Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Smart-Meter-Gateway

Cybersicherheit für die Digitalisierung der Energiewirtschaft

Inhaltsverzeichnis

1 Einleitung

Einleitung

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und unsere Gesellschaft insgesamt vor große Herausforderungen. Anstelle von wenigen Großkraftwerken werden eine Vielzahl von kleinen, dezentralen Erzeugungsanlagen (z. B. Photovoltaik), Anlagen zur Speicherung elektrischer Energie und flexible Verbrauchseinrichtungen (z. B. Elektromobile oder Wärmepumpen) in das intelligente Energienetz (Smart Grid) integriert. Im zukünftigen Smart Grid ist deswegen Flexibilität erforderlich, um Erzeugung und Verbrauch optimal aufeinander abzustimmen.

Um diese Ziele erfolgreich umsetzen zu können, müssen die Verteilnetze auf Basis intelligenter Messsysteme stufenweise digitalisiert werden. Auf der einen Seite lassen sich dadurch Effizienzsteigerungen sowie Prozessoptimierungen in der Wirtschaft und mehr Komfort für die Bürgerinnen und Bürger erreichen. Auf der anderen Seite steigt das Bedrohungspotential deutlich an, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen.

Durch die Verwendung von intelligenten Messsystemen – und der damit einhergehenden Verwendung zertifizierter Smart-Meter-Gateways (im Folgenden mit SMGW abgekürzt) – lassen sich Netzzustandsdaten erheben und übermitteln, sodass mehr Transparenz über die Leistungsflüsse im Verteilnetz entsteht. Steuerbare Verbrauchseinrichtungen, Stromspeicher und dezentrale Erzeugungsanlagen können über das SMGW gesteuert werden und lassen sich somit netz- und marktdienlich einsetzen.

Im Zuge der Energiewende gehören SMGW damit zu den Schlüsseltechnologien und sind ein gutes Beispiel dafür, welchen Einfluss digitale und vernetzte Technologien auf den Alltag der Verbraucherinnen und Verbraucher haben und wie wichtig in diesem Zusammenhang die frühzeitige Umsetzung von hohen Vorgaben zum Datenschutz und zur IT-Sicherheit sind („Security & Privacy by Design“). Aufgabe und Anspruch des Bundesamts für Sicherheit in der Informationstechnik

(BSI) ist es, die Informationssicherheit in der Digitalisierung zu gestalten und zu gewährleisten, dass die Anwenderinnen und Anwender von den Vorzügen innovativer Technologien profitieren können. Nur wenn Staat, Wirtschaft sowie Bürgerinnen und Bürger auf den Schutz ihrer Daten vertrauen können und ihre Daten gegen zunehmende Bedrohungen ausreichend geschützt sehen, wird die digitale Transformation der Energiewirtschaft gelingen und deren Potential voll ausgeschöpft werden können.

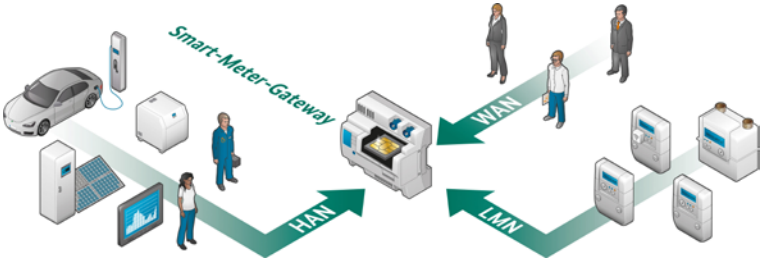
Hierfür sind nachweislich sichere Produktkomponenten und Systeme im Netz sowie eine sichere Kommunikationsinfrastruktur zwingend erforderlich. Im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) entwickelt das BSI daher Anforderungen an vertrauenswürdige Produktkomponenten (SMGW mit integriertem Sicherheitsmodul), an deren sicheren IT-Betrieb (Administration) sowie an die vertrauenswürdige Kommunikationsinfrastruktur (Smart-Metering-Public-Key-Infrastruktur) in Form von Schutzprofilen (engl.: Protection Profiles, PP) und Technischen Richtlinien (TR) als technische Standards.

In Zusammenhang mit den technischen Standards des BSI schafft das Messstellenbetriebsgesetz (MsbG), welches zuletzt durch das am 27. Mai 2023 in Kraft getretene Gesetz zum Neustart der Digitalisierung der Energiewende (GNDEW) novelliert worden ist, verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen in unterschiedlichen Einsatzbereichen und ermöglicht den agilen Rollout des SMGW.

2 Systemarchitektur

Systemarchitektur

Das intelligente Messsystem besteht im Kern aus einer Kommunikationseinheit, dem SMGW, welches die elektronischen Messeinrichtungen im Lokalen Metrologischen Netz (LMN) mit den verschiedenen Marktteilnehmern (z. B. Gateway-Administrator im Auftrag des Messstellenbetreibers, Verteilnetzbetreiber oder Energielieferant) im Weitverkehrsnetz (WAN) und dem lokalen Heimnetz (HAN) verbindet.



