DIE AUSWIRKUNG DES IT-SICHERHEITSGESETZES AUF DIE ENERGIEVERSORGER

Vom „IT-Sicherheitsgesetz“ zum „IT-Sicherheitskatalog“

TEXT
KRZYSZTOF PASCHKE
GRC Partner GmbH

In dem im Jahr 2012 erschienenen Bestseller „Blackout“ beschreibt Marc Elsberg einen europaweiten Zusammenbruch der Stromnetze. Die Hauptfigur Piero Manzano, ein italienischer Informatiker vermutet einen Hackerangriff und versucht die Behörden zu informieren. Ist das eine literarische Fiktion oder ein mögliches Katastrophenszenario?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Medien bestätigen täglich zahlreiche, technisch sehr gut durchdachte und gezielte Hackerangriffe auf die Wirtschaft und Privatsphäre der Bürger. Durch eine Reihe von Maßnahmen will die Bundesregierung gezielt die digitale Wirtschaft fördern und die Cybersicherheit erhöhen. Im Dezember 2014 beschloss die Bundesregierung den wesentlich überarbeiteten Entwurf des IT-Sicherheitsgesetztes. Es ist ein Baustein der „Digitalen Agenda 2014-2017“ (Grundsätze der Digitalpolitik der Bundesrepublik). Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist am 25.07.2015 in Kraft getreten. Ziel des Gesetzes ist eine signifikante Verbesserung der IT-Sicherheit in Unternehmen und Behörden in Deutschland durch die Einhaltung eines Mindestniveaus an IT-Sicherheit. Darüber hinaus wird der Schutz der Bürgerinnen und Bürger in einem sicheren Netz verstärkt. Betroffen von dem Gesetz sind die Betreiber der sogenannten Kritischen Infrastrukturen. Kritische Infrastrukturen werden als „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 würden“ verstanden [Quelle: BMI]. Dazu gehören u.a. die Energie und Wasserwirtschaft.

„IT-Sicherheitskatalog“ und seine Ziele

Im August 2015 veröffentlicht die Bundesnetzagentur (BNetzA) den „IT-Sicherheitskatalog“, in dem Strom- und Gasnetzbetreiber verpflichtet werden ein Mindeststandard an IT-Sicherheitsmaßnahmen umzusetzen [Quelle: BNetzA]. Durch die Umsetzung der IT-Sicherheitsmaßnahmen soll ein nachhaltiger und ordnungsmäßiger Betrieb der relevanten Telekommunikations- und Datenverarbeitungssysteme gewährleistet werden. Die rechtliche Grundlage dafür liefert § 11 Abs. 1 des Energiewirtschaftsgesetzes (EnWG). Im Vordergrund des „IT-Sicherheitskataloges“ steht der Schutz der drei Grundwerte der Telekommunikations- und elektronischen Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb erforderlich sind: Verfügbarkeit, Integrität und Vertraulichkeit. Die Schutzziele werden durch die Umsetzung vordefinierter technischer und organisatorischer Maßnahmen im Rahmen eines Informationssicherheits-Managementsystems (ISMS) erreicht. Hier schreibt der „IT-Sicherheitskatalog“ die Implementierung der DIN ISO/IEC 27001 in der aktuellen Fassung vor. Darüber hinaus müssen die DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 berücksichtigt werden [Quelle: IT-Sicherheitskatalog]. Die Normen DIN ISO/IEC 27001 und 27002 liefern eine allgemeingültige Methodik für die Planung, Umsetzung und Aufrechterhaltung eines Informationssicherheits-Managementsystems. Die Norm ISO DIN/IEC TR 27019 liefert eine Umsetzungsanleitung für die IT-Sicherheitsmaßnahmen der Prozessteuerungssysteme der Energieversorgung. Es handelt sich dabei neben dem Umsetzungsleitfaden um einen erweiterten Maßnahmenkatalog für die Energieversorgung. Beide Maßnahmenkataloge aus dem Anhang A der Norm ISO DIN/IEC 27002 und ISO DIN/IEC TR 27019 sind umzusetzen und zu dokumentieren. Ein wesentlicher Aspekt der Implementierung eines ISMS ist die permanente Überprüfung seiner Aktualität und Wirksamkeit. Es wird explizit die von der ISO präferierte Methode PDCA empfohlen. In der Planungs-Phase (P-Plan) werden die Rahmenbedingungen, wie z.B. Verantwortlichkeiten, Leitlinien und Ziele für die Informationssicherheit festgelegt. Die Durchführungs-Phase (D-Do) dient der Umsetzung der festgelegten ISMS-Ziele und Maßnahmen. Die Prüfungs-Phase (C-Check) ist für die Messung und Überprüfung der umgesetzten Ziele und Maßnahmen sowie der Präsentation der Ergebnisse der Unternehmensleitung bestimmt. Die Handeln-Phase (A-Act) nutzt die Erkenntnisse aus den internen Audits und schließt den Zyklus durch die Umsetzung der Vorbeugungs- oder Korrekturmaßnahmen ab. Die hier skizzierte Methode (oder Modell) ist pragmatisch und effektiv in der Umsetzung.

