4.3 Blaupause 7: IT-Sicherheit in der Energiewirtschaft

Blaupause	
Zielgruppen	KRITIS-Betreiber, ÜNB, VNB, VK-Betreiber, Komponenten-Entwickler
Ausgangslage und Problemstellung	Bedingt durch die neuen digitalen Kontrollstrukturen, die das digitalisierte Stromnetz mit sich bringt, als auch vor allem durch Steuereingriffe, die nicht mehr vor Ort physisch erfolgen müssen, sondern remote durch ein System getriggert, freigegeben, durchgeführt und quittiert werden, besteht die Gefahr, nicht nur von Fehlhandlungen von Systemen oder Betriebsführenden, sondern auch durch mögliche Angriffe. Dabei existieren verschiedene Arten von Angriffen, die durchaus unterschiedliche Fähigkeiten und finanzielle Möglichkeiten besitzen (vgl. TAB, 2010). Ziel ist es, wie am Beispiel SMGW klar zu erkennen, hier eine sichere Infrastruktur mit hohem Sicherheitsniveau aufzubauen.
Lösungsansatz	Es wurden neben dem iMSys und dem SMGW-Ökosystem auch zahlreiche weitere Lösungen zur Umsetzung von IT-Sicherheit in den SINTEG-Schaufenstern erprobt. Während der Laufzeit wurde bei vielen Konsortialpartnern ein ISMS nach ISO/IEC 27019 eingeführt, Sicherheitsanalysen für die neuen Systeme durchgeführt und / oder Angriffsvektoren analysiert, um die Systeme zu härten.
Einordnung der Blaupause	Blaupause in der Kategorie „IKT-Systemqualität von Smart Grids“
Technologiereifegrad (Spektrum der Detail-Blaupausen)	 Die vielfältigen Maßnahmen und Technologien erreichen unterschiedliche TRL. Jedoch erreichen alle einen TRL zwischen 6 und 9.
Eingeflossene SINTEG-Aktivitäten	■ Holistisches Zellenkonzept: IT-Sicherheit durch Standardisierung ■ CC EAL 4 Zertifizierung der kritischen Infrastruktur ■ Entwicklung eines ganzheitlichen ISMS-Konzepts ■ Erweiterung der IEC 62559 Use Case-Methodik um Assurance Cases ■ Schichtenmodell für die IT-Sicherheitsanalyse in der Energiewirtschaft ■ Schulungskonzept für das ISM in dezentralen und vernetzten Versorgungssystemen ■ Analyse und Auswertung von rechtlichen Rahmenbedingungen und Gefährdungsszenarien (Digitalisierungsstudie)
Innovationsgehalt	In SINTEG wurden bestehende Maßnahmen aus anderen Branchen, etwa ICS (Industrial Control Systems) oder des ISO/IEC 27001-Standards, aber auch neuartige Maßnahmen sowohl innerhalb der IT- als auch der Netzinfrastruktur auf verschiedenen Ebenen erstmals untersucht, entwickelt und / oder erprobt.
Bedingungen für die Übertragbarkeit und Skalierbarkeit	Allgemein wird das Thema IT-Sicherheit durch das Schaffen einer Sicherheitskultur, der Etablierung von Security-by-Design als Paradigma sowie der Aufmerksamkeit der Management-Ebene für das Thema gefördert. Konkretere Rahmenbedingungen sind die Awareness für das Thema Cyber Security, die Etablierung von Risikomanagement als Prozess, die Erfassung und Bewertung von Assets, die Bewertung von Angriffsszenarien, sowie eine Post-Mortem Analyse von Angriffen und eine Kultur des Teilens von Wissen.

HINTERGRUND UND PROBLEMSTELLUNG

Die Einführung eines hohen Sicherheitsniveaus und Umsetzung der NIS-Directive oder der ISO 27019 und eines verpflichtenden ISMS verursacht hohe Aufwände und Kosten, die selbstverständlich in einem geeigneten Risikomanagement abgewogen werden müssen.

Netzverbundpartner, wie etwa die Schweiz, setzten hier, anders als Deutschland bisher, auf einen eher subsidiären Ansatz der Branche. Schweizer Stromversorger sind gemäß einer aktuellen Umfrage des Bundes nur ungenügend gegen Cyberattacken geschützt (vgl. Mäder, 2021). Besonders schlecht seien die Firmen darauf vorbereitet, Angriffe zu erkennen und auf Vorfälle zu reagieren. Die Resultate der erstmaligen Umfrage dieser Art bei 124 Unternehmen verschiedener Größe seien im Schnitt „ernüchternd", schreibt das Bundesamt für Energie (BFE) in einem Bericht zur Cybersicherheit für die Schweizer Stromversorgung von Ende Juni. Auf einer Skala von 0 bis 4 punkto Cybersicherheit erreichten die Unternehmen einen Wert von knapp unter 1. Die Branche strebe eigentlich mit selbst verabschiedeten Minimalrichtlinien einen Wert von 2,6 an, so der Bericht. Von den befragten Unternehmen betrieben 113 Netze, 79 führten Messstellen und 54 produzierten Strom. Dies erlaubt die ableitende Schlussfolgerung, dass es für die in Deutschland früh ergriffenen Maßnahmen sinnvoll wäre, wenn diese im Kontext des Security-by-Design-Prinzips schon frühzeitig in aktuelle Forschungsthemen als Kernentwurfseigenschaften eingefordert werden.

