

Cyber-Schutz ist Chefsache

Wer Cyber-Resilienz auf technische Schutzmaßnahmen reduziert, greift zu kurz. Die Technik muss auch in entsprechende organisatorische Prozesse eingebettet sein, mit klaren Verantwortungsstrukturen und Entscheidungswegen. Cyber-Sicherheit wird somit zur Managementaufgabe.

Cyber-Sicherheit in der Energieversorgung wird oftmals von Technologien dominiert: Firewalls, Security Operations Center (SOC), Angriffserkennung oder Künstliche Intelligenz. Diese Werkzeuge sind wichtig, doch sie allein machen Unternehmen nicht resilient. Die Erfahrungen aus der Energiewirtschaft sowie die regulatorischen Anforderungen aus NIS2 zeigen: Cyber-Resilienz ist vor allem eine Frage von Führung, Organisation und Entscheidungsfähigkeit. Nicht fehlende Tools sind heute das größte Risiko, sondern fehlende Verantwortlichkeiten und unklare Entscheidungen.

Gerade Energieversorger stehen im Fokus. Die Bedeutung von Versorgungssicherheit und Energieverfügbarkeit, die zunehmende Digitalisierung von Geschäftsprozessen sowie die enge Verzahnung von IT und Betriebstechnologie (OT) vergrößern die Angriffsfläche. Gleichzeitig steigt die Bedrohungslage: Cyber-Angriffe werden professioneller, automatisierter und zunehmend durch KI unterstützt. Die entscheidende Frage lautet daher nicht mehr, ob ein Angriff erfolgt, sondern wie gut ein Unternehmen darauf vorbereitet ist.

Resilienz für Energieversorger bedeutet: die Fähigkeit, Störungen, Angriffe oder Krisen so zu bewältigen, dass die Versorgung aufrechterhalten oder schnell wiederhergestellt werden kann. Dafür

braucht es technische Schutzmaßnahmen. Vor allem aber braucht es Menschen und Organisationen, die unter Unsicherheit Entscheidungen treffen können. Denn im Ernstfall bleibt oft nur wenig Zeit. Risiken müssen bewertet und Kommunikationswege aktiviert werden, Maßnahmen sind zu priorisieren und Meldepflichten einzuhalten.

Die Realität zeigt jedoch, dass viele Unternehmen Cyber-Sicherheit noch immer primär als IT-Thema betrachten. Genau hier liegt eine der größten Herausforderungen. Denn Cyber-Resilienz entsteht nicht im Rechenzentrum, sondern im Zusammenspiel von Governance, Prozessen, Menschen und Technik.

NIS2 verändert die Perspektive

Mit der Umsetzung der europäischen NIS2-Richtlinie hat sich der Blick auf Cyber-Sicherheit grundlegend verändert. Erstmals rückt die Verantwortung der Unternehmensleitung ausdrücklich in den Mittelpunkt. Geschäftsführungen

und Vorstände müssen Sicherheitsmaßnahmen billigen, Risiken bewerten, Schulungen absolvieren und können bei Versäumnissen persönlich haftbar gemacht werden. Diese Entwicklung verdeutlicht einen wesentlichen Paradigmenwechsel: Cyber-Sicherheit wird zur Managementaufgabe.

Viele Unternehmen reagieren zunächst mit der Frage, welche technischen Maßnahmen sie nun umsetzen müssen. Doch ein Blick auf die Anforderungen zeigt, dass hinter den technischen Themen vor allem organisatorische Fragestellungen stehen: Wer priorisiert Risiken? Wer entscheidet über Investitionen? Wer übernimmt Verantwortung im Krisenfall? Und wer stellt sicher, dass Sicherheitsentscheidungen dokumentiert und nachvollziehbar sind? Die Komplexität der Anforderungen ist dabei oft nicht das eigentliche Problem. Schwierig wird es, wenn Verantwortlichkeiten unklar bleiben oder Entscheidungen aufgeschoben werden.

Verantwortung verankern

Resiliente Organisationen zeichnen sich durch klare Verantwortungsstrukturen aus. Sie verfügen

GISA GmbH



Der Autor: Jörn Haußen

Jörn Haußen ist Business Line Manager Utilities bei der GISA GmbH. Der Diplom-Ingenieur für Energie- und Versorgungstechnik (FH) verantwortet die GISA-Branchenstrategie im Bereich Energiewirtschaft und treibt innovative Lösungen für die digitale Transformation der Branche voran.

