Bundesamt
für Sicherheit in der
Informationstechnik

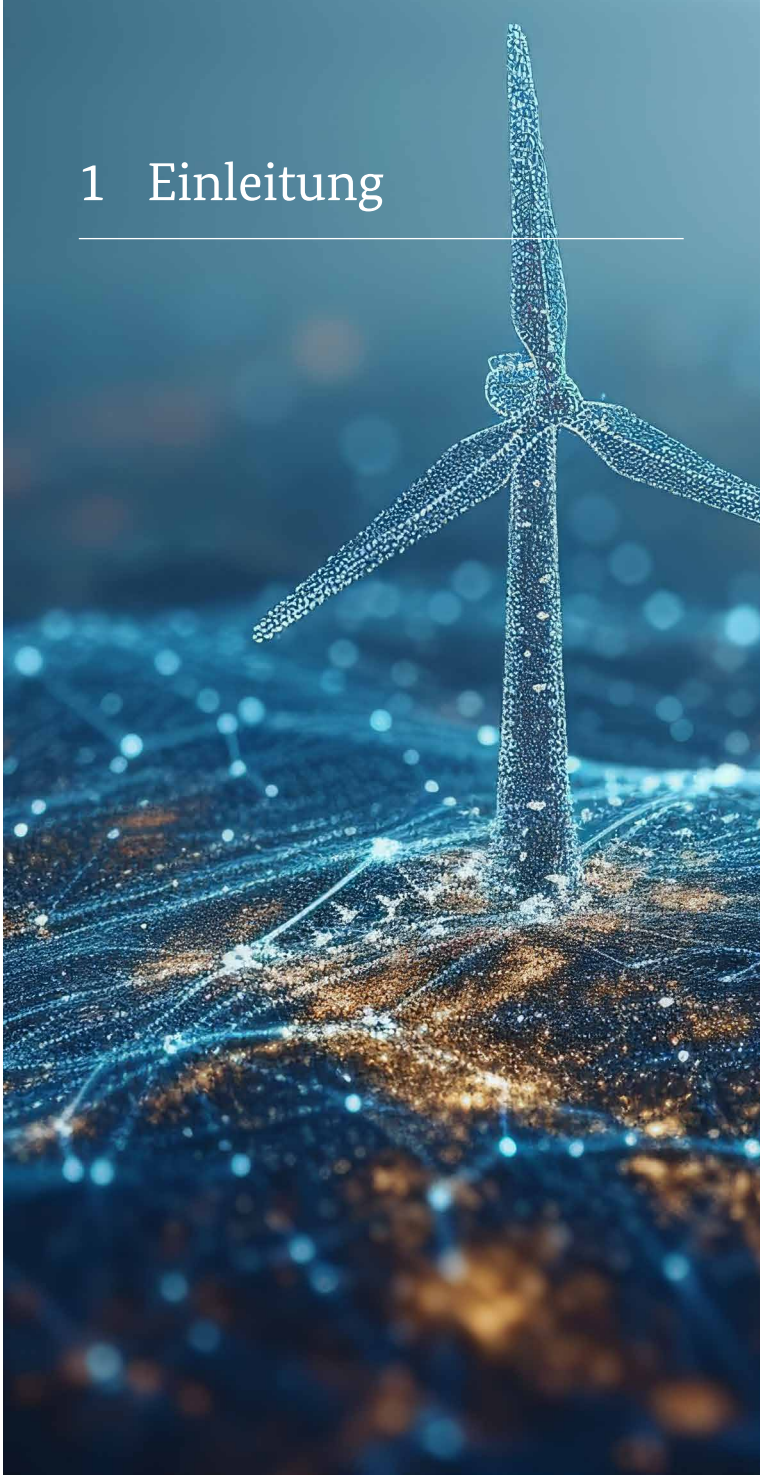
Deutschland
Digital•Sicher•BSI•

Smart-Meter-Gateway

Cybersicherheit für die Digitalisierung der Energiewirtschaft

Inhaltsverzeichnis

1 Einleitung



Die Energiewende steht im Zentrum der globalen Bemühungen zur Bekämpfung des Klimawandels. Die Digitalisierung der Energiewende spielt eine zentrale Rolle in dem Bestreben, die ehrgeizigen Klimaschutz- und Energiewendeziele zu erreichen.

