Sonderdruck

ENERGIE & MANAGEMENT
ZEITUNG FÜR DEN ENERGIEMARKT

B 13052 E 2. Mai 2015 9/15

IT-Sicherheit ist Chefsache

Die Pflicht, ein Information Security Management System einzuführen, wird kommen. Betreiber kritischer Infrastrukturen sollten jedoch nicht das Inkrafttreten des Gesetzes abwarten, sondern zügig mit der Umsetzung beginnen. VON HEIDI ROIDER

Bild: Fotolia.com, Maksim Kabakou

Es ist das Szenario mit Potenzial für einen Thriller: Hacker greifen große Energieversorger an und legen die Stromnetze deutscher Großstädte lahm. Katastrophenähnliche Zustände wären die Folge“, schreibt nicht ein Schriftseller. Diese beiden Sätze stehen auf der Internetseite des Deutschen Bundestages. Solche Szenarien soll das neue IT-Sicherheitsgesetz (IT-SiG) künftig verhindern. Die 1. Lesung fand am 20. März statt. Parallel zu diesem Entwurf müssen sich Energieversorger zudem mit dem IT-Sicherheitskatalog der Bundesnetzagentur (BNetzA) auseinandersetzen, der sich ebenfalls noch im Entwurfsstadium befindet. Branchenkenner gehen davon aus, dass das Gesetz vom Bundestag noch vor der Sommerpause verabschiedet wird – ohne dass noch größere inhaltliche Änderungen an den essenziellen Anforderungen zu erwarten sind.

ISMS ist ein rollierender Prozess

Die Betreiber solcher kritischer Infrastrukturen der Energiewirtschaft müssen dem Entwurf zufolge ein Information Security Management System (ISMS) nach der ISO-Norm 27001, unter der Berücksichtigung des ergänzenden Leitfadens Energieversorgung (aktuelle Version DIN/IEC TR 27019), einführen und zertifizieren lassen – und das innerhalb von zwei Jahren nach dem Inkrafttreten des Gesetzes. Die Aufgabe eines ISMS ist es vor allem, die „Verfügbarkeit, Authentizität, Vertraulichkeit und Integrität“ der kritischen Infrastrukturen sicherzustellen, sagt Mario Kaiser, IT- und Informationssicherheitsbeauftragter bei dem IT-Anbieter prego services in Saarbrücken. Anschließend muss regelmäßig eine Re-Zertifizierung erfolgen. Zudem müssen die Unternehmen bestimmte IT-Sicherheitsvorfälle künftig dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Von den neuen Regelungen werden lediglich Firmen ausgenommen sein, die weniger als zehn Mitarbeiter haben und deren Jahresbilanz oder Umsatz 2 Mio. Euro nicht überschreiten. So geht es aus dem derzeit vorliegenden Entwurf des IT-Sicherheitsgesetzes hervor, sagt Volker Noë, Berater für IT-Strategie und Grundsatzfragen bei der SPE Unternehmensberatung, ein Unternehmen der Fichtner-Gruppe. Er weist gleichzeitig darauf hin, dass sich Gas- und Stromnetz- sowie Anlagenbetreiber sich nicht auf diese Ausnahmeregelungen berufen können: „Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des EnWG sind von den Regelungen der relevanten §§ 8a und 8b des IT-Sicherheitsgesetzes ausgenommen. Für sie kommt stattdessen der IT-Sicherheitskatalog der Bundesnetzagentur zum Tragen, der sich aus der Neufassung der § 11 Absätze (1a) bis (1c) EnWG ableitet: Und weder im Entwurf des EnWG noch des IT-Sicherheitskataloges ist derzeit eine De-minimis-Regelung enthalten.“ Allerdings ist laut Noë aus Kreisen der BNetzA zu vernehmen, dass man aktuell über die Aufnahme einer solchen Regelung nachdenkt – konkrete Größenordnungen werden dabei jedoch nicht genannt.

Prinzipiell geht es bei der Einführung eines ISMS primär nicht darum, durch einmalige Verbesserungsmaßnahmen die IT- und die Telekommunikationssysteme der Unternehmen auf ein aktuell und allgemein anerkanntes Sicherheitsniveau zu heben. „Vielmehr ist ein ganzheitlicher Ansatz zu verfolgen, durch welchen die Unternehmen die Sicherheit ihrer Systeme auf Dauer gewährleisten können“, erläutert Noë. Es soll durch ein ISMS ein rollierender Prozess in den Unternehmen in Gang kommen, um die Informationssicherheit laufend zu überwachen und kontinuierlich zu verbessern. Rund 80 Prozent der Norm beschreiben deshalb auch organisatorische Anforderungen und Managementaufgaben, lediglich etwa 20 Prozent beziehen sich auf konkrete technische und umgebungsbezogene Vorgaben.

