Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anforderungskatalog zur MSB-Lieferkette

MSB-Lieferkette

Version 1.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Gemeinsames Vorwort von FNN und BSI

Das vorliegende Dokument ist in intensiver und enger Zusammenarbeit zwischen dem Forum Netztechnik/Netzbetrieb (FNN) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entstanden. Das Dokument enthält einen Anforderungskatalog zur Umsetzung einer sicheren Lieferkette für die Auslieferung von SMGW.

Es soll die flächendeckende Einführung intelligenter Messsysteme in Deutschland beschleunigen, indem die sichere Auslieferung von Smart-Meter-Gateways (SMGW) vereinfacht wird, ohne das hohe bestehende Sicherheitsniveau abzusenken. Zu diesem Zweck wurden in [PP-0073 v2.0] die formalen Voraussetzungen geschaffen, um die Verantwortung einer sicheren Lieferkette vom SMGW-Hersteller (GWH) auf den Messstellenbetreiber (MSB) zu übertragen. Hierbei wurden entsprechende Ermessensspielräume geschaffen, innerhalb derer es den MSB möglich ist, flexibel und auf Basis langjähriger Praxiserfahrung über die konkrete Ausgestaltung individueller, sicherer Lieferketten zu entscheiden.

Auf diese Weise wird eine Anwendung des Dokuments über alle grundzuständigen und wettbewerblichen MSB und deren jeweils individuell ausgeprägten Lieferketten ermöglicht, um den Gefährdungen für SMGW während der Auslieferung reduzierend entgegenzuwirken (s. Abschnitt 1.3).

1.2 Anwendungsbereich

Das Dokument betrachtet die Auslieferung von SMGW ab der Warenannahme der Erstauslieferung des GWH durch den MSB bis zu der in [PP-0073 v2.0] definierten Einsatzumgebung. Montage zur Inbetriebnahme und Demontage zur Wiederverwendung von SMGW durch einen Monteur im Auftrag des MSB sind ebenfalls Teil der betrachteten Auslieferung. Dahingegen werden SMGW für die Dauer ihres Betriebes in der Einsatzumgebung in diesem Dokument nicht betrachtet. Insbesondere sind der Ausbau und die Auslieferung zur Verschrottung, sowie die Hardware-Verschrottung nicht Teil der Sicherheitsbetrachtung und somit auch nicht Teil des Sicherheitskonzepts (s. Abschnitt 2.2).

Die Auslieferung, mit den oben genannten Einschränkungen, wird nachfolgend als „MSB-Lieferkette“ bezeichnet.

1.3 Zielsetzung

Das Ziel dieses Dokuments ist es, Massengeschäftstauglichkeit und Sicherheit der MSB-Lieferkette in angemessener Art und Weise miteinander zu vereinbaren, um ein Mindestmaß an Sicherheit während der Auslieferung von SMGW flächendeckend über alle MSB zu erreichen. Aus diesem Grund enthält das Dokument Anforderungen an MSB, deren Umsetzung das Erreichen dieses Zieles sicherstellt. Die Überführung der Anforderungen in konkrete Maßnahmen muss durch jeden MSB in einem individuellen Sicherheitskonzept erfolgen. Indem alle MSB diese Anforderungen erfüllen, ist ein Mindestmaß an Sicherheit für SMGW während der Auslieferung flächendeckend über alle MSB gewährleistet.

1.4 Zielgruppe

Dieses Dokument richtet sich an alle grundzuständigen und wettbewerblichen MSB.

Das vorliegende Dokument stellt keine Anforderungen an den Gateway-Administrator (GWA).

1.5 Fachlich zuständige Stelle

Fachlich zuständig für die Fortentwicklung dieses Dokuments ist das BSI.

Anschrift: Bundesamt für Sicherheit in der Informationstechnik

Referat D 21 – Digitalisierung der Energiewirtschaft

Postfach 20 03 63 222

53133 Bonn

E-Mail: smartmeter@bsi.bund.de

Anmerkungen zu diesem Dokument können an die oben genannte Anschrift oder E-Mail-Adresse gerichtet werden.

1.6 Terminologie

Die Inhalte dieses Dokuments sind nicht normativ. Die Anforderungen in Kapitel 5 sind geeignet und dringend empfohlen, um die Annahme A.Delivery in [PP-0073 v2.0] während der Auslieferung von SMGW zu erfüllen. Entscheidet sich ein MSB für die Anwendung dieses Dokuments, wird die Annahme A.Delivery nur dann als erfüllt betrachtet, wenn alle in Kapitel 5 genannten Anforderungen entsprechend ihrer Terminologie erfüllt sind. Insbesondere kann Konformität zwischen dem Sicherheitskonzept des MSB und diesem Dokument nur hergestellt werden, indem diese Bedingung erfüllt wird.

Dem MSB wird dabei ein großer Ermessensspielraum in der Umsetzung von Sicherheitsmaßnahmen ermöglicht, um das Dokument über alle MSB entsprechend der individuellen Gegebenheiten anwenden zu können. Dieser Ermessensspielraum wird maßgeblich durch die Formulierung der Anforderungen in Kapitel 5, aber auch durch nachfolgend erläuterte Modalverben erreicht. Die Formulierungen in Kapitel 5 haben insbesondere zur Folge, dass Prüfbarkeit kein Kriterium ist, das für Anforderungen in diesem Dokument gilt. D.h., es ist dem MSB überantwortet, im Zuge der Ausarbeitung von konkreten Maßnahmen, Prüfbarkeit herzustellen und Wirksamkeit sicherzustellen.

Kapitel 5 enthält Anforderungen mit den in Großbuchstaben geschriebenen Modalverben MUSS und SOLL. Die Modalverben werden entsprechend den sprachlichen Erfordernissen konjugiert und sind wie folgt beschrieben zu verstehen.

MUSS:

Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderungen, für die keine Risikoübernahme möglich ist).

SOLL:

Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

1.7 Aufbau des Dokuments

In diesem Dokument werden Anforderungen im Sinne eines Anforderungskatalogs formuliert. Hierfür werden in Kapitel 2 Rahmenbedingungen vorgestellt, auf die sich FNN und BSI verständigt haben. Sie bilden die Grundlage der Sicherheitsbetrachtung in diesem Dokument. Anschließend erläutert Kapitel 3 die Konzeptidee und eine mögliche Vorgehensweise zur Anwendung dieses Dokuments. Kapitel 4 bietet eine Übersicht der Prozesse, Schnittstellen und Prozessabweichungen innerhalb des Messstellenbetriebes, die als relevant erachtet und in Kapitel 5 durch entsprechende Bausteine mit Anforderungen adressiert sind. Zusätzlich sind in diesem Kapitel allgemeine Anforderungen enthalten, welche über alle Prozesse erfüllt werden müssen.

1.8 Übersicht über mitgeltende Anlagen

Keine.

1.9 Zusammenhang mit anderen Dokumenten

Das Erfüllen der Anforderungen in diesem Dokument erfüllt die Annahme A.Delivery in [PP-0073 v2.0].

1.10 Versionshistorie

Version	Datum	Beschreibung
1.0	21.10.2024	Erstveröffentlichung

2 Grundsätzliches

2.1 Verantwortung von GWH und MSB

Die Verantwortung des GWH für die sichere Auslieferung von SMGW endet unmittelbar nach Abschluss der Warenannahme der Erstauslieferung des GWH durch den MSB. Damit liegt die MSB-Lieferkette außerhalb der Zuständigkeit des GWH und wird auch im Rahmen der Common Criteria (CC) Zertifizierung von SMGW nicht betrachtet.

Die Verantwortung des MSB für die sichere Auslieferung von SMGW beginnt unmittelbar nach Abschluss der Warenannahme der Erstauslieferung des GWH durch den MSB. Damit liegt die MSB-Lieferkette vollständig innerhalb der Zuständigkeit des MSB. Wird das Eigentum an SMGW an einen anderen MSB übertragen, geht auch die Verantwortung im Sinne der MSB-Lieferkette auf den neuen MSB über.

2.2 Lebenszyklus-Phasen von SMGW

Zur Abstraktion möglicher konkreter Orte, an denen sich das SMGW im Rahmen der MSB-Lieferkette befinden kann, wird nachfolgend der Ort „Lieferweg“ verwendet. Der Lieferweg fasst alle Prozesse, sowie Schnittstellen zwischen Prozessen einer MSB-Lieferkette zusammen (s. Kapitel 4).

Der Lieferweg im Kontext der MSB-Lieferkette beginnt nach Abschluss der Lebenszyklus-Phase „Auslieferung zum MSB“.

Der Lieferweg wird in der nach [PP-0073 v2.0] definierten Einsatzumgebung jeweils nach Abschluss der Lebenszyklus-Phasen „Erstinstallation“ und „Wiederinstallation“ für die Dauer der Lebenszyklus-Phase „Betrieb“ unterbrochen (vgl. [Anlage VIII]). Daraus folgt, dass SMGW in der Lebenszyklus-Phase „Betrieb“ nicht Teil der Betrachtung der MSB-Lieferkette sind und in diesem Dokument keine Anforderungen an MSB in Bezug auf SMGW in dieser Phase gestellt werden.

