Der IT-Sicherheitskatalog der Bundesnetzagentur: Auswirkungen auf die Verteilernetzbetreiber

Andreas Lied, Stefan Brühl, Jan-Hendrik vom Wege und Michael Weise

Die IT-Sicherheit von Betreibern kritischer Infrastrukturen steht aktuell im Fokus des Gesetzgebers. Flankierend hierzu hat die Bundesnetzagentur bereits Ende letzten Jahres mit der Veröffentlichung eines Sicherheitskatalogs die Anforderungen an die IT-Sicherheit von Netzbetreibern (Strom und Gas) präzisiert. Der gegenwärtig noch im Entwurf befindliche Katalog wird – wenn in dieser Form final verabschiedet – erhebliche Auswirkungen auf die netzsteuerungsdienliche Informations- und Telekommunikationstechnologie (IKT) von Netzbetreibern haben.

Die IKT durchdringt heute nahezu alle Geschäftsabläufe eines Energieversorgungsunternehmens. Diese Unterstützung bringt vor allem im Bereich der Automatisierung von Prozessen viele Vorteile, jedoch geht mit der wachsenden Abhängigkeit von IKT-Systemen auch ein gesteigertes Risiko einher. Gesetzgeber, Bundesnetzagentur (BNetzA) und das Bundesamt für die Sicherheit in der Informationstechnik (BSI) haben hierauf reagiert und die Anforderungen an die IT-Sicherheit von Betreibern kritischer Infrastrukturen im Allgemeinen und bei Betreibern von Energieversorgungsnetzen im Besonderen verschärft [1].

IT-Sicherheitsgesetz

Mit Bearbeitungsstand vom 5.3.2013 hat das Bundesministerium des Innern (BMI) einen Referentenentwurf für ein „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" („ITSG") vorgelegt [2], mit dem insbesondere Vorschriften des BSI-Gesetzes [3] ergänzt werden sollen. Ziel ist es, für Betreiber kritischer Infrastrukturen („KRITIS") einen Mindeststandard an IT-Sicherheit festzulegen. Nach einer Definition des BMI [4] handelt es sich bei KRITIS um Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können [5].

Kernforderung des ITSG ist gemäß der vorgesehenen Ergänzung eines § 8a Abs. 1 BSI-Gesetz, dass Betreiber von KRITIS „angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen [haben], die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind." Die Betreiber von KRITIS und damit die konkreten Adressaten des ITSG sind noch in einer separaten Rechtsverordnung festzulegen; der Sektor „Energie" soll grundsätzlich dazu gehören [6].

§ 11 Abs. 1a EnWG

Bereits mit der EnWG-Novelle 2011 [7] 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, gemeinsam mit dem BSI einen Katalog von Sicherheitsanforderungen zu erstellen und zu veröffentlichen („IT-Sicherheitskatalog"). Ein angemessener Schutz der netzsteuerungsdienlichen IKT wird sodann gesetzlich vermutet, wenn dieser Katalog eingehalten und dies vom Netzbetreiber dokumentiert ist. Darüber hinaus hat die BNetzA gemäß § 11 Abs. 1a Satz 4 EnWG die Möglichkeit, per Festlegung nähere Bestimmungen zu Format, Inhalt und Gestaltung dieser Dokumentation zu treffen.

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 der Art (Netz der allgemeinen Versorgung oder geschlossenes Verteilernetz i. S. v. § 110 EnWG) und Größe des Netzes.

Eine gesetzliche Verpflichtung zur Umsetzung des IT-Sicherheitskatalogs besteht (derzeit) nicht. Der IT-Sicherheitskatalog hat selbst (in seiner aktuellen Entwurfsfassung) keinen rechtsverbindlichen Charakter. Es handelt sich insbesondere nicht um eine Festlegung.