Das SMGW stellt dabei sicher, dass alle Kommunikationsverbindungen verschlüsselt werden und dass nur bekannten Teilnehmern und Geräten vertraut wird. Die Einrichtung der Kommunikationsverbindungen obliegt dem Gateway-Administrator.

2.1 Lokales Metrologisches Netz (LMN)

Über das Lokale Metrologische Netz werden die Messeinrichtungen des Anschlussnutzers mit dem SMGW verbunden. Diese senden die erhobenen Verbrauchs- und Einspeisewerte sowie Netzzustandsdaten (z. B. Spannung, Phasenwinkel, Frequenz) an das SMGW, wo sie gespeichert und weiterverarbeitet werden.

Das SMGW nutzt je nach Tarif der Kundin oder des Kunden unterschiedliche Regelwerke, um die empfangenen Messwerte sowohl unter dem Gesichtspunkt des Eichrechts als auch des Datenschutzes weiterzuverarbeiten.

2.2 Weitverkehrsnetz (Wide Area Network, WAN)

Das SMGW kann über die WAN-Schnittstelle mit externen Marktteilnehmern kommunizieren, zu denen auch der Gateway-Administrator gehört. Dieser ist sowohl für die Konfiguration als auch für den sicheren Betrieb verantwortlich. Er muss u.a. das kryptographische Schlüsselmaterial für die Komponenten des intelligenten Messsystems beim Anschlussnutzer einspielen, aber auch die Konfiguration der Regelwerke für die Tarifierung vornehmen.

Aus Gründen der Sicherheit gehen sämtliche Kommunikationsverbindungen vom SMGW aus. Diese können bei Bedarf oder zu festgelegten Zeitpunkten durch das SMGW etabliert werden. Um aber auch auf spontane Ereignisse reagieren zu können, kann der Administrator das SMGW über einen Wake-Up-Dienst zu einem Verbindungsaufbau anstoßen.

Dabei handelt es sich um ein vom Administrator signiertes und nur für einen gewissen Zeitraum gültiges Datenpaket, auf welches das SMGW nach erfolgreicher Überprüfung reagiert, indem es eine gesicherte Verbindung zum Gateway-Administrator aufbaut.

2.3 Heimnetz (Home Area Network, HAN)

Die HAN-Schnittstelle ist dem Anschlussnutzer zuzuordnen. An dieser können steuerbare Geräte wie bspw. Wärmepumpen oder Photovoltaikanlagen angeschlossen werden, um externen Marktteilnehmern den Zugriff für Steuerungs- und Fernwartungs-

zwecke zu ermöglichen. Das SMGW stellt hierfür einen sicheren, transparenten Kanal zur Verfügung, welcher nur durch den Gateway-Administrator konfiguriert werden kann.

Darüber hinaus kann der Anschlussnutzer über diese Schnittstelle seine Verbrauchs- und ggf. Einspeisewerte abfragen. Er kann hierzu ein geeignetes Endgerät anschließen und erhält nach erfolgreicher Authentifizierung lesenden Zugriff auf die Daten. Insbesondere wird jeder Datenversand im Anschlussnutzer-Logbuch protokolliert und kann durch diesen nachvollzogen werden.

Die HAN-Schnittstelle ermöglicht zudem einem Servicetechniker, wichtige Informationen über den Systemzustand des SMGW in Erfahrung zu bringen. Diese werden benötigt, um im Fehlerfall die Ursache diagnostizieren zu können und das intelligente Messsystem zu entstören. Aus Datenschutzgründen hat der Servicetechniker dabei keinen Zugriff auf die im SMGW hinterlegten Messwerte bzw. mandantenspezifischen Daten.

3 Sicherheitstechnische Anforderungen

Sicherheitstechnische Anforderungen

3.1 Smart-Meter-Gateway – Schutzprofil (BSI-CC-PP-0073)

Das Schutzprofil beschreibt mögliche Bedrohungen eines SMGW in seiner Einsatzumgebung und definiert die Mindestanforderungen für entsprechende Sicherheitsmaßnahmen.

Der Aufbau eines Schutzprofils ist in den Common Criteria (CC) geregelt. Auf Basis eines Schutzprofils können Produkte evaluiert werden, die nach einer positiven Prüfung ein Zertifikat erhalten und somit nachweislich das Schutzziel erfüllen. Zugleich lässt das Schutzprofil dem Hersteller Spielraum bei der technischen Ausgestaltung der Sicherheitsanforderungen.

Das Schutzprofil für das SMGW konzentriert sich auf die zu erfüllende Sicherheitsleistung eines verbauten SMGW und definiert für die Schnittstellen zu den drei Netzen (LMN, HAN und WAN) sicherheitstechnische Anforderungen, die jedes SMGW bereitstellen muss.

Auf diese Weise ermöglicht das Schutzprofil, dass selbst bei unterschiedlicher Ausführung (Einfamilienhaus, Wohnungsgesellschaften, Ein- und Mehrgerätelösung) ein einheitlicher, hoher Sicherheitsstandard gewährleistet ist und stellt im Fall von neuen technischen Möglichkeiten eine kontinuierliche Weiterentwicklung der Produkte sicher.