Nach Demontage zur Wiederverwendung (vgl. Lebenszyklus-Phase „Ausbau zur Wiederverwendung“ in [Anlage VIII]) kann ein SMGW, unter Einhaltung der Vorgaben aus diesem Dokument, die Prozesse Lagerung, Transport und Montage erneut durchlaufen (s. Abschnitt 4.4.2), analog zu SMGW in der Lebenszyklus-Phase „Erstauslieferung“.

Der Lieferweg endet vor Beginn der Lebenszyklus-Phase „Ausbau zur Verschrottung“ (vgl. [Anlage VIII]).

Die Lebenszyklus-Phasen „Ausbau zur Verschrottung“, „Auslieferung zur Verschrottung“ und „Hardware Verschrottung“ (vgl. [Anlage VIII]) sind nicht Teil der Sicherheitsbetrachtung und somit auch nicht Teil des Sicherheitskonzepts. D.h. die MSB-Lieferkette stellt keine Anforderungen an MSB für SMGW, die zum Zweck der Verschrottung demontiert werden.

2.3 Schutzziele von SMGW auf dem Lieferweg

Die MSB-Lieferkette betrachtet das Gerät SMGW als einziges Asset. Schutzziele im Kontext der MSB-Lieferkette gelten ausschließlich dem Schutz dieses Assets. Folgende Schutzziele von SMGW werden betrachtet: Integrität, Authentizität.

Der Schutz der Integrität umfasst den Schutz von Hardware und Software gegen Manipulation. Der Schutz der Authentizität umfasst den Schutz gegen Austauschen oder Einschleusen von SMGW auf dem Lieferweg.

Die Betrachtung dieser Schutzziele ist erforderlich, um die Annahme A.Delivery in [PP-0073 v2.0] zu erfüllen. Die Schutzziele sind durch verschiedene Gefährdungen auf dem Lieferweg Risiken ausgesetzt, denen der MSB durch geeignete und angemessene Sicherheitsmaßnahmen begegnen muss.

2.4 Selbstschutz von SMGW auf dem Lieferweg

2.4.1 Sicherheitsmodul

Das Sicherheitsmodul (SM) wird während der Lebenszyklus-Phase „Integration“ (vgl. [Anlage VIII]) in ein SMGW integriert und befindet sich anschließend im SMGW. Da das SM integriert wird, bevor ein SMGW die Lebenszyklus-Phase „Erstauslieferung“ (vgl. [Anlage VIII]) durchläuft, wird angenommen, dass Informationen, die ausschließlich im Sicherheitsmodul gespeichert sind, über den gesamten Lieferweg angemessen gegen Angriffe geschützt sind.

Voraussetzung für die Wirksamkeit von diesem Schutzmechanismus ist, dass sich das SMGW in einer nichtöffentlichen Umgebung (bspw. in Räumlichkeiten oder Fahrzeugen des MSB oder seiner Dienstleister oder in einer sicheren Einsatzumgebung) befindet, sodass der Zugang nur einem definierten Personenkreis möglich ist.

2.4.2 Manipulationserkennung

Jedes SMGW-Gehäuse ist ab Werk mit einer Manipulationserkennung ausgestattet. Diese Manipulationserkennung wird beim Öffnen des Gehäuses irreparabel und eindeutig beschädigt, sodass angenommen wird, dass ein Öffnen des Gehäuses auch nach dem Wiederverschließen erkennbar ist. Typischerweise wird hierfür ein Gehäusesiegel verwendet. Das Gehäusesiegel wird im Rahmen einer CC-Zertifizierung geprüft. Da das Siegel nach der Lebenszyklus-Phase „Vorpersonalisierung II“ dasselbe Siegel ist, wie in der Lebenszyklus-Phase „Erstinstallation“ wird das Siegel als sicheres Erkennungsmerkmal für die Manipulation von SMGW betrachtet.

Voraussetzung für die Wirksamkeit von diesem Schutzmechanismus ist, dass sich das SMGW in einer nichtöffentlichen Umgebung (bspw. in Räumlichkeiten oder Fahrzeugen des MSB oder seiner Dienstleister oder in einer sicheren Einsatzumgebung) befindet, sodass der Zugang nur einem definierten Personenkreis möglich ist.

Voraussetzung für die Wirksamkeit von diesem Schutzmechanismus ist außerdem die Durchführung von Gehäusesichtprüfung und Prüfung der Manipulationserkennung, also die visuelle Prüfung von Gehäuse und bspw. Siegel durch fachkundiges, geschultes Personal.

2.4.3 Selbsttest

In [PP-0073 v2.0] wird eine Selbsttest-Funktion für SMGW gefordert. Der Selbsttest umfasst die Integrität der Firmware, die Korrektheit kryptographischer Operationen, sowie die Erreichbarkeit des Sicherheitsmoduls und dessen korrekten Betrieb. Da für SMGW ab Werk ein gültiges CC-Zertifikat angenommen wird, wird die kryptographische Funktion des Sicherheitsmoduls über den gesamten Lieferweg als angemessen geschützt betrachtet.

Voraussetzung für die Wirksamkeit von diesem Schutzmechanismus ist, dass sich das SMGW in einer nichtöffentlichen Umgebung (bspw. in Räumlichkeiten oder Fahrzeugen des MSB oder seiner Dienstleister oder in einer sicheren Einsatzumgebung) befindet, sodass der Zugang nur einem definierten Personenkreis möglich ist.

2.5 Schützenswerte Informationen

Zusätzlich zu den Schutzzielen von SMGW (s. Abschnitt 2.3) gibt es Informationen während der Auslieferung von SMGW, die kritisch und schützenswert sind[1], weil sie Angriffsszenarien auf Schutzziele von SMGW begünstigen oder ermöglichen. Schützenswerte Informationen können für die Durchführung der Prozesse einer individuellen Lieferkette wesentlich sein. Ihr Schutz ist erforderlich, um die Wirksamkeit von

[1] Insbesondere Informationen zur Identifikation, Verifikation und Reaktion (s. Abschnitt 4.6).

Maßnahmen zum Erreichen der Schutzziele von SMGW auf dem Lieferweg gewährleisten zu können. Aufgrund der Vielfältigkeit möglicher MSB-Lieferketten muss der MSB schützenswerte Informationen identifizieren und diese anschließend in angemessener Art und Weise in sein Sicherheitskonzept aufnehmen.

Es müssen zwei Varianten schützenswerter Informationen unterschieden werden:

1. Informationen, die außerhalb von SMGW vorliegen und im Kontext der MSB-Lieferkette übergeben oder verarbeitet werden,
2. Informationen, die ausschließlich in einzelnen SMGW gespeichert werden[2].

Für den angemessenen Schutz schützenswerter Informationen muss der MSB die entsprechenden allgemeinen Anforderungen (s. Abschnitt 5.1.5) und die prozessspezifischen Anforderungen (s. Abschnitt 5.2, 5.3 und Abschnitt 5.4) in diesem Dokument erfüllen, indem er auf Basis dieser Anforderungen angemessene Maßnahmen ableitet und umsetzt. Dabei ist zu berücksichtigen, dass kumulierte Informationen häufig sicherheitsrelevanter sind als einzelne Informationen. Durch den Schutz einzelner Informationen wird es Angreifern erschwert, in den Besitz kumulierter Informationen zu gelangen.

[2] Informationen, die ausschließlich im Sicherheitsmodul gespeichert sind, sind durch das Sicherheitsmodul angemessen geschützt.

3 Anwendungshinweis

Der MSB muss die Annahme A.Delivery in [PP-0073 v2.0] erfüllen, damit SMGW ihre Einsatzumgebung sicher, integer und authentisch erreichen und für diese Geräte im Betrieb ein zertifizierter Zustand im Sinne der CC angenommen werden darf. Das vorliegende Dokument stellt einen Anforderungskatalog für MSB dar und enthält Anforderungen an MSB, die mindestens umgesetzt werden müssen, wenn der MSB das Konzept der MSB-Lieferkette nutzen möchte, um die Annahme A.Delivery zu erfüllen. Kapitel 3 soll dem Anwender dieses Dokuments (MSB) eine Hilfestellung bieten, indem es die Konzeptidee und eine Vorgehensweise zur Erstellung eines Sicherheitskonzepts für eine MSB-Lieferkette erläutert.

Die Konzeptidee der MSB-Lieferkette basiert auf:

1. Sicherheitskonzept
2. Allgemeine Anforderungen
3. Prozessspezifische Anforderungen (Baustein-Prinzip)
4. Sicherheitsmaßnahme, Sicherheitsereignis, Sicherheitsvorfall und Meldestelle
5. Schützenswerte Informationen

Der MSB arbeitet ein Sicherheitskonzept für eine MSB-Lieferkette aus. Das Sicherheitskonzept kann auch mehrere MSB-Lieferketten umfassen. Ausgangspunkt der Ausarbeitung sind zunächst die allgemeinen Anforderungen (s. Abschnitt 5.1). Diese sind über den gesamten Lieferweg zu erfüllen und enthalten unter anderem Anforderungen an das Sicherheitskonzept. Prozessspezifische Anforderungen gelten hingegen nur für einen konkreten relevanten Prozess (s. Abschnitt 4.2, 4.3, 4.4) und sind über diesen immer einem Baustein zugeordnet. Der Begriff Baustein meint an dieser Stelle eine Gruppierung von Anforderungen (s. Abschnitt 5.2, 5.3, 5.4). Der Begriff ist dem [IT-GS] entnommen und soll es dem MSB mittels Baustein-Prinzip ermöglichen, mit vergleichsweise geringem Aufwand und geringer Redundanz individuelle Lieferketten in seinem Sicherheitskonzept abzubilden. Zusätzlich kann ein solches Konzept bei Bedarf modular aktualisiert oder auch erweitert werden.

