Sonderdruck (Nr. 7673)

ew

6 | 2019

Magazin für die Energiewirtschaft

>> www.ew-magazin.de

Kritische Infrastrukturen

Managerhaftung durch ungenügende IT-Sicherheit vermeiden

Eine rechtskonforme, technisch sichere und wirtschaftlich effiziente IT-Sicherheitsarchitektur ist für Betreiber kritischer Infrastrukturen ein Muss. Nur so können nicht nur gesetzliche Vorgaben eingehalten, sondern auch Reputationsschäden, Bußgelder oder Haftungsansprüche auch gegenüber dem Management vermieden werden. Dabei basiert ein verlässliches IT-Sicherheitskonzept immer auf den Basisdokumenten aus dem Qualitätsmanagement.

Aktuelle Hackerangriffe und IT-Sicherheitslücken bleiben heute oft über Monate unerkannt: Informationen können ausgespäht oder die IT-Infrastruktur kann unerkannt manipuliert werden. Kommt es zum Ernstfall und eine Cyberattacke greift spürbar in die öffentliche Versorgung ein, ist bei dem betroffenen Betreiber nicht nur mit Einnahmeausfällen und Reputationsschäden zu rechnen. Zudem kann ein Haftungsfall die verantwortlichen Personen im Unternehmen hart treffen. Laut den §§ 8a, 8b des BSI-Gesetzes müssen Betreiber kritischer Infrastrukturen (Kritis) angemessene organisatorische und technische Vorkehrungen zur Vermeidung von IT-Störungen treffen.

Auch wenn Kritis-Netzbetreiber ihre IT-Infrastruktur seit Mai 2018 mit einem branchenspezifischen Sicherheitskonzept geschützt und zertifiziert haben lassen müssen, ist die Realität eine andere. So gibt es immer noch Netzbetreiber, die ihre – für das Gemeinwesen als kritisch einzustufende – IT-Infrastruktur noch nicht ausreichend vor Cyberangriffen und Störungen gesichert haben. Folglich fehlen die gesetzlich verpflichteten Dokumentationen und Nachweise wie Zertifizierungen. Was bei alledem jedoch meist unterschätzt wird, sind die deutlich zunehmenden Haftungsrisiken, die für Vorstände, Aufsichtsräte und Geschäftsführer der Unternehmen virulent sind.

Unklar ist, ob alle Netzbetreiber, die unter die Schwellenwerte der BSI-Kritis-Verordnung fallen, ihrer Pflicht zur Implementierung einer angemessenen IT-Sicherheitsarchitektur bis Mai 2018 nachgekommen sind. Die Kritikalität müssen die Betreiber selbst feststellen – es gibt keinen Aufruf durch die Behörde. Doch die Auflagen steigen weiter. Um die Mindeststandards an die IT-Sicherheit im Energiesektor weiter zu konkretisieren, hat die Bundesnetzagentur (BNetzA) Ende Dezember 2018 den zweiten IT-Sicherheitskatalog nach § 11 Abs. 1b EnWG – für Betreiber von Erzeugungsanlagen – veröffentlicht. Dieser weitere Sicherheitskatalog richtet sich zusammen mit der BSI-Kritis-Verordnung an Anlagenbetreiber zur Stromerzeugung mit einer Netto-Nennleistung ab 420 MW sowie an größere Gasspeicher mit einer entnommenen Menge ab 5 190 GWh im Jahr.

Netzbetreiber und Erzeuger in der Pflicht

Die wesentliche Anforderung der beiden IT-Sicherheitskataloge im Energiesektor ist der Aufbau eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001. Während für die Kritis-Netzbetreiber die Umsetzungs- und Meldefristen längst abgelaufen sind, müssen die Betreiber kritischer Energieanlagen der BNetzA bis zum 31. März 2021 Zertifikate über die Informationssicherheit der betroffenen Anlagen vorlegen. Auch hier reicht die Bestätigung der internen IT-Abteilung oder eines unabhängigen Beraters zum sicheren IT-Betrieb nicht aus. Die Anforderungen an eine sichere IT müssen definiert, dokumentiert und durch eine akkreditierte Stelle zertifiziert sein. Zudem mussten die Betreiber der Erzeugungsanlagen bis Ende Februar 2019 Ansprechpartner für die IT-Sicherheit gemeldet haben.

Welche Folgen zeichnen sich ab? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den gesetzlichen Auftrag, die IT-Mindestsicherheitsstandards bei Kritis-Betreibern durchzusetzen. Dafür stehen außer der Überprüfung vor Ort Zwangsmittel der zuständigen Aufsichtsbehörde und die Verhängung von Bußgeldern durch das BSI selbst zur Verfügung. Allerdings wird mit dem seit Ende März 2019 vorliegenden Referentenentwurf zum IT-Sicherheitsgesetz 2 (IT-SiG 2.0) der rechtliche Rahmen der Strafverfolgungs- und Sicherheitsbehörden auf dem Gebiet der IT-Sicherheit deutlich erweitert. Geplant ist außerdem, dass die bestehenden Meldepflichten und Verpflichtungen zur Einhaltung der IT-Mindeststandards für Kritis-Betreiber auf weitere Bereiche der Wirtschaft ausgeweitet werden. Folglich dürfte auch die Abgrenzung der Kritikalität künftig schwieriger werden.