über definierte Rollen und Entscheidungswege sowie ein gemeinsames Verständnis von Risiken. Dabei ist nicht entscheidend, ob Funktionen wie Informationssicherheit, Risikomanagement, Compliance oder Datenschutz zentral oder dezentral organisiert sind. Es kommt darauf an, dass das gewählte Vorgehen Entscheidungen ermöglicht. Wer trägt die Verantwortung für Cyber-Risiken? Wer berichtet regelmäßig an die Geschäftsführung? Wer hat die Befugnis, Entscheidungen vorzubereiten und Maßnahmen einzuleiten? Solche Fragen müssen beantwortet sein, bevor über konkrete Technologien diskutiert wird.

In der Praxis zeigt sich immer wieder, dass Unternehmen während eines Sicherheitsvorfalls wertvolle Zeit verlieren, weil Zuständigkeiten ungeklärt sind. Technische Lösungen können Angriffe erkennen. Sie können jedoch nicht entscheiden, welche Systeme abgeschaltet werden dürfen, welche Risiken akzeptiert werden oder wie gegenüber Kunden, Behörden und Öffentlichkeit kommuniziert wird. Deshalb beginnt Cyber-Resilienz mit einer belastbaren Governance-Struktur.

Technik allein reicht nicht

Natürlich benötigen Energieversorger moderne Sicherheitslösungen. Angriffserkennung, Netzwerküberwachung, Back-up- und Wiederanlaufkonzepte, Multi-Faktor-Authentifizierung oder Security Operations Center bilden wichtige Bausteine einer resilienten Sicherheitsarchitektur.

Technologie entfaltet ihren Nutzen jedoch erst dann vollständig, wenn sie in organisatorische Prozesse eingebettet ist. Selbst die beste

Sicherheitsplattform hilft wenig, wenn niemand festgelegt hat, wer bei einem Alarm entscheidet und handelt. Hinzu kommt ein weiterer Aspekt: Mit der zunehmenden Nutzung von Künstlicher Intelligenz entstehen neue Chancen und Risiken. KI unterstützt Sicherheitsverantwortliche bei der Analyse großer Datenmengen, Anomalien werden schneller und präziser erkannt und Reaktions-

delegiert werden. Sie ist eine Gemeinschaftsaufgabe.

Handlungsfähig bleiben

Die Energiewirtschaft befindet sich in einem tiefgreifenden Wandel. Digitalisierung, Smart Grids, intelligente Messsysteme und KI schaffen neue Möglichkeiten, erhöhen aber gleichzeitig die Anforderungen an Sicherheit und Stabilität.



Cyber-Resilienz entsteht im Zusammenspiel von Governance, Prozessen, Menschen und Technik.

zeiten verkürzt. Gleichzeitig gehen damit gesteigerte Anforderungen an Governance, Transparenz, Datenqualität und Risikomanagement einher. Auch hier gilt: Technik unterstützt; die Verantwortung bleibt beim Menschen.

Cyber-Resilienz entsteht nicht allein auf Führungsebene. Sie muss Teil der Unternehmenskultur werden. Regelmäßige Schulungen, Awareness-Maßnahmen und ein offener Umgang mit Risiken sorgen dafür, dass Sicherheitsbewusstsein in allen Bereichen verankert wird – von der Leitwarte bis zum Vorstand. Gerade in der Energiewirtschaft, in der IT und OT in operativen Prozessen eng verknüpft sind, wird deutlich: Sicherheit kann nicht an einzelne Abteilungen

Wer Cyber-Resilienz auf technische Schutzmaßnahmen reduziert, greift zu kurz. Die Integration zwischen Technik und Organisation ist in jedem Unternehmen individuell und eigenverantwortlich zu implementieren und weiterzuentwickeln. Die entscheidenden Voraussetzungen sind klare Verantwortlichkeiten, wirksame Governance-Strukturen und die Bereitschaft, unter Unsicherheit Entscheidungen zu treffen. Resiliente Energieversorger investieren deshalb nicht nur in Technologien, sondern in Menschen, Führung, Organisation und Sicherheitskultur. Denn Resilienz entsteht dort, wo Unternehmen entscheidungsfähig werden. Cybersecurity ist deshalb keine Aufgabe der IT allein. Sie ist eine Kernverantwortung der Unternehmensleitung. ■