Dem Katalog kommt jedoch über die Verknüpfung mit der gesetzlichen Vermutungswirkung eines „angemessenen Schutzes" zumindest mittelbar Verbindlichkeit zu. Die gesetzliche Vermutung führt rechtlich zu einer „Beweislastumkehr": Kommt es zu einem Schadensfall (aufgrund eines Eingriffs in die netzsteuerungsdienliche IKT), so wird bei Umsetzung des IT-Sicherheitskatalogs vermutet, dass der Netzbetreiber für den (gesetzlich geforderten) angemessenen Schutz seiner IKT gesorgt hat (ihm kann also aus dieser Sicht kein Verschuldensvorwurf gemacht werden, der Voraussetzung für die zivilrechtliche Schadensersatzhaftung ist).

Umgekehrt führt die Nichtumsetzung des IT-Sicherheitskatalogs dazu, dass der betroffene Netzbetreiber in der vollen Darlegungs- und Beweislast für die Angemessenheit seines IT-Schutzes steht. Auch hat die Bundesnetzagentur gemäß § 11 Abs. 1a Satz 4 EnWG das Recht, die Einhaltung des IT-Sicherheitskatalogs zu überprüfen. Eine Nichtumsetzung könnte der Regulierungsbehörde Anlass geben, die Angemessenheit des IKT-Schutzes zu hinterfragen und ggf. Aufsichtsmaßnahmen einzuleiten. Darüber

hinaus stellt sich die Frage, inwieweit sich Versicherer von Netzbetreibern zur Notwendigkeit der Umsetzung des IT-Sicherheitskatalogs positionieren.

Aufgrund der mit dem IT-Sicherheitskatalog umzusetzenden Pflichten, die alle Netzbetreiber zunächst prinzipiell gleichermaßen treffen, stellt sich zum einen die Frage nach der verhältnismäßigen Anwendung im Einzelfall. So dürfte eine ausnahmslose Umsetzung aller Anforderungen des Sicherheitskatalogs kleinere Netzbetreiber überfordern und auch aufgrund des unterschiedlichen Gefahrenpotenzials zudem nicht ausnahmslos zu rechtfertigen sein. Zum anderen stellt sich vor dem Hintergrund des bei einer Nichtumsetzung bestehenden Haftungsrisikos die Frage nach Rechtsschutzmöglichkeiten für den Netzbetreiber. Auch wenn es sich bei dem IT-Sicherheitskatalog nicht um eine „förmliche" Festlegung handelt, erscheint aufgrund der vergleichbaren Regelungswirkung eine gerichtliche Überprüfung nicht von vornherein ausgeschlossen.

IT-Sicherheitskatalog

Adressaten des IT-Sicherheitskatalogs sind alle Netzbetreiber, welche Systeme/Komponenten im Einsatz haben, die der Netzsteuerung direkt dienen bzw. „unmittelbar Einfluss auf die Netzfahrweise nehmen". Hierzu zählen u. a.:

- zentrale Netzleit- und Netzführungssysteme;
- steuerbare, blindleistungsfähige Wechselrichter inkl. Sensoren;
- Rundsteueranlagen.

Explizit ausgenommen sind jedoch kundenseitig installierte intelligente Messsysteme (iMSys), da diese nach § 3 Nr. 16 EnWG nicht Teil des Netzes sind und somit auch nicht zu den vom IT-Sicherheitskatalog adressierten Systemen zählen. Zwar kann das zentrale Leitsystem auf Basis der von intelligenten Messsystemen gelieferten Daten (IST-Einspeisung von angeschlossenen Erzeugungsanlagen, Netzzustandsdaten etc.) die Netzfahrweise beeinflussen und sogar unmittelbar netzrelevante Schalthandlungen an steuerbaren Erzeugern durchführen [8], jedoch ist die Sicherheit des intelligenten Messsystems bzw. der Kommunikationseinheit (Smart Meter Gateway) bereits durch das BSI-Schutzprofil [9] im erforderlichen Maße gewährleistet.

Ein detaillierter Blick in den IT-Sicherheitskatalog verdeutlicht, dass hier eine Vielzahl von Kernsystemen bzw. Netzelementen aufgeführt sind, welche unweigerlich zum Betrieb eines Verteilernetzes benötigt werden. Auch wenn Teile der relevanten Systemlandschaft dienstleistend von Dritten betrieben werden oder gar die ganze Betriebsführung ausgelagert wurde, bleibt die Verantwortung zur vollen Umsetzung des IT-Sicherheitskatalogs beim Netzbetreiber.

