Datenschutz und Datensicherheit

Analysen für Smart Metering und Smart Grids | Für die Integration erneuerbarer Energien muss das Stromnetz modernisiert werden. Die Nutzung vorhandener Flexibilität kann den konventionellen Netzausbau zwar reduzieren, erfordert aber IKT. Mit der Digitalisierung wird diese kritische Infrastruktur angreifbarer. Das BFE untersuchte deshalb diverse Möglichkeiten zur Erhöhung der Datensicherheit.

TEXT MATTHIAS GALUS, BRUNO LE ROY, MOHAMED BENAHMED

Das Bundesamt für Energie publizierte 2015 die Smart-Grid-Roadmap [1], die mit vielen Interessengruppen, u.a. mit Vertretern der Strombranche, der Industrie und der Konsumenten, erarbeitet wurde. Sie bietet eine Vision und ein gemeinsames Verständnis von Smart Grids in der Schweiz. Erstmals wurde dabei auch Handlungsbedarf für Datenschutz und Datensicherheit ermittelt. Mit der Smart-Grid-Roadmap wurden 12 mögliche Anwendungsfälle identifiziert und die Informationsflüsse zwischen den Akteuren herausgearbeitet.

Datenschutz für Smart-Metering-Systeme

Mit der Energiestrategie 2050 sollen mittel- bis langfristig Smart-Metering-Systeme flächendeckend bei Schweizer Endverbrauchern eingeführt werden.[2] Hierzu wurde frühzeitig vom BFE ein Dokument mit technischen Mindestanforderungen für solche Systeme veröffentlicht, das gemeinsam mit Interessengruppen erarbeitet und verabschiedet wurde.[3]

Smart-Metering-Systeme erfassen viertelstündlich Verbrauchswerte bei Endverbrauchern, Produzenten oder Prosumern. Dabei stellen sich Fragen zum Datenschutz, die unter Einbezug des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Edöb) diskutiert wurden. Ein wichtiges Ergebnis war, dass die Vorgaben zu Datenschutz bei Smart-Metering-Systemen schweizweit zu harmonisieren sind. So sollte das Bundesgesetz über den Datenschutz über die kantonalen Bestimmungen Vorrang haben. Dies wurde in Art. 8d nStromVV umgesetzt.

Datensicherheit der Systeme

Hierzu hat das BFE 2016 eine schweizspezifische Schutzbedarfsanalyse (Identifikation der Gefährdungen, Einschätzung der Schäden und Ermittlung der Eintrittswahrscheinlichkeit) für Smart-Metering-Systeme erarbeitet [4] und so die Grundlagen für die Datensicherheit geschaffen. Es wurde eine bewährte Methodik basierend auf der Norm ISO 31000 verwendet. Für die Definition des untersuchten Systems wurden die erwähnten technischen Mindestanforderungen berücksichtigt.

Es werden 14 Kernrisikoszenarien identifiziert, die sich in Eintrittswahrscheinlichkeit und Schadensausmass unterscheiden. **Bild 1** zeigt die Ergebnisse der Schutzbedarfsanalyse und die identifizierten Risiken. Insbesondere Risiken für die Netzstabilität, für die Verfügbarkeit und die Integrität der Daten werden als «hoch» eingestuft. Die Risikomatrix und Bewertungsskalen leiten sich aus der Vorlage des Informatiksteuerungsorgans des Bundes für Informatiksicherheits- und Datenschutz-Konzepte ab.