Den wesentlichen Inhalt des Sicherheitskonzepts bilden die Sicherheitsmaßnahmen, die der MSB aus den Anforderungen ableitet. Der MSB muss Sicherheitsmaßnahmen ausarbeiten und im Sicherheitskonzept dokumentieren, bspw. um durch diese Maßnahmen direkt oder indirekt Sicherheitsereignissen und Sicherheitsvorfällen zu vermeiden, zu erkennen, zu melden oder zu behandeln (s. Abschnitt 4.6). Die Wirksamkeit und Messbarkeit von Sicherheitsmaßnahmen ist dabei durch den MSB herzustellen und sicherzustellen. Zusätzlich kann der MSB die Anforderungen aus diesem Dokument in die Dokumentation seines Sicherheitskonzeptes mit übernehmen (bspw. für ein Mapping von Anforderungen und Maßnahmen).

Für das Erkennen von Sicherheitsereignissen liegt der Fokus auf Prozessschnittstellen bzw. -übergängen. SMGW, die von einem Prozess in einen anderen übergeben werden, sind entsprechend der prozessspezifischen Anforderungen zu prüfen. Dabei wird aus Gründen der Massengeschäftstauglichkeit eine stichprobenartige Prüfung ermöglicht, um den Transport großer Mengen von SMGW nicht zu verzögern. Indem ein SMGW auf seinem Lieferweg Stichproben durchläuft (bspw. je eine Prüfung bei Wareneingang und Warenausgang nach Warenannahme der Erstauslieferung, s. Abschnitt 4.1) und abschließend während der Montage einer Einzelgeräteprüfung unterzogen wird, kann trotzdem ein angemessenes Maß an Sicherheit gewährleistet werden. Es wird erwartet, dass auf diese Weise korrumpierte SMGW auf dem Lieferweg erkannt und herausgefiltert werden. Die MSB-Lieferkette stützt sich somit nicht allein auf die Sicherheitsleistung durch den Monteur des MSB. Stattdessen gilt, je weniger korrumpierte SMGW die Einsatzumgebung erreichen, desto geringer ist die Wahrscheinlichkeit, dass ein Monteur ein solches Gerät fälschlicherweise montiert.

Damit Sicherheitsmaßnahmen eine breite Anwendung finden, wird auf die Dokumentation von Sicherheitsereignissen vollständig verzichtet. Eine Dokumentation wird ausschließlich für Sicherheitsvorfälle gefordert (s. Abschnitt 4.6) und ist durch die Meldestelle zu erbringen. Auf diese Weise soll das Melden von Sicherheitsereignissen niederschwellig und unbürokratisch erfolgen. Die Meldestelle hält

Ressourcen, Informationen und Kompetenzen vor, um zu prüfen, ob ein Sicherheitsvorfall vorliegt. Es wird angenommen, dass Mitarbeiter der Meldestelle auch in der Lage sind, Schwachstellen und Sicherheitsvorfälle zu erkennen, die sich aus einer Verkettung oder Häufung von Sicherheitsereignissen ergeben. Die Meldestelle koordiniert die Reaktion auf einen Sicherheitsvorfall und beantragt die Sperrung von SM-PKI-Zertifikaten beim GWA. Abbildung 1 veranschaulicht die beschriebene Konzeptidee.

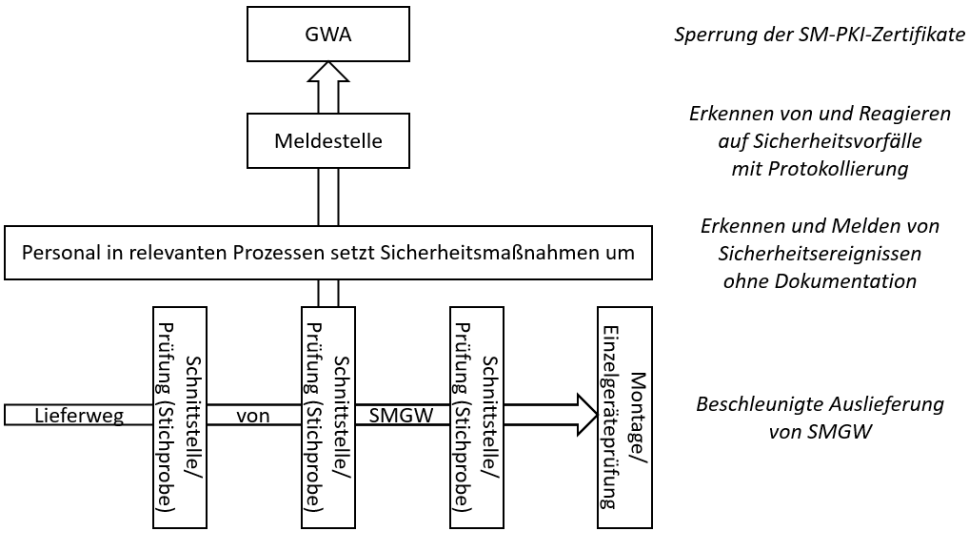

Abbildung 1: Konzeptschaubild zur MSB-Lieferkette

Ergänzt wird dieses Konzept durch das Instrument sogenannter schützenswerter Informationen (s. Abschnitt 2.5). Der MSB kann bestimmte Informationen als schützenswert einstufen. Das können z.B. Informationen sein, die zur Identifikation von SMGW verwendet werden. Prüft ein Mitarbeiter die Geräte-ID eines SMGW gegen einen Soll-Wert, sollte er sich darauf verlassen können, dass der Soll-Wert korrekt ist, also authentisch und integer. Ein anderes Beispiel sind Informationen über Sicherheitsvorfälle. Neben einem möglichen Imageschaden können solche Informationen für Angreifer von Interesse sein, um Stärken und Schwächen der betroffenen Lieferkette sondieren zu können. Der MSB muss schützenswerte Informationen für seine MSB-Lieferkette festlegen. Dabei steht es dem MSB frei, festzulegen, dass es in seiner MSB-Lieferkette keine schützenswerten Informationen gibt. Lediglich wenn der Transport einer großen Stückzahl von SMGW vorgesehen ist, dann müssen Geräte-ID und die Stückzahl der gelieferten Geräte als schützenswerte Informationen behandelt werden (s. Abschnitt 5.1.5 und Abschnitt 5.3).

Vor diesem Hintergrund wird eine mögliche Vorgehensweise zur Erstellung eines Sicherheitskonzepts für eine MSB-Lieferkette vorgestellt und erläutert:

1. Der MSB erstellt ein Dokument (Sicherheitskonzept) mit Erstellungsdatum (oder Versionsnummer) und Änderungshistorie.
2. Der MSB erarbeitet zunächst entlang allgemeiner Anforderungen (s. Abschnitt 5.1) Inhalte, die über alle MSB-Lieferketten gelten, für die dieses Sicherheitskonzept Gültigkeit hat. Hierzu zählen mindestens:
    a. Identifizierung relevanter Prozesse
    b. Definition der Meldestelle und Meldewege
    c. Festlegung zu betrachtender Sicherheitsereignisse (mind. Auflistung in Abschnitt 4.6.1)
    d. Festlegung zu betrachtender Sicherheitsvorfälle (mind. Verlust, Manipulation und Einschleusung von SMGW gemäß Abschnitt 4.6.2)
    e. Festlegung zu betrachtender schützenswerter Informationen
    f. Festlegung von Verantwortlichkeiten (bspw. für die Prozesse, für die Meldestelle, für die Dokumentation)
    g. Ausarbeitung von Richtlinien, Handlungsanweisungen und Regelungen (ggf. unter Einbeziehen bzw. Referenzieren bereits existierender Dokumente)
    h. Ausarbeitung allgemeiner Maßnahmen (bspw. Schulung von Mitarbeitenden, etc.)

3. Der MSB legt für jeden identifizierten Prozess einen Baustein an und erarbeitet je Baustein Sicherheitsmaßnahmen. Hier ist es sinnvoll, je Prozess (Lagerung, Transport, Montage) zunächst nur einen Baustein vollständig auszuarbeiten und anschließend in allen anderen Bausteinen dieses Prozesses auf diesen ersten Baustein zu verweisen, sodass lediglich die Unterschiede in den Bausteinen herauszuarbeiten sind. Auf diese Weise können Redundanzen vermieden werden. Bei Bedarf kann ein Baustein außerdem die Begründung für das Nicht-Erfüllen einer Soll-Anforderung, geeignete Meldewege oder verantwortliche Personen enthalten.
4. Der MSB setzt das Sicherheitskonzept um. Hierzu zählt die Schulung des Personals, der Aufbau einer Meldestelle, die Zuweisung von Verantwortlichkeiten und das Erteilen von Handlungsanweisungen.
5. Der MSB stellt sicher, dass Dokumentation und Sicherheitsmaßnahmen des Sicherheitskonzeptes aktuell sind und stellt sicher, dass die Maßnahmen wirksam umgesetzt sind.

