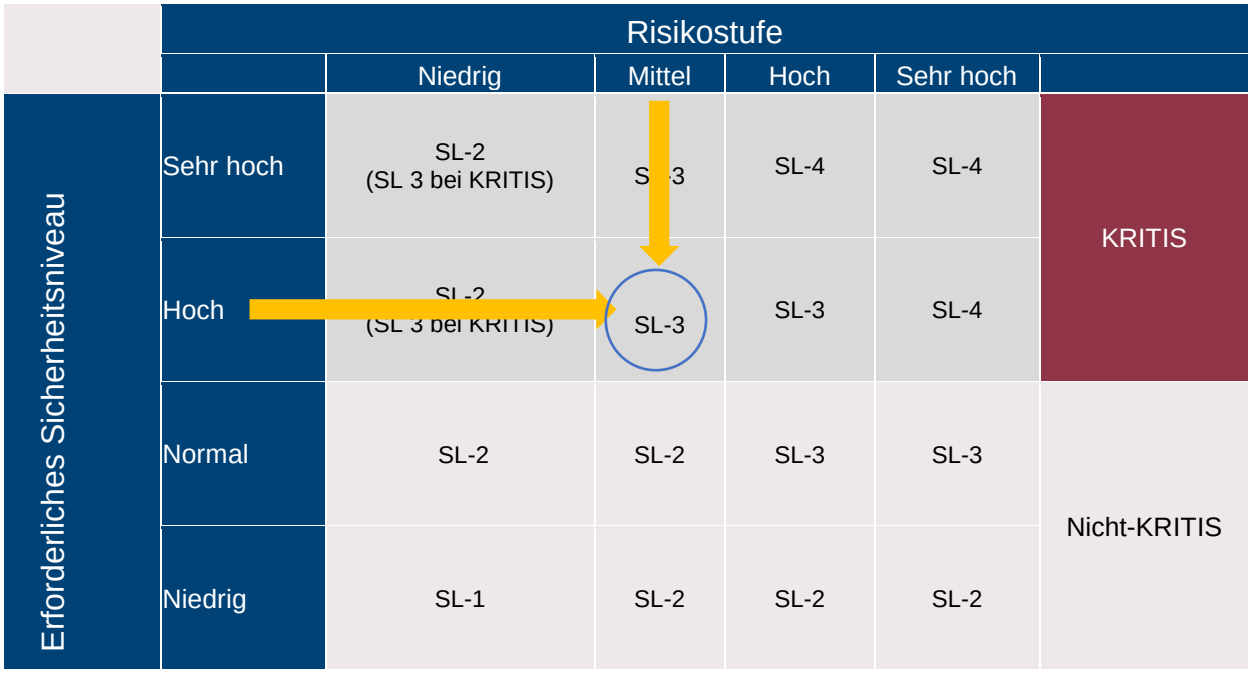
Nachdem das erforderliche Sicherheitsniveau (basierend auf dem Schutzbedarf der Informationen) und die Risikostufe bestimmt wurden, erfolgt die Festlegung des Sicherheitslevels für die Anwendung, den Service oder eine Komponente

Tabelle 7: SL Matrix Festlegungen der Bereiche für Sicherheitslevel

		Risikostufe				
		Niedrig	Mittel	Hoch	Sehr hoch	
Erforderliches Sicherheitsniveau	Sehr hoch	SL-2 (SL 3 bei KRITIS)	SL-3	SL-4	SL-4	KRITIS
	Hoch	SL-2 (SL-3 bei KRITIS)	SL-3	SL-3	SL-4	
	Normal	SL-2	SL-2	SL-3	SL-3	Nicht-KRITIS
	Niedrig	SL-1	SL-2	SL-2	SL-2	

KRITIS erzwingt mindestens hohes Sicherheitsniveau und mindestens SL-3.

Beispiel:
Im Beispiel wurde für das Erforderlichen Sicherheitsniveaus die Stufe hoch ermittelt und die mittlere Risikostufe. Damit ergibt sich für diesen Service ein Sicherheitslevel SL3.



Prozesse und Anforderungen des Security Life Cycle Managements

Die Services der UP und der MP unterliegen, wie jedes andere Produkt auch, einem Lebenszyklus. Dieser beginnt bei der ersten Idee und endet bei der Entsorgung bzw. bei der Deinstallation des Service. Damit die geforderte Sicherheit über alle Lebensphase eines Produkts sichergestellt werden kann, bedarf es Vorgaben und Maßnahmen für die jeweiligen Lebensphasen zu definieren und umzusetzen. Das Security Life Cycle Management befasst sich hierbei mit der IT-Sicherheit der Services der ESP. Durch Security LCM soll sichergestellt werden, dass die Sicherheit der Services während des gesamten Lebenszyklus auf dem erforderlichen Sicherheitslevel gehalten werden. Das Security LCM beginnt mit der Definition von Anforderungen und dem Einsatzgebiet, welche ein Hersteller oder ein Kunde eines Service festlegt, über den Entwicklungs- und Freigabeprozess, das Deployment und über das Update-Management im Betrieb und endet mit der sicheren Deinstallation und dem Löschen von vertraulichen Informationen (inkl. einer Datensicherung sofern erforderlich) sowie dem Löschen von Berechtigungen.

Da das Sicherheitskonzept in SynErgie auf den definierten Sicherheitslevels aufbaut, ist es nur konsequent, dass die Anforderungen im Security LCM in den Lebensphasen, je nach angestrebtem Sicherheitslevel, variieren. Als Basis für die Festlegung der unterschiedlichen Lebenszyklen wurde die Vorgehensweise nach dem Security Development Lifecycle (SDL) der Firma Microsoft® herangezogen (Microsoft 2021). Die Anforderungsbeschreibungen selbst erfolgten basierend auf einer Auswahl weiterer Standards und Empfehlungen zum Life Cycle Management. Dabei wurden folgenden Standards oder Empfehlungen mit einbezogen und eigene Ergänzungen und Anpassungen vorgenommen:

- NIST – Lifecycle Management nach NIST SP.800-160 (Ross et al. 2018), SP.800-100 (Bowen et al.)
- BSI: IT-Grundschutz-Bausteine und Guideline zu Common Criteria, insbesondere Assurance class “Life-Cycle Support (ALC) (Bundesamt für Sicherheit in der Informationstechnik 2021) und (ISO/IEC 15408-1:2009-12)
- OWASP: SDLC -Software Development Lifecycle (OWASP SDLC 2021); SAMM (Software Assurance Maturity Model) (OWAPS SAMM 2.0) und Application Security Verification (OWASP Security Qualitative Metrics 2021)

Die Gesamtheit der betrachteten Lebenszyklen eines Service im Security LCM zeigt Abbildung 6.

Abbildung 6: Lebensphase im LCM

Das Security LCM definiert für jede Lebensphase Anforderungen, die sich nach gefordertem Sicherheitslevel unterscheiden können. Anforderungen und resultierende Maßnahmen, die für höhere SLs als verbindlich gelten und umzusetzen sind, können auch für niedrigere SLs umgesetzt werden, sind dann aber optional. Da die Überprüfung der definierten Anforderungen in der Praxis nur im Rahmen einer Überprüfung durch eine autorisierte Stelle oder eine Zertifizierung tatsächlich möglich wäre, ist die Durchsetzung und Verifikation der Umsetzung derzeit noch offen. In jeder Lebensphase sollte beim jeweiligen Unternehmen der eigene Prozess zur IT-Sicherheit hinsichtlich der Einhaltung der im Security LCM benannten Anforderungen überprüft werden. Im Falle einer Zertifizierung nach etablierten IT-Sicherheitsstandards sind die hierfür notwendigen Maßnahmen ohnehin umzusetzen und nachzuweisen.

Allgemeine Ziele von (Security) Life Cycle Management:

- Schutz des Kunden durch sichere Software
- Reduzierung der Anzahl an Schwachstellen und Verringerung des Schweregrads von Vorfällen
- Berücksichtigung von Compliance-Anforderungen
- Proaktiv, vorausschauend Anforderungen definieren
- Eliminieren von Redundanzen, Koordination der Prozesse und Steigerung der Produktivität
- Kostenreduktion: Fehlerbehebung nach dem Release sind deutlich teurer als während der Entwicklung
- Steigerung des Vertrauens

Fasst man die wichtigsten Regeln und Konzepte der Security- und Privacy-Prinzipien zusammen und lässt diese in die Prozesse des LCM mit einfließen, erhält man bereits eine fundierte Basis für die IT-Sicherheit der Services und Plattformen

Zunächst sollen die Grundsätze für die Entwicklung sicherer Software benannt werden. Die Auflistung geht auf das SDL (Security Development Life Cycle) der Firma Microsoft zurück und wurde in manchen Punkten[15] um aus Autorensicht wichtige Aspekte ergänzt.

Grundsätze der Entwicklung

Secure by design

Schon in der Planungsphase und im Entwicklungsprozess soll auf die Sicherheitsbelange der Software eingegangen werden. Hierfür gibt es die folgenden grundlegenden Forderungen:

- Sicherheitsanforderungen als essentielle Architekturkriterien aufnehmen.
- Bedrohungen modellieren (Threat Modeling) und behandeln (Threat Mitigation).
- Quellcode und Softwareartefakte hinsichtlich Sicherheitsproblemen überprüfen*.
- Unsichere, veraltete Protokolle und Verfahren nicht unterstützen.

[15] Ergänzungen der Grundsätze der Entwicklung zu den Vorgaben aus dem SDL von Microsoft sind mit * gekennzeichnet. Hintergrund sind Aktualisierungen in der DSVGO und beim Stand der Technik.

Secure by default

Die Standardkonfiguration soll die „sicherste“ Konfiguration sein, u. a. da trotz sorgfältiger Planung und Entwicklung Sicherheitslücken vorhanden sein können:

- Im System haben Komponenten und Nutzer stets nur die nötigen Berechtigungen (Principle of least privilege, PoLP).
- Es werden mehrschichtige Sicherheitsmaßnahmen umgesetzt (Defense in depth).
- Standardeinstellungen sind möglichst konservativ gewählt.
- Die entwickelte Software ändert die Einstellungen des umgebenden Systems nicht zu einer weniger sicheren Konfiguration.
- Selten benutzte Funktionen sind standardmäßig deaktiviert.

Änderungen an diesem Standard muss ein Nutzer bewusst konfigurieren und nach Möglichkeit nur temporär anwenden*.

Secure in deployment

- Die mitgelieferten Dokumentationen sollen die Administratoren dabei unterstützen, die Software möglichst sicher einzurichten.
- Es werden Werkzeuge bereitgestellt, die Analyse und Verwaltung vom Sicherheitszustand der Software (hinsichtlich Konfiguration und Aktualisierungen) einfach machen.
- Für das Einspielen von Aktualisierungen werden sichere und effiziente Wege und Werkzeuge bereitgestellt.

Communications (Security)

- Die Entwickler reagieren auf mögliche Sicherheitslücken und stellen schnell Patches oder Workarounds zur Verfügung.
- Die Produzenten kommunizieren proaktiv und offen hinsichtlich Sicherheitsaspekten ihrer Software, wie Sicherheitsproblemen und Sicherheitsaktualisierungen.

Privacy by design

Schon in der Planungsphase sollen Datenschutzbelange der Software berücksichtigt werden. Insbesondere soll das Konzept folgendes vorsehen:

- Es werden so wenige personenbezogene Daten wie möglich für die jeweilige Funktionalität erhoben und gespeichert.
- Betroffene werden über die Erhebung von Daten informiert und werden vorzugsweise um Zustimmung gebeten.
- Möglichkeiten zur Korrektur und Löschung von Daten werden implementiert*.
- Angemessene IT-Sicherheitsmaßnahmen zum Schutz der Daten werden ergriffen.
- Organisatorische Maßnahmen in Bezug auf die Datenverarbeitung werden umgesetzt*.

Die Datenschutz-Grundverordnung (Datenschutz-Grundverordnung (DSGVO) 2017)) der EU schreibt dieses Vorgehen zwingend vor.

Privacy by default

- Die Standardeinstellungen hinsichtlich Erhebung, Speicherung, Nutzung und Weitergabe (kurz Verarbeitung) von personenbezogenen Daten sollen konservativ gewählt werden, d. h. es sollen so wenige Daten wie möglich in der Standardeinstellung ausgewählt sein, auch wenn dies eine geringere Funktionalität des Produkts bedeutet. Was darüber hinausgeht, müssen Nutzer aktiv freischalten.
- Standardmäßig soll die Verarbeitung von personenbezogenen Daten nur basierend auf Zustimmung geschehen. Hiervon wird nur abgewichen, falls die Verarbeitung aufgrund bestimmter Anforderungen zwingend erforderlich ist*.

Privacy in deployment

- Datenschutzmechanismen sollen offengelegt werden, um es Administratoren zu ermöglichen, die internen Datenschutzrichtlinien des Unternehmens umzusetzen.