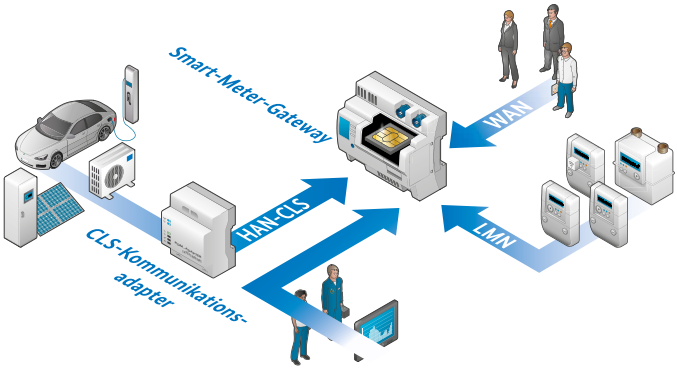
In Deutschland hat sich der Energiesektor stark gewandelt: Anstelle weniger großer Kraftwerke wird die Energieversorgung zunehmend durch zahlreiche kleine, dezentrale Erzeugungsanlagen wie Photovoltaikanlagen, Energiespeicher und flexible Verbrauchseinrichtungen im Verteilnetz bestimmt. Um eine optimale Abstimmung von Erzeugung und Verbrauch und die Vermeidung eines kostenintensiven Netzausbaus zu erreichen, müssen die dezentralen Erzeugungsanlagen in das intelligente Energienetz (Smart Grid) integriert werden. Ein leistungsfähiges Smart-Grid trägt damit erheblich zur Reduktion der CO_2-Emissionen im Energie-, Verkehrs- und Wärmesektor bei. Hierfür werden intelligente Messsysteme benötigt, um die heterogene Landschaft der Verteilnetze schrittweise zu standardisieren und zu digitalisieren. Durch die Verwendung von intelligenten Messsystemen – und die damit einhergehende 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. Smart-Meter-Gateways stellen dabei als dezentrale Kommunikationsplattform die Schlüsseltechnologie für die sichere Digitalisierung der Energiewende dar.

Um dem gestiegenen Bedrohungspotenzial durch Cyberkriminalität zu begegnen, spielt die frühzeitige Umsetzung von hohen Vorgaben an Datenschutz und zur IT-Sicherheit („Security & Privacy by Design“) eine entscheidende Rolle. Aufgabe und Anspruch des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist es, die Informationssicherheit in der Digitalisierung zu gestalten und zu gewährleisten, sodass die Anwenderinnen und Anwender von den Vorzügen innovativer Technologien profitieren können. Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWE) 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) verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen in unterschiedlichen Einsatzbereichen.

Nur wenn Staat, Wirtschaft sowie Bürgerinnen und Bürger auf den Schutz ihrer Daten vertrauen können, wird die digitale Transformation der Energiewirtschaft gelingen und deren Potenzial voll ausgeschöpft werden können.

2 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 im lokalen Heimnetz (HAN) verbindet.

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

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 den sicheren Betrieb verantwortlich. Er muss u. a. das kryptografische 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)

Das HAN ist rollenbasiert in die Bereiche HAN-CLS (Dienste für angeschlossene Geräte, M2M-Kommunikation) und HAN-CON (Dienste für Anschlussnutzer und Servicetechniker) geteilt.

Im HAN-CLS kommuniziert das SMGW mit lokalen Kommunikationspartnern zur Anbindung von Energieverbrauchs- und Erzeugungseinrichtungen wie z. B. Wärmepumpen, Wechselrichtern von Photovoltaikanlagen, Ladeeinrichtungen für E-Fahrzeuge, Energiemanagementsystemen (EMS) sowie Ausstattungen zur Verbrauchserfassung (Datenkonzentratoren für Heizkostenverteiler). Diesen Geräten kann beispielsweise

eine synchronisierte Zeit oder zur Eigenverbrauchsoptimierung benötigte Messwerte bereitgestellt werden. Ebenso wird berechtigten externen Marktteilnehmern der Zugriff für Steuerungs- und Fernwartungszwecke ermöglicht. Das SMGW stellt hierfür einen sicheren, transparenten Kanal (TLS-Proxy-Kanal) zur Verfügung, welcher nur durch den Gateway-Administrator konfiguriert werden kann.

Die HAN-CON-Schnittstelle ermöglicht es einem Servicetechniker, wichtige Informationen über den Systemzustand des SMGW in Erfahrung zu bringen. Diese werden benötigt, um im Fehlerfall die lokale Diagnostik und Entstörung durchführen zu können. Aus Datenschutzgründen hat der Servicetechniker dabei keinen Zugriff auf die im SMGW hinterlegten Messwerte bzw. mandantenspezifischen Daten. Darüber hinaus kann der Anschlussnutzer über HAN-CON seine Verbrauchs- und ggf. Einspeisewerte abfragen. Er kann hierzu ein geeignetes Endgerät anschließen und erhält nach erfolgreicher Authentifizierung lesenden Zugriff auf die Daten. Durch die Interoperabilitätsvorgaben der TR-03109-1 werden die Daten künftig in einem einheitlichen Format bereitgestellt, was eine Weiterverarbeitung in Smart-Home-Systemen ermöglicht.