Die beschriebene Vorgehensweise ist exemplarisch. Sie enthält Beispiele und ist insbesondere nicht abschließend. Sie veranschaulicht, wie das vorliegende Dokument grundsätzlich angewendet werden kann, ohne andere Vorgehensweisen auszuschließen, solange die Anforderungen in diesem Dokument erfüllt werden.

4 Prozesse

4.1 Übersicht

Die nachfolgenden Abschnitte geben eine Übersicht über die im Kontext der MSB-Lieferkette relevanten Prozesse sowie über Schnittstellen zwischen diesen Prozessen und den Umgang mit Prozessabweichungen.

Abbildung 2 zeigt den Anwendungsbereich (s. Abschnitt 1.2) für das vorliegende Dokument, sowie die Schnittstellen zu vor- und nachgelagerten Prozessen außerhalb der MSB-Lieferkette. Die Abbildung ordnet die drei relevanten Prozesse mit den gängigsten möglichen Varianten in den Gesamtprozess der MSB-Lieferkette ein.

Insbesondere kann ein SMGW eine Messstelle nach Demontage zur Wiederverwendung (s. Abschnitt 4.4.2) wieder verlassen und mittels der Prozesse Lagerung, Transport und Montage erneut verwendet werden. Ein SMGW muss nach Demontage zur Wiederverwendung weder erneut eingelagert noch erneut transportiert werden. Der Wechsel zwischen Einsatzumgebungen kann durch den Monteur im Rahmen der Montage erfolgen (s. Abschnitt 4.4.1). Der Prozess der Montage umfasst sowohl die Montage zur Inbetriebnahme als auch die Demontage zur Wiederverwendung. D.h., es gelten für beide Prozesse dieselben prozessspezifischen Anforderungen (s. Abschnitt 5.4).

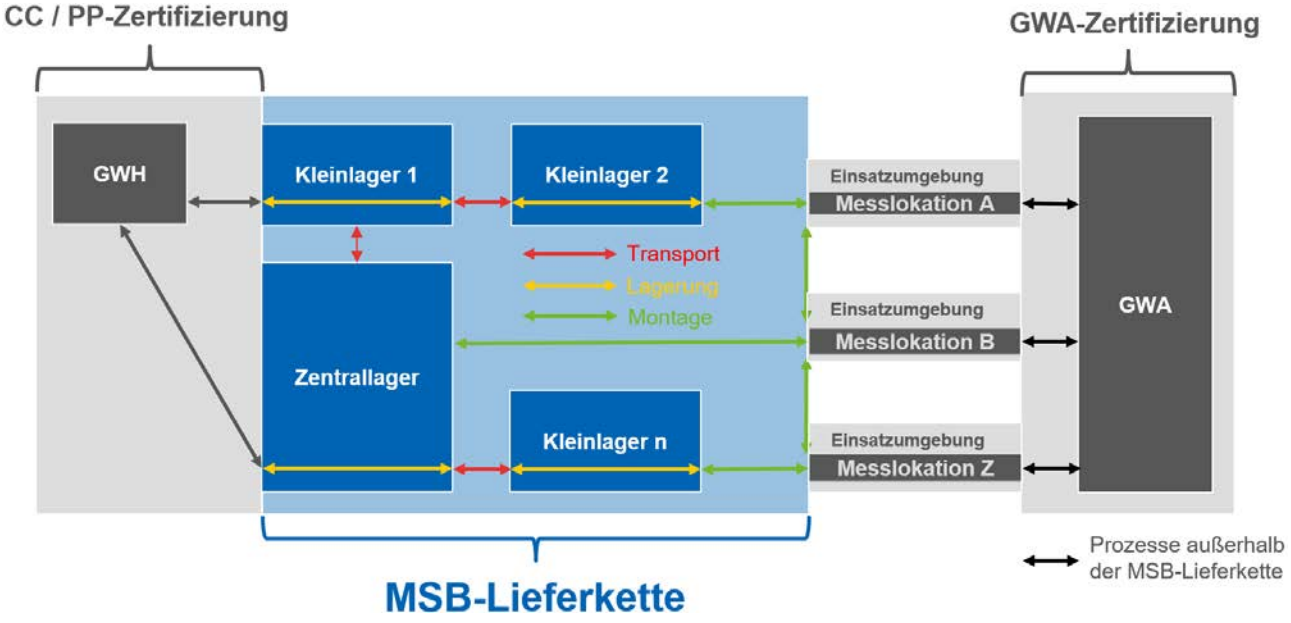

Abbildung 2: Prozessschaubild zum Anwendungsbereich der MSB-Lieferkette

Nachfolgende Betrachtungen erfolgen ausschließlich im Kontext der MSB-Lieferkette. Prozesse in der Zuständigkeit des MSB, die in keinem direkten Zusammenhang mit der Auslieferung von SMGW stehen, sind von nachfolgenden Betrachtungen ausgenommen.

4.2 Lagerung

Dieser Prozess bezeichnet den Abschnitt der Lieferkette, in dem ein oder mehrere SMGW gelagert werden. SMGW befinden sich während diesem Prozess, durchgehend an einem festen Ort, der als Lager bezeichnet wird. Der MSB setzt diesen Prozess für Lager innerhalb seiner MSB-Lieferkette um. Beispiele für Lager im Sinne dieses Bausteins sind: Zentrallager, Nebenlager, Kleinlager. Der MSB ist verantwortlich für den sicheren Betrieb seiner Lager (s. Abschnitt 2.1).

Dieser Prozess ist durch die Anforderungen zum Baustein Lagerung (s. Abschnitt 5.2) im gleichnamigen Abschnitt abgedeckt.

4.3 Transport

Dieser Prozess bezeichnet den Abschnitt der Lieferkette, bei dem ein oder mehrere SMGW transportiert werden. Der Transport kann zwischen Lagern, zwischen Lager und Montagebetrieb oder bis zur Einsatzumgebung erfolgen. Dabei kann der Transport z.B. per Kurier-, Express- oder Paketversand erfolgen.

Die Verantwortung für den Transport bspw. per Kurier-, Express- oder Paketversand liegt beim MSB (s. Abschnitt 2.1). Das gilt auch dann, wenn der Endkunde eine Lieferung von SMGW entgegennimmt.

Dieser Prozess ist durch die Anforderungen zum Baustein Transport (s. Abschnitt 5.3) im gleichnamigen Abschnitt abgedeckt.

4.4 Montage

4.4.1 Montage zur Inbetriebnahme

Dieser Prozess bezeichnet den Abschnitt der Lieferkette, bei dem sich ein SMGW auf dem Weg zur oder bereits in der Einsatzumgebung befindet. In dieser als Montage bezeichneten Phase wird das SMGW durch einen Monteur zunächst in die Einsatzumgebung befördert und dann montiert. Daran schließt sich die Inbetriebnahme durch den GWA an. Die Inbetriebnahme durch den GWA ist kein Bestandteil der MSB-Lieferkette.

4.4.2 Demontage zur Wiederverwendung

Dieser Prozess bezeichnet den Abschnitt der Lieferkette, bei dem ein SMGW nach der Demontage zur Wiederverwendung vorgesehen ist. Voraussetzung für die Wiederauslieferung und die anschließende Wiederinstallation ist gemäß [PP-0073 v2.0], dass die Nutzerdatenbereinigung gemäß [TR 03109-1 v2.0] vor der Demontage zur Wiederverwendung erfolgreich durchgeführt wird. Falls die Nutzerdatenbereinigung an der Messstelle fehlschlägt, muss sie unverzüglich nach der Demontage nachgeholt werden. Nach durchgeführter Nutzerdatenbereinigung ist ein SMGW analog einem SMGW in der Erstauslieferung zu behandeln und die Anforderungen in diesem Dokument gelten entsprechend.

Dieser Prozess (sowohl Montage zur Inbetriebnahme als auch Demontage zur Wiederverwendung) ist durch die Anforderungen zum Baustein Montage (s. Abschnitt 5.4) im gleichnamigen Abschnitt abgedeckt.

4.5 Schnittstellenbetrachtung

Die Übergänge zwischen den oben beschriebenen Prozessen sind für die Betrachtung der Sicherheit der MSB-Lieferkette von besonderer Bedeutung, weil über diese Schnittstellen Waren zwischen System- und Zuständigkeitsbereichen wechseln und jedes SMGW auf seinem Lieferweg mindestens einmal eine solche Schnittstelle passiert.