3.2 Bedrohungslage

Das Schutzprofil des SMGW unterscheidet mögliche Bedrohungen anhand des potenziellen Angreifers, der versucht, auf das SMGW einzuwirken. Zum einen gibt es den lokalen Angreifer, der vor Ort direkten Zugriff auf das SMGW besitzt, um es somit auf physischem Wege zu kompromittieren. Beispielsweise könnte ein Angreifer über Eingriffe am SMGW versuchen, abrechnungsrelevante Daten oder Netzzustandsdaten zu manipulieren. Aber auch Angriffe auf die Systemuhr des SMGW, das Ausspähen von Verbrauchsdaten, die Manipulation der Geräteeinstellungen oder ein Auslesen und Verändern der Firmware gehören mit zu den möglichen Angriffszielen.

Zum anderen bietet die kommunikative Anbindung des SMGW ein hohes Angriffspotenzial für Angreifer, die von außen versuchen, eine Vielzahl von intelligenten Messsystemen anzugreifen. Die potenziellen Angriffe aus dem WAN ähneln größtenteils denen, die lokal ein Risiko darstellen, sind im Risikomanagement aufgrund möglicher Schwarmeffekte jedoch als kritischer zu bewerten.

3.3 Sicherheitsziele

Um den zuvor beschriebenen Bedrohungen entgegenzuwirken, definiert das Schutzprofil eine Reihe von Sicherheitszielen, die durch das SMGW umgesetzt werden müssen. Um seiner Rolle als Bindeglied zwischen drei unterschiedlichen Netzen (LMN, HAN und WAN) gerecht zu werden, schottet das SMGW die Netze gegeneinander ab. Hierzu sind seitens des Herstellers u. a. Firewall-Mechanismen in das SMGW zu integrieren. Neben der Separierung der jeweiligen Netze und Schnittstellen muss ebenfalls sichergestellt werden, dass nur Kommunikationsverbindungen von innen nach außen aufgebaut werden können. Daneben werden sämtliche Kommunikationsflüsse, unabhängig in welches Netz kommuniziert wird, nach einer gegenseitigen Authentifizierung grundsätzlich verschlüsselt und integritätsgesichert. Ein besonderes Augenmerk legt

das Schutzprofil auf die Kommunikation zu den angeschlossenen Zählern. Das SMGW stellt hierfür Funktionen zum Empfang und zur Abfrage von Einspeise- und Verbrauchswerten sowie Netzzustandsdaten in konfigurierbaren Zeitintervallen zur Verfügung.

Aktuelle Informationen zum Schutzprofil des SMGW sind unter dem nachfolgenden QR-Code abrufbar:

Web:
https://bsi.bund.de/dok/smgw-schutzprofil

3.4 Zertifizierungsverfahren

Die Zertifizierung nach Common Criteria (CC) dient dem Nachweis, dass die im Schutzprofil (PP) geforderten IT-Sicherheitseigenschaften im Produkt vollständig und wirksam implementiert sind. Sie umfasst auch den Nachweis einer sicheren Produktions- und Entwicklungsumgebung beim Gerätehersteller sowie eine sichere Auslieferung des Produkts an den Verwendungsort.

Erteilte CC-Zertifikate sind bis zu acht Jahre gültig, sofern eine erfolgreiche Neubewertung (Re-Assessment) die Gültigkeit alle zwei Jahre bestätigt.

Eine Auflistung der zertifizierten SMGW-Hersteller sowie jener Hersteller, die sich aktuell im Zertifizierungsverfahren befinden, sind unter dem nachfolgenden QR-Code abrufbar:

Web:
https://bsi.bund.de/dok/
smgw-zertifizierungsverfahren

4 Technische Richtlinie TR-03109

Technische Richtlinie TR-03109

Das BSI veröffentlicht unter dem Dach der Technischen Richtlinie TR-03109 mehrere Teile zu unterschiedlichen Bereichen, insbesondere um das Zusammenspiel der verschiedenen Komponenten zu gewährleisten. Damit die digitale Kommunikation in einem intelligenten Messsystem und der angeschlossenen Infrastruktur reibungslos funktioniert, müssen alle daran Beteiligten funktionale Vorgaben erfüllen. Für das Smart-Meter-Gateway kommt dazu, dass die im Schutzprofil getroffenen Sicherheitsanforderungen und -annahmen in einer Technischen Richtlinie funktional näher spezifiziert werden müssen.

Thematisch widmen sich damit die Teile der Technischen Richtlinie TR-03109 neben dem SMGW und dem Sicherheitsmodul auch der Infrastruktur, z. B. der Public-Key-Infrastruktur (PKI) oder dem Gateway-Administrator.