Nach § 11 Absatz 1 EnWG müssen Betreiber von Energieversorgungsnetzen ihr Netz sicher betreiben. Der Betrieb eines sicheren Energieversorgungsnetzes umfasst nach § 11 Absatz 1a EnWG auch den angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Ein angemessener Schutz liegt gemäß § 11 Absatz 1a S. 4 EnWG vor, wenn ein von BNetzA und BSI erstellter Katalog an Sicherheitsanforderungen vom Betreiber eines Energieversorgungsnetzes eingehalten wird.[9] Kernforderung des Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001 sowie die Zertifizierung durch eine unabhängige, hierfür zugelassene Stelle (vgl. BNetzA, 2015).

Daneben sind Betreiber von Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind und als kritische Infrastruktur nach BSI-Kritis-V eingestuft sind, nach § 11 Absatz 1b EnWG verpflichtet, einen für sie geltenden IT-Sicherheitskatalog umzusetzen.[10]

Kernforderung ist auch hier die Einführung eines ISMS gemäß DIN ISO/IEC 27001.[11] Die Umsetzung der Zertifizierung musste bis zum 31.3.2021 erfolgen (vgl. BNetzA, 2018: S. 19).

Anlagen oder Systeme zur Steuerung bzw. Bündelung elektrischer Leistung (Aggregationsanlagen oder auch virtuelle Kraftwerke), die nicht von Betreibern von Energieversorgungsnetzen eingesetzt werden, fallen dagegen nicht in den Anwendungsbereich des IT-Sicherheitskatalogs nach § 11a oder § 11b EnWG. Für sie gilt ein branchenspezifischer, vom BDEW erstellter IT-Sicherheitsstandard für „Anlagen zur Steuerung/Bündelung elektrischer Leistung" (B3S) (vgl. BDEW, 2021). Das BSI hat den Sicherheitsstandard anerkannt. Entsprechend müssen Betreiber solcher Anlagen einen Nachweis gegenüber dem BSI erbringen, dass der Stand der Technik hinsichtlich IT-Sicherheitsanforderungen umgesetzt wurde. Zu diesem Zweck beschreibt u. a. die Technische Richtlinie (TR) 03109-1 V1.01 des BSI die minimalen Anforderungen an die ***dezentrale Messwertverarbeitung*** sowie -übermittlung von Smart Meter Gateways (SMGW) in 13 sogenannten Tarifanwendungsfällen (TAF) (vgl. BSI, 2021).

9 BNetzA, IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG, August 2015, hier abrufbar: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf [11.11.2021].

10 Gemäß § 8 Abs. 3 Nr. 2 BSIG besteht die Pflicht zur Umsetzung des § 11 EnWG nur für Netzbetreiber und Energieanlagenbetreiber.

11 BNetzA, IT-Sicherheitskatalog gemäß § 11 Absatz 1b EnWG, Dezember 2018, S. 12, hier abrufbar: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf [11.11.2020].

IN SINTEG AUFGEZEIGTE LÖSUNGSANSÄTZE UND ERKENNTNISSE

In SINTEG wurde u. a. untersucht, inwiefern die ersten in Deutschland zertifizierten sowie (noch) nicht zertifizierten SMGWs die Anforderungen an die TR 03109-1 V1.01 erfüllen. So sind SMGW in der Smart Meter-Public Key Infrastruktur (SM-PKI) unter anderem zur Erprobung von TAF[12] 9 und 10 in der Smart Meter-Test Public Key Infrastruktur (SM-Test-PKI) eingesetzt und zusammen mit verschiedenen Steuerboxen getestet worden – unter anderem über den Controllable Local Systems-Kanal (CLS-Kanal) des SMGW.

Best Practice-Ansätze im Bereich Smart Meter haben sich bislang noch nicht gezeigt. Der Einsatz von zertifizierten intelligenten Messsystemen (iMSys) in der SM-PKI konnte aufgrund des erst in 2020 erfolgten Beginns des Rollouts im Rahmen von SINTEG nicht wie geplant stattfinden. Das Ziel des SINTEG-Programms, unter anderem SMGWs, Kommunikationseinheit eines iMSys, in der Praxis zu erproben, ist in den Schaufenstern dennoch teilweise verwirklicht worden. So wurden bspw. zunächst unzertifizierte SMGWs ausgerollt, sodass bereits frühzeitige Feldtests erfolgen konnten und die Erfahrungen in die späteren Feldtests mit zertifizierten SGMWs einfließen konnten, sobald diese im letzten Projektjahr verfügbar waren.