3 Smart-Meter-Gateway – Schutzprofil Version 2.0

Das Schutzprofil Version 2.0 (BSI-CC-PP-0073-V2) beschreibt mögliche Bedrohungen eines SMGW in seiner Einsatzumgebung und definiert die Mindestanforderungen an Sicherheitsfunktionen, die durch das SMGW gewährleistet werden müssen.

Der Aufbau eines Schutzprofils ist in den international gültigen Common Criteria (CC) geregelt. Auf Basis eines Schutzprofils erhalten Hersteller zunächst generische Vorgaben dazu, welche Funktionen ihre Produkte bereitstellen müssen, und erhalten genügend Spielraum für dessen Umsetzung. Sie konkretisieren diese Vorgaben in Form ihres Produkts und können dieses nach Common Criteria evaluieren lassen. Nach einer positiven Evaluation wird mittels eines Zertifikates bescheinigt, dass das Produkt nachweislich die beschriebenen Sicherheitsanforderungen und das Schutzziel erfüllt.

Das Schutzprofil für das SMGW basiert auf dem aktuellen Stand der CC, 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 in unterschiedlichen Einbauorten (Einfamilienhaus, Wohnungsgesellschaften etc.) ein einheitlicher, hoher Sicherheitsstandard gewährleistet ist, und stellt im Fall von neuen technischen Möglichkeiten eine kontinuierliche Weiterentwicklung der Produkte sicher.

3.1 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.

Hierbei ist zu berücksichtigen, ob ein SMGW nur die Daten eines Netzanschlusses erfasst und dessen Steuerung absichert (beispielsweise in einem Einfamilienhaus) oder ob die Daten mehrerer Netzanschlüsse erfasst und die Steuerung von Anlagen mehrerer Netzanschlüsse abgesichert wird.

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.

3.2 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.

3.3 Steuerung durch das SMGW

Neben der Erfassung der Messwerte und der Absicherung der Kommunikation zu steuerbaren Verbrauchern (beispielsweise Wärmepumpen, Wallboxen oder PV-Anlagen) erlaubt das Schutzprofil optional auch eine Steuerung von Verbrauchern durch das SMGW selbst. Sofern Hersteller diese Funktion in ihrem SMGW bereitstellen, enthält das Schutzprofil sogenannte Funktionspakete, welche die hierfür zusätzlich erforderlichen Sicherheitsfunktionen des SMGW definieren.

3.4 Anbindung von RLM-Zählern

Das neue Schutzprofil ermöglicht die Anbindung von RLM-Zählern. Zusätzlich zu einer Anbindung über LMN ist übergangsweise auch eine Anbindung an der HAN-Schnittstelle unter Nutzung des TLS-Proxy-Kanals zulässig.

3.5 Bereitstellung von Daten am HAN

Neben den oben genannten Funktionen bietet das SMGW einen Service zur Zeitsynchronisation, zur Erstellung von kryptografischen Schlüsseln und zum Abruf von Messwerten über eine API an. Das Schutzprofil erlaubt die entsprechenden Informationsflüsse und ermöglicht so Steuerungseinrichtungen, RLM-Zählern und weiteren CLS-Produkten die verbesserte Nutzung der Services des SMGW.

3.6 Optimierung Sichere Lieferkette

Um Messstellenbetreibern die Ausgestaltung der sicheren Auslieferungen unabhängig von den Vorgaben der SMGW-Hersteller zu ermöglichen, ist im Schutzprofil der Übergang der Verantwortung für die sichere Auslieferung entsprechend modelliert worden. Ab Erhalt der SMGW trägt der MSB die Verantwortung für die sichere Auslieferung von SMGW und muss diese mit angemessenen Sicherheitsmaßnahmen absichern.

Damit trotzdem über alle MSB ein vergleichbares Sicherheitsniveau bei der Auslieferung erreicht werden kann, hat das BSI gemeinsam mit der Projektgruppe PG SiLKe des Forums Netztechnik/Netzbetrieb im VDE (FNN) einen „Anforderungskatalog zur MSB-Lieferkette“ erarbeitet. Dieser BSI-Katalog wurde in das Schutzprofil Version 2.0 referenziert.

MSB müssen zukünftig die Anforderungen aus dem Dokument in ein individuelles Sicherheitskonzept überführen und können damit ihrer neuen Verantwortung gerecht werden. Im Fokus stehen Prozesse ab Übernahme der SMGW durch den MSB vom Hersteller bis zur Montage an der Messstelle. Die Demontage zur Wiederverwendung von SMGW durch eine Monteurin oder einen Monteur im Auftrag des MSB ist ebenfalls Teil der Betrachtung.