4.1 TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

Teil 1 der Technischen Richtlinie TR-03109 beinhaltet die funktionalen Anforderungen, die ein SMGW mindestens erfüllen muss. Das Dokument beschreibt das Schnittstellenverhalten des SMGW an den drei Schnittstellen LMN, HAN und WAN in Form von detaillierten technischen Vorgaben. Darüber hinaus werden interne, logische Abläufe weiter ausgeführt (z. B. die Tarifierung anhand von Regelwerken oder das Zusammenspiel zwischen SMGW und Sicherheitsmodul).

4.2 TR-03109-2: Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls

Das Schutzprofil für das SMGW fordert den Einsatz eines zertifizierten Sicherheitsmoduls, das das SMGW vor allem bei der Signaturerstellung und -prüfung sowie bei der Schlüssel- und Zufallszahlengenerierung unterstützt.

Zudem dient das Sicherheitsmodul als sicherer Schlüsselspeicher, u. a. für das private Schlüsselmaterial. Es stellt damit einen wichtigen Vertrauensanker im SMGW dar. Diese und weitere funktionale Anforderungen, auch unter dem Gesichtspunkt der herstellerübergreifenden Interoperabilität, finden sich in der Technischen Richtlinie TR-03109-2 wieder.

4.3 TR-03109-3: Kryptographische Vorgaben – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen

Welche kryptographischen Verfahren oder Schlüssellängen im SMGW und dessen unmittelbarem Umfeld zum Einsatz kommen, definiert Teil 3 der Technischen Richtlinie. Dieser basiert u. a. auf den BSI-Richtlinien TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ und TR-03111 „Elliptische-Kurven-Kryptographie“.

4.4 TR-03109-4: Smart-Metering-PKI – Public-Key-Infrastruktur für Smart-Meter-Gateways

Dieser Teil der Technischen Richtlinie spezifiziert die Architektur der Smart-Metering-Public-Key-Infrastruktur (SM-PKI), mit der die Authentizität der bei dieser Kommunikation eingesetzten öffentlichen Schlüssel der Kommunikationspartner sichergestellt wird. Technisch wird der Authentizitätsnachweis der Schlüssel über digitale Zertifikate aus der SM-PKI realisiert.

4.5 TR-03109-5: Kommunikationsadapter

In der TR-03109-5 werden Mindestvorgaben zur Gewährleistung von IT-Sicherheit und Interoperabilität an Produkte im HAN des SMGW (z.B. Steuerungs- und Submetereinrichtungen) gestellt, die dafür den sog. Kommunikationsadapter implementieren und direkt mit dem SMGW verbunden sind. Die Vorgaben umfassen Mindestanforderungen an die sichere Anbindung und den Betrieb dieser Produkte im HAN des SMGW. Die TR-03109-5 kann somit das Vertrauen in die Infrastruktur rund um das intelligente Messsystem steigern und die Risiken von Angriffen auf diese HAN-Komponenten minimieren.

4.6 TR-03109-6: Smart-Meter-Gateway-Administration

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Gateway-Administrator verantwortlich. Daher muss sichergestellt sein, dass der Betrieb beim Administrator den Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt. Der Nachweis der Umsetzung der definierten Mindestanforderungen kann zum einen durch eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz und zum anderen durch eine Zertifizierung gemäß ISO/IEC 27001 erbracht werden.

Die Technischen Richtlinien und das Schutzprofil sind unter dem nachfolgenden QR-Code abrufbar:

Web:
https://bsi.bund.de/dok/smgw-pp-tr

5 Sicherstellung der Interoperabilität des intelligenten Messsystems

Sicherstellung der Interoperabilität des intelligenten Messsystems

Neben der Einhaltung der sicherheitstechnischen Anforderungen stellt die Interoperabilität des SMGW als Vertrauensanker und zentrale Kommunikationsplattform einen wichtigen Eckpfeiler für einen erfolgreichen Rollout des intelligenten Messsystems dar. Aus diesem Grund spezifiziert das BSI in Form von Technischen Richtlinien funktionale Anforderungen zur Etablierung einer Mindest-Interoperabilität bei den SMGW sowie weiteren technischen Komponenten, wie z. B. bei den in den SMGW verbauten Sicherheitsmodulen.

Durch diese Festlegungen wird sichergestellt, dass sich beim Austausch eines SMGW durch das SMGW eines anderen Herstellers die umliegenden Komponenten wie Zähler, steuerbare Geräte oder Backend-Systeme zur Administration weiterverwenden lassen.

Die Anforderungen der TR-03109-1 werden mittels funktionaler Testfälle überprüft. In Konformitätsbewertungsverfahren (der sog. TR-Zertifizierung) wird die Einhaltung der Anforderungen von einer unabhängigen Prüfstelle überprüft und vom BSI abschließend bescheinigt. Dabei werden sich die Anforderungen an die Interoperabilität, die durch die Geräte zu erfüllen sind, mit der Technischen Richtlinie kontinuierlich weiterentwickeln.