Mehrere Anforderungen in diesem Dokument adressieren gezielt die Warenannahme und Warenausgabe und haben die wesentliche Funktion, das Erkennen von Verlust, Manipulation oder Einschleusung von SMGW zu gewährleisten. Die Wirkungsweise ist vergleichbar mit der Funktion eines Filters. Je häufiger ein SMGW eine Filterfunktion (Schnittstelle) passiert, desto höher ist die Wahrscheinlichkeit, dass korrumpierte Geräte erkannt und aus dem Verkehr gezogen werden. Um Redundanzen in der Schnittstellenbetrachtung zu vermeiden, findet diese verstärkt für die Prozesse Lagerung und Montage und weniger für den Prozess Transport statt. Das ist auch darauf zurückzuführen, dass SMGW den Prozess Transport nicht durchlaufen müssen (s. Abbildung 1). Während für den Prozess Lagerung aus Gründen der Massengeschäftstauglichkeit stichprobenartige Kontrollen genügen, wird für den Prozess Montage u.a. eine Einzelgeräteprüfung gefordert.

Auf diese Weise wird die Verhältnismäßigkeit von Nutzen und Aufwand über alle Prozesse berücksichtigt und in Kombination mit weiteren Anforderungen dieses Dokuments ein angemessener Schutz von SMGW auf dem Lieferweg erreicht.

Eine besondere Schnittstelle in Bezug auf den Kurier-, Express- und Paketversand stellt der Endkunde am Installationsort dar. Sendet der MSB SMGW per entsprechendem Dienstleister zum Installationsort, agiert der Endkunde im Prozess Transport als Empfänger und übergibt anschließend empfangene SMGW immer an einen Monteur im Prozess Montage. Der Endkunde kann somit als eine Schnittstelle zwischen den genannten Prozessen betrachtet werden. Im Kontext der MSB-Lieferkette und in Anlehnung an [PP-0073 v2.0] gilt der Endkunde als nicht vertrauenswürdig. Aus diesem Grund muss der Monteur SMGW, die er vom Endkunden entgegennimmt, prüfen (s. Abschnitt 5.4).

4.6 Umgang mit Prozessabweichungen

4.6.1 Sicherheitsereignisse

Für jeden der oben beschriebenen Prozesse können Abweichungen zum Regelprozess auftreten. Solche Prozessabweichungen können sicherheitsrelevante Ereignisse, nachfolgend Sicherheitsereignisse genannt, darstellen. Der Umgang mit Prozessabweichungen ist daher ein wesentlicher Bestandteil dieses Dokuments.

Grundsätzlich lassen sich Prozessabweichungen in zwei Stufen, nachfolgend Sicherheitsereignis und Sicherheitsvorfall genannt, unterscheiden. Zunächst ist jede Prozessabweichung, die im Kontext der MSB-Lieferkette relevant ist, als Sicherheitsereignis einzustufen. Falls ein Ereignis besondere Bedeutung erlangt, indem es die Schutzziele von SMGW (s. Abschnitt 2.3) verletzt, wird es zum Sicherheitsvorfall hochgestuft.

Das Erkennen und Melden von Sicherheitsereignissen ist durch Mitarbeitende des MSB mit Aufgaben im Kontext der MSB-Lieferkette zu leisten (s. Abschnitt 5.1.2 und Abschnitt 5.1.3), während die Bewertung und Einstufung von Sicherheitsereignissen und Sicherheitsvorfällen nur durch das Personal einer Meldestelle des MSB vorzunehmen ist. Auf diese Weise soll vermieden werden, dass Sicherheitsmaßnahmen Regelprozesse im Messstellenbetrieb verzögern und gleichzeitig kann so gewährleistet werden, dass die Bewertung, Einstufung, Protokollierung und Reaktion auf Sicherheitsvorfälle durch Personal durchgeführt und koordiniert wird, dem alle hierfür notwendigen Informationen gebündelt zur Verfügung stehen.

Beide Arten von Prozessabweichungen (Sicherheitsereignis und Sicherheitsvorfall) werden in Kapitel 5 durch Anforderungen adressiert, die durch den MSB in Sicherheitsmaßnahmen überführt werden müssen. Besondere Bedeutung sollte Maßnahmen beigemessen werden, die zum Ziel haben, Sicherheitsereignisse zu erkennen und zu melden, sowie Sicherheitsvorfälle zu bewerten, zu behandeln und die Ursachen für das Auftreten nachhaltig zu beheben.

Der MSB kann in seinem Sicherheitskonzept jedes beliebige Sicherheitsereignis definieren und adressieren. Der Begriff Sicherheitsereignis meint in diesem Dokument jedoch mindestens die nachfolgende Auflistung:

- Ein SMGW ist keiner Bestellung eindeutig zuzuordnen (Herkunft der Lieferung ist unbekannt)
- Ein SMGW ist einer Lieferung eindeutig zuzuordnen, die ohne erkennbaren Grund mit außergewöhnlicher Verspätung (bspw. über Stunden) ankommt
- Ein SMGW ist einer Lieferung eindeutig zuzuordnen, die ohne erkennbaren Grund nicht ankommt
- Ein SMGW ist über einen längeren Zeitraum (bspw. über Stunden) nicht auffindbar (bspw. während einer Inventur)
- Ein SMGW ist nicht eindeutig identifizierbar oder die Identifikation ist nicht eindeutig verifizierbar:
    - Geräte-ID ist nicht lesbar
    - Geräte-ID ist nicht eindeutig
    - Geräte-ID entspricht nicht dem Soll-Wert (Eintrag im (elektronischen) Lieferschein)
- Ein SMGW ist nicht authentisch:
    - Ungewöhnliches Gehäuse
    - Ungewöhnliches Gehäusesiegel
    - Ungewöhnliches Gehäusebeschriftung (bspw. falsche Darstellung der richtigen Geräte-ID)
- Ein SMGW ist beschädigt:
    - Beschädigte Umverpackung (sofern vorhanden)
    - Beschädigte Anschlüsse

    - Beschädigtes Gehäuse
    - Beschädigtes Gehäusesiegel
- Ein SMGW ist irregulär über einen längeren Zeitraum (bspw. über Stunden) nicht überwacht und unbeschränkt physisch zugänglich gewesen (bspw. unverschlossene Tür oder Fenster in einem verlassenen Montagefahrzeug oder in einem Lager außerhalb der Regelarbeitszeiten).

Hinweis:
Das sichere Verwahren von SMGW durch den Endkunden ist Teil regulärer Prozesse (s. Abschnitt 4.5).

Wenn ein MSB schützenswerte Informationen (s. Abschnitt 2.5) in seinem Sicherheitskonzept festlegt, dann kann er folgende Sicherheitsereignisse zusätzlich in das Sicherheitskonzept aufnehmen:

- Schützenswerte Informationen über viele SMGW sind möglicherweise offengelegt worden (bspw. Verlust von Informationen über Sicherheitsvorfälle oder Verluste von digitalen Datenträgern mit Daten über viele SMGW)
- Schützenswerte Informationen über viele SMGW sind möglicherweise ohne erkennbaren Grund verändert worden (bspw. hinzugefügt, manipuliert, gelöscht)
- Schützenswerte Informationen über viele SMGW können nicht eindeutig auf eine authentische Quelle zurückgeführt werden (bspw. die Herkunft eines Lieferscheins ist nicht eindeutig)
- IT-Systeme weisen ein außergewöhnliches Verhalten auf
- IT-Systeme stellen Zugriffe fest, die keiner zugriffsberechtigen Person zugeordnet werden können oder weisen ungewöhnliche Zugriffsmuster auf (bspw. zugriffsberechtigte Person ist eingeloggt und im Urlaub)
- Endgeräte (bspw. Montage-Tablet) auf denen schützenswerte Informationen hinterlegt sind (bspw. Zugangsdaten) werden verloren gemeldet oder nicht zurückgegeben
- Schlüssel (inkl. Zugangskarten und -token) werden verloren gemeldet oder nicht zurückgegeben

Der Umgang mit Sicherheitsereignissen ergibt sich aus den allgemeinen Anforderungen (s. Abschnitt 5.1) und ist immer gleich. Der feststellende Mitarbeiter meldet das Ereignis direkt oder über einen Ansprechpartner an eine Meldestelle. Diese Meldestelle hält die Qualifikation und Ressourcen vor, um für jedes gemeldete Sicherheitsereignis zu entscheiden, ob ein Sicherheitsvorfall vorliegt oder nicht. Somit stellt ein Sicherheitsereignis immer einen Verdachtsfall dar. Erst wenn eine Meldestelle einen Sicherheitsvorfall als solchen einstuft, handelt es sich bei dem Sicherheitsereignis zusätzlich auch um einen Sicherheitsvorfall.