Communications (Privacy)

- Datenschutzerklärungen sollen klar formuliert werden.
- Nutzer sollen Transparenz über die sie betreffende Daten erhalten, d. h. sie sollen befähigt werden, jederzeit einen Überblick über erhobene, gespeicherte und weitergegebene Daten erlangen zu können.
- Die Produzenten kommunizieren proaktiv und offen hinsichtlich Datenschutzaspekten der Software, um über deren Verarbeitung von personenbezogenen Daten aufzuklären*.
- Ein qualifiziertes Team zur Reaktion auf Datenschutzvorfälle soll eingerichtet werden.

Als Basis für das Secure Life Cycle Management werden die Entwicklungsphasen des SDL nach Microsoft (Microsoft 2021) herangezogen und um Betrieb und Außerbetriebnahme ergänzt. Nachfolgend sollen nur die Anforderungen beschrieben und die Relevanz für den jeweiligen Sicherheitslevel benannt werden. Dabei wird eine Unterteilung in die verschiedenen Phasen des LCM vorgenommen. Allgemeine Anforderungen, die bei einer Phase des LCM vorausgesetzt werden, werden immer am Anfang der jeweiligen Phase beschrieben. Bei der Relevanz von Anforderungen wird bei den Sicherheitsleveln nachfolgend noch einmal gesondert darauf eingegangen, wenn im Falle von KRITIS eine Verschärfung der Anforderungen vorzusehen ist.

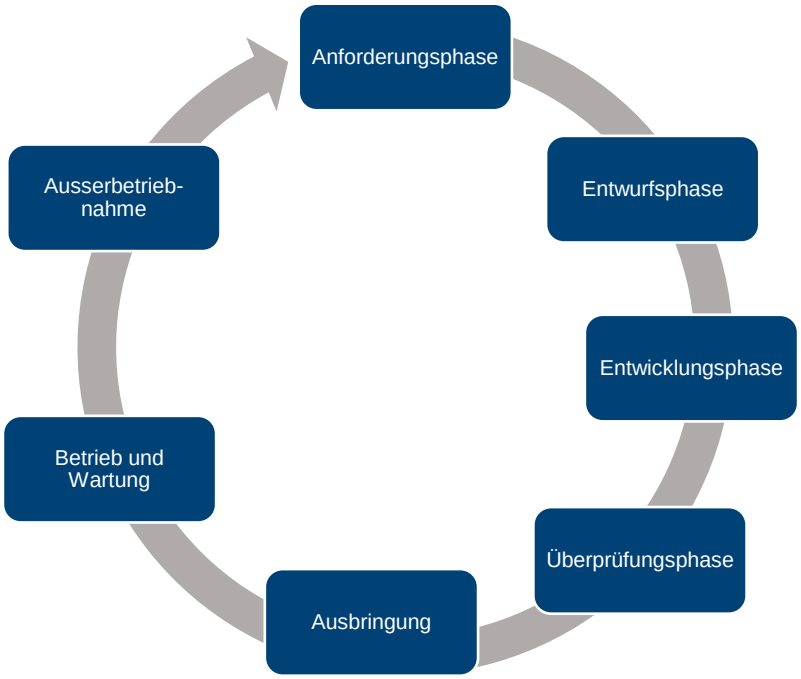


Abbildung 7**:** Phasen des Life Cycle

Tabelle 8: Legende zu den nachfolgenden Anforderungslisten

Phasenbezeichnung in Maßnahmenkürzel	**Attribute für Maßnahmen**
A – Awareness (generelles Sicherheitsbewusstsein) **REQ** – Requirement (Anforderungsphase) **CON** – Concept (Entwurfsphase) **DEV** – Development (Entwicklungsphase) **T** – Test (Überprüfungsphase) **D** – Deployment (Ausbringungsphase) **OP** – Operation (Betrieb und Wartung) **DEC** – Decommissioning (Außerbetriebnahme)	**M** – Mandatory (Pflichtmaßnahme) **O** – Optional, but recommended (optionale, empfohlene Maßnahme)

Awareness- und Schulungsprogramm

Regelungen zur Teilnahme an Schulungsprogrammen sind eine übergeordnete Maßnahme, die für alle Phasen des LCM gelten. Die Entscheidung, ob eine Notwendigkeit besteht, sollte auf Basis der im Unternehmen umgesetzten allgemeinen Sicherheitsrichtlinien erfolgen, die sich aus Zertifizierungen oder der Konformität zu gesetzlichen Vorgaben oder branchenüblichen Standards ergeben.

Generell ist anzumerken, dass der Secure-LCM-Prozess ohne ein effektives Awareness- und Schulungsprogramm gefährdet ist. Dies gilt für die Entwicklung von Services aber auch für alle anderen Phasen des LCM. Fehlt das Bewusstsein für die Informationssicherheit oder die fachliche Kompetenz, kann dies in allen Phasen des LCM zu einer Schwächung der IT-Sicherheit führen, begonnen bei der Entwicklung, über die Verteilung, Installation und Konfiguration, den Betrieb bis zur Außerbetriebnahme.

Tabelle 9: Awarenessprogramm – Schulungen

Nr.	Beschreibung	SL1	SL2	SL3	SL4
A.1	Durchführung von Schulungen zur IT-Sicherheit		O	M	M

Involvierte Rollen

Auf übergeordneter Ebene sollten folgende Rollen in einem Unternehmen[16] etabliert werden:

- Datenschutzbeauftragter
- Informationssicherheitsbeauftragter
- IT-Awareness Manager

Die Notwendigkeit dieser Rollen hängt von bestimmten Randparametern ab, wie Unternehmensgröße, Branche. Hierzu sind die rechtlichen Bestimmungen einzuhalten.

Die **Aufgaben des Informationssicherheitsbeauftragten** sind im Wesentlichen:

- gemeinsame Ziele zwischen dem Bereich der industriellen Steuerung und dem gesamten ISMS verfolgen und Projekte aktiv unterstützen,
- allgemeine Sicherheitsvorgaben und Richtlinien für den ICS-Bereich umsetzen,
- Risikoanalysen für den ICS-Bereich durchführen,
- Sicherheitsmaßnahmen für den ICS-Bereich festlegen und umsetzen,
- Sicherheitsrichtlinien und Konzepte für den ICS-Bereich unter Berücksichtigung von Anforderungen der Funktionssicherheit („Safety") erstellen und die Mitarbeiter schulen,
- Ansprechpartner für die Mitarbeiter vor Ort und für die gesamte Institution sein,

[16] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_05/Lektion_2_05_node.html

- Schulungen und Maßnahmen zur Sensibilisierung konzipieren,
- Sicherheitsvorfälle zusammen mit dem ISB bearbeiten,
- Dokumentation.

Datenschutzbeauftragter – die Aufgaben und Rahmenbedingungen ergeben sich aus der DSVGO (Datenschutz-Grundverordnung (DSGVO) 2017)

- Der Datenschutzbeauftragte berät den Verantwortlichen in allen datenschutzrechtlichen Belangen und unterstützt ihn bei der Umsetzung der datenschutzrechtlichen Anforderungen.
- Der Datenschutzbeauftragte ist Ansprechpartner sowohl für den Arbeitgeber als auch für die Arbeitnehmer oder den Betriebsrat. Auch Externe, wie Kunden, Vertragspartner oder Lieferanten können sich an den Datenschutzbeauftragten wenden.
- Ebenso sollte der Datenschutzbeauftragte bei der Schulung der Mitarbeiter eingebunden werden. So können die Mitarbeiter mit den datenschutzrechtlichen Anforderungen ihrer täglichen Arbeit vertraut gemacht werden.
- Der Datenschutzbeauftragte arbeitet zugleich mit der Aufsichtsbehörde zusammen, er ist Anlaufstelle für die Aufsichtsbehörde im Zusammenhang mit allen datenschutzrechtlichen Fragestellungen.
- Der Datenschutzbeauftragte berät den Verantwortlichen in allen datenschutzrechtlichen Belangen und unterstützt ihn bei der Umsetzung der datenschutzrechtlichen Anforderungen.
- Der Datenschutzbeauftragte ist Ansprechpartner sowohl für den Arbeitgeber als auch für die Arbeitnehmer oder den Betriebsrat. Auch Externe, wie Kunden, Vertragspartner oder Lieferanten können sich an den Datenschutzbeauftragten wenden.
- Ebenso sollte der Datenschutzbeauftragte bei der Schulung der Mitarbeiter eingebunden werden. So können die Mitarbeiter mit den datenschutzrechtlichen Anforderungen ihrer täglichen Arbeit vertraut gemacht werden.
- Der Datenschutzbeauftragte arbeitet zugleich mit der Aufsichtsbehörde zusammen, er ist Anlaufstelle für die Aufsichtsbehörde im Zusammenhang mit allen datenschutzrechtlichen Fragestellungen.

IT-Awareness Manager

Der Awareness Manager organisiert unter anderem für die Durchführung von IT-Sicherheitsschulungen und sorgt so bei den Mitarbeitern für die notwendige Awareness hinsichtlich IT-Sicherheit.

Anforderungsphase

In der Anforderungsphase werden die funktionalen Anforderungen und auch nicht-funktionalen Anforderungen ermittelt. Ebenso werden gesetzliche Anforderungen aufgenommen.

Die Definition der Produktanforderungen läuft oft auf einen Kompromiss zwischen den geschäftlichen Anforderungen eines Kunden und dem erforderlichen Sicherheitsniveau zum Schutz seiner Vermögenswerte hinaus. Dies kann nur durch das Sammeln und gründliche Analysieren von marktbasierten Anforderungen, geltenden Gesetzen und Vorschriften sowie Standards und Best Practices erreicht werden.

Abbildung 8: Prozesse der Anforderungsphase

Marktbasierte Anforderungen

Bei der marktbasierten Anforderungserhebung wird das Problem des Kunden identifiziert, dass durch ein Produkt oder eine Dienstleistung gelöst werden soll. Daher ist es in diesem Schritt wichtig, viele Dinge zu klären, z. B. die Art der zu schützenden Daten, die notwendige Funktionalität des Produkts, etwaige Einschränkungen in Bezug auf die Betriebsumgebung und so weiter.

Gesetze und Vorschriften

Die frühzeitige Berücksichtigung aller geltenden Gesetze und Vorschriften senkt die Kosten, die Risiken der Nichteinhaltung sowie die Markteinführungszeit (engl. Time to Market = TTM) des Produkts insgesamt.

Standards und Best Practices

Obwohl Gesetze und Vorschriften in der Regel nicht die Einhaltung von Standards und Best Practices vorschreiben, sind letztere für jeden Anbieter, der wettbewerbsfähig sein will, zwingend erforderlich.

Tabelle 10: Anforderungsphase – Anforderungen

Nr.	Beschreibung	SL1	SL2	SL3	SL4
REQ.1	Ermittlung der gesetzlichen Vorgaben zur IT-Sicherheit	M	M	M	M
REQ.2	Ermittlung der kundenspezifischen Sicherheitsanforderungen	M	M	M	M
REQ.3	Recherche Standards und Best Practices	O	M	M	M

Involvierte Rollen

Kundenanforderungsmanager

Erfasst die Anforderungen potenzieller Kunden und Interessenten der UP und erfasst die funktionalen Anforderungen eines Service.

Anforderungsmanager

Nimmt Anforderungen (funktional aber auch die IT-Sicherheit betreffend) des Kunden entgegen oder ermittelt potenzielle Anforderungen aufgrund seiner Kenntnisse den Einsatzbereich des Service betreffend.

IT-Service-Sicherheitsarchitekt (Compliance Manager)

- Recherche gesetzliche Vorgaben, (ggf. auch DSVGO-Beauftragter)
- Kundespezifische Sicherheitsanforderungen
- Auswahl einzuhaltender Standards (allgemein)
- Macht Vorgaben bezüglich der IT-Sicherheit

Entwurfsphase – Planung und Konzeption

Abbildung 9: Prozesse der Entwurfsphase

In der Entwurfsphase erfolgen Planung und die Konzeption. Neben der rein funktionalen Beschreibung eines Service wird hier die Bestimmung des notwendigen Sicherheitslevels, basierend auf der Einstufung des erforderlichen Schutzbedarfs der zu verarbeitenden Daten und des Risikos, durchgeführt. Ebenso erfolgt hierbei die Bedrohungsmodellierung (Threat Modeling). Daraus leiten sich nachfolgend die Anforderungen für die zu ergreifenden IT-Sicherheitsmaßnahmen und die zu treffenden Anforderungen an den Lebenszyklus eines Service ab. Am Ende der Entwurfsphase steht eine Grobspezifikation zur Verfügung.

In dieser Phase werden die gesammelten Anforderungen analysiert, um festzulegen, wie ein Produkt diese erfüllen soll und wie man diese Erfüllung zuverlässig und sicher machen kann. Deshalb soll auch eingesetzte Software von Drittanbietern untersucht werden und es sollte eine Angriffsflächenanalyse und eine Bedrohungsmodellierung erfolgen.

Analyse der Angriffsfläche

Der Zweck dieser Analyse ist es, zu identifizieren, welche Angriffspunkte für einen Angreifer verfügbar sind und folglich von ihm genutzt werden können, um diese so weit wie möglich zu minimieren.