BIG 5

VERÄNDERUNG · INTERNET OF THINGS · SOURCING · CYBER DEFENSE · EFFIZIENZ

Netzstrukturplan

Eine elementare Voraussetzung für die Feststellung des Schutzbedarfs und gezielte Umsetzung der geplanten IT-Sicherheitsmaßnahmen ist die genaue Kenntnis der Unternehmensorganisation, involvierten Anwendungen und IT-Komponenten. Die Struktur der Übersicht ist aus dem White Paper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ des Bundesverbandes der Energie- und Wasserwirtschaft e.V. (BDEW) abgeleitet worden und strikt in drei Bereiche strukturiert: Leitsysteme und Systembetrieb, Übertragungstechnik/Kommunikation, Sekundär-, Automatisierungs- und Fernwirktechnik [Quelle: BDEW]. Es wird ausdrücklich empfohlen die Komplexität des Netzstrukturplanes zu reduzieren (vgl. BSI-Standard 100-2).

Risikoanalyse

Grundvoraussetzung für die Planung und Angemessenheit der Maßnahmen ist die Durchführung einer Risikoanalyse auf die Komponenten, die für einen sicheren Netzbetrieb verantwortlich sind. Generell geht es darum festzustellen, welche internen und externen Gefährdungen, zusammengefasst in sieben Kategorien, zur negativen Beeinträchtigung der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) führen können. Sie ist explizit in der ISO DIN/IEC 27001 vorgeschrieben. Eine detaillierte Beschreibung der Risikoanalyse liefert die ISO DIN/IEC 27005. Sie ist wiederum von der ISO DIN 31001 abgeleitet worden. Der Risikomanagementprozess wird in der Regel in vier Schritten durchgeführt. Das sind Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikobehandlung. Bei der Risikobewertung sollen durch den „IT-Sicherheitskatalog“ vorgegebene und nur für Energie- und Gasversorger spezifische Schadenskategorien berücksichtigt werden.

Fristen

Die Umsetzungsfrist und eine adäquate Zertifizierung für die im „IT-Sicherheitskatalog“ genannten Normen und damit verbundene Maßnahmen ist von der Bundesnetzagentur für den 30.01.2018 festgesetzt worden. Verpflichtend ist auch die Nennung eines Ansprechpartners für alle IT-Sicherheitsaspekte des „IT-Sicherheitskataloges“.

Fazit

Die im „IT-Sicherheitskatalog“ definierten Anforderungen sind durch die Nennung der Normen, die umgesetzt werden müssen, klar vorgegeben. Nicht zu unterschätzen ist allerdings die zur Verfügung stehende Zeit. Grundvoraussetzung für eine erfolgreiche Umsetzung der gestellten Anforderungen ist eine klare Projektorganisation und vollständige Unterstützung der Geschäftsleitung mit Verständnis, qualifizierten Ressourcen und Budget. Unabdingbar für den Erfolg des Projektes ist die Mitwirkung aller Mitarbeiter aus den involvierten Bereichen bei der Umsetzung der Maßnahmen.

Literatur

[Quelle: BMI] www.bmi.bund.de/DE/Themen/Bevoelkerungsschutz/Schutz-Kritischer-Infrastrukturen/schutz-kritischer-infrastrukturen_node.html

[Quelle: BNetzA] www.bundesnetzagentur.de/DE/Sachgebiete/Elektrizitaetund-Gas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html

[Quelle: IT-Sicherheitskatalog] vgl. Seite 10 Normen

[Quelle: BDEW] BDEW Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ 2012

IT-Sicherheit & Notfallmanagement – Ein Integriertes Managementsystem

- IT-Grundschutz (BSI 100-2)
- (IT-)Notfallmanagement (BSI 100-4)
- IT-Risikoanalyse (BSI 100-3)
- ISMS (ISO 27001)
- IT-Risikoanalyse (ISO 27005)
- TR-RESISCAN (BSI-TR 03138)
- Datenschutz (BDSG, LDSG)
- Verfahrensdokumentation und IKS
- ISO (9001, 14001, 50001, …)

GRC Partner ▪ Schauenburgerstraße 116 ▪ 24118 Kiel ▪ Tel.: 0431 53033 990 ▪ info@grc-partner.de ▪ **grc-partner.de**