4.6.2 Sicherheitsvorfälle

Ein Sicherheitsvorfall liegt immer dann vor, wenn aufgrund eines oder mehrerer Sicherheitsereignisse davon ausgegangen werden muss, dass die Schutzziele von SMGW (s. Abschnitt 2.3) verletzt worden sind. Es ist jedoch nicht zu erwarten, dass in der Praxis mit vertretbarem Aufwand ein eindeutiger Nachweis über den akuten Status der Schutzziele von SMGW erbracht werden kann. Insbesondere kann die Integrität der Software nur mit hohem Aufwand zweifelsfrei festgestellt werden. Aus diesem Grund liegt es im Ermessensspielraum der MSB und der jeweiligen Meldestelle, die Einstufung eines Sicherheitsereignisses zu einem Sicherheitsvorfall vorzunehmen. Dabei gilt, jeder erkannte Verlust, jede erkannte Manipulation und jedes erkannte Einschleusen von einem SMGW ist als Sicherheitsvorfall einzustufen (s. Abschnitt 5.1.3). Kann der Verdacht nicht hinreichend widerlegt werden, ist eine Einstufung als Sicherheitsvorfall die durch das BSI empfohlene Vorgehensweise. Die Einstufung als Sicherheitsvorfall resultiert gemäß den allgemeinen Anforderungen (s. Abschnitt 5.1.3) immer in dem nachfolgenden Umgang mit Sicherheitsvorfällen:

1. Auftrag zur Sperrung der SM-PKI-Zertifikate von betroffenen SMGW an den GWA und
2. Verschrottung der SMGW (wenn möglich) und
3. Protokollierung des Sicherheitsvorfalls und der tatsächlich umgesetzten Maßnahmen.

Der zweite Schritt ist nicht immer möglich. Ein SMGW, dass als Verlust gemeldet wird, kann nicht verschrottet werden. In Schritt drei werden die tatsächlich umgesetzten Maßnahmen der Schritte eins und zwei protokolliert.

5 Anforderungen

5.1 Allgemeine Anforderungen

5.1.1 Anforderungen an das Sicherheitskonzept

Der MSB MUSS ein Sicherheitskonzept zur MSB-Lieferkette ausarbeiten und anwenden, indem er die allgemeinen Anforderungen und die prozessspezifischen Anforderungen dieses Dokuments erfüllt. Der MSB MUSS das Sicherheitskonzept dokumentieren. Jedes Dokument MUSS ein Erstellungsdatum (oder eine Versionsnummer) und eine Änderungshistorie enthalten.

Der MSB MUSS innerhalb seiner unternehmensinternen Prozesse diejenigen Prozesse identifizieren und dokumentieren, die relevanten Prozessen im Kontext der MSB-Lieferkette (s. Kapitel 4) entsprechen, also Lagerung, Transport und Montage.

Der MSB MUSS allgemeine Anforderungen auf dem gesamten Lieferweg erfüllen.

Der MSB MUSS prozessspezifische Anforderungen für den entsprechenden relevanten Prozess erfüllen.

Der MSB MUSS prüfen und sicherstellen, dass Richtlinien, Handlungsanweisungen und Regelungen im Kontext der MSB-Lieferkette innerhalb der Prozesse wirksam umgesetzt werden.

Der MSB MUSS die Umsetzung der Anforderungen aus diesem Dokument organisieren und Verantwortlichkeiten definieren, dokumentieren und Personen zuweisen.

Der MSB MUSS Tätigkeiten und Verantwortlichkeiten mindestens so dokumentieren, dass diese in Art und Umfang eine verbindlich einzuhaltende Handlungsanweisung an die verantwortlichen Personen darstellen.

Der MSB MUSS das Sicherheitskonzept regelmäßig und anlassbezogen aktualisieren, um die Wirksamkeit der Maßnahmen weiterhin zu gewährleisten (bspw. PDCA-Zyklus) und erkannte Schwachstellen aufzulösen.

5.1.2 Organisation und Personal

Mitarbeitende des MSB mit Aufgaben im Kontext der MSB-Lieferkette MÜSSEN durch den MSB aufgabenspezifisch über Richtlinien, Handlungsanweisungen und Regelungen aus dem Sicherheitskonzept zur MSB-Lieferkette (z.B. zum Erkennen und Melden von Sicherheitsereignissen) verbindlich belehrt werden. Im Sinne dieser Anforderungen MÜSSEN relevante Informationen aktuell und für Mitarbeitende des MSB mit Aufgaben im Kontext der MSB-Lieferkette einfach zugänglich zur Verfügung gestellt werden. Insbesondere MÜSSEN diesen Mitarbeitenden Meldewege und Ansprechpartner für Sicherheitsereignisse oder zentrale Meldestellen (s. Abschnitt 4.6) bekannt gemacht werden.

Der MSB MUSS seine Mitarbeitenden mit Aufgaben im Kontext der MSB-Lieferkette für Gefährdungen der Schutzziele von SMGW eingehend sensibilisieren und allen Mitarbeitenden das Verständnis vermitteln, dass die Umsetzung geltender Sicherheitsmaßnahmen und das Melden von Sicherheitsereignissen (s. Abschnitt 4.6.1) Bestandteil der Arbeit und der Arbeitsabläufe ist.

Hinweis:
Gefährdungen, die sich aus der unzureichenden Umsetzung von Sicherheitsmaßnahmen (bspw. Schließplan wird nicht konsequent umgesetzt) ergeben können, sollen Teil der Sensibilisierung von Mitarbeitenden sein.

Diese Anforderungen gelten sinngemäß gleichermaßen für Führungskräfte, Vertretungen und externes Personal (das Personal von Transportdienstleistern ist von dieser Anforderung ausgenommen).

Der MSB SOLL sich bei der Planung und Durchführung von Sensibilisierungsmaßnahmen an entsprechenden IT-Grundschutz-Bausteinen orientieren (vgl. [IT-GS]).

5.1.3 Sicherheitsereignisse, Sicherheitsvorfälle und Meldestellen

Sicherheitsereignisse

Mitarbeitenden des MSB mit Aufgaben im Kontext der MSB-Lieferkette MÜSSEN geeignete Informationen zur Verfügung stehen, um Sicherheitsereignisse erkennen zu können. Wird eine Prozessabweichung festgestellt und handelt es sich dabei um ein Sicherheitsereignis (s. Abschnitt 4.6.1), dann MUSS dieses Ereignis durch den feststellenden Mitarbeitenden entsprechend den geltenden Meldewegen unverzüglich gemeldet werden.

Sicherheitsvorfälle

Sicherheitsvorfälle können in jedem Prozess der Lieferkette auftreten (Lagerung, Transport, Montage) und MÜSSEN erfasst und aufgelöst werden. Eine Meldekette des MSB MUSS so definiert sein, dass über diesen Weg die Sperrung von Zertifikaten durch den GWA möglich ist. Durch ein strukturiertes und reproduzierbares Verfahren zur Behandlung von Sicherheitsvorfällen können nicht nur konkrete, ad hoc auftretende Vorfälle individuell behandelt werden, sondern auch kurz- und langfristig wirksame Erkenntnisse zur Verbesserung der Informationssicherheit abgeleitet werden (Vermeidung wiederkehrender Schwächen, „lessons learned"). Die konkrete Ausgestaltung erfolgt unter Berücksichtigung der Angemessenheit und obliegt dem jeweiligen MSB und den individuellen Erfordernissen (Aufwand/Nutzen-Abwägungen).

Es MUSS eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen unter Berücksichtigung von Abschnitt 4.6.2 definiert werden. Die Meldestelle MUSS diese Vorgehensweise umsetzen. Es MUSS regelmäßig überprüft werden, ob die Vorgehensweise noch aktuell und wirksam ist. Bei Bedarf MUSS die Vorgehensweise angepasst werden.

Der MSB MUSS Sicherheitsereignisse, die Verlust, Manipulation oder Einschleusung von SMGW umfassen, als Sicherheitsvorfall einstufen.

Handelt es sich bei einem Sicherheitsereignis um einen Sicherheitsvorfall[3], dann MUSS der MSB die Sperrung der SM-PKI-Zertifikate beauftragen und betroffene Geräte verschrotten. Der MSB MUSS die Umsetzung dieser Maßnahmen sicherstellen und protokollieren (s. Abschnitt 4.6.2).

Meldungen von Sicherheitsereignissen

Eine Meldestelle zur Erfassung von Sicherheitsereignissen MUSS eingerichtet werden. Es MUSS sichergestellt werden, dass Meldungen jederzeit erfolgen können. Die Meldung MUSS bestätigt werden (bspw. Empfangsbestätigung der Meldestelle). Die Mitarbeitenden der Meldestelle MÜSSEN angemessen geschult sein, u.a. zur Erkennung und Behandlung von Sicherheitsvorfällen, und für die Belange der Informationssicherheit sensibilisiert sein.

Der MSB MUSS sicherstellen, dass ein SMGW, für das ein oder mehrere Sicherheitsereignisse gemeldet wurden, erst dann montiert wird, wenn das Ergebnis der Prüfung aller Ereignisse durch die Meldestelle vorliegt und kein Sicherheitsvorfall festgestellt wurde.

Die Behandlung von Sicherheitsvorfällen MUSS unverzüglich umgesetzt und dokumentiert werden. Es SOLLEN standardisierte Verfahren eingesetzt werden. Die Dokumentation einer Meldung SOLL folgende Informationen mindestens enthalten:

- Name des Melders
- Zeitpunkt der Meldung
- Beschreibung des Vorfalls
- Eingeleitete Maßnahmen

[3] Ein Sicherheitsvoll liegt erst dann vor, wenn ein Sicherheitsereignis durch eine Meldestelle als Sicherheitsvorfall eingestuft worden ist (s. Abschnitt 4.6).