Bedrohungsmodellierung

Die Bedrohungsmodellierung ist einer der kritischsten Schritte bei der Entwicklung eines Produkts im Hinblick auf die Sicherheit. Daher muss unter Berücksichtigung der Erkenntnisse aus dem vorherigen Schritt ein Bedrohungsmodell entwickelt werden. Anschließend wird das Modell verwendet, um das erforderliche Sicherheitsniveau zu bestimmen und geeignete Sicherheitskontrollen auszuwählen, die im Produkt implementiert werden müssen, um die Informationen angemessen zu schützen. Zusätzlich ist eine Risikobewertung durchzuführen.

Tabelle 11: Entwurfsphase – Sicherheitslevel und Bedrohungsmodellierung

Nr.	Beschreibung	SL1	SL2	SL3	SL4
CON.1	Bestimmung des erforderlichen Sicherheitslevels (umfasst Schutzbedarfsanalyse und Risikobewertung)	M	M	M	M
CON.2	Dokumentation des Schutzbedarfs	O	O	M	M
CON.3	Dokumentation der Risiken	O	O	M	M
CON.4	Durchführung eines Threat Modelings (Dokumentation der Angriffsflächen und der potentiell darauf einwirkenden Bedrohungen)		O	M	M

Security Architecture

Tabelle 12: Entwurfsphase – Security Architecture

Nr.	Beschreibung	SL1	SL2	SL3	SL4
CON.5	Definition der Sicherheitsarchitektur für die Services		O	M	M
CON.6	Definition der Rollen (Entwickler, Tester, Nutzer, Nutzer mit erweiterten Rechten, Administrator)	O	M	M	M
CON.7	Festlegung der Zugriffsrechte je Rolle	O	M	M	M
CON.8	Definition eines sicheren Deployments		O	M	M
CON.9	Anforderungen an ein sicheres Konfigurationsmanagement		M	M	M
CON.10	Definition eine sicheren Anmelde- und Abmeldeprozesses		O	M	M

Security Requirements

Tabelle 13: Entwurfsphase – Security Requirements

Nr.	Beschreibung	SL1	SL2	SL3	SL4
CON.11	Festlegung von Auswahlkriterien für Fremdsoftware		O	M	M
CON.12	Festlegung von Auslieferungskriterien			M	M
	Authentifizierung				
CON.13	• Festlegung von Authentifizierungsverfahren	M	M	M	M
CON.14	• Festlegung von kryptographischen Authentifizierungsverfahren			M	M
CON.15	• Mehrfaktorauthentifizierung			O	M
	Vertraulichkeit				
CON.16	• Festlegung von Verfahren zum Schutz der Vertraulichkeit von Daten	M	M	M	M
CON.17	• Festlegung von kryptographischen Verschlüsselungsverfahren			M	M
	Integrität				
CON.18	• Auswahl von Verfahren zur Erkennung von Integritätsverlust	M	M	M	M
CON.19	• Festlegung von kryptographischen Signaturverfahren			M	M
CON.20	Auswahl von sicherheitsrelevanten Protokollen (TLS, …)			M	M
CON.21	Auswahl geeigneter kryptographischer Bibliotheken			M	M
CON.22	Definition eines sicheren Konfigurationsmanagements		O	M	M
CON.23	Festlegung eines einheitlichen Loggings (Event-Loggins) als Basis zur Erkennung von Fehlfunktionen und sicherheitsrelevanter Events	M	M	M	M

CON.24	Definition von Services-Policies. Festlegung eines Regelwerks für die Kommunikation zwischen Services innerhalb der UP			M	M
CON.25	Festlegung eines Signaturverfahrens für Nachrichten auch innerhalb der UP			M	M

Involvierte Rollen

IT-Sicherheitsarchitekt/Designer

- Kennt die regulatorischen Rahmenbedingungen.
- Ermittlung des Schutzbedarfs einem Service
- Vorgaben zu Umsetzung der IT-Sicherheitsanforderungen
- Durchführung von Threat-Modeling
- Festlegung Secure Coding Requirements
- Entwicklungsvorgaben (Build-Umgebungen, sonst Tools)
- Auswahl der kryptographischen Bibliotheken

Risikomanager

- Ermittlung der potenziellen Bedrohungen und Risiken für einen Service
- Kennt aktuelle Bedrohungslagen und die Assets, die bei einem Cyber-Angriff betroffen wären

Nachfolgend wird zusätzlich auf Rollenbeschreibungen, welche durch ITIL definiert werden, verwiesen[17]. Ob diese zu besetzen sind, ist im Einzelfall zu entscheiden.

Anwendungssystem-Analytiker

- Der Anwendungssystem-Analytiker ist eine Rolle im Application Management, die Anwendungen über ihren gesamten Lebenszyklus hinweg verwaltet.
- Typischerweise gibt es einen Anwendungssystem-Analytiker oder ein Team von Analytikern für jede wichtige Anwendung.
- Diese Rolle ist tragend, wenn es um anwendungsbezogene Aspekte beim Designen, Testen, Betreiben und Verbessern von IT-Services geht.
- Sie ist auch verantwortlich für die Entwicklung der für den Betrieb der Anwendungen erforderlichen Kompetenzen.

Risikomanager

- Der Risikomanager ist verantwortlich für die Identifikation, Bewertung und Überwachung von Risiken.

[17] Siehe *https://wiki.de.it-processmaps.com/index.php/Rollen_in_ITIL*

- Dies umfasst eine Analyse des Wertes von Assets für das Unternehmen und die Identifikation möglicher Bedrohungen für diese Assets sowie die Einschätzung der jeweiligen Gefährdung der Assets.

Information Security Manager

- Der Information Security Manager ist verantwortlich dafür, dass alle Güter, Informationen, Daten und IT-Services eines Unternehmens jederzeit hinsichtlich ihrer Vertraulichkeit, Integrität und Verfügbarkeit geschützt sind.
- Er ist normalerweise eingebunden in ein unternehmensweites Security Management, das einen breiteren Wirkungsbereich als der Service-Provider hat; dieses umfasst u.a. auch einen den Sicherheitsaspekten genügenden Umgang mit Schriftstücken und Telefonaten innerhalb des Gesamtunternehmens sowie die Zugangskontrolle zu Betriebseinrichtungen.

Service Level Manager

- Der Service Level Manager trägt die Verantwortung für das Verhandeln von Service-Level-Vereinbarungen und stellt sicher, dass diese auch erfüllt werden.
- Er gewährleistet, dass alle IT-Service-Management-Prozesse, Vereinbarungen auf Betriebsebene (Operational Level Agreements/ OLAs) und Verträge mit Drittparteien (Underpinning Contracts/ UCs) geeignet sind, um die Ziele der vereinbarten Service Levels zu erreichen.
- Der Service Level Manager überwacht die Service Levels und stellt entsprechende Reports zu den Service Levels zur Verfügung.

Entwicklungsphase

Abbildung 10: Prozesse der Entwicklungsphase

Die Entwicklungsphase umfasst sowohl die Erstellung der Feinspezifikationen als auch die Implementierung selbst. Im Rahmen der Entwicklung erfolgt ebenfalls die Auswahl von einzusetzender Drittsoftware (Bibliotheken) und die Auswahl der Entwicklungswerkzeuge. Die Implementierung folgt dabei den Vorgaben der Programmierrichtlinien. Die Vorgaben sind hierbei abhängig vom jeweiligen erforderlichen Sicherheitslevel. Ebenso ist die Durchführung von Codeüberprüfung und eine erste entwicklungsbegleitende Durchführung von Tests (Unit-Tests, Modultests) Bestandteil dieser Phase.

Sicherer Coding-Standard

Sichere Programmierpraxis konzentriert sich in erster Linie auf die Vermeidung von Programmierfehlern während der Entwicklungsphase. Dies kann erreicht werden durch:

- Implementierung eines strengen Secure-Coding-Standards (Turpin 2010), (SEI CERT 2022)
- Überwachung und Kontrolle seiner Erfüllung durch die Durchführung von Code-Analysen und
- Integration aktueller automatisierter Werkzeuge (statischer Analyzer, Compiler, Versionskontrollmechanismen u. a.) in die Software-Entwicklungsumgebung.

Ein weiterer Punkt ist die Awareness und die Schulung von Mitarbeitern.

Code-Analyse

Code-Analysen, die von Sicherheitsexperten durchgeführt werden, und Peer-Code-Reviews dienen dazu, Fehler bereits in den frühesten Entwicklungsschritten zu beseitigen. Sie sind sehr effektiv, um Logikfehler zu entdecken, unabhängig davon, ob diese Fehler absichtlich gemacht wurden oder nicht.

Automatisierte Werkzeuge

Automatisierte Entwicklungswerkzeuge (z. B. Compiler, Versionskontrollwerkzeuge, statische Code-Analysatoren usw.) und deren entsprechende Konfiguration sind für die Softwareentwicklung notwendig. Außerdem sollten sie auf dem neuesten Stand gehalten werden, um maximal effektiv zu sein. Alle Werkzeuge sollten direkt in die Entwicklungsumgebung integriert sein.

Secure Build

Tabelle 14: Entwicklungsphase – Secure Build

Nr.	Beschreibung	SL1	SL2	SL3	SL4
DEV.1	Auswahl vertrauenswürdiger und sicherer Entwicklungswerkzeuge			M	M
DEV.2	Monitoring von Updates der Entwicklungswerkzeuge			M	M
DEV.3	Auswahl und Einsatz einer Versions- und Revisionsverwaltung	M	M	M	M
DEV.4	Auswahl und Einsatz eines Bug-Tracking-Systems			M	M

Secure Development

Tabelle 15: Entwicklungsphase – Secure Development

Nr.	Beschreibung	SL1	SL2	SL3	SL4
DEV.5	Anwendung von Coding Standards		O	M	M
DEV.6	Strukturierte Programmierung und Dokumentation	O	M	M	M
DEV.7	Sichere Programmierung: Eingabeüberprüfung, Bereichsüberprüfung, Overrun-Underun-Checks, …		M	M	M
DEV.8	Ausfallsichere Programmierung: Fehlerbehandlung, zusätzliche Maßnahmen zur Härtung, Umsetzung einer Fehlertoleranz			(M)	M
DEV.9	Durchführung einer Code-Analyse mittels statischer Codeanalyse	O	O	M	M
DEV.10	Durchführung von Code-Analyse mittels Code-Review			M	M
	Einsatz von kryptographischen Bibliotheken:				
DEV.11	• Überprüfung der Eignung der Bibliotheken für die kryptographischen Verfahren			M	M
DEV.12	• Einsatz der letzten freigegebenen stabilen Version			M	M
DEV.13	• Überprüfung der Authentizität der Bibliotheken				M
	Drittsoftware				
DEV.14	• Einsatz der neuesten freigegebenen stabilen Version		O	M	M
DEV.15	• Überprüfung der Authentizität eingesetzter Drittsoftware		O	M	M
DEV.16	Umsetzung einer sicheren Standardkonfiguration	M	M	M	M
DEV.17	Umsetzung minimaler Rechte bei Standardkonfiguration	O	O	M	M
DEV.18	Monitoring von Updates und Patches eingesetzter Drittsoftware		O	M	M
DEV.19	Monitoring von Updates und Patches der eingesetzten kryptographischen Bibliotheken			M	M

DEV.20	Umsetzung entwicklungsbegleitender Unit-Test		O	M	M
DEV.21	Entwicklungsbegleitende Tests der Sicherheitsfunktionen		M	M	M

Zusätzliche ausgewählte präventive Maßnahmen

Tabelle 16: Entwicklungsphase – Präventive Maßnahmen

Nr.	Beschreibung	SL1	SL2	SL3	SL4
DEV.22	Umsetzung eines einheitlichen Loggings	M	M	M	M
DEV.23	Umsetzung einer syntaktischen Validierung der Eingangsdaten	M	M	M	M
DEV.24	Umsetzung semantischer Validierung von Eingangsdaten		M	M	M
DEV.25	Umsetzung einer Kontext-Validierung und Umsetzung eines Log-Events im Fehlerfall			M	M
DEV.26	Umsetzung eines Autorisierungsmechanismus von Services innerhalb der UP		M	M	M
DEV.27	Umsetzung eines Signaturverfahrens für Nachrichten auch innerhalb der UP und Generieren von Events bei Empfang ungültiger Signaturen			M	M
DEV.28	Umsetzung einer Konfiguration ausschließlich im Offline-Modus	M	M	M	M
DEV.29	Umsetzung eines Single-Sign-On-Verfahrens für die Benutzerverwaltung und Authentifizierung innerhalb der UP		M	M	M
DEV.30	Einsatz von etablierten Bibliotheken und Frameworks für die Nutzerverwaltung		M	M	M
DEV.31	Ermittlung (Abschätzung) und Dokumentation des regulären Ressourcenbedarfs als präventive Maßnahme gegen DoS	M	M	M	M
DEV.32	Vermeidung von angreifbaren Datenformaten (XML, YAML, ZIP) als präventive Maßnahme gegen DoS-Angriffe		M	M	M
DEV.33	Umsetzung einer Möglichkeit Limits für den Empfang und die Verarbeitung von ext. Daten zu setzen (konfigurierbar)			M	M
DEV.34	Limits von Services für eine Betriebssystem-Konfiguration vorgeben		M	M	M

Involvierte Rollen

Service Ersteller / Independent Service Vendor

- Entwickelt den Service nach der funktionalen Anforderungsspezifikation und den sicherheitsrelevanten Anforderungen
- Erstellt eine ausführliche Dokumentation
  - funktionale Beschreibung des Service
  - vorgesehener Einsatzbereich (Sicherheitslevel)
  - Interfacebeschreibung (Inputdaten und unterstützte Formate, Outputdaten und unterstützte Formate)

Überprüfungsphase – Verifikation

Abbildung 11: Prozesse der Überprüfungsphase

Das Secure Life Cycle Management fokussiert in der Testphase auf das (Ab-)Testen von geforderten Sicherheitsfunktionen. Das rein funktionale Testen eines Service (Test der Anwendung) ist Teil der „normalen“ Software-Entwicklung. Im Secure LCM werden die in der Entwurfsphase definierten Maßnahmen zur IT-Sicherheit überprüft. Auch hier kann zwischen eher funktionalem Testen und nicht-funktionalem Testen unterschieden werden. Funktionales Testen beträfe hier beispielsweise die Überprüfung von Login-Verfahren, Auswahl der spezifizierten Krypto-Algorithmen, während das nicht-funktionale Testen die Robustheit beispielsweise gegen Angriffe im Fokus hat. Am Ende der Verifikation steht die Freigabe des entwickelten Service durch den Hersteller. Sollte eine Zertifizierung erforderlich sein, ist diese ebenfalls in dieser Phase durchzuführen. Je nach Sicherheitslevel kann hier eine Hersteller-Signatur der Software sinnvoll sein. Die Testtiefe und der Testumfang ist abhängig vom jeweiligen Sicherheitslevel.