Eine wichtige Rolle komme dabei auch der Geschäftsleitung zu, betont der Berater: „IT-Sicherheit nach der aktuellen ISO 27001 ist Chef-Sache und die Geschäftsleitung hat eine Vorreiterrolle einzunehmen. Damit soll das Bewusstsein für mehr Informationssicherheit im Unternehmen gestärkt werden, und das gelingt nur, wenn auch der Chef dahintersteht.“ So widmet sich Kapitel 5 der ISO 27001:2013 ausschließlich dem Thema Führung; der IT-Grundschutz des BSI sieht sogar explizit die Benennung eines für die Informationssicherheit verantwortlichen Managers vor, etwa eines Mitgliedes der Geschäftsleitung. Die Geschäftsführung ist beispielsweise für die Veröffentlichung von Sicherheitsrichtlinien verantwortlich, die im Einklang mit den Geschäftszielen stehen müssen. „Die Leitungsebene, aber auch jede einzelne Führungskraft, muss sich sichtbar zu ihrer Verantwortung bekennen und allen Mitarbeitern die Bedeutung der Informationssicherheit klarmachen.“

Handlungsempfehlungen zur Umsetzung eines ISMS

Quelle: SPE/Noe

Zügig mit Implementierung des ISMS beginnen

Mit der Pflicht, ein solches Information Security Management System zu etablieren, müssen Energieversorger künftig auch einen „IT-Sicherheitsbeauftragten als zentralen Ansprechpartner bestellen“, sagt Kaiser von prego services. Dieser betreue und überwache als Hauptverantwortlicher das ISMS und stehe den Behörden für Fragen rund um den Umsetzungsgrad von Maßnahmen oder Sicherheitsvorfällen zur Verfügung. Darüber hinaus ist eine Warn- und Alarmierungsstruktur einzurichten, die rund um die Uhr verfügbar sein muss.

„Um sich rechtzeitig auf die Erfüllung der Anforderungen vorzubereiten, sollten sich Energieversorger so schnell wie möglich mit dem Thema ISMS auseinandersetzen“, rät Kaiser. Aus seiner Erfahrung werde der Aufwand oftmals unterschätzt. „Ein zertifizierungsfähiges Information Security System führt man nicht von heute auf morgen ein. Selbst kleinere Unternehmen müssen mit Projekten rechnen, die mehr als ein halbes Jahr in Anspruch nehmen.“

Auch Noe empfiehlt, mit der Implementierung des ISMS zügig zu beginnen. Zum einen müsse sich ein solches System bereits über einen gewissen Zeitraum im produktiven Einsatz befinden, damit es auditiert und zertifiziert werden kann: Eine bloße Absichtserklärung zum Betrieb eines ISMS genügt hierfür nicht – sein Einsatz muss nachgewiesen werden. Zum anderen sollten Netzbetreiber unter wirtschaftlichen Aspekten die Anreizregulierung im Blick behalten. Denn 2015 stellt für die Gasnetzbetreiber ein Basisjahr dar, 2016 folgt das Fotojahr (das heißt, die letzte Möglichkeit für die anstehende Regulierungsperiode, die Kosten des Netzbetriebes unmittelbar in der nächsten Periode geltend zu machen) für die Sparte Strom. „Als Gas- oder Stromnetzbetreiber würde ich darauf achten, dass die ISMS-Einführungskosten noch im jeweiligen Basisjahr entstehen, damit ich sie umgehend in der nächsten Regulierungsperiode ansetzen kann – auch wenn das Gesetz noch nicht final verabschiedet ist.“

Da die ISO-Normen sehr abstrakt gehalten seien, sei es ohne Unterstützung schwierig, die konkret in der Praxis und unternehmensindividuell umzusetzenden Maßnahmen daraus abzuleiten. Laut Noë biete der IT-Grundschutz des BSI zwar vergleichsweise ausführliche und konkrete Ausführungen und Handlungsempfehlungen, die der jeweilige Sicherheitsbeauftragte heranziehen könne. Jedoch empfehlen Noë und Kaiser, sich von einem Dienstleister Unterstützung zu holen – auch wegen des engen zeitlichen Rahmens. Die Umsetzungsfrist für das ISMS wird wahrscheinlich zwei Jahre betragen.

Unternehmen sollten Soll-Ist-Abgleich vornehmen

Bevor Unternehmen damit beginnen, das System einzuführen, sollten sie zuvor einen Soll-Ist-Abgleich vornehmen, rät Noë weiter: „Unternehmen anderer Branchen, die sich bereits nach ISO 27001 haben zertifizieren lassen, erfüllten die damit einhergehenden Anforderungen in der Regel zu 20 bis 40 Prozent aus dem Stand – und auch in der Energieversorgerbranche ist es sicher nicht so, dass IT-Sicherheit bisher ein völliges Fremdwort gewesen ist.“ E&M