Die bisherigen bereits zertifizierten Lieferketten nach altem Schutzprofil Version 1.3 sind weiterhin gültig und können weiterhin genutzt werden.

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

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

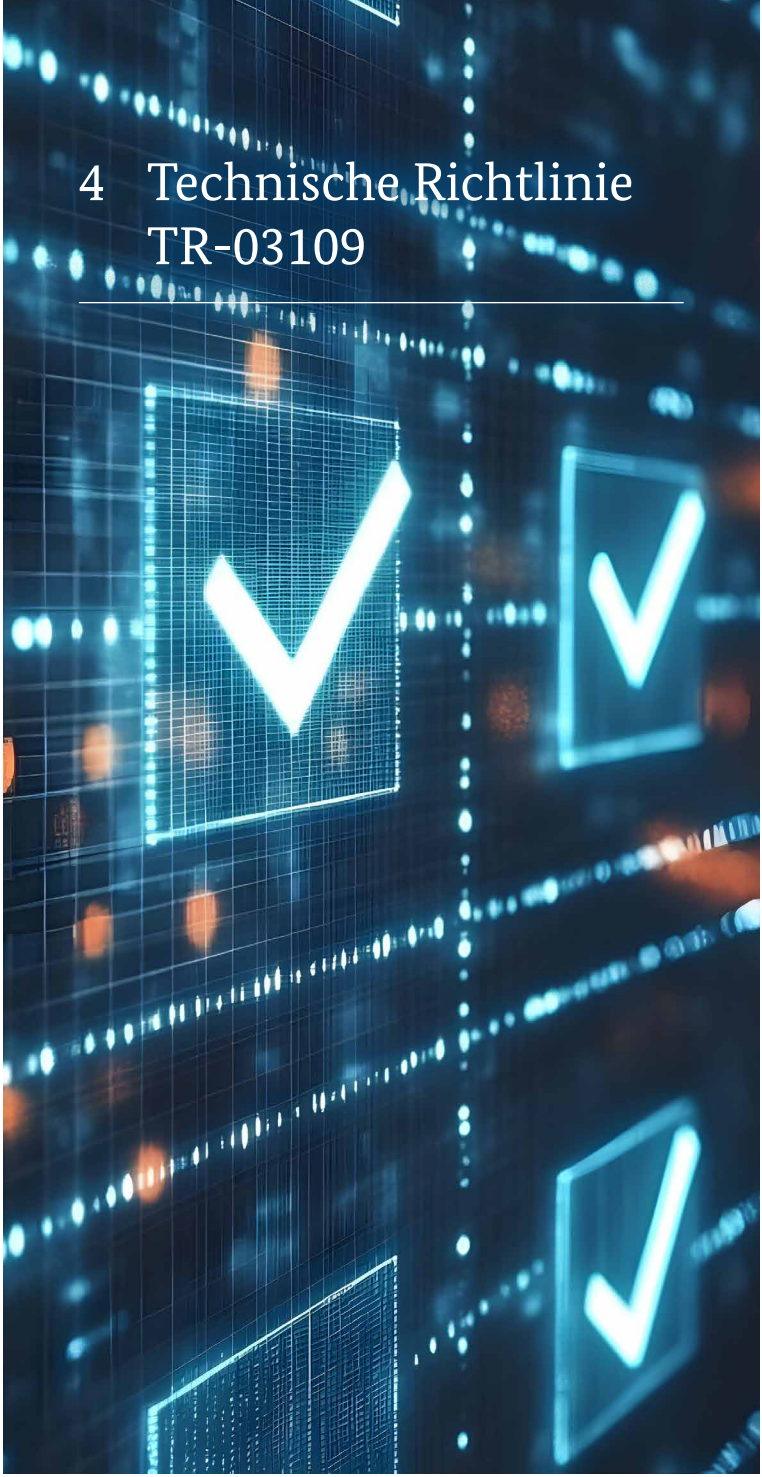
3.7 Zertifizierungsverfahren

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, ist unter dem nachfolgenden QR-Code abrufbar:

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

4 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. Smart-Metering-Public-Key-Infrastruktur (SM-PKI) oder dem Gateway-Administrator.

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

Der 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 der Schlüssel- und Zufallszahlengenerierung unterstützt. Zudem dient das Sicher-

heitsmodul 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, sind in der Technischen Richtlinie TR-03109-2 enthalten.