Was bedeutet der IT-Sicherheitskatalog konkret?

Der eigentliche Kern des IT-Sicherheitskatalogs – und auch der Namensgeber der Norm ISO 27001 – ist das Informationssicherheitsmanagementsystem (ISMS). Das Rad wird hierfür vom IT-Sicherheitskatalog nicht neu erfunden, stattdessen werden vielmehr Teile des internationalen ISO 27001 Standards präzisiert und spezifiziert, namentlich die Erfassung der schutzbedürftigen Systeme (Netzstrukturplan) sowie die darauf folgende Risikoanalyse (Schutzbedarfsermittlung) der relevanten Systeme.

Abb. 1 Die drei thematischen Säulen, die IT-Sicherheit definieren

Man sollte die Etablierung eines ISMS in mehrere Phasen unterteilen: Vorbereitungsphase, die aus einer „Ist-Analyse", dem Netzstrukturplan, besteht und einer Risikoanalyse mit der Ermittlung des sog. Schutzbedarfes. Danach folgt entweder die ISO 27001-Zertifizierungsphase oder die Überlegung, statt einer ISMS-Einführung und des damit verbundenen Aufwands einen Dienstleister zu suchen.

Im Netzstrukturplan sind alle Systeme/Komponenten sowie deren Verbindungen und Schnittstellen aufzuführen, unterteilt in die Technologiekategorien „Leitsystem/Systembetrieb", „Übertragungstechnik" und „Sekundär-, Automatisierungs- und Fernwirktechnik". Die Einführung dieser Kategorien ist der Besonderheit der IKT-Landschaft von Netzbetreibern geschuldet. „Herkömmliche" Unternehmen haben meist alle sicherheitsrelevanten Systeme und Komponenten in einem räumlich zusammenhängenden und nach außen abgegrenzten Gebiet, bei Netzbetreibern hingegen befindet sich ein relevanter Teil der Komponenten verteilt im Netzgebiet. In der Praxis kann die Anzahl an betrachteten Systemen sowie die Verbindungen zwischen diesen zu einer erhöhten Komplexität führen, daher kann es in bestimmten Fällen sinnvoll sein, gleichartige Systeme nach bestimmten Kriterien zu gruppieren.

Nach der Erstellung des Netzstrukturplans muss für die darin aufgeführten Systeme und Komponenten der angemessene Schutzbedarf in den drei Grundwerten der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) [10] ermittelt werden (siehe Abb. 1). Der Schutz personenbezogener Daten und Informationen ist nicht Gegenstand des IT-Sicherheitskatalogs, da hierfür bereits weitreichende Regelungen, wie z. B. das Bundesdatenschutzgesetz, bestehen.

Die Ermittlung des Schutzbedarfs ist indes kein triviales Unterfangen; hier müssen gleich mehrere Effekte sowie wechselseitige Systemabhängigkeiten berücksichtigt werden. Benötigt bspw. das zentrale Leitsystem für den Betrieb einen dedizierten Daten-

bankserver, so müssen die Sicherheitsanforderungen des Leitsystems auch eins zu eins auf das unterstützende, für den Betrieb notwendige System - hier der Datenbankserver - übertragen werden. Solche starken Interdependenzen sind jedoch anhand eines umfassend erstellten Netzstrukturplans im Grundsatz leicht identifizierbar. Herausfordernder ist die Identifizierung von sog. Kumulationseffekten. Hierbei führt eine Anhäufung (meist) kleinerer Schäden in der Summe zu einem insgesamt höheren Schaden, frei nach dem Motto „Das Ganze ist mehr als die Summe seiner Teile". Aber auch den gegenläufigen Verteilungseffekt gilt es zu beachten. Hier führt bspw. der Ausfall eines redundant vorgehaltenen Netzwerkrouters nicht zum Schadensfall, da für diesen Fall ein funktional gleichwertiger Router einspringt.