In dieser Phase wird überprüft, ob ein Produkt den Anforderungen der Spezifikation und dem erforderlichen Sicherheitsniveau entspricht. Während Integrations-, Regressions- und Unit-Tests für die funktionale Bewertung hilfreich sind, sind Sicherheitstests, Schwachstellen-Scans und Penetrationstests ein wichtiger Teil der Sicherheitstests, die in der Verifizierungsphase durchgeführt werden.

Essentiell bei der Durchführung von Tests ist es, dass diese Tests nicht vom Entwickler selbst durchgeführt werden. Der Entwickler selbst ist geneigt die korrekte Funktion zu bestätigen, währen ein Tester bestrebt ist, Fehler zu entdecken.

Sicherheitstests

In dieser Phase müssen die Sicherheitskontrollen getestet werden, um zu überprüfen, ob sie ordnungsgemäß entwickelt wurden und tatsächlich das erforderliche Maß an Sicherheit bieten.

Schwachstellen-Scanning

Automatisierte Schwachstellen-Scans werden regelmäßig durchgeführt, um Schwachstellen zu erkennen und zu beseitigen, bevor ein Produkt veröffentlicht wird. Zusätzlich wird empfohlen, in

diesem Schritt Fuzzing[18] durchzuführen, um zu prüfen, ob ein Programm sowohl auf erwartete als auch auf unerwartete Eingabewerte korrekt reagiert, um Pufferüberläufe, Eingabevalidierungsfehler sowie andere Sicherheitslücken zu identifizieren.

Penetrationstests

Penetrationstests, die von Sicherheitsexperten durchgeführt werden, sind effektiv für die Entdeckung anspruchsvoller Schwachstellen und ergänzen daher die von automatisierten Tools durchgeführten Schwachstellenscans auf fruchtbaren Boden.

Requirement-driven Testing

Tabelle 17: Überprüfungsphase – Requirement-driven Testing

Nr.	Beschreibung	SL1	SL2	SL3	SL4
T.1	Testplanerstellung	M	M	M	M
T.2	Überprüfung der ordnungsbemäßen Funktion der kryptographischen Verfahren (Verschlüsselung, Signatur, …) nach Spezifikation. Wird tatsächlich das spezifizierte Verfahren eingesetzt.		(M)	M	M
T.3	Überprüfung der Sicherheitsmechanismen, falls keine kryptographischen Verfahren eingesetzt werden (IDs, Checksummen, Passwortschutz). Prüfung der Wirksamkeit. Test ob Fehlererkennung funktioniert	M	M	(M)	(M)
T.4	Überprüfung der sicherheitstechnischen Vorgaben zum Deployment und der Installation, den Service betreffend: - Herstellersignatur - Registrierung bei der MP - Upload/Download von Services			M	M
T.5	Überprüfung der Installationsmechanismen; Ordnungsgemäße Anmeldung am System	M	M	M	M
T.6	Überprüfung des spezifizierten Schlüsselmanagements (Verteilung, Update, Sperren)		(M)	M	M
T.7	Überprüfung des Zertifikatsmanagements (Verteilung, Update, Sperren)		(M)	M	M
T.8	Überprüfung des Konfigurationsmanagements		M	M	M
T.9	Überprüfung der Datensicherung und der kryptographischen Maßnahmen (Verschlüsselung, Zugriffsschutz)			M	M
T.10	Überprüfung Update und Patchmechanismen	M	M	M	M
T.11	Überprüfung der spezifizierten Mechanismen zum Authentitäts-Check Hersteller Signatur/Provider Signatur		O	M	M
T.12	Durchführung von Zertifizierungen			M	M

[18] Fuzzing oder Fuzz-Testing ist eine automatisierte oder teilautomatisierte Softwaretesttechnik, bei der ungültige, unerwartete oder zufällige Daten als Eingaben in ein Computerprogramm eingegeben werden.

Security Testing

Tabelle 18: Überprüfungsphase – Security Testing

Nr.	Beschreibung	SL1	SL2	SL3	SL4
T.13	Testplanerstellung	M	M	M	M
T.14	Durchführung von Schwachstellen-Scans		O	M	M
T.15	Durchführung von Beta-Tests	O	M	M	M
T.16	Durchführung von Penetration Tests		O	M	M
T.17	White Box Testing, Überprüfung und Tests von äußerst wichtigem Code		O	M	M

Involvierte Rollen

Reviewer

Ist entsprechend dem Sicherheitslevel ein Code Review vorgesehen, wird dies vom Reviewer durchgeführt. Für die Durchführung können ergänzend entsprechende Tools eingesetzt werden.

Test Manager

Verantwortlich für die Durchführung der funktionalen und nicht-funktionalen (sicherheitsrelevanten Tests). Dies schließt auch die Tests zur Sicherstellung der Einhaltung der Sicherheitslevel ein und er erteilt die Freigabe der Services.

Zertifizierer

Diese Rolle ist optional. Der Zertifizierer erhält Einblick in die gesamte Dokumentation des Entwicklungsprozesses und die Testergebnisse. Je nach Sicherheitslevel kann auch eine Sichtung der sicherheitsrelevanten Codepassagen erforderlich sein. Ebenso kann der Zertifizierer eigene Tests durchführen. Der Zertifizierer erteilt die Freigabe und erteilt ein Zertifikat. Die Rolle des Zertifizierers kann auch vom App-Store Betreiber (Marktplatzbetreiber) eingenommen werden.

Ausbringungsphase – Sicheres Deployment

Abbildung 12: Prozesse eines sicheren Deployments

Im Secure LCM stehen die Verfahren zum sicheren Bezug inklusive einer Freigabe von Services (auch) durch einen Service-Provider im Vordergrund. Hierzu gehört auch die Prüfung der Authentizität einer Software. Der Freigabeprozess sollte abhängig vom erforderlichen Sicherheitslevel sein. Dies kann von einer einfachen Überprüfung der grundlegenden Funktionen und Interfaces bis zu einem Code-Review und einer Zertifizierung und Signatur durch den Service-Provider reichen. Neben der IT-Sicherheit müssen hierbei aber auch Fragen der Haftung und der Verantwortlichkeiten getragen werden und somit auch die Wege oder Varianten des Deployments.

Ziele sind: der Schutz der Software vor Manipulation (beim Transfern vom Hersteller zum Shop, vom Shop zur UP), Überprüfbarkeit der Authentizität des Herstellers
Überprüfung des Zusammenspiels von Services (als Dienstleistung, Bundle Manager)

Richtlinien zur Auswahl des ISV

- Vertrauenswürdigkeit, Zuverlässigkeit, hohe Qualitätsansprüche
- Nachweis der Einhaltung der SLs?
- First und Second Level Support
- Meldesystem für das Melden von erkannten Mängeln (speziell auch Sicherheitsmängel)
- Wartung, Bereitstellung von Updates, Hotfixes für Sicherheitsmängel

Sicheres Deployment – Abschließende Sicherheitsüberprüfung / Zertifizierung

Die abschließende Sicherheitsüberprüfung konzentriert sich in erster Linie auf die Bewertung der Produktreife durch einen Service Provider oder Betreiber eines App-Stores, einschließlich der Fragen, die mit seiner Sicherheit zusammenhängen, und, falls erforderlich, auf die

Zertifizierung eines Produkts durch den App-Store-Betreiber, sowie auf die weitere Entscheidung, ob ein Produkt durch ihn auf den Markt gebracht werden soll oder nicht.

Tabelle 19: Ausbringung – Deployment

Nr.	Beschreibung	SL1	SL2	SL3	SL4
D.1	Zusammenstellung von Releases (Überprüfung der Kompatibilität von unterschiedlichen Software-Ständen einzelner Services); Gesamtpaket		O	M	M
D.2	Durchführung von Integrationstests durch den Provider		O	M	M
D.3	Umsetzung eines Secure-Deployments (automatisiert, zertifikatsbasiert)		O	M	M
D.4	Update und Patch-Management (Sicherheitsupdates)		O	M	M
D.5	Gesicherter An- und Abmeldeprozess		O	M	M
D.6	Zertifizierung und Vergabe eines Sicherheits-Label[19]			O	O

Involvierte Rollen

Marktplatzbetreiber

Der Marktplatzbetreiber betreibt den Marktplatz für die Bereitstellung und den Download von Services. Hierfür muss er einen Verzeichnisdienst anbieten. Zusätzlich stellt er Updates bereit und ist Anlaufstelle für 1st Level Support. Er überprüft die Authentizität der Services, die er von Herstellern erhält und den UPs zur Verfügung stellt. Ein weiteres Sicherheitsmerkmal wäre, dass er die von ihm angebotenen Services prüft und eine eigene Freigabe erteilt, so dass über die Installation von Services nicht die Sicherheit der UP bzw. der ESP gefährdet wird. Zu einem späteren Zeitpunkt wäre die Unterteilung der Rolle in

- Onboarding Manager
- Accounting Manager
- Support Manager (1st Level Support)

vorzunehmen.

Zertifizierer (optional)

Der Zertifizierer erteilt die Freigabe und erteilt ein Zertifikat. Die Rolle des Zertifizierers kann auch vom App-Store Betreiber (Marktplatzbetreiber) eingenommen werden.

[19] Die Vergabe eines Sicherheits-Labels kann/könnte im Rahmen der Zertifizierung von Services als Sicherheitsmerkmal erteilt werden.

Bundle Manager

Der Bundle Manager prüft die Kompatibilität und Interoperabilität von Services. Dabei ist auch die Interoperabilität von Services unterschiedlicher Versionsstände sicherzustellen. Der Bundle Manager kann dies als Dienstleistung im Rahmen des Marktplatzbetriebs anbieten oder es ist eine Rolle, die beim UP Betreiber angesiedelt ist.

Nachfolgend wird zusätzlich auf Rollenbeschreibungen, welche durch ITIL definiert werden, verwiesen[20]. Ob diese zu besetzen sind, ist im Einzelfall zu entscheiden.

1st Level Support

- Der Bearbeiter im 1st Level Support sorgt bei eingehenden Störungsmeldungen für die Registrierung und Einordnung und unternimmt einen unmittelbaren Lösungsversuch zur schnellstmöglichen Wiederherstellung des definierten Betriebszustands eines Service.
- Ist dies nicht möglich, leitet er die Störung an spezielle Bearbeiter Gruppen im 2nd Level Support weiter.
- Der 1st Level Support bearbeitet auch Service-Requests und informiert die User regelmäßig über den Bearbeitungsstand der Incidents.