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

Im Teil 3 der Technischen Richtlinie wird definiert, welche kryptografischen Verfahren oder Schlüssellängen im SMGW und in dessen unmittelbarem Umfeld zum Einsatz kommen. Dieser basiert u. a. auf den BSI-Richtlinien TR-02102 „Kryptografische Verfahren: Empfehlungen und Schlüssellängen“ und TR-03111 „Elliptische-Kurven-Kryptografie“.

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 sogenannten 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.

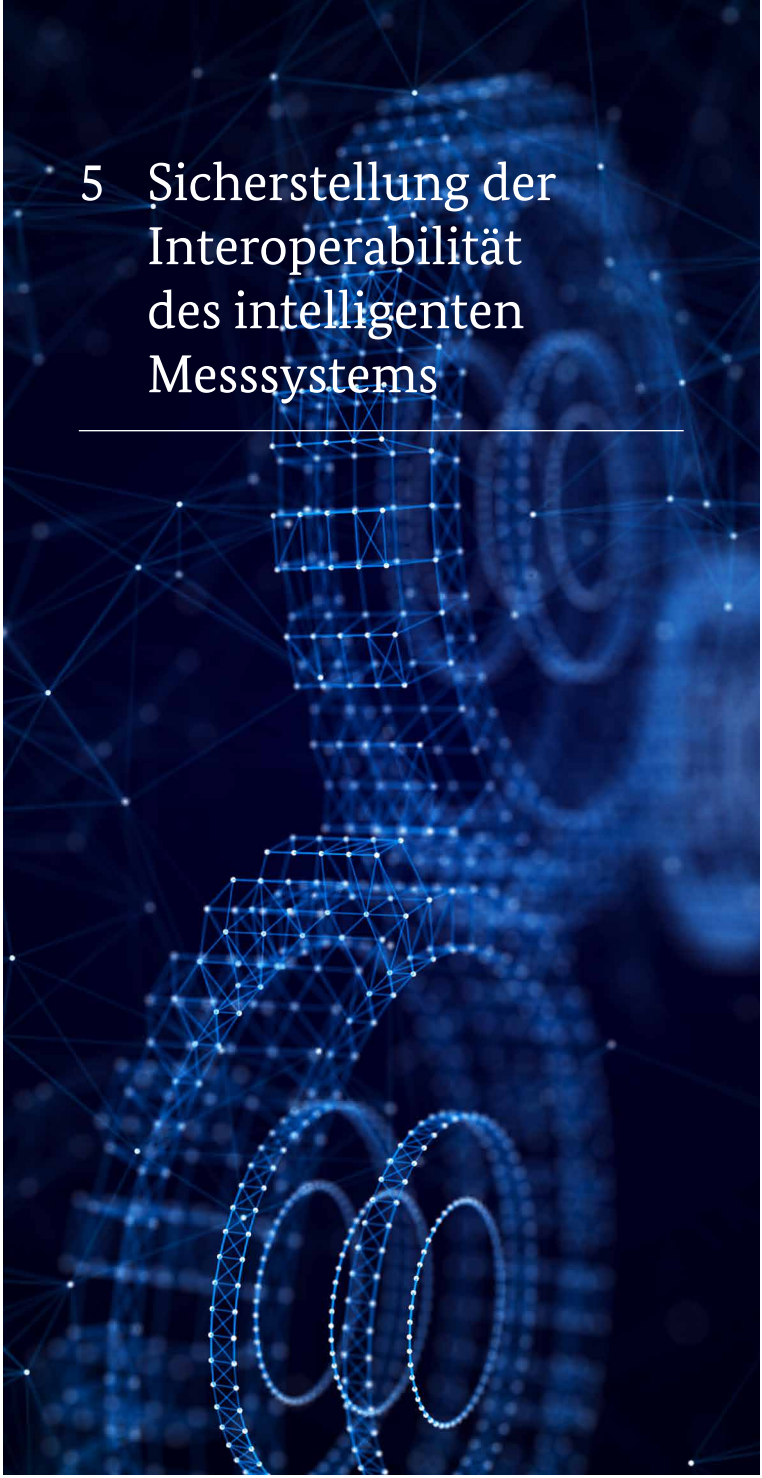
Die TR-03109-5 kann somit das Vertrauen in die Infrastruktur rund um das intelligente Messsystem steigern und die Risiken von Angriffen auf diese HAN-Komponenten minimieren. Der Nachweis zur Einhaltung der Anforderungen erfolgt über Zertifizierungsverfahren des BSI. Der Nachweis der Interoperabilität erfolgt über eine Konformitätsbewertung nach Technischer Richtlinie und ist immer notwendig. Bei Vorhandensein weiterer IT-Schnittstellen ist zusätzlich der Nachweis der IT-Sicherheit notwendig. Dieser erfolgt über die sogenannte Beschleunigte Sicherheitszertifizierung (BSZ).