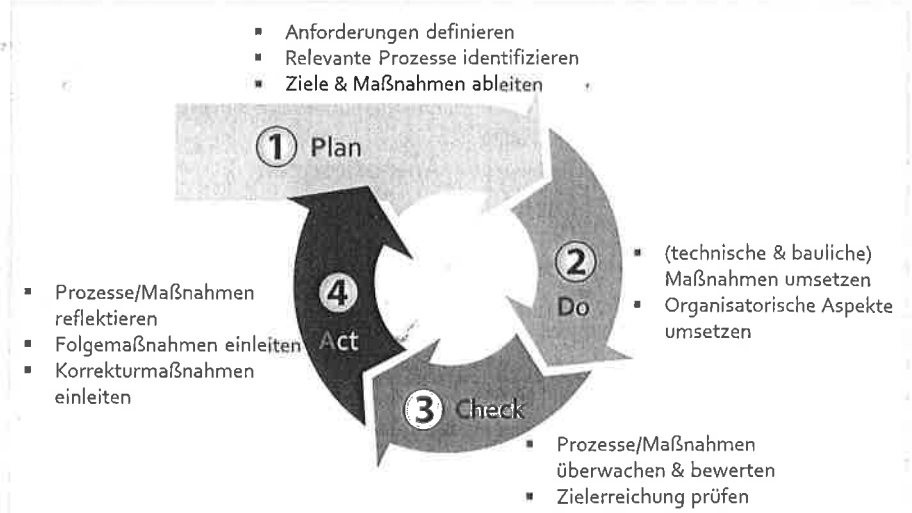

Abb. 2 Kontinuierliche Verbesserung der IT-Sicherheit durch den PDCA-Zyklus

Eine weitere Anforderung des IT-Sicherheitskatalogs ist die Benennung eines IT-Sicherheitsbeauftragten. Dieser soll für die Koordination, Verwaltung und Kommunikation der IT-Sicherheit zuständig sein. Er muss ebenfalls der BNetzA als zentraler Ansprechpartner genannt werden und ist ihr gegenüber auskunftspflichtig hinsichtlich des ISMS-Umsetzungsstandes.

Sicherheit als kontinuierlicher Prozess

Die in der aktuellen Version 27001:2013 vorliegende Norm spezifiziert die Anforderungen an die Einführung, den Betrieb und Verbesserung eines ISMS. In Abb. 2 ist der Regelzyklus eines ISMS abgebildet, welcher eine kontinuierliche Verbesserung der IT-Sicherheit gewährleisten soll. Vom Grundgedanken ist das ISMS mit anderen Managementsystemen, wie bspw. dem bekanntesten Vertreter dieser Gattung, dem Qualitätsmanagementsystem nach ISO 9001 [11], vergleichbar. Es ist ein Rahmengerüst, welches methodische Vorgehensweisen zur Erfüllung bestimmter Aufgaben vorgibt, um ein vorab definiertes Ziel zu erreichen. Die große Besonderheit gegenüber bekannten ISMS-Zertifizierungen nach ISO 27001 oder ähnlichen Risikomanagementsystemen für die IT-Sicherheit ist, dass es eine eigene fachlich spezifische Ergänzungsnorm ISO 27019 gibt, die die energiewirtschaftlichen Rahmenbedingungen eines ISMS für einen Energieversorger detaillierter festlegt, als es die recht allgemein formulierten Anforderungen der ISO 27001 tun.

Ähnlich wie in der Vorbereitungsphase hängt der Erfolg der Umsetzung und des Auditings zur Zertifizierung eines ISMS bei Energieversorgern nicht allein auf die Kenntnisse der „normalen" ISO 27000-Normenfamilie an, sondern auf die in der ISO 27019 für „Utilities" geforderten Ausprägungen.

Da war doch schon mal was?