Die Grundlage hierfür ist ein fortlaufender Entwicklungs- und Abstimmungsprozess mit den beteiligten Akteuren. Das Ziel dieses Abstimmungsprozesses ist es, durch die schrittweise Vertiefung der Interoperabilitätsanforderungen in der Technischen Richtlinie künftig die Austauschbarkeit der Geräte an den Schnittstellen zu ermöglichen. Im Sinne einer agilen Vorgehensweise müssen daher iterativ Anforderungen beschrieben, in der Praxis erprobt und unter Berücksichtigung der Erfahrungswerte weiter verfeinert werden. Interoperabilität ist demnach kein statischer Zustand, sondern ein Reifeprozess.

Um die regelmäßig notwendigen Re-Zertifizierungen nach TR-03109-1 zu beschleunigen, stellt das BSI eine Testumgebung zur Durchführung von (teil-)automatisierten Konformitätstests zur Verfügung und entwickelt diese kontinuierlich weiter. Diese Testumgebung kann zudem die SMGW-Hersteller bereits im Entwicklungsprozess dabei unterstützen, die TR-Konformität ihrer Produkte zu evaluieren.

Eine Auflistung der nach TR-03109-1 zertifizierten SMGW-Hersteller ist unter dem nachfolgenden QR-Code abrufbar:

Web:
https://bsi.bund.de/dok/
smgw-zertifizierungsverfahren

6 Smart-Metering-PKI

Smart-Metering-PKI

Um den Schutz der von den Haushalten übermittelten Messdaten zu gewährleisten, ist für die Verbindung des SMGW zu autorisierten Marktteilnehmern im Weitverkehrsnetz eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten, integritätsgesicherten Kanal. Zusätzlich werden die zu versendenden Inhaltsdaten vom SMGW für die Endempfängerin bzw. den Endempfänger verschlüsselt und signiert. Die hierfür notwendigen elektronischen Zertifikate werden durch die Smart-Metering-PKI (SM-PKI) zur Verfügung gestellt.

Das BSI ist Inhaber des Wurzelzertifikats der SM-PKI und für den Betrieb der Root-CA verantwortlich. Das Wurzelzertifikat der SM-PKI ist der Vertrauensanker der Smart-Meter-Gateway-Infrastruktur. Die Root-CA setzt die gesetzlichen Anforderungen auf technischer Ebene durch und berechtigt Unternehmen dazu, eine Sub-CA zu betreiben. Die Sub-CAs übernehmen als nachgeordnete Zertifizierungsstellen die Betreuung der Marktteilnehmer (EMT, GWA, GWH, SMGW) und stellen diesen die für die Teilnahme an der Smart-Meter-Gateway-Infrastruktur notwendigen Endnutzerzertifikate aus. Die technischen, personellen und organisatorischen Sicherheitsanforderungen für das Ausstellen, Verwalten, Benutzen, Erneuern und Zurückziehen der SM-PKI-Zertifikate werden von der Root-CA in der Certificate Policy (Root-CP) festgelegt.

Neben der Root-CA für den regulären Wirkbetrieb betreibt das BSI verschiedene Testsysteme zur Ausgabe von elektronischen Test-Zertifikaten. Hiermit können die SMGW und die für deren Betrieb benötigte Infrastruktur (z. B. im Rahmen der Entwicklung) unter Echtbedingungen erprobt werden.

Eine Auflistung der registrierten Zertifizierungsdienstleister (Sub-CAs) ist unter dem nachfolgenden QR-Code abrufbar:

Web:
https://bsi.bund.de/dok/
smgw-registrierte-sub-cas

7 Informationssicherheit bei Administration und Betrieb

Informationssicherheit bei Administration und Betrieb

Für den sicheren Betrieb des intelligenten Messsystems ist der Smart-Meter-Gateway-Administrator (GWA) verantwortlich. Damit alle GWA ein vergleichbares Niveau in Bezug auf die Informationssicherheit aufweisen, legt die Technische Richtlinie des BSI TR-03109-6 einheitliche organisatorische und technische Anforderungen sowie Maßnahmen für die Etablierung und Aufrechterhaltung der Informationssicherheit beim GWA fest.