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

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 Mindestinteroperabilität an das SMGW sowie an weitere technische Komponenten, wie z. B. das im SMGW verbaute Sicherheitsmodul und an angeschlossene CLS-Kommunikationsadapter. Durch diese Festlegungen wird sichergestellt, dass sich beim Austausch eines SMGW (auch durch ein SMGW eines anderen Herstellers) die umliegenden Komponenten wie Zähler, steuerbare Einrichtungen oder Backend-Systeme zur Administration weiterverwenden lassen.

Bei der Weiterentwicklung steht das BSI im kontinuierlichen Abstimmungsprozess mit den beteiligten Akteuren der Energiewirtschaft. Im Sinne eines kontinuierlichen Verbesserungsprozesses müssen daher iterativ Anforderungen beschrieben, in der Praxis erprobt und unter Berücksichtigung der Erfahrungswerte weiter verfeinert werden.

Den Wert einheitlicher Anwendungsprogrammierschnittstellen (API) gerade im Hochlauf des Steuerungsrollouts hat der Gesetzgeber im Zuge der Novellierung des MsbG im Rahmen des Gesetzes zum Neustart der Digitalisierung der Energiewende (GNDEW) hervorgehoben und das BSI mit der entsprechenden Standardisierung beauftragt.

Mit der TR-03109-1 in Version 2.0 wurden die HAN- und WAN-API des SMGW erweitert, vereinheitlicht und verpflichtend gefordert. Neben der lokalen Visualisierung und Verarbeitung von Echtzeitdaten aus den angeschlossenen Messeinrichtungen (z. B. zur Eigenverbrauchsoptimierung)

wird auch der Anschluss und Betrieb von Steuerungs- und Submetereinrichtungen an die HAN-CLS-Schnittstelle des SMGW deutlich vereinfacht und optimiert.

Mit der Vereinheitlichung der WAN-Schnittstelle werden für Betreiber von SMGW Integrations- und Wechselprozesse ebenso erheblich vereinfacht und insgesamt wirtschaftlicher.

Zudem wird das SMGW als zentrale Plattform weiter gestärkt, indem die Erfassung von Messwerten der Sparten Elektrizität, Gas, Wasser und Thermische Energie über die LMN-Schnittstelle unter Berücksichtigung von Datenschutz und -sicherheit ermöglicht wird.

Die Anforderungen der TR-03109-1 werden mittels funktionaler Testfälle überprüft. In Konformitätsbewertungsverfahren (der sogenannten TR-Zertifizierung) wird die Einhaltung der Anforderungen von einer unabhängigen Prüfstelle überprüft und vom BSI abschließend bescheinigt.

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.

Im Rahmen der Zertifizierungen nach TR-03109-5 konnte die Testplattform bereits erfolgreich eingesetzt und evaluiert werden. Im Schnitt konnten Zertifizierungsverfahren im Vergleich zur herkömmlichen Prüfung in ca. einem Viertel der Zeit durchgeführt werden.

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

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.