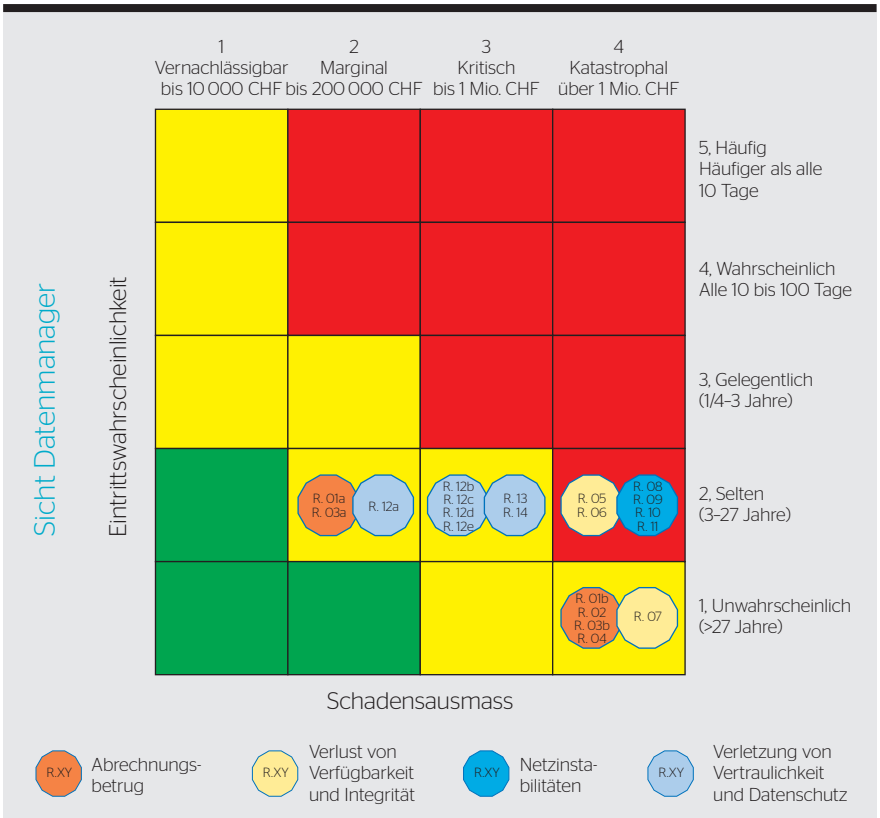

Bild 1 Risikobewertung für Datenmanager. Risikokategorien: gering (grün), mittel (gelb), hoch (rot).

Bilder: BFE

Aufgrund des notwendig hohen Schutzniveaus werden umfassende Schutzmassnahmen über alle Risikoszenarien hinweg als angezeigt erachtet. Ein entsprechender Massnahmenkatalog zur Umsetzung eines Grundschutzes, d.h. das Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus, für das Smart-Metering-System wird empfohlen. Der Grundschutz ist durch die Betreiber zu gewährleisten. Die Massnahmen betreffen nicht nur den intelligenten Zähler, sondern auch andere Teile eines Smart-Metering-Systems wie die vorgelagerte IKT-Infrastruktur.

Umsetzung und Validierung

Eine Analyse [5] zur Frage, wie die Datensicherheit bei Smart-Metering-Systemen implementiert werden kann, zeigt vier mögliche Ansätze auf, die sich in Spezifikationstiefe der gestellten Anforderungen und der Tiefe einer Prüfung/Validierung der Einhaltung dieser Anforderungen unterscheiden **(Bild 2)**:

- Variante 1: externe Penetrationstests gemäss Standard
- Variante 2: Konformitätsprüfung mit einem zugrunde liegenden Standard
- Variante 3: Konformitätsprüfung mit einem zugrunde liegenden Schutzprofil
- Variante 4: IKT-Sicherheitszertifikat mit zugrunde liegendem Schutzprofil

In der ersten Variante werden die IKT-Sicherheitsfunktionalitäten durch externe Penetrationstests auf ihre Wirksamkeit untersucht. Bestehende Produktstandards (z.B. branchen- oder industriespezifisch) können hierfür herangezogen werden. Es findet keine externe Prüfung der Ergebnisse der Penetrationstests statt.

Die zweite Variante sieht vor, dass ein Katalog von Anforderungen für die IKT-Sicherheit vorliegt und die Einhaltung dieser Anforderungen in einer Konformitätsbewertung geprüft wird. Die Anforderungen für die IKT-Sicherheit stützen sich auf Industriestandards. Die Prüfung erfolgt durch unabhängige, akkreditierte Prüfstellen (Labor). Ein Prüfschema gibt das konkrete Vorgehen zur Überprüfung der Vollständigkeit und der Wirksamkeit der IKT-Sicherheitsfunktionalitäten vor.