Dabei können u.a. folgende Informationen zusätzlich aufgenommen werden:

- Relevanz für den zertifizierten GWA-Betrieb: ja/nein
- Relevanz für den Datenschutz: ja/nein

5.1.4 Infrastruktur

Der MSB MUSS sicherstellen, dass der physische Zugang zu SMGW wirksam beschränkt ist.

Hinweis:
In dieser Anforderung wird zwischen dem physischen Zugang zu und dem Zugriff auf SMGW unterschieden. D.h., eine physische Zugriffsbeschränkung (bspw. gesicherte Umverpackung) ist hier nicht gefordert. Stattdessen ist über alle Prozesse der MSB-Lieferkette sicherzustellen, dass der physische Zugang zu SMGW und damit implizit deren Nutzung (inkl. Manipulation) durch unbefugte Personen wirksam beschränkt ist.

Gebäude

Ein Gebäude SOLL über einen Perimeterschutz, Sichtschutz und Einbruchsschutz verfügen, der ausreichende und den örtlichen Gegebenheiten angepasste Maßnahmen umsetzt. Folgende Komponenten kann der MSB auf ihren Nutzen und Umsetzbarkeit hin beim Perimeterschutz betrachten:

- äußere Umschließung oder Umfriedung,
- Sicherungsmaßnahmen gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze,
- Maßnahmen zur Erschwerung des beabsichtigten gewaltsamen Überwindens der Grundstücksgrenze,
- Freigelände-Sicherungsmaßnahmen,
- Personen- und Fahrzeugdetektion,
- Maßnahmen zur Beweissicherung (beispielsweise Videoaufzeichnung) sowie
- automatische Alarmierung.

5.1.5 Umgang mit Schützenswerten Informationen:

Der MSB MUSS schützenswerte Informationen (s. Abschnitt 2.5) identifizieren und im Sicherheitskonzept festlegen.

Der MSB MUSS sicherstellen, dass er schützenswerte Informationen (bspw. die Geräte-ID zur Identifizierung von SMGW oder die Stückzahl bei An- und Auslieferung von SMGW) nur aus zuverlässiger Quelle entgegennimmt.

Der MSB MUSS Zugang zu und Kenntnis von schützenswerten Informationen (bspw. Dokumentation im Kontext der MSB-Lieferkette) über SMGW auf einen möglichst kleinen Personenkreis begrenzen (Need-To-Know-Prinzip). Die Begrenzung MUSS gemäß dem Stand der Technik umgesetzt werden.

Der MSB MUSS mobile digitale Datenträger, auf denen schützenswerte Informationen über viele SMGW gespeichert werden, verschlüsseln.

Der MSB MUSS schützenswerte Informationen, die digital versendet werden, authentisch, integer und verschlüsselt versenden.

5.2 Anforderungen zum Baustein Lagerung

Physischer Zugangsschutz:

Der MSB MUSS den Zutritt zu SMGW-Lagerräumen beschränken. Für alle Schlüssel[4] zum Lagerraum SOLL ein Schließplan vorliegen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von diesen Schlüsseln SOLL zentral geregelt sein. Reserveschlüssel SOLLEN vorgehalten und gesichert, aber für Notfälle griffbereit aufbewahrt werden. Nicht ausgegebene Schlüssel SOLLEN sicher aufbewahrt werden. Jede Schlüsselausgabe SOLL dokumentiert werden (vgl. [IT-GS]).

Inventur:

Der MSB MUSS regelmäßig[5] und anlassbezogen eine Inventur[6] über den SMGW-Bestand durchführen. Abweichungen zwischen Ist- und Soll-SMGW-Bestand sind als Sicherheitsereignis einzustufen und zu melden.

Wareneingang und -ausgang:

Der MSB MUSS während der Annahme von SMGW eine Identifizierung der Lieferung vornehmen (bspw. anhand des Lieferscheines).

Der MSB MUSS jedes SMGW beim Wareneingang in ein Lager und beim Warenausgang aus einem Lager eindeutig identifizieren und verifizieren (bspw. Soll/Ist-Abgleich der Geräte-ID). Um der Zielsetzung der Massengeschäftstauglichkeit gerecht zu werden, kann der MSB die eindeutige Identifikation und Verifikation von SMGW für viele SMGW stichprobenartig vornehmen.

Die Vollständigkeit einer Lieferung (eingehend und ausgehend) MUSS geprüft werden. Die Prüfung einer Lieferung auf Vollständigkeit kann stichprobenartig erfolgen, indem ein Teil der Lieferung (wie Gebinde oder Ladungsträger) auf Vollständigkeit geprüft wird.

Der MSB MUSS jedes SMGW beim Wareneingang in ein Lager und beim Warenausgang aus einem Lager einer Manipulationserkennung unterziehen und MUSS hierfür mindestens folgende Punkte gemäß GWH-Vorgaben umsetzen:

- Gehäusesichtprüfung (inkl. Gehäusebeschriftung) und
- Prüfung der Manipulationserkennung (bspw. Siegelsichtprüfung).

Die Gehäusesichtprüfung und die Prüfung der Manipulationserkennung MÜSSEN jeweils auf Beschädigung und auf Fälschung durchgeführt werden. Um der Zielsetzung der Massengeschäftstauglichkeit gerecht zu werden, kann der MSB die Manipulationserkennung für viele SMGW stichprobenartig durchführen.

Der MSB MUSS seine Mitarbeitenden mit Aufgaben im Kontext der MSB-Lieferkette anhand der GWH-Vorgaben schulen, wie eine Gehäusesichtprüfung und eine Prüfung der Manipulationserkennung (bspw. Siegelsichtprüfung) durchzuführen ist und anhand welcher Kriterien ein Sicherheitsereignis zu erkennen ist.

Der MSB MUSS Stichproben im Kontext der Lagerung (bspw. während der Warenannahme/ -ausgabe) nach dem Stand der Technik durchführen.

[4] Der Begriff Schlüssel ist hier nicht auf mechanische Schlüssel begrenzt, sondern meint jede Art von Gegenstand, der dem Träger Zutritt zu Räumlichkeiten (bspw. Lager oder Fahrzeug) des MSB gewährt.

[5] Unter „regelmäßig“ wird in diesem Dokument mindestens ein jährliches Intervall verstanden, soweit keine stichhaltigen Gründe dagegensprechen.

[6] Eine Inventur im Kontext der MSB-Lieferkette kann durch eine Inventur nach Handelsgesetzbuch erfolgen. Für diesen Fall ist keine zusätzliche Inventur im Kontext der MSB-Lieferkette gefordert.

IT-Systeme:

Der MSB MUSS den Zugriff auf alle IT-Systeme und Dienste in Zusammenhang mit der Lagerung von SMGW durch angemessene Identifizierung und Authentifizierung der zugreifenden Personen, Dienste oder IT-Systeme absichern.

Der MSB MUSS für das Zurücksetzen von Zugangsdaten (bspw. Benutzername/ Passwort) ein angemessen sicheres Verfahren verwenden.

Der MSB MUSS festlegen, welche IT-Systeme vor Schadprogrammen geschützt werden müssen und wie der Schutz umgesetzt wird.

Der MSB MUSS die vorinstallierten Schutzmechanismen der verwendeten IT-Systeme kennen und anwenden. Diese Mechanismen MÜSSEN genutzt werden, sofern es keinen mindestens gleichwertigen Ersatz gibt.

5.3 Anforderungen zum Baustein Transport

Physischer Zugangsschutz:

Der MSB MUSS einen physischen Zugangsschutz während des Transports sicherstellen. (Dies kann z.B. erfolgen, in dem der Transporteur das Fahrzeug abschließt, während das Fahrzeug unbeaufsichtigt ist.)

Lieferung und Lieferdauer:

Der MSB MUSS sicherstellen, dass der Absender dem Empfänger für jeden Transport von SMGW den erwarteten Lieferzeitpunkt mitteilt.

Der MSB MUSS prüfen, ob eine außergewöhnliche Verspätung in Bezug auf den erwarteten Lieferzeitpunkt, vorliegt.

Hinweis:
Die Prüfung auf außergewöhnliche Verspätung kann beim Endkunden auch durch den Monteur zum Zeitpunkt der geplanten Montage durchgeführt werden.

Wenn eine außergewöhnliche Verspätung vorliegt, MUSS der MSB prüfen, ob die Verspätung plausibel begründet ist. Ist eine außergewöhnliche Verspätung nicht plausibel begründbar oder wenn ein Transport den Empfänger erwartbar nicht mehr erreichen wird (Ausnahmen: Stornierung), MUSS der MSB diesen Transport von SMGW als Verlust von SMGW behandeln.

Hinweis:
Eine Prüfung auf Plausibilität ist dabei Aufgabe der Meldestelle (s. Abschnitt 4.6). Es wird hier nicht von Mitarbeitenden außerhalb der Meldestelle erwartet, dass sie Informationen und Qualifikationen vorhalten, um abschließend bewerten zu können, ob eine Verspätung plausibel ist oder nicht. Es genügt, wenn Mitarbeitende außerhalb der Meldestelle eine außergewöhnliche Verspätung als solche erkennen und melden.

