Cyberrisiken bekämpfen

Autor(en): **[s.n.]**

Objekttyp: **Article**

Zeitschrift: **Energeia : Newsletter des Bundesamtes für Energie**

Band (Jahr): **- (2017)**

Heft 2

PDF erstellt am: **08.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-681848

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

CYBERRISIKEN BEKÄMPFEN

Wie arbeitet der Bund mit der Energiebranche zusammen, um Netze intelligenter und sicherer zu gestalten? Eine Schutzbedarfsanalyse des Bundesamts für Energie hilft bei der Risikoeinschätzung. Nun sollen einheitliche Branchenstandards definiert werden.

Bis 2025 sind intelligente Messsysteme Teil der meisten Schweizer Haushalte. So sieht es die Energiestrategie 2050 vor. Diese sogenannten Smart Meter könnten Energieversorgern und Endverbrauchern dabei helfen, Kosten zu sparen, indem sie automatisch regelmässig detaillierte Verbrauchsdaten erfassen.

Cyberrisiken einschätzen

Das Netz wird durch den Einsatz dieser intelligenten Messsysteme zwar smarter, aber auch angreifbarer. Die Herausforderung besteht darin, mögliche Schwachstellen und Sicherheitsrisiken vorgängig zu identifizieren. In welchen Bereichen es wie viel Schutz braucht, hat kürzlich eine Studie im Auftrag des Bundesamts für Energie analysiert. Diese Schutzbedarfsanalyse gewichtet mögliche Bedrohungen nach deren Eintrittswahrscheinlichkeit, um festzustellen, wie hoch das damit verbundene Sicherheitsrisiko ist.

Was bedeutet es beispielsweise, wenn tausend Smart Meter durch einen technischen Fehler oder durch Sabotage plötzlich ausfallen würden? Was wäre die Konsequenz davon? Wie teuer wäre dies? Wie sind Smart Meter vor externen Störungen und Cyberangriffen zu schützen?

Risikoszenarien analysiert

Mit derartigen Fragen befasst sich die Schutzbedarfsanalyse. Berücksichtigt wurden dabei Einzelfälle bis hin zu grossflächigen Ereignissen und vorsätzliche Handlungen wie eine Datenmanipulation, der Missbrauch von Zugriffrechten oder falsche Abrechnungen über mehrere Jahre. Als katastrophal gelten dabei jene Fälle, die über eine Million Franken kosten würden. Für die Risikoeinstufung wurde auf eine Vorlage des Informatiksteuerungsorgans des Bundes zurückgegriffen.

Grosser Schutzbedarf erkannt

Im Grunde wurden 14 Risikoszenarien und verschiedene Varianten davon entworfen und aus Sicht des Verteilnetzbetreibers oder eines dritten Messdienstleisters (Datenmanager) sowie des Endverbrauchers analysiert. «Plausible Szenarien wurden hierfür berücksichtigt», sagt Bruno Le Roy, Fachspezialist für Netze beim Bundesamt für Energie. «Die Analyse hat gezeigt, dass der Schutzbedarf für die Smart-Metering-Infrastruktur gross ist.» Für jedes Szenario wurde der jeweilige Schutzbedarf ermittelt, und darauf basierend wurden geeignete Sicherheitsmassnahmen empfohlen.

Branchenstandards festlegen

Jetzt liegt der Ball bei der Branche: Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) muss einheitliche Vorgaben und Standards für die Cybersicherheit von Messsystemen definieren und diese für sich dokumentieren. Eine unabhängige Stelle soll prüfen, wie sie umgesetzt werden.

«Damit haben wir für die Schweiz eine flexible, subsidiäre Lösung gefunden, die den Marktakteuren Spielraum lässt, um die Mindestanforderungen selbst festzulegen», sagt Le Roy. Andere Länder würden hingegen ein eher starres und kostenintensiveres System kennen. Das Schweizer Modell soll laut dem Experten einfacher umzusetzen sein. *(bra)*

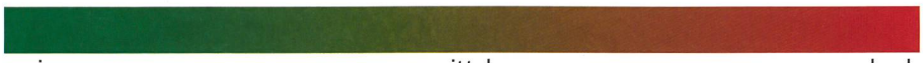
Aufgabenteilung

Der Bund macht eine Schutzbedarfsanalyse.

Die Branche definiert Standards.

Eine Prüfstelle wacht über die Implementierung.

Risiko einschätzen



gering — mittel — hoch

Schadenausmass x Eintrittswahrscheinlichkeit = Risikoniveau
Daraus resultieren der Schutzbedarf und geeignete Massnahmen.

Quelle: BFE