Der deutschen Energiewirtschaft - oder genauer: den Messstellenbetreibern/grundzuständigen Netzbetreibern - kommt die Forderung zur Zertifizierung nach ISO 27001 bereits aus einer anderen Richtung bekannt vor. Die im Zuge der Einführung von intelligenten Messsystemen neu geschaffene Funktion/Rolle Smart-Meter-Gateway-Administrator (GWA) muss sich lt. Messsystemverordnung nach ISO 27001 auf Basis IT-Grundschutz zertifizieren lassen. In der bisherigen Diskussion wurden immer wieder die hohen Kosten für eine solche Zertifizierung ins Feld geführt, um eine geringe Anzahl von Smart-Meter-Gateway-Administratoren zu rechtfertigen.

Der dieser Idee zugrunde liegende Skaleneffekt - die Verteilung der hohen Fixkosten (u. a. durch ISO 27001 Zertifizierung) auf eine große Anzahl an Messsystemen - lässt sich jedoch grundsätzlich schon auf einer tieferen Stufe schöpfen. Ein Beispiel hierfür ist die Abbildungsvariante „Software as a Service" - hierbei wird das für die Administration notwendige Softwaresystem in

einem zertifizierten Rechenzentrum betrieben, die operative Bedienung erfolgt durch den Messstellenbetreiber/grundzuständigen Netzbetreiber. Der Löwenanteil der Zertifizierung sowie der baulich notwendigen Maßnahmen entfällt auf den Dienstleister, der Messstellenbetreiber hingegen muss nur noch einen sehr geringen Teil seiner Organisation und IT-Systeme der Zertifizierung unterziehen.

Sollte nun ein Netzbetreiber seine netzdienliche IKT-Landschaft nach ISO 27001 zertifizieren lassen, ergibt sich eine vollkommen neue Startposition für die GWA-Strategie. Denn hier bestehen durchaus Synergien zwischen der GWA-Zertifizierung und der Zertifizierung nach dem IT-Sicherheitskatalog, auch wenn im GWA-Bereich der Zusatz „auf Basis IT-Grundschutz" mehr Aufwand verursachen wird. Daher sollte die gewählte GWA-Strategie nochmals auf den Prüfstand gestellt werden, denn es kann durchaus sein, dass die veränderten Rahmenbedingungen (z. B. Ansetzbarkeit der Kosten für die Zertifizierung nach IT-Sicherheitskatalog in der Anreizregulierung) zu einem anderen Ergebnis führen.

Anmerkungen

[1] Vgl. hierzu auch de Wyl, C.; Weise, M.; Bartsch, A.: Das Energieversorgungsnetz als kritische Infrastruktur – aktuelle rechtliche Anforderungen und Haftungsrisiken für Verteilernetzbetreiber, in: Versorgungswirtschaft 2014 (im Erscheinen).

[2] Vgl. hier: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile

[3] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) v. 14.8.2009, BGBl. I, S. 2821.

[4] Vgl. BMI: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Stand: 17.6.2009, S. 3.

[5] Vgl. auch die Definition im Referentenentwurf zu einem „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", mit dem Regelungsvorschlag zu § 2 Abs. 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz).

[6] Vgl. Artikel 1 Nr. 1 ITSG (Ergänzung eines § 2 Abs. 10 BSI-Gesetz).

[7] Gesetz zur Neuregelung energiewirtschaftsrechtlicher Vorschriften vom 28.7.2011, BGBl. I 2011, S. 1554.

[8] Vgl. BSI: Kapitel 4.2.3 „Anwendungsfälle für steuerbare Anlagen" sowie Kapitel 4.2.4 „Anwendungsfälle für Netzzustandsdatenerhebung" der Technischen Richtlinie BSI TR-03109-1, Version 1.0 vom 18.3.2013.

[9] BSI-CC-PP-0073 (Smart Meter Gateway PP) vom 18.3.2013 und BSI-CC-PP-0077 (Security Module PP) vom 18.3.2013.

[10] Vgl. „Leitfaden Informationssicherheit" des Bundesamts für Informationssicherheit.

[11] ISO: Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2008) von Dezember 2008.

Dr. A. Lied, Vorstand, S. Brühl, Business Consultant, Becker Büttner Held Consulting AG, München; J. H. vom Wege, MBA, Rechtsanwalt und Partner, Dr. M. Weise, Rechtsanwalt, Becker Büttner Held, Berlin
andreas.lied@bbh-beratung.de