Die Informations- und Telekommunikationstechnologie (IKT) durchdringt heute nahezu alle Geschäftsabläufe eines Energieversorgungsunternehmens. Neben den Vorteilen entstehen damit aber auch neue Risiken für die Versorgungssicherheit.

Ein Fachbeitrag von Dr. Andreas Lied, Vorstand der Becker Büttner Held Consulting AG und Dr. Michael Weise, Rechtsanwalt der Sozietät Becker Büttner Held, Berlin.

Foto: BBH

Neue Anforderungen an die IT-Sicherheit von Netzbetreibern

- Der IT Sicherheitskatalog der Bundesnetzagentur -

Die Gefahr, dass durch Angriffe auf die IKT-Systeme die Versorgungssicherheit beeinträchtigt wird, wächst. Der Gesetzgeber arbeitet deshalb u.a. an einem IT-Sicherheitsgesetz, um insbesondere Betreiber kritischer Infrastrukturen (wie Versorgungsnetzbetreiber) auf einen Mindestschutz ihrer IT-Systeme zu verpflichten.

Bereits in 2011 hat der Gesetzgeber mit einer Ergänzung des EnWG auf diese Gefahren reagiert; flankierend hierzu hat die Bundesnetzagentur (BNetzA) jüngst einen Katalog an IT-Sicherheitsanforderungen veröffentlicht, der in seiner Entwurfsfassung mit erheblichen Auswirkungen für Strom- und Gasnetzbetreiber verbunden ist. Kernforderung dieses „IT-Sicherheitskatalogs" ist die Einführung und Umsetzung eines Information-Security-Management-System (ISMS). Das ISMS ist keine „Unbekannte": es wird bereits in der Technischen Richtlinie TR-03109-1 für die Administration von („intelligenten") Messsystemen – genauer: Smart Meter Gateways – vorgeschrieben. In diesem Bereich gilt sie als wesentliche Hürde für die Wahrnehmung der Funktion eines Smart Meter Gateway Administrators. Mit den Anforderungen des IT-Sicherheitskatalogs muss diese „Hürde" jedoch ggf. anders bewertet werden.

Gesetzlicher Hintergrund

Mit der EnWG-Novelle 2011 hat der Gesetzgeber den in § 11 Abs. 1 EnWG verankerten gesetzlichen Auftrag der Netzbetreiber (Strom und Gas) zum Betrieb eines sicheren Energieversorgungsnetzes mit Einfügung des § 11 Abs. 1a EnWG präzisiert. Danach umfasst der Betrieb eines sicheren Energieversorgungsnetzes auch einen angemessenen Schutz gegen Bedrohungen der IKT, die der Netzsteuerung dient.

Zur Präzisierung eines solchen „angemessenen Schutzes" enthält § 11 Abs. 1a EnWG einen gesetzlichen Auftrag an die BNetzA, zusammen mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) einen Katalog von Sicherheitsanforderungen zu erstellen und zu veröffentlichen („IT-Sicherheitskatalog"). Angemessener Schutz der netzsteuerungsdienlichen IKT wird gesetzlich vermutet, wenn dieser Katalog eingehalten und dies vom Netzbetreiber dokumentiert ist. Die BNetzA hat gemäß § 11 Abs. 1a Satz 4 EnWG die Möglichkeit, per Festlegung nähere Bestimmungen zu Format, Inhalt und Gestaltung dieser Dokumentation zu treffen.

In diesem Zusammenhang sind auch die Bemühungen des Gesetzgebers zu erwähnen, ein sog. IT-Sicherheitsgesetz zu verabschieden. Ein entsprechender Referentenentwurf („Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme") datiert bereits vom 05.03.2013. Mit diesem Gesetz sollen im Schwerpunkt Ergänzungen des „Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik„ (BSI-Gesetz) erfolgen, um einen Mindeststandard für den IT-Schutz von Betreibern kritischer Infrastrukturen (KRITIS) festzulegen. Nach dem Entwurf dieses Gesetzes gehört der

Sektor Energie zu den KRITIS; die konkreten Adressaten dieses Gesetzes werden jedoch noch in einer separat zu verabschiedenden Rechtsverordnung festgelegt.

IT-Sicherheitskatalog

Am 12.12.2013 hat die BNetzA den Entwurf eines IT-Sicherheitskatalogs veröffentlicht und zur Konsultation gestellt. In seiner Entwurfsfassung adressiert der IT-Sicherheitskatalog sämtliche Strom- und Gasnetzbetreiber, unabhängig von Art (Netz der allgemeinen Versorgung oder geschlossenes Verteilernetz) und Größe. Der IT-Sicherheitskatalog hat keinen rechtsverbindlichen Charakter; es handelt sich insbesondere nicht um eine Festlegung. Rechtsschutzmöglichkeiten in der Form einer Beschwerde bestehen nicht. Mittelbare Verbindlichkeit erlangt der Katalog jedoch über die Verknüpfung mit der gesetzlichen Vermutungswirkung eines „angemessenen Schutzes".

