Für mehr **Sicherheit**

Die aktuelle **Cyberbedrohungslage** hat zu weitreichenden Initiativen auf internationaler Ebene geführt. Guido Gluschke* stellt sie vor.

In Onlineforen ist die Rede von einem vertraulichen Lagebericht des Cyberabwehrzentrums deutscher Sicherheitsbehörden, der vor Stromausfall in ganz Europa durch Cyberattacken warnt. Auch der ehemalige US-General Petraeus führte bei einer Cybersicherheitskonferenz im Mai in Tallinn aus, dass sein schlimmstes Szenario ein massiver Cyberangriff auf die Stromversorgung der USA sei. Diese Befürchtung beruht nicht nur auf dem Wissen, dass Cyberangriffe auf kritische Infrastrukturen wie Stromnetze schon jetzt Realität sind, sondern auch darauf, dass es keine internationalen Normen für Cyberkonflikte gibt. Daher existiert auch bei Angriffen von militärischer Qualität nach Meinung vieler Experten keine formale Schwelle zum Kriegszustand, die überschritten werden könnte. Damit würde die neue Cyberabwehr des Bundesverteidigungsministeriums nicht zum Einsatz kommen. Solche Angriffe müssen also von den Betreibern kritischer Infrastrukturen selbst abgefangen werden. Deutsche Energieversorger können jederzeit Ziel eines solchen Cyberangriffs werden, und sei es nur, um die Wirksamkeit von Cyberwaffen zu testen. Darauf müssen sie vorbereitet sein.

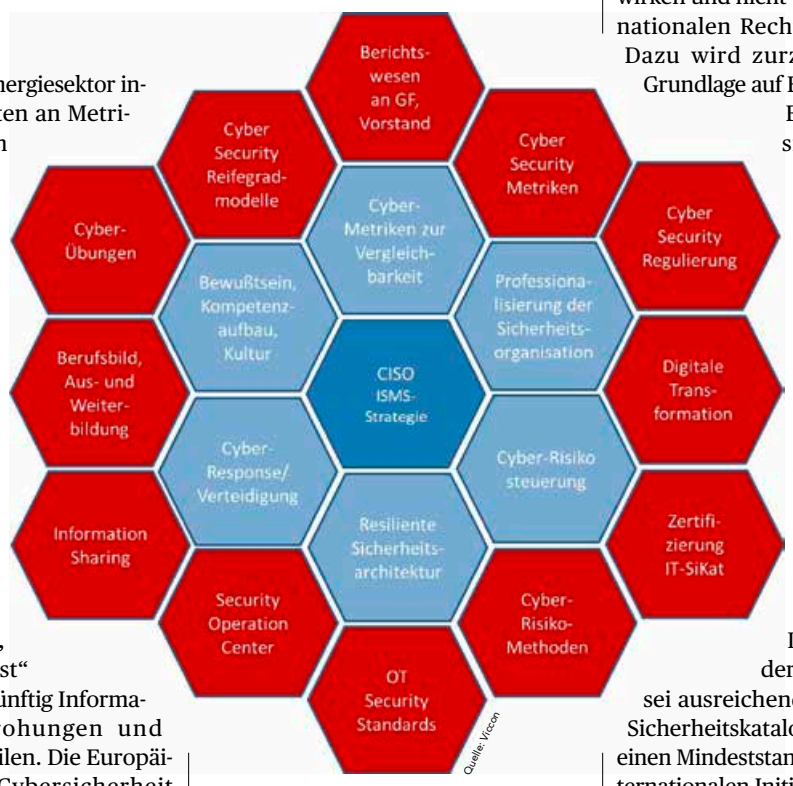
Informationen über Bedrohungen und Schwachstellen sollen geteilt werden