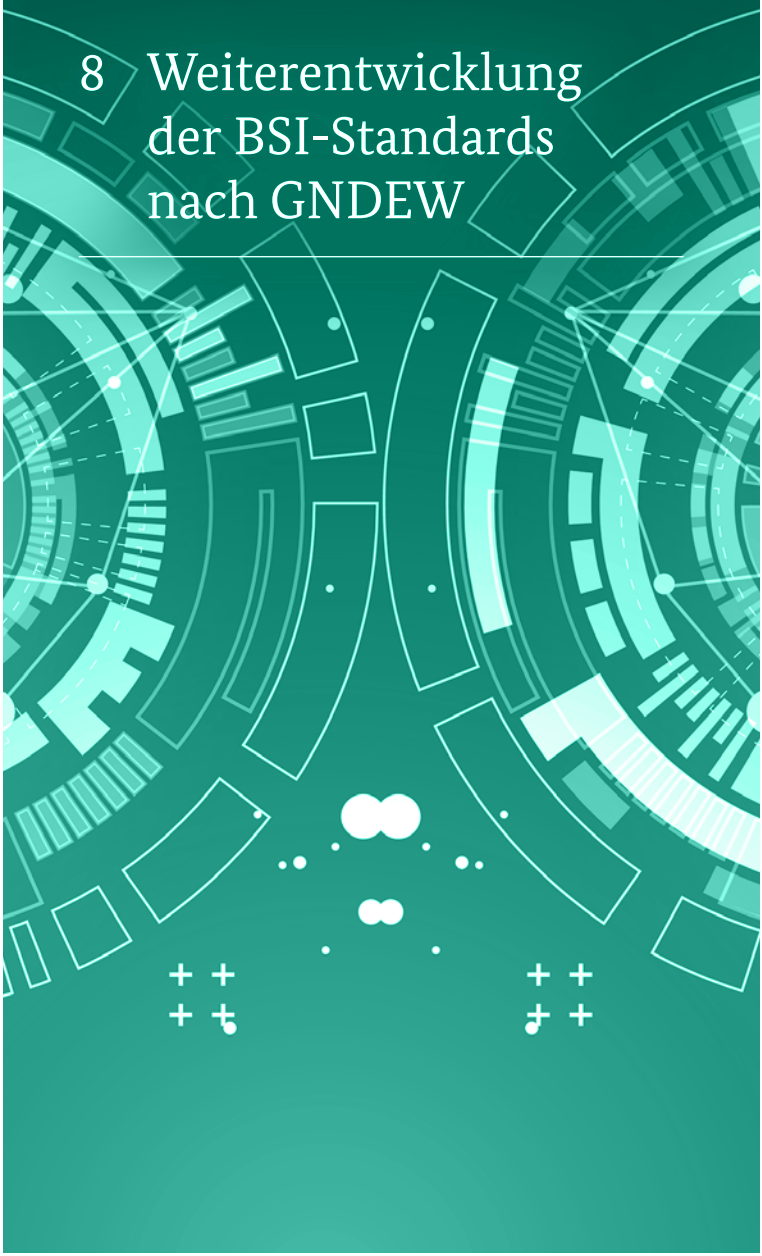
Die TR-03109-6 definiert ausgehend von den Aufgaben und Anwendungsfällen des GWA die zu schützenden werthaltigen Objekte (Assets), beschreibt die zu beachtenden Schutzziele und trifft eine Abschätzung des Bedrohungs- und Risikopotenzials. Daraus werden angemessene Mindestmaßnahmen abgeleitet, die die vorher identifizierten Bedrohungen und Risiken geeignet berücksichtigen und minimieren. Der GWA muss ein Informationsmanagementsystem betreiben, das sämtliche GWA-Aufgaben erfasst und die Umsetzung der Mindestmaßnahmen der TR-03109-6 sicherstellt und ergänzt.

Die Umsetzung der Mindestanforderungen der TR-03109-6 muss durch einen hierfür zugelassenen Auditor geprüft und abschließend im Rahmen der Zertifizierung des ISMS bestätigt werden. Das ISMS kann nach „ISO 27001 auf Basis von IT-Grundschutz“ oder nach „ISO/IEC 27001“ zertifiziert werden.

Weitere Informationen lassen sich mit dem nachfolgenden QR-Code abrufen:

Web:
https://bsi.bund.de/dok/smgw-administration-betrieb

8 Weiterentwicklung der BSI-Standards nach GNDEW



Weiterentwicklung der BSI-Standards nach GNDEW

Mit dem Inkrafttreten des Gesetzes zum Neustart der Digitalisierung der Energiewende (GNDEW) wird der Rollout von intelligenten Messsystemen beschleunigt. Durch verbesserte Rahmenbedingungen und dem im Gesetz verankerten Rollout-Fahrplan wird die Planungs- und Investitionssicherheit für die am Rollout beteiligten Unternehmen erhöht. Zusätzlich wird klargestellt, dass auf Basis der etablierten und bereits umgesetzten BSI-Standards der Rollout von intelligenten Messsystemen fortgeführt werden kann.

Es werden klare Zuständigkeiten und Verantwortungsbereiche für die Standardisierung definiert. Zukünftig kann das BSI neben der eigentlichen Entwicklung von BSI-Standards für das SMGW auch Standardisierungspartnerschaften mit Regelsetzern eingehen, die wichtige Standardisierungsvorhaben für das Gelingen der Digitalisierung der Energiewende verfolgen. Ebenso wird das BSI weiterhin Förderprojekte des BMWK begleiten, um im engen fachlichen und technischen Austausch zu Realisierung von Innovationsthemen über die SMGW-Plattform mit den Stakeholdern zu stehen, mit dem Ziel, wichtigen Input für die Weiterentwicklung der BSI-Standards zu erhalten. Unter den Rahmenbedingungen des GNDEW wird das BSI zudem den Dialog-Prozess mit der Branche fortsetzen, um die Weiterentwicklung der BSI-Standards für die SMGW-Plattform gemeinsam mit den Stakeholdern zu konkretisieren.