Die dritte Variante umfasst die Erarbeitung eines Schutzprofils und die Prüfung der Einhaltung dieser Anforderungen über eine Konformitätsbewertung. Im Gegensatz zur Variante 2 können die Anforderungen in der nötigen Breite und Tiefe z.B. auf die in einer spezifischen Schutzbedarfsanalyse identifizierten Schwachstellen und Risiken abgestimmt und in einer schweizspezifischen Lösung definiert werden. Das Schutzprofil ersetzt also Industriestandards im Vergleich zur Variante 2. Es umfasst sicherheitstechnische Anforderungen, Prüfgegenstände, die einzelne Anforderungen erfüllen müssen, und mindestens ein Prüfschema. Bei der Erarbeitung kann auf die Subsidiarität abgestellt werden. Betreiber und Hersteller zusammen mit Prüfstellen können so gemeinsam Angemessenheit und Umsetzbarkeit sicherstellen. Das Schutzprofil bietet eine detaillierte Wegleitung für die Umsetzung der IKT-Sicherheitsfunktionalitäten in Design und Herstellung. Danach findet eine Konformitätsbewertung der Prüfgegenstände durch eine Prüfstelle statt, die durch eine Kontrollstelle validiert wird. Die Kontrollstelle sichtet die Prüfergebnisse und erteilt bei zufriedenstellenden Ergebnissen eine Zulassungsermächtigung (ähnlich wie bei Eichverfahren).

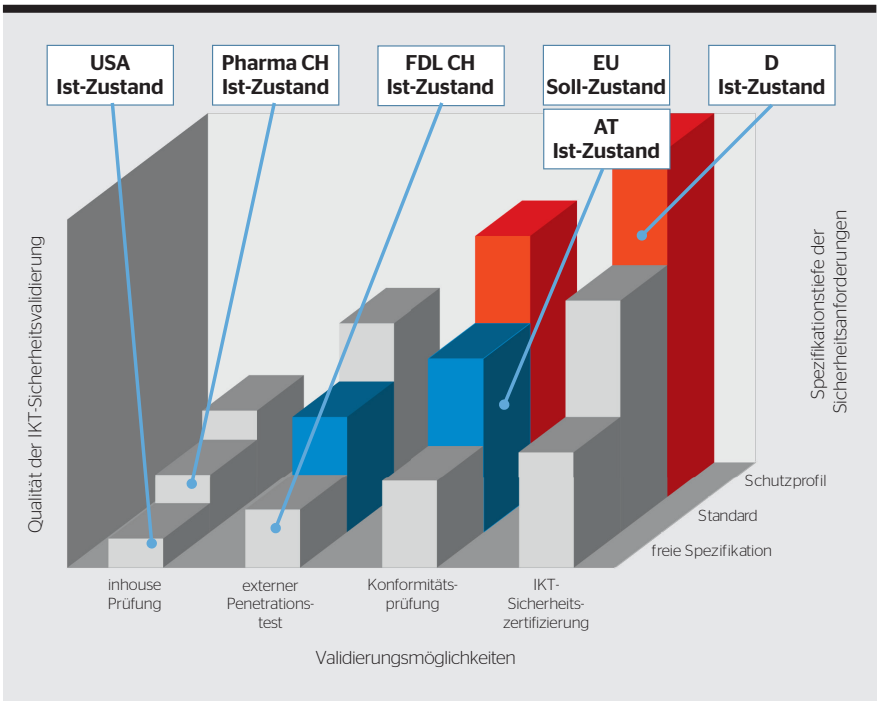

Bild 2 Ausgewählte Varianten zur Diskussion von Vor- und Nachteilen bei der Gewährleistung der Datensicherheit von Smart-Metering-Systemen. FDL:Finanzdienstleistung.[5]