Aus diesem Grund hatte die Europäische Kommission 2015 ein Expertengremium, die Energy Expert Cyber Security Platform (EECSP), eingesetzt, das Lücken in der bestehenden Gesetzgebung zur Cybersicherheit in der Energieversorgung aufdecken sollte. In seinem 2017 veröffentlichten Bericht werden vier strategische Prioritäten empfohlen: Aufbau eines effektiven Bedrohungs- und Risikomanagements für den Cyberraum, Aufbau einer effektiven Cyberverteidigung, kontinuierliche Verbesserung der Cyberwiderstandsfähigkeit sowie Aufbau der benötigten Cyberfähigkeiten und Kompetenzen. Während Deutschland selbst auf dem Energiesektor in diesen vier Feldern eher zurückhaltend agiert, finden sich die strategischen Prioritäten in europäischen und internationalen Aktivitäten wieder. So hat das Weltwirtschaftsforum im Mai 2018 eine Arbeitsgruppe zur Cyberwiderstandsfähigkeit (Resilience) bei der Stromversorgung eingerichtet, die einen Bericht erarbeitet, um dieses Thema auf höchster Ebene zu adressieren und Handlungsempfehlungen anzubieten. Aus dieser Initiative haben sich jüngst Organisationen zusammengefunden, die das Ziel haben, international anerkannte Metriken für Cybersicherheit im Energiesektor zu entwickeln, sodass Cyber Security auch für Unternehmenslenker greifbar und messbar wird. Sowohl Acer – als EU-Agentur der Regulierer für Energie und Mitglied dieser Gruppe – wie auch CEER – als Rat der europäischen Regulierer – sind stark an europaweiter Messbarkeit und Vergleichbarkeit von Cybersicherheit im Energiesektor interessiert und arbeiten an Metriken, die dann von den Energieversorgern zu bedienen sind.

Andere Organisationen haben sich zum European Energy Information Sharing and Analysis Center (EE-ISAC) zusammengeschlossen, das sich zurzeit um den Austausch von Informationen zwischen Energieversorgern und dritten Parteien kümmert. Ziel ist es, ein „Network of Trust“ aufzubauen und zukünftig Informationen über Bedrohungen und Schwachstellen zu teilen. Die Europäische Behörde für Cybersicherheit Enisa sowie das Cyber Defence Center der Nato in Tallinn sind Mitglied im EE-ISAC und können gewonnene Gefährdungsinformationen beisteuern. Darüber hinaus arbeitet die Europäische Kommission an der Weiterentwicklung der Regulierung zur Cybersicherheit im Energiesektor. Eine neue Expertenkommission erarbeitet bis Ende 2018 auf Grundlage des EECSP-Reports einen Network Code, wie er als Instrument der Entso-E für Übertragungsnetzbetreiber heute schon verwendet wird. Damit soll eine Auswahl an relevanten Themen der vier strategischen EECSP-Prioritäten weiterentwickeln. Dazu zählen:

- Reifegradmodell für Energieversorger
- Rahmenwerk für Cyberverteidigung im Energiesektor
- Zertifizierung von digitalen Geräten für das Stromnetz
- Methode zur Bestimmung der Wertigkeit von Informationen im Energiesektor
- Benachrichtigungssystem für Vorfälle mit einer größeren Auswirkung
- Harmonisierte Auswahlkriterien von kritischen Infrastrukturbetreibern
- Mindeststandards für Cybersicherheit von Energieversorgern.

Das Ergebnis dieser Entwicklungen soll via Network Code direkt für die Verteilnetz- und Übertragungsnetzbetreiber wirken und nicht über den Umweg des nationalen Rechts geregelt werden. Dazu wird zurzeit die juristische Grundlage auf EU-Ebene geschaffen.