Release Manager

- Der Release Manager ist verantwortlich für die Planung und Überwachung der Überführung von Releases in die Test- und Live-Umgebungen.
- Insbesondere stellt der Release Manager sicher, dass die Integrität der Live-Umgebung geschützt wird und dass nur zuvor geprüfte Komponenten ausgerollt werden

[20] Siehe *https://wiki.de.it-processmaps.com/index.php/Rollen_in_ITIL*

Betrieb und Wartung

Abbildung 13: Prozesse der Betriebs- und Wartungsphase

Der sichere Betrieb beginnt mit dem Prozess der Installation, des Einbindens oder Anbindens eines Service in oder an eine der Plattformen der ESP. Dazu ist zusätzlich ein Identitäts-Management, ein Key-Management oder ein Zertifikatsmanagement, je nach Sicherheitslevel erforderlich. Ebenso sind Dokumentationen zum Service notwendig, die einem Nutzer oder dem Administrator die Inbetriebnahme und Konfiguration erleichtern und diese sicher machen. Weiterhin ist für den sicheren Betrieb ein Event-Logging-Mechanismus hilfreich, wenn es um die Nachvollziehbarkeit von Fehlfunktionen oder um die Früherkennung von Angriffen geht. In einer weiteren Stufe wäre Monitoring zu nennen. Monitoring unterscheidet sich vom reinem Logging durch die Analyse und Auswertung der erfassten Daten. Damit ist Monitoring ein wichtiges Mittel der Früherkennung von Angriffen und somit ein Instrumentarium zur Abwehr von Angriffen. Angriffe erfolgen oft in mehreren Schritten. Wird der erste Schritt erkannt, der zumeist eine erste Analyse möglicher Schwachstellen ist, können Maßnahmen zur Abwehr des nachfolgenden eigentlichen Angriffes eingeleitet werden.

Da sich Angriffsvektoren und die Fähigkeiten von Angreifern im Leben einer Anwendung laufend ändern, ist die Aufrechterhaltung der Sicherheit ein dynamischer Prozess, der ständig Anpassungen unterliegt. Dazu ist es erforderlich, dass der Software-Entwickler regelmäßig überprüft, ob es Sicherheitsvorfälle bei der eingesetzten Software gibt oder ob es bei eingesetzter Fremdsoftware zu Sicherheitsvorfällen kam. Lücken sind durch ein Patch- oder Update-Management zu schließen. Dafür braucht es entsprechenden Support.
Je nach Sicherheitslevel ist ein Alarmmanagement erforderlich, um bei unerwarteten Ereignissen einen Alarm auszulösen, damit notwendige Maßnahmen eingeleitet werden können. Im Falle der kritischen Infrastrukturen ist hierzu auch die Gesetzeslage zu betrachten und es muss ggf. die entsprechende Behörde informiert werden, wenn es zu sicherheitsrelevanten Vorfällen kam.

Ein zusätzlicher Faktor ist ein Notfall-Management im Fehlerfall. Im Kontext der Verfügbarkeit soll das Notfallmanagement sicherstellen, dass eine N-1 Sicherheit besteht, sofern die Verfügbarkeit essentiell ist, ein Notbetrieb ermöglicht wird oder sonstige Maßnahmen eingeleitet werden können, die schwerwiegende Auswirkungen abschwächen oder sogar vermeiden können.

Fast jedes Out-of-the-Box-Produkt muss ordnungsgemäß konfiguriert werden, um in der Produktionsumgebung zu funktionieren. Danach muss das Produkt überwacht und bei Bedarf aktualisiert werden (z. B. aufgrund der Veröffentlichung einer neuen Version des Produkts, der Notwendigkeit, aufgedeckte Codierungsfehler oder Schwachstellen zu korrigieren), um weiterhin das erforderliche Sicherheitsniveau zu gewährleisten.

Update-Management: Da sich Angriffsvektoren und die Fähigkeiten von Angreifern im Leben einer Anwendung laufend ändern, ist die Aufrechterhaltung der Sicherheit ein dynamischer Prozess, der ständig Anpassungen unterliegt.

Alarm-Management: Je nach Sicherheitslevel ist ein Alarmmanagement erforderlich, um bei unerwarteten Ereignissen einen Alarm auszulösen, damit notwendige Maßnahmen eingeleitet werden können. Im Falle der kritischen Infrastrukturen ist hierzu auch die Gesetzeslage zu betrachten und es muss die entsprechende Behörde (BSI) informiert werden, wenn es zu schwerwiegenden sicherheitsrelevanten Vorfällen kam.

Notfall-Management: Das Notfallmanagement sorgt dafür, dass erforderliche Maßnahmen zur Wiederaufnahme der Systemfunktionen nach einem erfolgreichen Angriff umgesetzt werden.

Sichere Konfiguration: Eine sichere Konfiguration ist erforderlich, damit ein Produkt in der jeweiligen Produktionsumgebung auch zuverlässig funktioniert.

Operational Management

Tabelle 20: Betrieb und Wartung – Operational Management

Nr.	Beschreibung	SL1	SL2	SL3	SL4A
OP.1	Betrieb und Anbindung an eine PKI (Unterstützung Zertifikatsmanagement)		O	M	M
OP.2	Betrieb und Anbindung an eine zentrale CA für die MP und die UP (Zertifikatsmanagement externe Services)		O	M	M
OP.3	Betrieb und Anbindung an Sub-CAs in den Unternehmen für Zertifikatsmanagement (UP Services)		O	M	M
OP.4	Management für Sicherheits-Patches und Updates; Betrieb Updateserver; Informationsplattform, …			M	M
OP.5	Anbindung an eine ESP Meldesystem für Bugs / Sicherheitsvorfälle		O	M	M
OP.6	Logging und Monitoring von ungewöhnlichen Ereignissen, als präventive Maßnahmen für Angriffsversuche	M	M	M	M
OP.7	Alarmmanagement zur Einleitung von Notfallmaßnahmen		M	M	M

Plan zur Reaktion auf Vorfälle

Kein Unternehmen möchte anfällige Software entwickeln. Dennoch passieren Fehler, Versäumnisse und andere unerwünschte Dinge, ebenso wie die Entdeckung neuer Schwachstellen. Daher ist ein fertiger Incident Response Plan entscheidend, um Zeit und Geld zu sparen.

Incident Management

Tabelle 21: Betrieb und Wartung – Incident Management

Nr.	Beschreibung	SL1	SL2	SL3	SL4
OP.8	Erstellung von Notfallplänen und Umsetzung Maßnahmen in Notfällen (speziell auch zum Thema KRITIS)		O	M	M
OP.9	Betrieb eines Secure Backupkonzept zur Wiederherstellung nach einem Angriff			M	M
OP.10	Anbindung an ein Behördenmeldesystem zur Meldung von Vorfällen (speziell im Falle KRITIS)			M	M
OP.11	Betrieb eine Meldesystems (Hersteller oder App-Store Betreiber) zur Meldung von Fehlern		M	M	M

Die nachfolgenden Rollenbeschreibungen beziehen sich zum größten Teil auf Rollen, die im jeweiligen Unternehmen angesiedelt sind, welche die Plattformen (UP und MP) betreiben. Ausnahme bilden hierbei der Marktplattbetreiber und der ISV. Dieses sind im Rahmen der Aufrechterhaltung der Sicherheitslevel: Rollen für Support, Change-Management und Updates (speziell sicherheitsrelevante Updates) externe Rollen, die Dienste oder Dienstleistungen bereitstellen müssen.

Involvierte Rollen

Service Ersteller (ISV) – zusätzliche Aufgaben

In SynErgie wird vorgesehen, dass sowohl der 2nd Level Support, als auch der 3rd Level Support beim Service-Ersteller zu erfolgen hat. Zusätzlich ist der Service-Ersteller dafür verantwortlich entsprechende Updates oder bei festgestellten Sicherheitslücken zeitnah Hotfixes zur Verfügung zu stellen.

Marktplatzbetreibers – zusätzliche Aufgaben im Betrieb

Der Marktplatzbetreiber stellt im Betrieb den 1st Level Support sicher und stellt Updates oder Hotfixes den UPs zur Verfügung.

Spezifische Rollen und Aufgabe der MP in der Betriebsphase

Die nachfolgenden Rollen der MP wurden in zusammen mit den Verantwortlichen für die Kernkomponenten der MP ermittelt und deren Funktion definiert.

(Deployment) und Betrieb	Externe Services	IT-Sicherheit uns Resilienz
• MP Hoster (IaaS) • MP Betreiber (PaaS) • Root CA Admin • Sys Admin • Operativer Admin • User Manager • User Support • Root CA Betreiber	• Service Anbieter • Nicht-registrierter Services Nutzer • Registrierter Service Nutzer	• IT-Security Operator • Incident Manager • Backup Manager

Abbildung 14: Zentrale Rollen zum Betrieb der MP

Spezifische Rollen der UP in der Betriebsphase

Rollen - Vorbereitung	Deployment und Betrieb	IT-Sicherheit uns Resilienz

• Flex Auditor
• Systemarchitekt
• System-Integrator
	• UP Hoster (IaaS)
	  • Sys-Admin
	• UP Betreiber (ggf. PaaS)
	  • *UP Service Kurator*
	  • *UP Service Integrator*
	  • *UP IAM Manager*
	  • *UP Service Admin*
	• UP Service Nutzer
	• UP Services Anbieter (ISV)
	• Marktplatz Betreiber (UP Services)
		• IT Security Operator
		• Incident Manager
		• Backup Manager

Abbildung 15: Zentrale Rollen zum Betrieb der UP

Zusätzlich wurden unter dem Aspekt IT-Sicherheit und Resilienz weitere Rollen definiert.

IT-Sicherheit und Resilienz

Abhängig davon, wie groß ein möglicher Schaden bei einem erfolgreichen Cyber-Angriff sein kann, sollten zusätzliche Rollen in einem Unternehmen definiert werden. Ob und welche Unternehmen hiervon betroffen sind, muss im Detail geklärt werden. Dies hängt einmal davon ab, ob die jeweilige Plattform in einem Betrieb eingesetzt wird, der als Kritische Infrastruktur zugehörig eingestuft wird oder nicht. Falls nicht ist es keine gesetzliche Vorgabe, kann die Instanziierung der nachfolgenden Rollen im Unternehmen sinnvoll sein, damit größere Ausfälle vermieden werden. Nach aktueller Kenntnislage wird dies vorrangig auf die UPs und ihren Betrieb zutreffen, da der Ausfall der MP und die Wiederherstellung nicht unmittelbar als hoch kritisch einzustufen ist und es somit nicht zwingend Notlaufeigenschaften geben muss. Bei datenschutzrechtlichen Aspekten (Verlust der Vertraulichkeit von Daten) kann aber auch hier die Einführung der nachfolgenden Rollen erwogen werden.

IT Security Operator (KRITIS)

Überwacht die ordnungsgemäße Funktion der UP und der Services; Erkennung von ungewöhnlichem Verhalten zur Erkennung von Cyber-Attacken. Übernimmt die Umsetzung der geforderten Funktionen des IT-Sicherheitsgesetzes 2.0 zur frühzeitigen Angriffserkennung und Abwehr. Erkennung von Cyberangriffen (Früherkennung) und Einleiten von Gegenmaßnahmen. Die Rolle ist für KRITIS nach IT-Sicherheitsgesetz 2.0 erforderlich. Er übernimmt bei KRITIS die Meldung erheblicher Sicherheitsvorfälle an die Meldestelle (BSI).

Incident Manager

Der Incident Manager ist verantwortlich für die effektive Durchführung des Incident-Management-Prozesses und führt das entsprechende Berichtswesen durch. Er ist die erste Eskalationsstufe für Incidents, falls diese nicht innerhalb der vereinbarten Service Levels gelöst werden können. Das IT-Incident Management (IT-Störungsmanagement) umfasst hierbei alle organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Betriebsstörungen in den IT-Bereichen.

Backup Manager

Führt regelmäßige Backups durch und ist im Falle eines Angriffs oder Ausfalls zusammen mit dem Incident Manager dafür verantwortlich, dass die Aufnahme des Betriebs schnellstmöglich wieder erfolgen kann (Notfallbetrieb und nachfolgend Aufnahme des Normalbetriebs)

Nachfolgend wird zusätzlich auf Rollenbeschreibungen, welche durch ITIL definiert werden, verwiesen[21]. Ob diese zu besetzen sind, ist im Einzelfall zu entscheiden.

2nd Level Support

- Der Bearbeiter im 2nd Level Support übernimmt Störungsmeldungen vom 1st Level Support, die dieser nicht selbständig lösen kann.
- Bei Bedarf wird er Unterstützung von Herstellern (3rd Level Support) anfordern.
- Ziel ist die schnellstmögliche Wiederherstellung des definierten Betriebszustands eines Service.
- Ist keine ursächliche Störungsbeseitigung möglich, übergibt er die Störung zur weiteren Bearbeitung an das Problem Management.

3rd Level Support

- Der Bearbeiter im 3rd Level Support ist typischerweise bei einem Hersteller von Hardware- oder Softwareprodukten angesiedelt; er wird vom 2nd Level Support mit einbezogen, wenn dies zur Beseitigung von Störungen erforderlich ist.
- Ziel ist die schnellstmögliche Wiederherstellung des definierten Betriebszustands eines Service.

IT Operations Manager

- Der IT Operations Manager trägt die gesamtheitliche Verantwortung für verschiedene Aktivitäten in Service Operation.
- Er stellt unter anderem sicher, dass alle operativen Routine-Aufgaben zeitgerecht und zuverlässig ausgeführt werden.

IT Operator

- IT Operatoren sind Mitarbeiter, die die Betriebs-Tätigkeiten des Tagesgeschäfts ausführen.
- Ihre typischen Aufgaben umfassen beispielsweise das Erstellen von Backups, die Planung von Batch-Jobs, und das Installieren von Standard-Komponenten.