Variante	Vorteile	Nachteile
1	- Einfache Durchführung der Penetrationstests	- Keine Reproduzierbarkeit der Ergebnisse der Prüfung - Keine Kontrolle der Korrektheit - Kleines Schutzniveau
2	- Einheitliches Vorgehen dank einheitlichen IKT-Schutzanforderungen und einer Konformitätsprüfung - Reproduzierbarkeit der Ergebnisse der Prüfung	- IKT-Schutzanforderungen auf Basis von Standards zu offen, gewährleisten kein adäquates Sicherheitsniveau - Keine Kontrolle der Korrektheit
3	- Einheitliches Vorgehen dank einheitlichen IKT-Schutzanforderungen und einer Konformitätsprüfung - Reproduzierbarkeit der Ergebnisse der Konformitätsprüfung - Kontrolle der Korrektheit	- Erarbeitung von spezifischen IKT-Schutzanforderungen (Schutzprofil) notwendig
4	- Einheitliches Vorgehen dank einer Sicherheitszertifizierung - Reproduzierbarkeit der Ergebnisse der Prüfung - Kontrolle der Korrektheit - Hohes Schutzniveau	- Erarbeitung von spezifischen IKT-Sicherheitsanforderungen - Umsetzung Sicherheitszertifizierung schwierig, kostenintensiv und innovationshemmend

Tabelle 1 Vor- und Nachteile der ausgewählten Varianten.

Schnittstellenklassen	Schadensausmass		Eintrittswahrscheinlichkeit	Risikoniveau
	SGIS-Security-Level	Direkte Effekte im Betrieb		
1. Zwischen Kontrollsystemen innerhalb einer Organisation	4	1	1	5
2. Zwischen Kontrollsystemen verschiedener Organisationen	4	1	1	5
3. Zwischen Back-Office-Systemen unter gemeinsamer Verantwortung	3	1	2	8
4. Zwischen Back-Office-Systemen unter getrennter Verantwortung	3	1	3	12
5. Verbindungen zwischen Finanz- oder Marktsystemen	2	0	5	10
6. Zwischen Systemen, die das AMI-Netz nutzen	2	1	5	15
7. Zwischen Systemen, die das AMI-Netz für hochverfügbare Funktionen nutzen	3	1	4	16
8. Zwischen externen Systemen und Kundenanschluss	2	1	5	15
9. Zwischen Systemen und mobilen Endgeräten der Crew im Feld	3	1	2	8
10. Im Zählerbereich	1	1	5	10
11. Zwischen Wartungs-/Konfigurationssystemen und Kontrollgeräten	2	0	1	2

Tabelle 2 Gesamtrisikobetrachtung beim Zugriff auf die Flexibilität in den Verteilnetzen (maximales Risiko: 30; AMI: Advanced Metering Infrastructure).

Die vierte Variante ist die Maximalvariante. Dabei werden sehr tiefgehende und breite Anforderungen an IKT-Sicherheit definiert in Kombination mit einem strikten IKT-Sicherheitszertifizierungsprozess. Dieser Prozess stützt sich auf ein vorgegebenes Prüfverfahren und erfordert, dass die Prüfstelle auch als Kontrollstelle fungiert. **Tabelle 1** fasst die Vor- und Nachteile der untersuchten Varianten zusammen.

Zwischenfazit

Die Analyse konnte Variante 3 als bestgeeignet einstufen. Die Konformitätsbewertung gegen schweizspezifisches Schutzprofil ist eine pragmatische Lösung und bietet ein gutes Verhältnis von Aufwand zu Ertrag (Sicherheit), eine gute Reproduzierbarkeit der Ergebnisse sowie insgesamt ein gutes Sicherheitsniveau. Die Erarbeitung des Schutzprofils erfolgt durch die Netzbetreiber zusammen mit Herstellern, weiteren Akteuren und unabhängigen Dritten, z.B. IKT-Sicherheitsexperten, und zollt so dem Prinzip der Subsidiarität in der Schweiz Tribut.