BEISPIELE AUS DEN SCHAUFENSTERN

In den SINTEG-Schaufenstern konnten erste erfreuliche Testergebnisse zur Erprobung von TAF 9 und 10 sowie zur Anbindung der Steuerbox über den CLS-Kanal des Gateways gesammelt werden. Die vielfach geforderte Umsetzung des TAF 9, der die Ist-Einspeisung von Erzeugungsanlagen im 60-Sekunden-Takt betrifft, wurde sowohl bei Erzeugungsanlagen als auch bei einer Verbrauchsanlage in der SM-Test-PKI getestet. Die derzeit zertifizierten SMGWs sind zwar bislang nicht standardmäßig TAF 9-fähig, können jedoch nach Aussage des BSI und der Hersteller der iMSys durch ein Softwareupdate nachträglich auf das SMGW aufgespielt werden. Auch das nachträgliche Softwareupdate ist bei der Verbrauchsanlage auf einem Testgerät erfolgreich durchgeführt worden. Die 60-Sekunden-Werte kommen zuverlässig am Zielpunkt an. Die Tests haben darüber hinaus gezeigt, dass TAF 9 grundsätzlich auch bei Verbrauchsanlagen funktioniert.

Obwohl der Test von TAF 9 an den 20 Erzeugungsanlagen (PV-Anlagen) in einem innerhalb von SINTEG betriebenen Flexmarkt und die Installation des Softwareupdates nicht mehr im Rahmen von SINTEG realisiert wurde, konnte die Steuerbox bzw. deren Ansteuerung, die über die CLS-Verbindung an das SMGW angeschlossen ist, bereits erfolgreich getestet werden. Die Ansteuerung der Steuerbox und die Nutzung der CLS-Verbindung funktionierte in dem bisherigen Testumfang zuverlässig. Als Fazit des hier durchgeführten Feldversuchs kann festgehalten werden, dass der technische und prozessuale Durchstich unter Anwendung der Test-PKI erfolgreich war.

In den Schaufenstern wurden darüber hinaus in Hinblick auf die Funktionalitäten der SMGWs und des Rollouts gemischte Erfahrungen gemacht. Während der Diskussion in der AG Rechtsrahmen stellte sich dabei keine eindeutige Position heraus. Einzelne Teilnehmer gaben an, dass nicht alle Funktionalitäten der SMGWs, die das MsbG und die BSI TR vorsehen, in den Projekten getestet werden konnten. Am ehesten lässt sich daher das Ergebnis zu Erfahrungen mit dem Einsatz der verwendeten Messtechnik, neben den bereits dargestellten Ergeb-

12 Gemäß BSI TR-03109-1 „Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“ Version 1.0.1:
- TAF 9: Abruf der Ist-Einspeisung einer Erzeugungsanlage.
- TAF 10: Abruf von Netzzustandsdaten.

nissen, wie folgt beschreiben: Die Schaufenster haben wertvolle Erkenntnisse bei der Integration der ersten zertifizierten SMGWs in der SM-PKI und nicht zertifizierter Funktionalitäten des SMGW in der SM-Test-PKI sammeln können, aber auch die technische Komplexität im Aufbau sowie der Operativsetzung erfahren. Bedingt durch die frühen Entscheidungen über die zu untersuchenden Anwendungsfälle und die zum Teil eigenständig entwickelten Messlösungen lassen sich jedoch nicht alle Erkenntnisse vollumfänglich auf die Zielarchitektur des MsbG übertragen.

BISLANG ERREICHTER KENNTNIS- UND ENTWICKLUNGSSTAND

Ein erwarteter Konflikt von IT-Sicherheit und Datenschutz konnte durch die Projekte nicht festgestellt werden. Dennoch ist ersichtlich, dass beide Themen in einem Zielkonflikt mit Funktionalitäten (vor allem Datenschutz) und Performanz einer Lösung (IT-Sicherheit, z. B: aufwendige Verschlüsselung oder fehlervermeidende redundante, aber langsamere Protokolle) stehen können, wenn etwa Datenschutz verhindert, dass z. B. IT-Logdateien erstellt werden, deren Auswertung für die Verbesserung einer Optimierungsfunktion genutzt werden könnten. Infolgedessen überwiegt in den Schaufenstern im Bereich Datenschutz weiterhin die Erkenntnis, dass die Einhaltung der datenschutzrechtlichen Vorgaben zwar sehr aufwendig, aber grundsätzlich machbar ist. Die Umsetzung der Anforderungen aus dem MsbG sei möglich gewesen, habe jedoch viel zeitliche und personelle Kapazitäten beansprucht.