Elemente einer Strategie für ein Informationssicherheits-managementsystem

„Es ist unumgänglich, sich mit den Entwicklungen außerhalb des eigenen Blickfelds und Tagesgeschäfts zu beschäftigen“

Es ist abzusehen, dass sich für einen Chief Information Security Officer (CISO) zukünftig weitere Aufgaben aus den genannten Themenfeldern ergeben. Vorteile haben die Unternehmen, die diese Entwicklungen erkannt und schon in ihrer Planung berücksichtigt haben im Gegensatz zu denen, die glaubten, eine pure Erfüllung des IT-Sicherheitskatalogs der Bundesnetzagentur sei ausreichend. Dabei sagt der IT-Sicherheitskatalog selbst, dass er nur einen Mindeststandard darstellt. Die internationalen Initiativen fokussieren jedoch nicht so sehr auf Investitionen in IT-Maßnahmen, sondern vielmehr auf die Professionalisierung der Sicherheit, Vergleichbarkeit und Transparenz für die Entscheidungsträger bei Energieversorgern und Regulierern.

Reife Unternehmen entwickeln eine Strategie für ein Informationssicherheitsmanagementsystem (ISMS), das zukünftige Cyberentwicklungen mit berücksichtigt.

Wichtiges Element einer solchen ISMS-Strategie ist die Cyber-Response-Fähigkeit, also die Fähigkeit, mit außergewöhnlichen Situationen im Cyberraum umzugehen, um das eigene Unternehmen wirkungsvoll verteidigen zu können. Diese Reaktionsfähigkeit setzt neben Vorbereitung und Wissen ein permanentes Cyberlagebild und situationsangemessene Handlungsfähigkeit voraus. Letztere entsteht durch das Cyberlagebild, gepaart mit der Fähigkeit, angemessen auf Ereignisse zu reagieren. Hier helfen speziell entwickelte Cyberübungen.

Ein Baustein für ein permanentes Cyberlagebild, also der sofortigen Erkennung und Abwehr von Cyberangriffen, ist die Existenz eines Security Operation Center (SOC). In diesem werden Bedrohungsinformationen analysiert und mit Schwachstelleninformationen verknüpft, um ein gutes Verständnis der eigenen Verwundbarkeit zu bekommen. Dabei werden sogenannte Indicators of Compromise (IoC), also strukturierte Informationen über Cybergefahren, ausgetauscht und zu einem Cyberlagebild verarbeitet. Ein Pilotprojekt ist gerade im EE-ISAC mit seinen Partnern im Aufbau, während ein Referenzmodell für ein Energy-SOC von einem der Partner entwickelt wird.

Innogy ist Vorreiter in Sachen Cybersicherheit

Beim Einsatz einer so schnelllebigen und gefährlichen Technologie, wie sie das Internet darstellt, ist es unumgänglich, sich mit den Entwicklungen außerhalb des eigenen Blickfelds und Tagesgeschäfts zu beschäftigen. Vorreiter der deutschen Energieversorger auf dieser internationalen Bühne ist einzig Innogy. Es stellt sich die Frage, ob es der Branche an strategischer Vorstellungs- und Innovationskraft fehlt, die, gemessen am Engagement, im benachbarten europäischen Ausland deutlich stärker ausgeprägter ist. Da die Digitalisierung kommt, ist gute Cyber Security essenziell.

Dabei basiert Cyber Security auf Gesetzen der Informatik – Teil der Ingenieurswissenschaften und somit deutsche Domäne. Aber anstelle von bewährten ingenieurstechnischen Ansätzen werden häufig Personen ohne entsprechende Ausbildung mit dem Thema betraut. Dies mag dem Fachkräftemangel oder dem fehlenden Verständnis der Entscheider geschuldet sein. Ohne ein Umdenken an dieser Stelle und ohne ähnliche fachliche Qualifikationsanforderungen wie im Ingenieurwesen wird sich ein Stromnetz in Zukunft jedoch nicht mehr sicher und effizient betreiben lassen. Der Studiengang „Security Management“ an der TH Brandenburg ist zum Beispiel ein Baustein für den langfristigen Erfolg von Energieversorgern. **E&M**

* Guido Gluschke, Co-Direktor des Institute for Security and Safety an der Technischen Hochschule Brandenburg

ENERGIE & MANAGEMENT
ZEITUNG FÜR DEN ENERGIEMARKT