Für die Durchführung der Konformitätsbewertung sollten eine akkreditierte, privatrechtlich organisierte Prüfstelle und darüber hinaus eine unabhängige Kontrollstelle, welche beim Bund angesiedelt ist, etabliert werden. Die Kontrollstelle sorgt für eine konstant hohe Qualität der Konformitätsbewertungsstellen und der durchgeführten Prüfungen. Dieser Ansatz wurde in der Teilrevision der StromVV zur Energiestrategie 2050 bereits aufgenommen (Artikel 8b nStromVV).

Schutzbedarfsanalyse für Smart Grids

Auch für Smart-Grid-Anwendungen, die sich künftig etablieren werden, muss der Bedarf an Datensicherheit ermittelt werden, so z.B. für den Fall des Zugriffs auf Flexibilität (z.B. steuerbare Produktion, steuerbare Verbraucher und Speicher) in den Verteilnetzen. In Untersuchungen des BFE wurden Lösungen für eine Koordination zwischen Markt und Netz analysiert, wenn Flexibilität in Verteilnetzen sowohl für marktliche als auch für netztechnische Belange eingesetzt werden sollen.[6,7] 2016 hat das BFE eine entsprechende Schutzbedarfsanalyse betreffend dem Zugriff und dem Einsatz von Flexibilität publiziert.[8] Auch sie stützt sich auf die Norm ISO 31000 zum Risikomanagement.

Nach der Modellierung der Anwendungsfälle für die Flexibilitätsnutzung wurden Schnittstellen bzw. Schnittstellenklassen zwischen den jeweils beteiligten Akteuren identifiziert. Für diese wurde das Risikoniveau geschätzt und der Schutzbedarf ermittelt. Die Schnittstellenklassen sind in **Tabelle 2** aufgelistet. Grundlage für die Risikoeinstufungen war u.a. die Branchenrichtlinie zu IKT Continuity. **Tabelle 2** zeigt das Gefährdungspotenzial (Schadensaus-

RÉSUMÉ

Protection et sécurité des données

Des analyses pour le smart metering et les smart grids

L'augmentation du nombre d'installations de production décentralisées dans le cadre de la Stratégie énergétique 2050 (SE 2050) constitue un défi majeur pour les réseaux d'électricité. Les réseaux électriques intelligents peuvent constituer, selon les cas, une alternative efficace et économiquement compétitive par rapport au développement conventionnel du réseau. Cependant, l'usage croissant des technologies de l'information et de la communication (TIC) rend l'infrastructure du réseau plus vulnérable aux cyberrisques (cf. Feuille de route pour un réseau intelligent publiée par l'OFEN en 2015). La SE 2050 place les données des systèmes de mesure intelligents sous le régime de la Loi fédérale sur la protection des données (LPD) et formule des exigences concernant le traitement de ces données par des tiers.

Les exigences réglementaires et techniques en matière de protection et de sécurité des données dans les systèmes de mesure intelligents et les réseaux électriques intelligents ont vocation à être révisées régulièrement.

La SE 2050 établit un cadre clair pour le traitement des données des systèmes de mesure, de commande et de réglage intelligents. BFE

mass) bei Verlust, Offenlegung oder Fehlnutzung der Daten der Schnittstellenklassen. Die letzte Spalte zeigt das Risikoniveau, das sich aus dem Schadensausmass und der Eintrittswahrscheinlichkeit ergibt. Die Risiken können für den Zugriff auf Flexibilität als hoch eingestuft werden.

Die Bestimmung von Schutzmassnahmen erfolgt auf Basis des Smart-Grid-Standards NISTIR 7628. Er legt IKT-Sicherheitsanforderungen zum Schutz vor Angriffen auf diese Schnittstellenklassen fest. Die Massnahmen ermöglichen einen Grundschutz und sollten zu einer geeigneten Absicherung des Systems beim Zugriff auf die Flexibilität umgesetzt werden. Für die Implementierung und Prüfung des Grundschutzes wird der gleiche pragmatische Ansatz wie für Smart-Metering-Systeme empfohlen.