[21] Siehe *https://wiki.de.it-processmaps.com/index.php/Rollen_in_ITIL*

Major Incident Team

- Das Major Incident Team ist ein dynamisch gegründetes Team von IT Managern und technischen Experten, normaler Weise unter der Führung des Incident Managers.
- Es wird einberufen, um gemeinsam die Lösung für einen Major Incident (schwerwiegenden Incident) zu erarbeiten.

Problem Manager

- Der Problem Manager ist dafür verantwortlich, alle Probleme über ihren gesamten Lebenszyklus zu verwalten.
- Seine vorrangigen Ziele bestehen darin, der Entstehung von Incidents vorzubeugen und die negativen Auswirkungen von Incidents, die nicht verhindert werden können, möglichst gering zu halten.
- Zu diesem Zweck pflegt er die Informationen zu bekannten Errors und Workarounds.

Außerbetriebnahme

Abbildung 16:Prozesse der Außerbetriebnahme

Bei der Außerbetriebnahme ist ein besonderes Augenmerk darauf zu legen, dass schützenswerte Daten einerseits nicht verloren gehen (Datensicherung und Aufbewahrung), sofern diese aus bestimmten Gründen weiterhin benötigt werden (gesetzliche Aufbewahrungspflicht, Firmen-Know-how, etc.) aber andererseits auch nicht in falsche Hände geraten (Mediensanitisierung). Die gilt auch für Zertifikate, Secret Keys, lokal gespeicherte Passwörter oder Zugangsdaten. Ebenso wichtig ist ein geordneter Abmeldeprozess eines Service vom System, damit dieser nicht von einem Angreifer genutzt werden kann, um sich Zugang zum System zu verschaffen.

Wenn es an der Zeit ist, ein Produkt zu entsorgen (aufgrund seiner Veralterung, einer notwendigen Aktualisierung oder aus anderen Gründen), müssen geschützte Informationen weiterhin sicher aufbewahrt werden. Um dies richtig anzugehen, sollte ein Entsorgungsprozess geplant und im Voraus durchdacht werden, wobei auf Sicherheitsmaßnahmen geachtet werden sollte, die zur Erhaltung wertvoller Informationen, zur Desinfektion von Medien sowie insgesamt zur Entsorgung von Hard- und Software angewendet werden sollten.

Bewahrung der Informationen

Die Bewahrung der wertvollen Informationen bedeutet nicht nur die Sicherstellung der Verfügbarkeit dieser Informationen (z. B. wenn dies gesetzlich vorgeschrieben ist), sondern auch die Gewährleistung ihres Schutzes während und ggf. nach der Produktentsorgung.

Mediensanitisierung und Entsorgung

Besonderes Augenmerk muss auf die Mediensanitisierung (durch Überschreiben, Entmagnetisierung (Degaussing) oder physische Zerstören) gelegt werden, die erforderlich ist, um die Offenlegung sensibler Informationen zu verhindern. Dies kann durch die Verwendung zugelassener Techniken und Geräte erfolgen, die entsprechend der erforderlichen Sicherheitsstufe ausgewählt werden.

Hardware- und Software-Entsorgung

Während die physische Entsorgung von Hardware fast immer nur dann erforderlich ist, wenn sensible Informationen nicht auf andere Weise bereinigt werden können, wird die Entfernung von veralteter Software in der Regel dringend empfohlen, da diese Software sonst zu neuen Risiken führen kann.

Tabelle 22: Außerbetriebnahme – Sichere Entsorgung

Nr.	Beschreibung	SL1	SL2	SL3	SL4
DEC.1	Datensicherung – Bewahrung von Daten	O	O	M	M
DEC.2	Sichere Mediensanitisierung (sicheres Vernichten von vertraulichen Daten, Secrete Keys, Zertifikaten)		O	M	M
DEC.3	Umsetzung eines gesicherter Abmeldeprozesses		O	M	M
DEC.4	Sichere Entsorgung von Hardware- und Software			M	M

Datenrettung

Bei der Ausmusterung von Software und Hardware ist darauf zu achten, dass Daten, die weiterhin verfügbar sein sollen (gesetzliche Aufbewahrungspflicht oder aus betrieblicher Notwendigkeit) gesichert werden.

Entsorgung

Bei der Entsorgung Hardware ist darauf zu achten, dass vor der Weitergabe an einen Entsorger die darauf enthaltenen Daten sicher gelöscht werden, so dass diese nicht wieder rekonstruiert werden können. Für Software gilt, dass der Zugriff und die Berechtigungen entsprechend gelöscht oder angepasst werden. **Involvierte Rollen**

- Backup Manager
- IT Security Operator
- Vertrauenswürdiger Entsorger

Beschreibung präventiver Maßnahmen und Empfehlungen

Nachfolgend werden präventive Maßnahmen beschrieben, die sich bei Schwachstellenanalysen immer wieder zeigen und sich auch bei der Durchführung des Threat-Modelings der Plattformen der ESP als mögliches Angriffspunkte gezeigt haben. Die Präventiven Maßnahmen sind bei den Anforderungen im Life Cycle Management mit aufgenommen. Zusätzlich erfolgt eine Beschreibung allgemeiner Empfehlungen.

Präventive Maßnahmen

Bedrohung: Fehlendes Logging

Maßnahme Logging umsetzen
Alle Services müssen sicherheitsrelevante Events loggen. Wenn das Betriebssystem diese Aufgabe nicht übernimmt, muss zusätzlich auch die Anbindungen an einen Log-Server implementiert werden. Die Maßnahme ist ab SL-1 umzusetzen.

Maßnahme Einheitliches Log-Format
Alle Services sollen ein einheitliches Format für Log-Events verwenden.
Dies erleichtert die Analyse der Log-Events eines Service und die Vergleichbarkeit von Log-Events verschiedener Services. Dabei reicht es nicht einfach nur ein Format, wie JSON zu verwenden, sondern auch die Namen und die Formate der Felder sollten festgehalten werden.
Die Maßnahme ist ab SL-1 umzusetzen.

Bedrohung: Unzureichende Datenvalidierung

Maßnahme Syntaktische Validierung
Sobald ein Service eine Eingabe erhält, muss der Service das Format/die Syntax der Eingabe überprüfen bevor diese Eingabe verarbeitet wird. Hält die Eingabe der Überprüfung nicht stand muss die Eingabe verworfen werden und darf nicht verarbeitet werden.
Das gleiche gilt für festgelegt Formate innerhalb der Eingabe, wie Datumsformate, URLs und Zahlen. Für alle Eingaben sollte ein Format festgelegt werden, um möglich früh ungültige Eingaben zuerkennen. Die Formate sollten möglichst einfach und leicht überprüfbar sein. (Eine natürliche Zahl wie 21 sollte also nicht auch mit 0b10101, 025, 0o25, 0x15, 21., 21.0, 21.0e0 beschreibbar sein). Zusätzlich muss ein Log-Event erstellt werden, welches eine invalide Eingabe dokumentiert. Die Quelle der Eingabe ist dem Log-Event anzuhängen.
Die Maßnahme ist ab SL-1 umzusetzen.

Maßnahme Semantische Validierung
Sobald ein Service eine Eingabe erhält, muss der Service nach der Syntaxvalidierung die Plausibilität der Eingaben überprüfen. Ob eine Eingabe plausibel ist, hängt natürlich von der Anwendung ab. Zum Beispiel kann überprüft werden, ob ein Erfüllungszeitpunkt bereits in der Vergangenheit liegt, ein Endzeitpunkt nach einem Startzeitpunkt liegt oder eine Mengenangabe nicht negativ ist. Für häufig verwendet Formate, wie das EFDM, empfiehlt es sich Testdaten zu erzeugen, welche Syntax- und Semantikfehler enthalten.
Die Maßnahme ist ab SL-2 umzusetzen.

Maßnahme Kontext Validierung
Bei kritischen Services empfiehlt es sich, zusätzlich Wissen über den Kontext mit zu validieren. Kontextwissen ist jegliches Wissen, welches der Service über sein Umfeld hat und erfahren kann. Dies können Aspekte sein, wie die aktuelle Uhrzeit, oder, dass neue EFDMs von einem identischen Absender ein neueres Erstellungsdatum haben müssen als zuvor empfangene EFDMs.
Das Kontextwissen kann vom Administrator vorgegeben werden, es ist jedoch auch denkbar, dass der Service dieses Wissen lernt. Wenn die Validierung scheitert, muss ein Log-Event erstellt werden. Der Kontext sollte mitgeloggt werden.
Die Maßnahme ist ab SL-3 umzusetzen.

Bedrohung: Fehlende Autorisierung in der UP

Maßnahme Autorisierung als Standard
Services innerhalb der UP, welche über den MSB kommunizieren, sollten immer einen Autorisierungsmechanismus umsetzen, auch dann, wenn keine Policy vorhanden ist oder eine Authentifizierung möglich ist.
Wird eine Anwendung direkt so entwickelt wird, dass eine Nachricht oder Anfrage abgelehnt werden könnte, dann ist es deutlich leichter im Nachhinein komplexere Regeln und eine Authentifizierung einzubauen.
Bei einer fehlgeschlagenen Autorisierung muss ein Log-Event erstellt werden.
Die Maßnahme ist ab SL-2 umzusetzen.

Maßnahme Service-Policy definieren
Services innerhalb der UP, welche über den MSB kommunizieren, müssen eine Policy (Regelwerk) festlegen, in der festgehalten ist, welcher Kommunikationspartner welche Funktion aufrufen darf. Die Berechtigungen hängen vom jeweiligen Service ab.
In einfachen Fällen reicht es aus, festzulegen, wer eine Funktion aufrufen darf.

Bei komplexeren Abläufen und Daten kann es nötig sein, dass kontextabhängige Regeln verwendet werden müssen: z.B. darf nur der Smarte Konnektor mit der ID XY5 EFDMs für die Anlage ABC123 erstellen. Die Maßnahme ist ab SL-3 umzusetzen.

Bedrohungen:

- ***Fehlende Autorisierung in der UP***
- ***Unbekannte Quelle über den MSB***
- ***Manipulierbare Nachrichten in der UP***
- ***Versand in der UP ist abstreitbar***

Maßnahme Signatur der Nachrichten durch den Sender
Services innerhalb der UP, welche über den MSB kommunizieren, müssen in der Lage sein, den Sender einer Nachricht bestimmen zu können. Dies ist eine Voraussetzung, um eine Autorisierung durchführen zu können. Die präferierte Methode ist, dass die Nachrichten vom Sender signiert werden und der Empfänger ein Verzeichnis hat mit allen autorisierten Kommunikationspartnern und deren öffentlichen Schlüsseln. Bei einer ungültigen Signatur muss ein Log-Event erstellt werden. Die Maßnahme ist ab SL-3 umzusetzen.

Bedrohungen:

- ***Konfigurationsschnittstellen***

Maßnahme Offline Konfiguration
Um die Angriffsfläche innerhalb der Services zu verringern, sollte auf die Möglichkeit verzichtet werden, die Services im Betrieb umzukonfigurieren. Diese Konfigurationsschnittstellen sind häufig schlecht gesichert und bieten nur einen geringen Mehrwert in einem Produktionsbetrieb. Zusätzlich ist der Aufwand größer, da eine API, ein Datenformat und die Software rekonfigurierbar entwickelt werden muss. Eine Konfiguration über eine Konfigurationsdatei sollte in den meisten Fällen ausreichen. Diese kann online über etablierte Protokolle (SSH) verändert werden. Die Rekonfiguration des Service erfolgt dann nach dem Neustart.
Nur, wenn es für die Funktion des Service absolut notwendig ist, dass nicht IT-Personal den Service umkonfiguriert, sollte eine solche Schnittstelle entwickelt und betrieben werden. Die Maßnahme ist ab SL-1 umzusetzen.

Bedrohung: Selbst entwickelte Benutzerverwaltung

Maßnahme Verwendung eines zentralen SSO in der UP
Für die Benutzerverwaltung und Authentifizierung innerhalb der UP von Benutzern sollte ein Single-Sign-On-Service verwendet werden.
Dadurch verringern sich Angriffsflächen der Services und auch das Risiko Benutzerdaten (Passwörter) zu verlieren. Zusätzlich bieten Single-Sign-On-Services Zwei-Faktor-Authentifizierung. Die Maßnahme ist ab SL-2 umzusetzen.

Maßnahme Verwendung von etablierten Bibliotheken
Für die Benutzerverwaltung und Authentifizierung sollten etablierte Bibliotheken und Frameworks verwendet werden. Die Maßnahme ist ab SL-2 umzusetzen.

Bedrohung: Denial-of-Service via Ressourcenerschöpfung

Maßnahme Beschreibung der verwendeten Ressourcen
Jeder Service sollte eine Einschätzung vornehmen, welche Ressourcen verwendet werden und wie diese dimensioniert sein müssen. Dies erleichtert die Arbeit der Administratoren. Denn nur, wenn diese die benötigte Dimension einer Ressource und den Bedarf im Betrieb kennen, können sie diese auch ins Monitorring aufnehmen und Limits setzen. Die Maßnahme ist ab SL-1 umzusetzen.