Hohe Bußgelder drohen im Haftungsfall

Wer haftet? Bei einem Vorfall und Verstoß, der einer unzureichend dokumentierten und umgesetzten IT-Sicherheit geschuldet ist, haftet zunächst der Kritis-Betreiber, also das Unternehmen. Laut BSI-Gesetz werden Verstöße als Ordnungswidrigkeiten mit Bußgeldern von bis zu 100 000 € geahndet. Noch drastischer können die Bußgelder bei datenschutzrechtlich relevanten IT-Sicherheitsvorfällen sein – bis zu 20 Mio. € oder 4 % des Jahresumsatzes des Betreibers.

Erst danach ist eine persönliche Haftung der Entscheider in der Unternehmensleitung möglich. Um das Management oder auch den Aufsichtsrat eines Kritis-Unternehmens in die Haftung nehmen zu können, sind die Schadensersatzvorschriften aus dem Gesellschaftsrecht und dem allgemeinen Zivilrecht relevant. Für die beiden gängigen Unternehmensformen, die AG und GmbH, verlangen die relevanten Haftungsnormen von Verantwortlichen die Beachtung des Sorgfaltsmaßstabs. Verstößt ein Manager in zumindest fahrlässiger Weise gegen diese Sorgfalt, kann ein behördlich auferlegtes Bußgeld letztlich auf das einzelne Mitglied der Geschäftsleitung durchschlagen.

Während bei Ordnungswidrigkeiten gemäß BSI-Gesetz höchstens eine Geldbuße von 100 000 € in Betracht kommt, kann bei Straftaten beispielsweise im Datenschutzrecht die Geldbuße des Managers auf maximal 1 Mio. € steigen. Auch eine direkte Haftung des Managers gegenüber dem Staat oder einem Geschädigten ist möglich, zum Beispiel wenn Versäumnisse bei der Implementierung der IT-Sicherheitsarchitektur und der Meldepflichten vorliegen.

Qualitätsmanagement für Energieversorger

An einer rechtskonformen, technisch sicheren und wirtschaftlich effizienten IT-Sicherheitsarchitektur führt vor allem für Kritis-Betreiber kein Weg vorbei. Der effektivste Weg zur Vermeidung von Reputationsschäden, Bußgeldern und Haftungsansprüchen ist die Validierung durch Dritte. Dieser Nachweis kann durch die Zertifizierung vor allem nach dem weltweit zugelassenen Standard ISO 27001 erbracht werden.

Was ist zu tun? Voraussetzung für ein hohes Sicherheits- und Qualitätsniveau ist die Dokumentation. In dem neuen IT-Sicherheitsgesetz 2 werden beispielsweise für den Energiesektor die folgenden Kernkomponenten als kritisch in puncto Sicherheit genannt: »IT-Produkte für die Kraftwerksleittechnik, Netzleittechnik oder für die Steuerungstechnik zum Betrieb von Anlagen oder Systemen zur Stromversorgung, Gasversorgung, Kraftstoff- oder Heizölversorgung oder Fernwärmeversorgung«.

Entscheidend ist, dass sich die Verantwortlichen im Unternehmen einen Überblick über die internen und externen Anforderungen ihrer kritischen Infrastruktur verschaffen. Sie müssen die einzelnen IT-Komponenten, Dienste und Prozesse kennen, um diese mit einer angemessenen Schutzklasse bewerten und steuern zu können. Erst daraus ergeben sich der notwendige Dokumentationsaufwand sowie Umfang und Art der umzusetzenden technischen und organisatorischen Maßnahmen.

Letztlich baut eine belastbare Informations- und Datensicherheit immer auf der Highlevel-Struktur des klassischen Qualitätsmanagements nach ISO 9001:2015 auf. Dieses Qualitätsmanagement – in Kombination mit einem Managementsystem für Informationssicherheit (ISMS) nach DIN EN ISO/IEC 27001 – beschreibt technische und organisatorische Maßnahmen sowie die bewerteten Schutzklassen. Erst in Verbindung mit den Maßnahmen zur Informationssicherheit für die Energieversorgung (ISO/IEC 27019:2017), die spezifische Anforderungen des Sektors enthalten, sind die Kritis-Anforderungen erfüllt.

Um das angestrebte IT-Sicherheitsniveau zu definieren und kontinuierlich an die aktuelle Gefährdungslage anzupassen, ist die Dokumentation der IT-Prozesse ein Muss. Es ist gleichsam ein wichtiges Signal, dass sich das Unternehmen strukturiert mit der IT-Sicherheit befasst. So gründet ein verlässliches IT-Sicherheitskonzept immer auf den Basisdokumenten aus dem Qualitätsmanagement. Diese Dokumente zu erstellen, kann nicht an einen IT-Beauftragten delegiert werden, sondern das Statement eines sicheren IT-Betriebs liegt im Verantwortungsbereich des Managements.

Manfred Grühn,
Industry Expert und Auditor,
Dekra Certification GmbH,
Berlin/Stuttgart

Dr. **Hans v. Gehlen**,
Rechtsanwalt und Partner,
Beiten Burkhardt
Rechtsanwaltsgesellschaft
mbH, Frankfurt am Main

Johannes Jäger,
Rechtsreferendar,
Beiten Burkhardt
Rechtsanwaltsgesellschaft
mbH, Frankfurt am Main

>> cybersecurity.de@dekra.com

>> www.dekra-certification.de
www.beiten-burkhardt.com