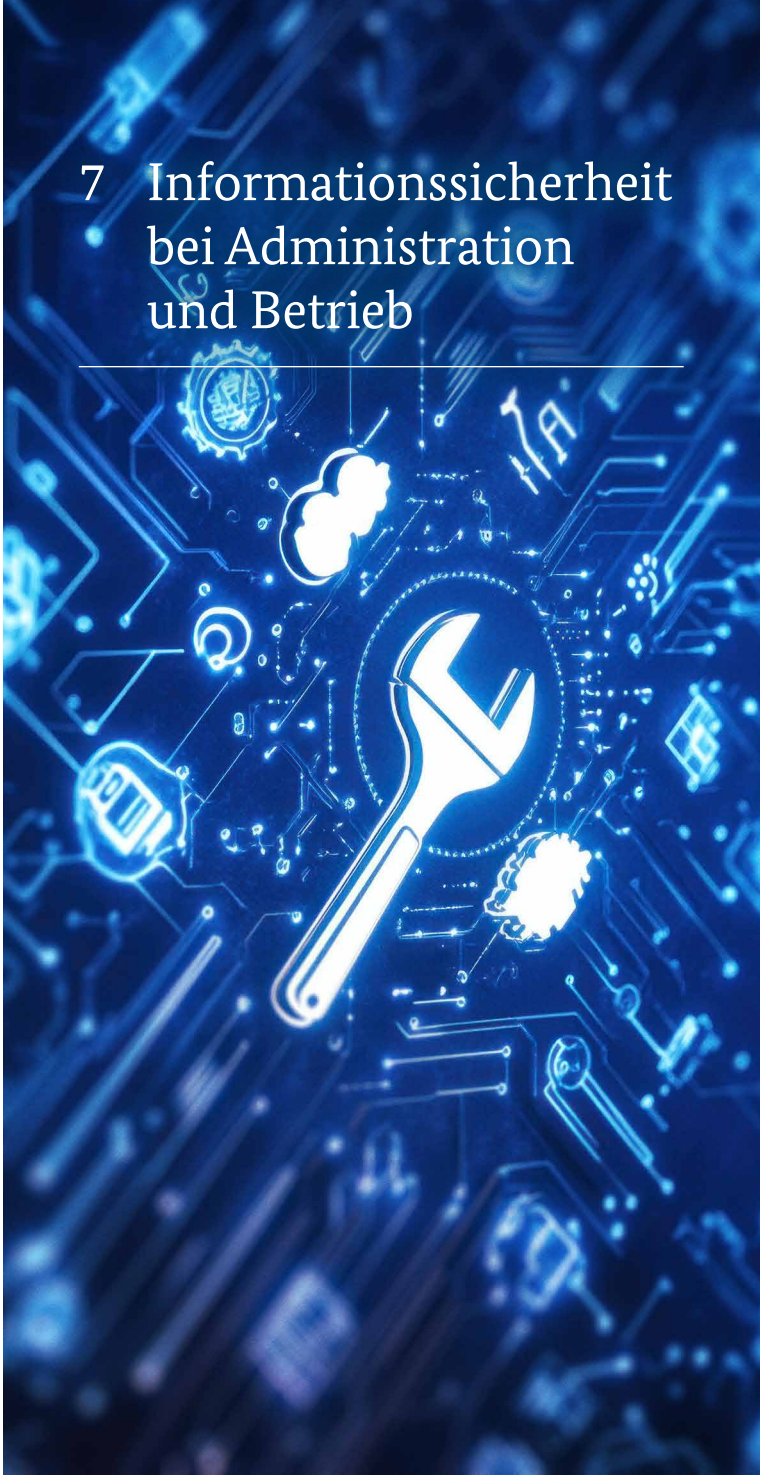
Das BSI ist Inhaber des Wurzelzertifikats der SM-PKI und für den Betrieb der Root-CA (Certificate Authority) verantwortlich. Das Wurzelzertifikat der SM-PKI ist der Vertrauensanker der Smart-Meter-Gateway-Infrastruktur. Die Root-CA setzt die gesetzlichen Anforderungen auf technischer Ebene durch und 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 Realbedingungen 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



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 Branchenkonsultation der BSI-Standards

Für eine zukunfts- und zielorientierte Weiterentwicklung der BSI-Standards setzt das BSI auf eine enge Zusammenarbeit mit Stakeholdern der Branche und steht in engem fachlichem Austausch mit u. a. Verbänden, Regelsetzern, Partnerbehörden und verschiedenen Marktakteuren.

Über die BSI-Branchenkonsultation werden aktuelle Entwürfe der Standards den Branchenexpertinnen und Branchenexperten vorgestellt, wertvoller Input für die Weiterentwicklung der Standards für das intelligente Messsystem erfasst und konsolidiert. Am Ende wird der finale zwischen der Branche und dem BSI konsolidierte Entwurf zur Abstimmung an den Ausschuss Gateway-Standardisierung bereitgestellt.

Im Zuge der Weiterentwicklung der Standards zur Integration des Brancheninputs setzt das BSI neben den eigenen Standardisierungsvorhaben auch auf gemeinsame Vorhaben innerhalb von Standardisierungspartnerschaften mit Regelsetzern. Ziel dieser Partnerschaften ist die jeweils gegenseitige Unterstützung bei Standardisierungsvorhaben, die sowohl die sicherheitstechnischen Vorgaben des BSI als auch die technischen Anforderungen der Branche berücksichtigt. Beispiele für die erfolgreiche Zusammenarbeit sind die Optimierung der sicheren Lieferkette (FNN), die Entwicklung der WAN-API (DKE), die Entwicklung von Vorgaben zur sicheren Anbindung von Gaszählern an das SMGW (DVGW) und die Integration der BSI-Vorgaben in den EEBus-Standard (EEBus-Initiative).

Um die Zukunft der Digitalisierung der Energiewende aktiv mitzugestalten, begleitet das BSI zudem Förderprojekte des BMWE (Digitalisierung von Energienetzen – DigENet). Von besonderem Interesse ist hierbei die Erforschung von neuen und innovativen Ansätzen zur Weiterentwicklung der SMGW-Infrastruktur. Das BSI steht dabei den Projekten als fachlicher Ansprechpartner beratend zur Seite und profitiert wiederum von den Projekten als Inputgebern für den Weiterentwicklungsprozess der BSI-Standards.