Maßnahme Vermeidung von angreifbaren Datenformaten
Services sollten Datenformate vermeiden, welche sich leicht für Angriffe nutzen können. Datenformate wie XML, YAML, ZIP, usw. erlauben rekursive Datendefinitionen, mit denen die Ressourcen CPU, RAM und Festspeicher erschöpft werden können.
Die Empfehlung ist hierfür Formate zu verwenden, welche einfach zu parsen und wenige Funktion haben, besonders, wenn diese über Verbindungen von außen kommen.
Formate wie JSON sind hier zu bevorzugen. Die Maßnahme ist ab SL-2 umzusetzen.

Maßnahme Limits für externe Daten setzen
Wenn Daten von außen empfangen wurden, sollte der Service Limits für die Verarbeitung dieser Daten setzen. Die Limits sollten konfigurierbar sein. Wird ein Limit überschritten, muss ein Log-Event erstellt werden.
Beispiel für Limits sind

- Maximale Größe in Bytes

- Verschachtelungstiefe bei verschachtelten Daten (JSON, XML).
- Maximale CPU-Zeit bei der Verarbeitung

Die Maßnahme ist ab SL-3 umzusetzen.

Maßnahme Limits für das Betriebssystem vorschlagen
Betriebssysteme verfügen über verschiedene Funktionen, um die verwendeten Ressourcen eines Programms einzuschränken. Die Services sollten zu der Beschreibung der verwendeten Ressourcen auch angeben, welche Limits vom Betriebssystem gesetzt werden könnten. Besonders bei dem verwendeten Festspeicher verfügen die Betriebssysteme über mehr Möglichkeiten. Die Maßnahme ist ab SL2 umzusetzen.

Weitere allgemeine Empfehlungen zu Maßnahmen

Signieren der EFDM-Nachrichten
Innerhalb der UP werden Informationen zwischen Services über den MSB ausgetauscht, hieraus ergibt sich, dass keine Ende-zu-Ende gesicherten Kanal zwischen den involvierten Services existiert. Was geschützt ist, ist die Kommunikation zwischen dem Service und dem MSB. Viele Services vertrauen aber darauf, dass der MSB ihnen nur Informationen und Nachrichten zustellt, die von bestimmten Services kommen (z.B. Smarter-Konnektor schickt EFDM an die Optimierer). Dabei ist aber nicht ausgeschlossen, dass der MSB als „Confused Deputy“[22] (Hardy 1988) handelt.

Kontinuierliche Integration der Software-Komponenten
Beim Review der Threat-Models ist es offensichtlich geworden, dass es bei so einem großen Projekt zu Missverständnissen bzgl. Komponenten unterschiedlicher Teams kommen kann. Solche Missverständnisse schwächen die Verlässlichkeit der Software, können aber auch zu Sicherheitslücken führen. Dies hat sehr individuelle Gründe, denen aber mit einer koordinierten kontinuierlichen Integration entgegengewirkt werden kann. Regelmäßige Integrationen erlauben es, Missverständnisse früher zu erkennen und die betroffenen Stakeholder zu identifizieren.

Testdaten für das empfangene Datenformat
Für die Übertragung von Daten, wie dem EFDM, wird das EFDM in ein JSON-Format serialisiert. JSON ist der De-Facto-Standard für die Übertragung von Daten im Web geworden. Allerdings hat der JSON-Standard einige Unklarheiten und Fallstricke. Um solchen Problemen zuvorzukommen, sollte eine Datenbasis an validen und nicht validen Testdaten für das EFDM

[22] Als Confused Deputy gilt ein Computerprogramm, welches unschuldig von einer anderen Partei dazu verleitet wird, seine Befugnisse zu missbrauchen. Es handelt sich dabei um eine besondere Form der Ausweitung von Berechtigungen.

erstellt werden. Mit solchen Testdaten können dann alle Services, welche EFDMs empfangen, auf deren Konformität mit dem EFDM-Format überprüft werden.

Bessere Unterstützung für ein automatisiertes Deployment
Viele Services auf der UP bieten eine Web-Schnittstelle an, mit welcher der Service im laufenden Betrieb neu konfiguriert werden kann. Dies verursacht zwei Probleme: Zum einen kann eine solche Web-Schnittstelle nicht ohne weiteres automatisch ausgerollt werden, zum anderen benötigt diese Web-Schnittstelle eine Authentifikation und Autorisierung, welche innerhalb des Service umgesetzt werden muss. Es ist daher empfehlenswert, anstelle dessen eine Konfigurationsdatei zu verwenden, die durch die Authentifikation und Autorisierung des Betriebssystems geschützt werden kann. Eine Konfigurationsdatei lässt sich auch einfacher in CI/CD-Pipelines verwenden.

Kapselung auf Netzwerk- und Anwendungsebene
Umfangreiche IT-Infrastrukturen erfordern eine fortschrittliche Strategie für die Netzwerksicherheit. Hier reicht es nicht, das gesamte Netzwerk mit einer Firewall nach außen abzugrenzen. Vielmehr sollte das interne Netzwerke in kleine, logische Einheiten segmentiert sein, und alle diese Einheiten sollten mit Netzwerksicherheitsmaßnahmen voneinander gekapselt werden. Dies verhindert, dass ein Angreifer, der an einer Stelle in das Firmennetz eingedrungen ist, sich ungestört weiträumig im Netzwerk bewegen kann und so schnell viele weitere Systeme infiltrieren kann. Zudem hat die äußere Firewall eines Unternehmens in der heutigen vernetzten Welt viele Öffnungen, so dass die äußere Angriffsfläche groß und unübersichtlich ist. Durch geeignete Segmentierung kann man hier zu übersichtlichen, geschützten Bereichen gelangen.

Für die Einbettung der UP in eine Unternehmensinfrastruktur bedeutet dies, dass sie idealerweise in einem eigenständigen, geschützten Netzwerksegment oder in einer geschützten Cloud-Umgebung betrieben wird. Verbindungen mit anderen, ebenfalls gekapselten Bereichen wie dem Büronetz oder dem Produktionsnetz sind somit nur über explizit freigegebene und geschützte Zugriffswege möglich. Ebenso ist es zu vermeiden, dass beliebige Komponenten der UP Verbindungen mit Systemen außerhalb haben können. Stattdessen sind hierfür in der Architektur der UP dedizierte Konnektoren sowie der Marktinformationsbeschaffungsservice und die Vermarktungskomponente vorgesehen. Weiterhin sollten die einzelnen Services innerhalb der UP gegeneinander gekapselt sein, d. h. nur über definierte Schnittstellen zugänglich sein Ergänzend hierzu sollten sie Eingangsdaten bzgl. Format, Struktur und Inhalt validieren, sowie für die eigene Datenhaltung private Ablageorte haben, die gegen den Zugriff anderer Services geschützt sind.

Filterung der Daten an der Datenquelle – Vererbung von Anforderungen
Eine Erkenntnis der durchgeführten Workshops zu Sicherheitslevel und Threat-Modeling war,

dass die Schnittstellen zu den ERP- und MES-Systemen zu einem Großteil noch nicht völlig bekannt sind. Ebenso ist damit nicht bekannt, welchen Vertraulichkeitsgrad die Daten und Informationen haben, die der UP zur Verfügung gestellt werden. Dabei sollte das Prinzip der Datensparsamkeit zur Anwendung kommen. Dies bedeutet, dass Daten, die in die UP eingespeist werden, nur die zwingend erforderlichen Informationen enthalten sollen, die ein Service für die Erfüllung seiner Aufgabe benötigt. Die Daten sollten – sofern dies möglich ist – bereits an der Datenquelle entsprechend gefiltert und soweit abstrahiert oder anonymisiert werden, dass die Anforderungen an die Vertraulichkeit und dementsprechend die erforderlichen Maßnahmen überschaubar und handelbar bleiben. Ansonsten könnte die Anforderung einer Ende-zu-Ende Verschlüsslung von Daten erforderlich sein, was durch den MSB erschwert wird.

Fazit

Der Security Guide dokumentiert als Gesamtwerk Anforderungen und Maßnahmen zur Umsetzung eines angepassten Maßes an IT-Sicherheit für die Entwicklung und den Betrieb der Services der ESP und die Komponenten der ESP selbst (UP und MP). Hierfür wurden Methoden und Maßnahmen erarbeitet und vorgestellt, mit deren Hilfe der Schutzbedarf ermittelt werden kann, Schwachstellen erkannt werden können und mittels Einstufung in Sicherheitslevel passgerechte Anforderungen und Maßnahmen zur Einhaltung der erforderlichen IT-Sicherheit erzielt werden sollen.

Der Security Guide bedient sich hierzu zu einem erheblichen Teil der Empfehlungen und Vorgaben aus dem BSI-Grundschutz, weiterer relevanter Standards nationaler, sowie internationaler Behörden und Institutionen aber auch nicht-behördlicher Organisationen zum Thema IT-Sicherheit. Dies sowohl bei der Definition von Anforderungen, als auch bei der Auswahl und Adaption von Methoden und Verfahren, z.B. bei der Einstufung in Sicherheitsklassen, Methoden der Schwachstellenerkennung, Rollendefinitionen und Schutzbedarfsdefinition. Hierfür werden anerkannte und etablierte Verfahren angewandt oder adaptiert. Ziel ist es, dass im Falle einer späteren Zertifizierung, die Nachvollziehbarkeit der angewandten Verfahren gegeben ist.

Literaturverzeichnis

Akram, Mehwish; Barker, William C.; Clatterbuck, Rob; Dodson, Donna; Everhart, Brandon; Gilbert, Jane et al. (2020): Securing web transactions TLS server certificate management. Gaithersburg, MD, zuletzt geprüft am 01.06.2022.

bdew (2019): B3S Aggregatoren. Bundesverband der Energie- und Wasserwirtschaft e.V. Online verfügbar unter https://www.bdew.de/media/documents/Awh_20190301_B3S-fuer-Anlagen-zur-Steuerung-und-Buendelung-elektrischer-Leistung.pdf, zuletzt geprüft am 17.09.2020.

Bowen, P.; Hash, J.; Wilson, M.: Information security handbook: a guide for managers. Online verfügbar unter https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf, zuletzt geprüft am 11.10.2021.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2021): BSI-Kritisverordnung. Online verfügbar unter https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf, zuletzt geprüft am 10.03.2022.

BSI-Standard 200.2: BSI-Standard 200.2. BSI-Standard 200.2. BSI-Standard 200.2. BSI – Bundesamt für Sicherheit in der Informationstechnik (BSI-Standard 200.2, BSI-Standard 200.2), zuletzt geprüft am 31.05.2022.

Bundesamt für Sicherheit in der Informationstechnik (2021): IT-Grundschutz-Bausteine (Edition 2020). Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/2020/Bausteine_Download_Edition_2020_node.html, zuletzt aktualisiert am 26.01.2021, zuletzt geprüft am 15.04.2021.

Bundesamt für Sicherheit in der Informationstechnik (2022): Lerneinheit 4.1: Grundlegende Definitionen - Lerneinheit 4.1. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/4_01_Definitionen.html, zuletzt aktualisiert am 14.03.2022, zuletzt geprüft am 31.05.2022.

Bundesamt für Sicherheit in der Informationstechnik - Verschlüsselung (2021): Arten der Verschlüsselung. Hg. v. Bundesamt für Sicherheit in der Informationstechnik - Verschlüsselung. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/Arten-der-Verschluesselung/arten-der-verschluesselung_node.html, zuletzt aktualisiert am 22.01.2021, zuletzt geprüft am 01.06.2022.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2021a): Die Lage der IT-Sicherheit in Deutschland 2021. Hg. v. BSI. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 01.06.2022.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2021b): Arten der Verschlüsselung - Arten der Verschlüsselung. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/Arten-der-Verschluesselung/arten-der-verschluesselung.html, zuletzt aktualisiert am 22.01.2021, zuletzt geprüft am 31.05.2022.

Bundesdruckerei (2022): Sechs Tipps für den erfolgreichen Aufbau einer PKI. Online verfügbar unter https://www.bundesdruckerei.de/de/innovation-hub/sechs-tipps-fuer-den-erfolgreichen-aufbau-einer-pki, zuletzt aktualisiert am 01.06.2022, zuletzt geprüft am 01.06.2022.

Bundesministerium der Justiz und für Verbraucherschutz (31.05.2022): StromNZV - nichtamtliches Inhaltsverzeichnis. Online verfügbar unter https://www.gesetze-im-internet.de/stromnzv/, zuletzt geprüft am 31.05.2022.

Bundesnetzagentur: BK6-18-249, Beschluss vom 20.05.2020. Online verfügbar unter https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2018/BK6-18-249/BK6-18-249_Beschluss_vom_20_05_2020.pdf;jsessionid=31123B6826AD6AECF0325430849739F9?__blob=publicationFile&v=1, zuletzt geprüft am 31.05.2022.

Bundesnetzagentur (2018): IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz. Bundesnetzagentur. Online verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf?__blob=publicationFile&v=4, zuletzt geprüft am 31.05.2022.