Das GNDEW hebt hervor, dass Cybersicherheit die Voraussetzung für eine erfolgreiche Digitalisierung der Energiewende und deren zentraler Anker die Smart-Meter-Gateway-Plattform ist. Bei der Weiterentwicklung der BSI-Standards werden nachfolgende Schwerpunkte adressiert:

1. Für den digitalen Netzanschlusspunkt soll zukünftig das Smart-Meter-Gateway die sichere Fernsteuerbarkeit von steuerbaren Einrichtungen ermöglichen. Das BSI hat hierzu die BSI-Vorgaben weiterentwickelt, um Datenschutz und Datensicherheit für diese wichtigen Smart-Grid-Anwendungsfälle zu gewährleisten.

2. Zur Gewährleistung der Nachhaltigkeit und zur Steigerung der Interoperabilität sollen bis zum 31.12.2024 einheitliche und ausreichend beschriebene Spezifikationen für APIs (Anwendungsprogrammierschnittstellen) durch das BSI bereitgestellt werden. Mit dem Ziel der Austauschbarkeit und der gesteigerten Interoperabilität an den Schnittstellen des SMGW werden verbesserte Integrations-, Update- und Wechselprozesse ermöglicht und zugleich die Realisierung von weiteren Innovationen beschleunigt.

3. Der begonnene Optimierungsprozess des BSI zur Verbesserung des SMGW-Lifecycles soll vorangetrieben werden. Dabei soll die Verbesserung der Logistikkette für die sichere Auslieferung des Smart-Meter-Gateways bei gleichbleibenden Sicherheitsniveau durch das BSI fokussiert verfolgt werden und im Sinne der Nachhaltigkeit der Aus- und Wiedereinbau von Smart-Meter-Gateway berücksichtigt werden.

4. Zur Ermöglichung der RLM-Anwendungsfälle Strom und Gas und der sicheren Anbindung von RLM-Zählern an das SMGW sollen erweiterte BSI-Standards bis 2025 bereitgestellt werden, um für den gesetzlich geforderten Rollout-Start der wichtigen Einbaugruppen RLM rechtzeitig bereitzustehen.

5. Durch den beschleunigten Einbau von intelligenten Messsystemen soll die Erfassung, Verarbeitung und Versendung von Messwerten verschiedener Sparten durch das SMGW

einheitlich ermöglicht werden. Hierzu soll das BSI die BSI-Standards zur Ermöglichung von Haupt- und Untermessungen weiterer Sparten weiterentwickeln, um Datenschutz- und Datensicherheit für verschiedene Datenerhebungen mit dem SMGW zu gewährleisten und zugleich den Plattformgedanken des Smart-Meter-Gateways weiter auszubauen.

6. Zukünftige Messsysteme sollen nicht nur am Netzanschlusspunkt zum Einsatz kommen, sondern auch am Netzknotenpunkt betrieben werden dürfen. Hierzu soll das BSI die BSI-Standards bis zum 31.12.2024 weiterentwickeln, sodass der Anwendungsbereich des Smart-Meter-Gateways erweitert und zugleich die Bündelung von Zählpunkten am Netzknotenpunkt ermöglicht wird.

Durch den gesetzlich festgelegten Fahrplan für den Rollout intelligenter Messsysteme und den Schwerpunktthemen wird somit zukünftig sichergestellt, dass die Anforderungen der Digitalisierung der Energiewende für weitere Einsatzbereiche der Smart-Meter-Gateway-Plattform stetig weiterentwickelt werden. Zugleich werden im Zuge der Weiterentwicklung der BSI-Standards die verschiedenen Marktakteure, Verbände und Partnerbehörden eng eingebunden. Durch den fachlichen Austausch wird wichtiger Branchen-Input berücksichtigt.

Weitere Informationen lassen sich mit dem nachfolgenden QR-Code abrufen:

Web:
https://bsi.bund.de/dok/smgw-roadmap-prozess

9 Fazit

Fazit

Die zügige Umsetzung einer umfassenden Digitalisierung im Energienetz ist maßgeblich für den Erfolg der Energie- und Verkehrswende. Die Integration von Millionen Photovoltaik-Anlagen, Wärmepumpen, Stromspeichern und Elektromobilen mit informationstechnischer Anbindung bedingt in einer zunehmend vernetzten Energiewelt ein erhebliches Gefährdungspotential für die Sicherheit der Energieversorgung in Deutschland und Europa. Die ständig wachsende Zahl von Cyberangriffen erfordert es zwingend, IT-Sicherheit von Beginn an in den Mittelpunkt dieser Entwicklung zu stellen.

Eine sichere zertifizierte Kommunikationsplattform wie das SMGW stellt den zentralen Baustein in der Absicherung der Energienetze dar. Im Zusammenspiel mit weiteren organisatorischen und technischen Maßnahmen bietet sie die Schlüsseltechnologie für einen wirksamen Schutz und leistet einen entscheidenden Beitrag zum Gelingen der Digitalisierung der Energiewende.