Zu den Anforderungen des IT-Sicherheitskatalogs gehört die Benennung eines IT-Sicherheitsbeauftragten. Dieser soll u. a. als Ansprechpartner für die BNetzA dienen und die Umsetzung des IT-Sicherheitskatalogs überwachen. Kernforderung dieses Katalogs ist dass jeder Netzbetreiber, der mittels IKT-Systemen Einfluss auf die Netzsteuerung nehmen kann, ein Information-Security-Management-System (ISMS) einführt. Damit werden im Kern dieselben Anforderungen gestellt, die auch die (ebenfalls noch im Entwurfsstand befindliche) Messsystemverordnung (MsysV) vom (zukünftigen) Smart Meter Gateway Administrator verlangt.

Auswirkungen auf die IT

Die Anforderungen an die IT-Sicherheit betreffen unterschiedliche Teile der IKT-Systemlandschaft eines integrierten Energieversorgers. Für die Smart Meter Gateway Administration muss das ISMS alle Systeme, Anwendungen und Daten umfassen, welche an der Administration von Smart Meter Gateways beteiligt sind.

»Kernforderung dieses Katalogs ist, dass jeder Netzbetreiber, der mittels IKT-Systemen Einfluss auf die Netzsteuerung nehmen kann, ein Information-Security-Management-System (ISMS) einführt.«

Zur Wahrung der IT-Sicherheit im Netzbetrieb hingegen muss das ISMS alle Systeme abdecken, die der Netzsteuerung direkt dienen bzw. unmittelbar Einfluss auf die Netzführung nehmen. Hierunter fallen insbesondere die zentralen Netzleitsysteme, übertragungstechnische Netzelemente, Rundsteueranlagen, Messsysteme an Trafostationen sowie jegliche Sensoren und Aktoren im Feld.

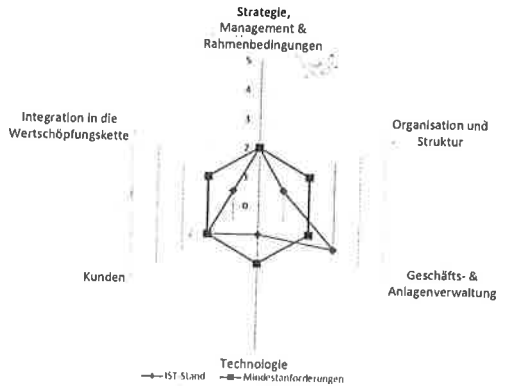
Die gewachsenen Abhängigkeiten zwischen den eingesetzten IT-Systemen bzw. Anwendungen führen zu einer erschwerten Umfangsdefinition des ISMS. Beispielsweise sind alle datenliefernden Systeme einzubeziehen, die Auswirkungen auf das Leitsystem und damit die Netzfahrweise haben. Dies kann etwa die stammdatenführende Verbrauchsabrechnung sein, welche Anlagestammdaten von Erzeugungsanlagen bereitstellt oder auch ein Energiedatenmanagementsystem, von welchem aus „near-real-time"-Lastgänge in das Leitsystem importiert werden. Ob ein System damit unter den „Schirm" des ISMS muss, kann nur durch eine detaillierte Analyse der betroffenen IT-(Teil-)Landschaft entschieden werden.

Während für die Zertifizierung des Netzbetriebs nach IT-Sicherheitskatalog eine „einfache" ISO 27001 ff. Zertifizierung ausreicht, schreibt die Technische Richtlinie für die Smart Meter Gateway Administration eine Zertifizierung nach ISO 27001 ff. auf Basis des sog. IT-Grundschutzes vor (der IT-Grundschutzkatalog umfasst allein mehr als 4000 Seiten).

Dennoch haben beide Zertifizierungsarten eine gemeinsame Schnittmenge. Aus diesem Grund ist es wichtig, diese Überschneidungen (und damit ggf. verbundene Skaleneffekte) in die strategischen Überlegungen zum Thema Smart Meter Rollout und Umsetzung bzw. Auslagerung der Funktion des Smart Meter Gateway Administrators zu berücksichtigen. Einige Kostenbestandteile könnten sich bei näherem Hinsehen zu „eh-da" Kosten wandeln, wie insbesondere die fixen Kosten für Teile des ISMS.

www.bbh-online.de www.derenergieblog.de

Durch die Gegenüberstellung des IST-Standes und der zu erfüllenden Anforderungen können Handlungsfelder identifiziert und konkrete Maßnahmen abgeleitet werden.
Das Reifegradmodell dient als Standortbestimmung der eigenen Leistungsfähigkeit und schafft so die Basis für die Umsetzungsphase des Smart Meter Rollouts sowie die langfristige Ertüchtigung des Netzes zum Smart Grid.



© BBHC: grafische Darstellung SOLL-IST Vergleich (Beispiel)