Bundesrepublik Deutschland (2005): EnWG - Energiewirtschaftsgesetz. Online verfügbar unter https://www.gesetze-im-internet.de/enwg_2005/, zuletzt geprüft am 17.09.2020.

Bundesrepublik Deutschland (2021a): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, zuletzt geprüft am 08.10.2021.

Bundesrepublik Deutschland (2021b): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetzestexte/it-sicherheitsgesetz-2.pdf;jsessionid=7F2D645924636EFF53D40716B2812189.1_cid364?__blob=publicationFile&v=1, zuletzt geprüft am 08.10.2021.

Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) (2019): Rollenmodell für die Marktkommunikation im deutschen Energiemarkt. Online verfügbar unter https://www.bdew.de/media/documents/Awh_20190507_Rollenmodell-MAK-Version1-2-END.pdf, zuletzt geprüft am 31.08.2020.

Datenschutz PRAXIS für Datenschutzbeauftragte (2019): Berechtigungskonzept: Schritt für Schritt umgesetzt. Online verfügbar unter https://www.datenschutz-praxis.de/tom/berechtigungskonzept-die-

wasserdichte-pruefung/?icomefrom=/fachartikel/berechtigungskonzept-die-wasserdichte-pruefung/, zuletzt aktualisiert am 12.07.2021, zuletzt geprüft am 31.05.2022.

Datenschutz-Grundverordnung (DSGVO) (2017): Art. 39 DSGVO – Aufgaben des Datenschutzbeauftragten - Datenschutz-Grundverordnung (DSGVO). Online verfügbar unter https://dsgvo-gesetz.de/art-39-dsgvo/, zuletzt aktualisiert am 02.06.2017, zuletzt geprüft am 31.05.2022.

Deutsches Institut für Normung e.V.: DIN EN ISO/IEC 27001:2017. Deutsches Institut für Normung e.V. Berlin (27001:2017).

DIN EN 62443-3-2:2018-10 - Entwurf: Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 65/690/CDV:2018). Berlin. Online verfügbar unter https://www.beuth.de/de/norm-entwurf/din-en-62443-3-2/294546806, zuletzt geprüft am 07.10.2021.

DIN EN IEC 62443-4-2:2019-12: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS) (IEC 62443-4-2:2019); Deutsche Fassung EN IEC 62443-4-2:2019. Deutsches Institut für Normung e.V. Online verfügbar unter https://www.beuth.de/de/norm/din-en-iec-62443-4-2/312858287, zuletzt geprüft am 07.10.2021.

DIN EN ISO/IEC 27001:2017-06: Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015). Online verfügbar unter https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716, zuletzt geprüft am 07.10.2021.

Dreißigacker, Arne; Skarczinski, Bennet von; Wollinger, Gina Rosa (2021): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020. Hannover: Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN) (Forschungsbericht / KFN, Kriminologisches Forschungsinstitut Niedersachsen e.V, Nr. 162). Online verfügbar unter https://www.pwc.de/de/im-fokus/cyber-security-privacy/cyberangriffe-gegen-unternehmen-in-deutschland-folgebefragung.pdf, zuletzt geprüft am 01.06.2022.

ENTSO-E (2020): The harmonised electricity market role model. Online verfügbar unter https://www.entsoe.eu/Documents/EDI/Library/HRM/Harmonised_Role_Model_2020-01.pdf, zuletzt geprüft am 31.08.2020.

EU-Richtlinie 2008/114/EG: Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Fundstelle: Amtsblatt der Europäischen Union. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008L0114, zuletzt geprüft am 17.09.2020.

NIST (CDC) FIPS 199: FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. Online verfügbar unter https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf, zuletzt geprüft am 11.10.2021.

NIST (CDC) FIPS 200: FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, zuletzt geprüft am 11.10.2021.

Hardy, N. (1988): The Confused Deputy: (or why capabilities might have been invented). In: *ACM SIGOPS Operating Systems Review* 22 (4), S. 36–38.

VDS Richtlinie 3473: Informationsicherheitsmanagementsystem für kleinere und mittlere Unternehmen (KMU). Online verfügbar unter https://shop.vds.de/de/download/766b96741ea1d8c70d0368c5a6b60e24/, zuletzt geprüft am 25.09.20.

ISO/IEC 15408-1:2009-12: Informationstechnik - IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit - Teil 1: Einführung und allgemeines Modell (15408-1 - 2009-12). Online verfügbar unter https://www.beuth.de/de/norm/iso-iec-15408-1/125041003, zuletzt geprüft am 11.10.2021.

ITU-T: ITU-T Rec. X.509 Corrigendum 1 (10/2021) Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks Technical Corrigendum 1, zuletzt geprüft am 31.05.2022.

Kohnfelder, L.; Garg, P. (1999): The threats to our products. In: *Microsoft Interface, Microsoft Corporation* 33.

Kondruss, Bert (2022): Ransomware & Cyberangriffe aktuell heute 2022. In: *KonBriefing.com*, 01.06.2022. Online verfügbar unter https://konbriefing.com/de-topics/cyber-angriffe.html, zuletzt geprüft am 01.06.2022.

Kuhn, D. R.; Hu, V.; Polk, W. T.; Chang, Shu-Jen H.: Introduction to public key technology and the federal PKI infrastructure, zuletzt geprüft am 01.06.2022.

Larcom, B.; Eddington, M. (2005): Trike v1 methodology document. In: *Draft, work in progress*.

Mccandless, David (2013): World's Biggest Data Breaches & Hacks — Information is Beautiful. In: *Information is Beautiful*, 22.07.2013. Online verfügbar unter https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, zuletzt geprüft am 01.06.2022.

Menci, Sergio Potenciano; Fridgen, Gilbert; van Stiphoudt, Christine; Schilp, Johannes; Köberlein, Jana; Bauernhansl, Thomas et al. (2021): Referenzarchitektur der Energiesynchronisationsplattform. Online verfügbar unter doi.org/10.24406/IGCV-N-642369.

Microsoft (2021): Microsoft Security Development Lifecycle (SDL) – version 5.2. Online verfügbar unter https://docs.microsoft.com/de-de/previous-versions/windows/desktop/cc307748(v=msdn.10), zuletzt aktualisiert am 11.10.2021, zuletzt geprüft am 11.10.2021.

Network Working Group (2022): RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Online verfügbar unter https://datatracker.ietf.org/doc/html/rfc5280, zuletzt aktualisiert am 01.06.2022, zuletzt geprüft am 01.06.2022.

NIST (CDC) FIPS 199: Standards for Security Categorization of Federal Information and Information Systems. NIST Computer Security Division (CSD). Online verfügbar unter https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf, zuletzt geprüft am 11.10.2021.

OWAPS SAMM 2.0: OWASP SAMM v2.0 - Core Model Document. Online verfügbar unter https://raw.githubusercontent.com/OWASP/samm/master/Supporting%20Resources/v2.0/OWASP-SAMM-v2.0.pdf, zuletzt geprüft am 26.03.2021.

OWASP SDLC (2021): OWASP in SDLC. Online verfügbar unter https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdlc/, zuletzt aktualisiert am 23.02.2021, zuletzt geprüft am 03.03.2021.

OWASP Security Qualitative Metrics (2021): OWASP Security Qualitative Metrics. Online verfügbar unter https://owasp.org/www-project-security-qualitative-metrics/SECURITY-QUALITATIVE-METRICS.html, zuletzt aktualisiert am 12.03.2021, zuletzt geprüft am 25.03.2021.

Ross, R.; McEvilley, M.; Oren., J. (2018): Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1. Gaithersburg, MD. Online verfügbar unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf, zuletzt geprüft am 11.10.2021.

SEI CERT (2022): Top 10 Secure Coding Practices - CERT Secure Coding - Confluence. Online verfügbar unter https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices, zuletzt aktualisiert am 01.06.2022, zuletzt geprüft am 01.06.2022.

Shevchenko, N.; Chick, T. A.; O'Riordan, P.; Scanlon, T. P.; Woody, C. (2018): Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United.

Shostack, Adam (2014): Threat Modeling: Designing for Security. 1st: Wiley Publishing.

Threat Modeling Manifesto (2020). Online verfügbar unter https://www.threatmodelingmanifesto.org/, zuletzt aktualisiert am 27.11.2020, zuletzt geprüft am 15.10.2021.

Turpin, Keith (2010): Secure Coding Practices - Quick Reference Guide, zuletzt geprüft am 01.06.2022.

UcedaVelez, T.; Morana, M. M. (2015): Risk Centric Threat Modeling: process for attack simulation and threat analysis: John Wiley & Sons.

VDI/VDE 2182 Blatt 1, 2020-01: VDI/VDE 2182 Blatt 1, Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell.

Wynn, J.; Whitmore, J.; Upton, G.; Spriggs, L.; McKinnon, D.; McInnes, R. et al. (2011): Threat assessment & remediation analysis (tara): Methodology description version 1.0. MITRE CORP. Bedford, MA.

Anhang

Architektur der Energiesynchronisationsplattform

Für die Festlegung des Sicherheitslevels ist die Kenntnis über die Gesamtarchitektur des ESP erforderlich, sowie eine Beschreibung der Geschäftsprozesse. Eine vollumfängliche Beschreibung erfolgt im Detailpapier zur Referenzarchitektur zum Diskussionspapier (Menci et al. 2021) . Die nachfolgenden Abbildungen sollen einen groben Überblick über das Gesamtsystem geben.

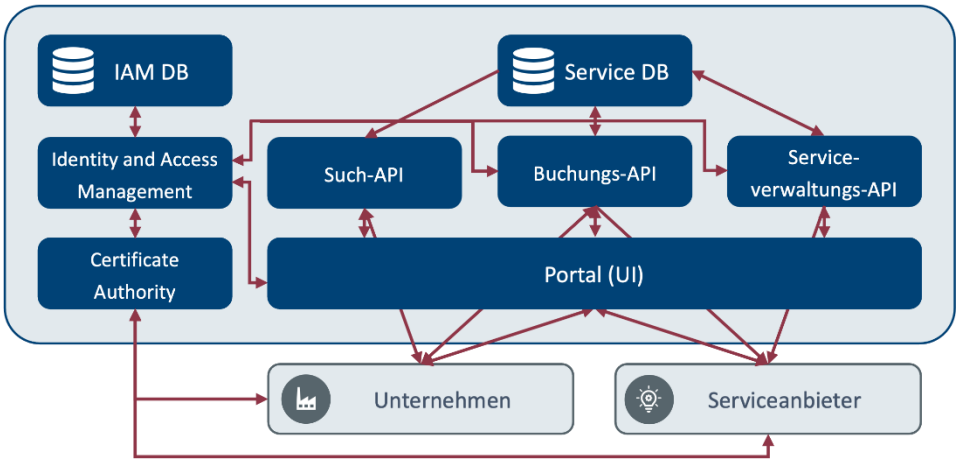


Abbildung 17: Aufbau der MP

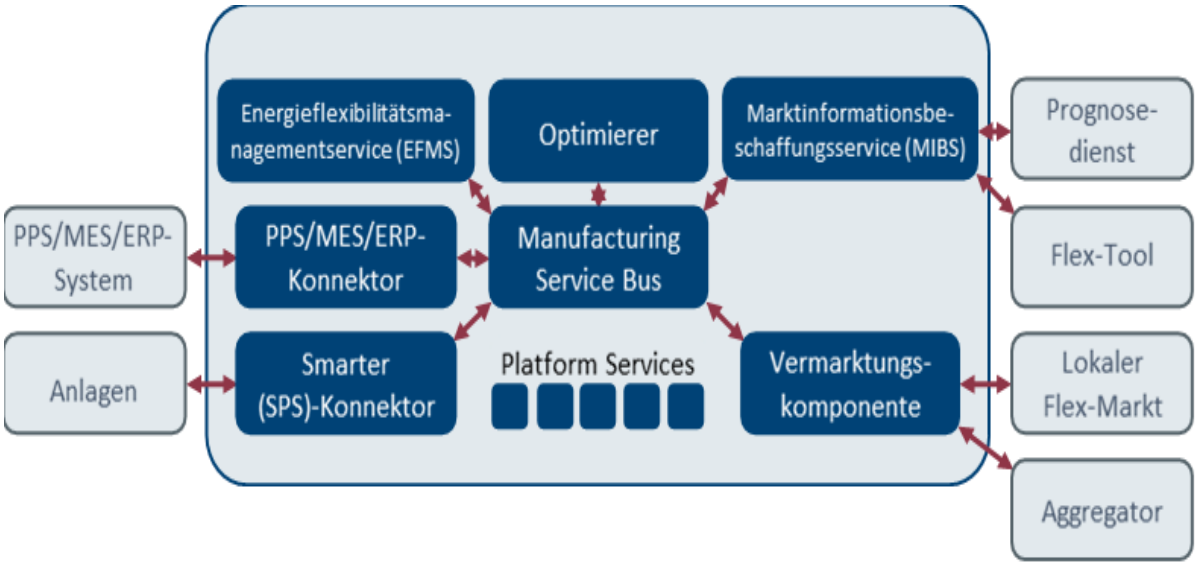


Abbildung 18: Aufbau der UP