Zukünftig soll die Rollout-Begleitung bei der Umsetzung der BSI-Standards weiter intensiviert werden. Ziel des BSI ist es dabei, den Rollout zu unterstützen und Fragen bei der Umsetzung schnellstmöglich zu beantworten.

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

Web:
https://bsi.bund.de/dok/Branchenkonsultation

9 Fazit

Die beschleunigte Umsetzung einer umfassenden und sicheren Digitalisierung ist maßgeblich für den Erfolg der Energiewende. In vielen Regionen Deutschlands werden zertifizierte Smart-Meter-Gateways als Schlüsseltechnologie fortlaufend erfolgreich installiert und liefern bereits wertvolle Daten zur Optimierung der Energienutzung. Bis 2032 wird ein enormer Anstieg der Einbaufälle auf ca. 27 Mio. intelligente Messsysteme prognostiziert. Bereits Ende 2024 konnte das millionste Smart-Meter-Gateway installiert werden.

Die entwickelten Vorgaben des BSI an Produktkomponenten (Smart-Meter-Gateway mit integriertem Sicherheitsmodul und CLS-Komponenten), deren sicherer IT-Betrieb (Administration) und die vertrauenswürdige Kommunikationsinfrastruktur (Smart-Metering-PKI) sowie die Prüfung der Einhaltung der Vorgaben im Rahmen von Prüf- und Zertifizierungsverfahren gewährleisten Datenschutz und -sicherheit und bilden somit die Grundlage für eine sichere Infrastruktur.

Bei der Fortentwicklung bestehender BSI-Standards setzt das BSI auf den direkten Austausch und die enge Kooperation mit der Branche. Alle zu veröffentlichenden Standards werden im engen fachlichen Austausch mit wichtigen Stakeholdern der Branche abgestimmt. Zudem arbeitet das BSI partnerschaftlich mit Regelsetzern an der gemeinsamen Umsetzung von Standardisierungvorhaben zusammen. Darüber hinaus gestaltet das BSI aktiv die zukunftsorientierte, innovative Weiterentwicklung des SMGW durch die Begleitung von Forschungsprojekten des BMWE mit.

Gemeinsam mit Akteuren der Energiewirtschaft aus Politik, Wissenschaft, Wirtschaft und den Verbraucherinnern und Verbrauchern kann die Energiewende erfolgreich vorangebracht und eine nachhaltige, cyberresiliente und effiziente Energiezukunft in Deutschland vorausschauend gestaltet werden. Deutschland ist damit auf dem besten Weg, Vorreiter für die Digitalisierung der Energie-, Wärme- und Verkehrswende in Europa zu werden.

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

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.

Die Digitalisierung ist für die Zukunft des Standorts Deutschland ein wesentlicher Erfolgsfaktor. Deshalb beschäftigt sich das BSI damit, in welchen Anwendungsfeldern der Digitalisierung Risiken für die Informationssicherheit 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 und Themen der Informationssicherheit fachlich zu analysieren. Aus der Analyse heraus werden konkrete Angebote für unterschiedliche Zielgruppen in Staat, Wirtschaft und Gesellschaft abgeleitet. 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. Dazu kann das IT-Sicherheitskennzeichen beantragt werden, das Transparenz für Verbraucherinnen und Verbraucher schafft, indem es die grundlegenden Sicherheitseigenschaften von IT-Produkten erkennbar macht. 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.

Web:
www.bsi.bund.de/VerbraucherInnen

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 87
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
Januar 2025

Artikelnummer
BSI-SMGW25/001

Angaben zur Druckerei
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 3a
96277 Schneckenlohe
www.ak-druck-medien.de

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

Bildnachweis
Titel: AdobeStock © SirinPorn
S. 2: AdobeStock © Ben
S. 4/5: AdobeStock © Maxim Zaikov
S. 6: AdobeStock © Ian
S. 9: AdobeStock © Dabarti
S. 10: AdobeStock © Ashi
S. 16: AdobeStock © queen
S. 20: AdobeStock © Dmitry
S. 22: AdobeStock © alphaspirit
S. 24: AdobeStock © buraratn
S. 26/27: AdobeStock © Pixel Matrix
S. 28: AdobeStock © Anak
S. 30: AdobeStock © Andrei
S. 32/33: AdobeStock © Funtap
S. 34: AdobeStock © panumas
S. 35: AdobeStock © vegefox.com

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

www.bsi.bund.de