Schlussfolgerungen

Die Smart-Grid-Roadmap unter der Leitung des BFE hat frühzeitig einen Bedarf an Datenschutz und Datensicherheit für Smart-Metering-Systeme und für den Bereich Smart Grid klar aufgezeigt. Um eine schweizweit einheitliche Regelung für den Datenschutz zu schaffen, stützt sich die ES 2050 auf das Bundesgesetz über den Datenschutz und setzt einen regulatorischen Rahmen zur Nutzung der Daten und zum Schutz der Endverbraucher.

Für die Gewährleistung der Datensicherheit ist ein pragmatischer Ansatz sinnvoll. Zwei Schutzbedarfsanalysen haben gezeigt, dass die Einführung von Smart-Metering-Systemen und die Umsetzung von Smart-Grid-Anwendungsfällen für den Zugriff auf Flexibilität mit hohen Risiken aus Sicht der Datensicherheit behaftet sind. In beiden Fällen ist ein Grundschutz sehr wichtig. Die Erarbeitung von entsprechenden und spezifischen IKT-Sicherheitsanforderungen für den zu erreichenden Grundschutz sollte subsidiär, aber branchenweit harmonisiert, erfolgen und die Ergebnisse der Schutzbedarfsanalysen berücksichtigen. Die umgesetzten IKT-Sicherheitsmassnahmen sollten auf ihre Wirksamkeit geprüft und im Rahmen einer Konformitätsbewertung validiert werden. Dies sollte durch eine unabhängige und öffentliche Kontrollstelle beaufsichtigt werden. Dieser Ansatz wird für Smart-Metering-Systeme bereits in den Verordnungen zur ES2050 vollumfänglich aufgenommen. So können von Anfang an eine hohe IT-Sicherheit und ein guter Datenschutz bei der Einführung von Smart-Metering-Systemen gewährleistet werden. Einzig die IKT-Sicherheitsanforderungen fehlen noch, obwohl sie seit bald zwei Jahren in der Branche in Arbeit sind. Es ist nun an der Zeit, die Arbeiten abzuschliessen. Die Verordnungen treten voraussichtlich am 1. Januar 2018 in Kraft.

Referenzen

[1] Bundesamt für Energie, «Smart-Grid-Roadmap», 2015, www.bfe.admin.ch/smartgrids/index.html?lang=-de&dossier_id=06726.
[2] Vernehmlassungsentwurf der Verordnungen zur Umsetzung der Energiestrategie 2050.
[3] Bundesamt für Energie, «Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz», 2014, www.bfe.admin.ch/smartgrids/index.html?lang=-de&dossier_id=06728.
[4] AWK Group, Schutzbedarfsanalyse Smart Metering in der Schweiz, 2016, www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06727.
[5] vZsecurITy, Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern. 2015, www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06727.
[6] Consentec GmbH, «Koordination von Markt und Netz – Ausgestaltung der Schnittstelle», 2015, www.bfe.admin.ch/smartgrids/index.html?lang=-de&dossier_id=06730.
[7] Frontier Economics, Praktische Aspekte bei der Ausgestaltung der Schnittstelle Markt-Netz im Verteilnetz, 2016, www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06730.
[8] Offis Energie, Fachhochschule Salzburg, Ecofys, Schutz- und Sicherheitsanalyse im Rahmen der Entwicklung von Smart Grids in der Schweiz, 2016, www.bfe.admin.ch/smartgrids/index.html?lang=-de&dossier_id=06727.

Autoren

Dr. **Matthias Galus** ist Leiter Task Force Digitalisierung und stv. Leiter Netze.
→ BFE, 3003 Bern
→ matthias.galus@bfe.admin.ch

Bruno Le Roy ist Asset-Optimierer bei Alpiq.
→ Alpiq AG, 4601 Olten
→ bruno.leroy@alpiq.com

Dr. **Mohamed Benahmed** ist Leiter Netze beim Bundesamt für Energie.
→ mohamed.benahmed@bfe.admin.ch.