Mit dem „Gesetz zum Neustart der Digitalisierung der Energiewende“ wurden zentrale Rahmenbedingungen für eine Beschleunigung des Rollouts intelligenter Messsysteme gestellt. Auf Basis der etablierten und umgesetzten BSI-Standards kann der Rollout nun beschleunigt fortgeführt werden.

Neben der Entwicklung von BSI-Standards für das SMGW unterstützt das BSI-Förderprojekte des BMWK und Regelsetzer im Rahmen von Standardisierungspartnerschaften. Gemeinsam mit den Stakeholdern entwickelt das BSI so die Standards im Sinne des GNDEW weiter und gestaltet auch in Zukunft die Digitalisierung der Energiewende.

Hier finden Sie die Einstiegsseite zum Thema Smart-Metering sowie die digitale Version dieser Broschüre:

Web:
www.bsi.bund.de/SmartMeter

Über diese E-Mail-Adresse können Sie mit dem BSI Kontakt aufnehmen:
smartmeter@bsi.bund.de

Impressum

Herausgeber
Bundesamt für Sicherheit
in der Informationstechnik (BSI)
53175 Bonn

E-Mail
bsi@bsi.bund.de

Internet
www.bsi.bund.de

Bezugsquelle
Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail
smartmeter@bsi.bund.de

Internet
www.bsi.bund.de/SmartMeter

Telefon
+49 (0) 22899 9582 – 0

Telefax
+49 (0) 22899 9582 – 5400

Stand
Juli 2023

Angaben zur Druckerei
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 3a
96277 Schneckenlohe

Internet:
www.ak-druck-medien.de

Texte und Redaktion
Bundesamt für Sicherheit
in der Informationstechnik (BSI)

Bildnachweis
Titel: AdobeStock ©lassedesignen;
S. 4, S. 8, 12, 16, 20, 24, 28, 30, 34:
AdobeStock ©deepagopi2011;
S. 5: AdobeStock ©XtravaganT;
S. 6: AdobeStock ©metamorworks;
S. 9, 13: ©BSI; S. 11: AdobeStock ©tl6781;
S. 21: AdobeStock ©vladimircaribb;
S. 22: AdobeStock ©vegefox.com;
S. 26: AdobeStock ©jijomathai;
S. 35: AdobeStock ©photolars

Artikelnummer
BSI-Bro23/332

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Als Cybersicherheitsbehörde des Bundes ist es Aufgabe des BSI, Deutschland digital sicher zu machen. Seit seiner Gründung 1991 hat sich das BSI zu einem Kompetenzzentrum für Fragen der Informationssicherheit entwickelt, dessen fachliche Expertise national und international anerkannt ist.

Für die Zukunft des Standorts Deutschland ist die Digitalisierung ein wesentlicher Erfolgsfaktor. Voraussetzung einer erfolgreichen Digitalisierung ist die Informationssicherheit. Deshalb beschäftigt sich das BSI damit, in welchen Anwendungsfeldern der Digitalisierung Risiken entstehen könnten und wie man diese Risiken kalkulierbar und beherrschbar machen kann.

Durch seine ausgeprägte Vernetzung nach innen und außen ist das BSI in der Lage, Know-how in den Bereichen Prävention, Detektion und Reaktion zu bündeln, Themen der Informationssicherheit fachlich zu analysieren und aus der Analyse heraus konkrete Angebote für unterschiedliche Zielgruppen in Staat, Wirtschaft und Gesellschaft abzuleiten. Das BSI nutzt dazu seine integrierte Wertschöpfungskette der Cybersicherheit, die von der Abwehr und Analyse von Cyberangriffen über Beratungsdienstleistungen und Zertifizierung bis hin zur Entwicklung sicherheitstechnischer Empfehlungen, Best Practices und Standards reicht.

Cybersicherheit und digitaler Verbraucherschutz

Die Digitalisierung kann nur gelingen, wenn Anwenderinnen und Anwender Vertrauen in neue Technologien entwickeln und diese zu ihrem Nutzen sicher einsetzen können. Im Rahmen des Digitalen Verbraucherschutzes verfolgt das BSI einen ganzheitlichen Ansatz: Hersteller von digitalen Produkten werden aufgefordert, diese bereits mit angemessenen Sicherheitseigenschaften auf den Markt zu bringen. Gleichzeitig sensibilisiert das BSI Privatanwenderinnen und -anwender für Risiken, damit sie selbstbestimmt Gefahren abwehren und souverän agieren können. Sie profitieren dabei von praxisgerechten und für Laien verständlichen Informationen und Handlungsempfehlungen für mehr Sicherheit im Internet, die das BSI auf seiner Webseite www.bsi.bund.de/VerbraucherInnen (siehe QR-Code) oder per Hotline unter 0800-2741000 bereitstellt. Bei der Umsetzung der Cybersicherheitsstrategie der Bundesregierung entwickelt das BSI derzeit zudem ein IT-Sicherheitskennzeichen, um künftig den Verbraucherinnen und Verbrauchern eine Einschätzung zur Cybersicherheit von IT-Produkten und -Services zu erleichtern.

Web:
www.bsi.bund.de/VerbraucherInnen

www.bsi.bund.de