Informationssicherheit:

Der MSB MUSS sicherstellen, dass der Absender dem Empfänger für jeden Transport von SMGW Informationen zur Identifizierung von SMGW (wie Geräte-ID) sowie zur An- und Auslieferung von SMGW (wie Anzahl) authentisch und integritätsgesichert mitteilt.

Informationen zur Identifizierung von SMGW (wie Geräte-ID) sowie zur An- und Auslieferung von SMGW (wie Anzahl) sind für große Stückzahlen von SMGW schützenswert und MÜSSEN durch den MSB entsprechend Abschnitt 2.5 behandelt werden.

Wenn der MSB gemäß Abschnitt 2.5 Informationen aus der SMGW-Beschriftung als schützenswert klassifiziert, MÜSSEN die SMGW blickdicht verpackt werden, sodass keine Informationen (wie Aufdruck) von außen erkennbar sind.

Hinweis:
Die Anforderungen in diesem Abschnitt stellen keine Anforderungen an den Endkunden am Installationsort (bspw. für Kurier-, Express- oder Paketversand). Es wird angenommen, dass der Endkunde immer Empfänger einer Lieferung ist, obgleich in der Praxis auch ein Rückversand (Retoure) vom Endkunden zum MSB denkbar ist. Des Weiteren wird angenommen, dass der Endkunde am Installationsort die sichere Verwahrung von empfangenen SMGW angemessen sicherstellt, bis zur Entgegennahme durch den Monteur (s. Abschnitt 4.5 und Abschnitt 5.4).

5.4 Anforderungen zum Baustein Montage

Physischer Zugangsschutz:

Der MSB MUSS für die Nutzung von Fahrzeugen Handlungsanweisungen erarbeiten und anwenden, mit dem Ziel, Fahrzeuge vor unerlaubtem Zutritt und Diebstahl zu schützen.

Der MSB MUSS einen physischen Zugangsschutz während der Montage sicherstellen. (Dies kann z.B. erfolgen, in dem der Monteur das Fahrzeug abschließt, während das Fahrzeug unbeaufsichtigt ist.)

Inventur:

Der MSB MUSS sicherstellen, dass der Monteur regelmäßig und anlassbezogen eine Inventur über den SMGW-Bestand durchführt. Abweichungen zwischen Ist- und Soll-SMGW-Bestand sind als Sicherheitsereignis einzustufen und zu melden.

Wareneingang und -ausgang:

Variante 1: Monteur empfängt SMGW aus einem Transport (s. Abschnitt 4.3)

Der MSB MUSS sicherstellen, dass der Monteur beim Wareneingang eines Transports

- jedes SMGW eindeutig identifiziert und verifiziert (bspw. Soll/Ist-Abgleich der Geräte-ID). Um der Zielsetzung der Massengeschäftstauglichkeit gerecht zu werden, kann der Monteur die eindeutige Identifikation und Verifikation von SMGW stichprobenartig vornehmen.
- die Vollständigkeit der Lieferung überprüft. Die Prüfung einer Lieferung auf Vollständigkeit kann stichprobenartig erfolgen, indem ein Teil der Lieferung (wie Gebinde oder Ladungsträger) auf Vollständigkeit geprüft wird.
- jedes SMGW beim Wareneingang eines Transports einer Manipulationserkennung unterzieht und MUSS hierfür mindestens folgende Punkte gemäß GWH-Vorgaben umsetzen:
  - Gehäusesichtprüfung (inkl. Gehäusebeschriftung) und
  - Prüfung der Manipulationserkennung (bspw. Siegelsichtprüfung).

Hinweis:
Diese Variante schließt den Fall mit ein, dass der Monteur SMGW vom Endkunden entgegennimmt.

Variante 2: Monteur nimmt SMGW im Lager persönlich entgegen (s. Abschnitt 4.4)

Wenn der Monteur SMGW in einem Lager gemäß Abschnitt 4.2 persönlich entgegennimmt und seitens des Lagerpersonals bereits die eindeutige Identifikation und Verifikation der einzelnen ausgegebenen SMGW, sowie die Prüfung auf Vollständigkeit und die Manipulationserkennung erfolgt ist, so ist keine erneute Identifikation und Verifikation der einzelnen SMGW oder eine Prüfung auf Vollständigkeit oder eine Manipulationserkennung erforderlich.

Die Gehäusesichtprüfung und die Prüfung der Manipulationserkennung MÜSSEN jeweils auf Beschädigung und auf Fälschung durchgeführt werden. Um der Zielsetzung der Massengeschäftstauglichkeit gerecht zu werden, kann der Monteur die Manipulationserkennung stichprobenartig durchführen.

Montage/ Demontage zur Wiederverwendung:

Der MSB MUSS sicherstellen, dass der Monteur während der Montage und während der Demontage zur Wiederverwendung:

- jedes SMGW eindeutig identifiziert und verifiziert und
- jedes SMGW einer Manipulationserkennung unterzieht und hierfür mindestens folgende Punkte gemäß GWH-Vorgaben umsetzt:
    - Gehäusesichtprüfung (inkl. Gehäusebeschriftung) und
    - Prüfung der Manipulationserkennung (bspw. Siegelsichtprüfung).

Die Gehäusesichtprüfung und die Prüfung der Manipulationserkennung MÜSSEN jeweils auf Beschädigung und auf Fälschung durchgeführt werden.

Der MSB MUSS sicherstellen, dass der GWA die Rückmeldung über die erfolgreiche Montage oder Demontage unter Angabe von Geräte-ID und Einsatzumgebung erhält.

Der MSB MUSS sicherstellen, dass vor jeder Demontage zur Wiederverwendung eine Nutzerdatenbereinigung erfolgreich durchgeführt wird (s. Abschnitt 4.4.2). Falls die Nutzerdatenbereinigung an der Messstelle fehlschlägt, muss sie unverzüglich nach der Demontage wiederholt werden, bis die Durchführung erfolgreich ist. Anschließend ist das SMGW analog zu einem SMGW in der Erstauslieferung zu behandeln (s. Abschnitt 2.2).

Der MSB MUSS Stichproben im Kontext der Montage (bspw. während der Warenannahme/ -ausgabe) nach dem Stand der Technik durchführen.

Informationssicherheit:

Der MSB MUSS sicherstellen, dass er dem Monteur Informationen zur Identifizierung von SMGW (wie Geräte-ID), sowie zur Installation von SMGW, aus zuverlässiger Quelle (bspw. IT-Systeme des MSB) bereitstellt oder der Monteur derartige Informationen nur aus zuverlässiger Quelle entgegennimmt.

Der MSB MUSS sicherstellen, dass er dem Monteur die Möglichkeit bietet, bei Verdacht auf Informationen aus unzuverlässiger Quelle die Informationen mit dem MSB zu verifizieren.

Personal und Schulung:

Der MSB MUSS Monteure anhand von GWH-Vorgaben (inkl. Demontage zur Wiederverwendung) schulen, wie eine Gehäusesichtprüfung und eine Prüfung der Manipulationserkennung (bspw. Siegelsichtprüfung) durchzuführen ist und anhand welcher Kriterien ein Sicherheitsereignis zu erkennen ist.

Hinweis: Die Art und Weise der Schulung bzw. deren Durchführung (bspw. Live- oder Online-Schulung) liegt im Ermessensspielraum des MSB. Diese Anforderung gilt in Ergänzung zu den allgemeinen Anforderungen (s. Abschnitt 5.1.2).

Der MSB MUSS regelmäßig beurteilen, ob das eingesetzte Personal vertrauenswürdig ist. Zum Beispiel kann die Beurteilung der Vertrauenswürdigkeit durch eine Bewertung der Zuverlässigkeit der Zusammenarbeit erfolgen.

IT-Systeme:

Der MSB MUSS den Zugriff auf alle IT-Systeme und Dienste in Zusammenhang mit der Montage von SMGW durch angemessene Identifizierung und Authentifizierung der zugreifenden Personen, Dienste oder IT-Systeme absichern.

Der MSB MUSS für das Zurücksetzen von Zugangsdaten (bspw. Benutzername/ Passwort) ein angemessen sicheres Verfahren verwenden.

Der MSB MUSS festlegen, welche IT-Systeme vor Schadprogrammen geschützt werden müssen und wie der Schutz umgesetzt wird.

Der MSB MUSS die vorinstallierten Schutzmechanismen der verwendeten IT-Systeme kennen und anwenden. Diese Mechanismen MÜSSEN genutzt werden, sofern es keinen mindestens gleichwertigen Ersatz gibt.

Literaturverzeichnis

[PP-0073 v2.0]	Protection Profile for a Smart Meter Gateway (SMGW-PP), BSI, Version 2.0, 2024
[TR 03109-1 v2.0]	Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, BSI, Version 2.0, 2024
[Anlage VIII]	Anlage VIII: Lebenszyklus, BSI, Version 2.0, 2024
[IT-GS]	IT-Grundschutz-Kompendium, BSI, Edition 2023