Handelsblatt
DONNERSTAG, 12. FEBRUAR 2026, NR. 30

Kritische Infrastruktur

Mehr Schutz für das Energiesystem

Mit der Energiewende entstehen auch neue Angriffspunkte für Cyberattacken. Die Versorger treffen Vorkehrungen, könnten aber mehr tun. Jetzt macht die Politik Druck.

Ralph Diermann München

Das vergangene Jahr endete in Polen fast mit einem Stromausfall. Am 29. Dezember griffen mutmaßlich russische Saboteure mit einer Schadsoftware mehrere Umspannwerke an. Hier wird Strom aus Wind- und Solarparks sowie einem großen Heizkraftwerk übertragen. Die installierte IT-Security-Software konnte gerade noch verhindern, dass im Land die Lichter ausgehen.

Auch die deutsche Energieinfrastruktur wird immer wieder von Cybersaboteuren angegriffen. Zu Stromausfällen kam es dabei zwar noch nicht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Bedrohungslage dennoch als hoch ein. Insgesamt 68 kritische Vorfälle meldete die Energiebranche der Behörde im ersten Halbjahr 2025. Verantwortlich waren dafür laut dem BSI neben staatlich unterstützten, auf Destabilisierung und Spionage zielenden Hackern etwa aus Russland und China auch kriminelle Gruppen. Sie verschlüsseln die Daten der Energieunternehmen und erpressen für die Entschlüsselung Geld. Das BSI warnt zudem vor möglichen Cyberattacken radikaler Klimaschützer.

Die Energiewende hilft den Angreifern. Die Abkehr von Kohle und Kernkraft bedeutet auch, dass Energie nicht mehr in einzelnen, großen Kraftwerken erzeugt wird. Knapp sechs Millionen Photovoltaikanlagen und etwa 32.000 Windräder sind heute in Betrieb. Dazu kommen circa zwei Millionen Wärmepumpen, ungefähr 1,5 Millionen private Wallboxen sowie knapp 200.000 öffentliche Ladepunkte für Elektroautos, die als Stromverbraucher mit hoher Leistung ins System integriert werden müssen. „Die Zahl möglicher Einfallstore für Cyberattacken ist stark gewachsen“, sagt Alexander Giehl, Forscher am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC).

Denn viele der Anlagen sind über das Internet, Mobilfunk oder andere Kanäle vernetzt, um sie aus der Ferne überwachen und steuern zu können. Unternehmen bündeln Erneuerbare-Energien-Anlagen und Batteriespeicher für eine stärkere Position am Strommarkt zu virtuellen Kraftwerken. Servicefirmen nutzen digitale Plattformen zur Fernwartung von Anlagen, IT-Systeme steuern den Betrieb von Wärmepumpen und Wallboxen zentral. Dringen Angreifer in eines dieser Steuerungs- oder Kommunikationssysteme ein, können sie erheblichen Schaden anrichten – etwa indem sie Wärmepumpen in schnellem Rhythmus ein- und ausschalten, um die Netzfrequenz und damit die Versorgung zu destabilisieren.

Durch die Hintertür

Auch können die Anlagenkomponenten schon bei Lieferung Schwachstellen eingebaut haben. „Untersuchungen haben gezeigt, dass manche nicht europäischen Solar-Wechselrichter mit Hintertüren ausgestattet sind, die es theoretisch ermöglichen, alle angeschlossenen Anlagen abzuschalten“, sagt Giehl. „Dadurch entstehen Kaskadeneffekte, die weitreichende Konsequenzen bis zu einem großflächigen Stromausfall haben könnten.“

Versorger, Anlagen- und Netzbetreiber könnten sich vor solchen Angriffen „schon mit relativ einfachen Mitteln“ schützen, sagt Johannes Müller-Lahn, Geschäftsführer des Cybersicherheits-Dienstleisters Allgeier Cy Ris. Dazu gehöre ein leistungsstarkes System zur Früherkennung von Angriffen, aber auch Schutzmaßnahmen an Endgeräten wie Laptops oder Smartphones. Um die Wirksamkeit ihrer Schutzmaßnahmen zu prüfen, sollten die Unternehmen zudem regelmäßig Penetrationstests durchführen. Entscheidend sei, „dass die Cybersicherheit ganz oben im Unternehmen aufgehängt wird“, sagt Müller-Lahn. „Die Geschäftsführung muss dafür sorgen, dass sich alle Mitarbeiter der Bedeutung des Themas bewusst werden.“ Das verringere das Risiko, dass Beschäftigte den Angreifern unfreiwillig helfen, in ein System einzudringen, etwa durch das Öffnen infizierter E-Mail-Anhänge.

Auch KI-Werkzeuge können beim Schutz vor Cyberangriffen helfen, sagt Nikolai Puch, der wie Giehl am Fraunhofer AISEC forscht. „Beim Erkennen von Anomalien ist KI den alten regelbasierten Verfahren weit überlegen, weil sie Abweichungen von der Norm viel früher und flexibler erkennt.“ Solche Instrumente würden bereits vereinzelt in der Praxis eingesetzt. Puch erwartet, dass KI-Schutzsysteme künftig stark an Bedeutung gewinnen werden. Forscher arbeiten intensiv an deren Weiterentwicklung. Allerdings rüstet die Gegenseite ebenfalls auf: Hacker nutzen KI-Instrumente etwa, um Schwachstellen in den Schutzmaßnahmen zu finden oder per Phishing Beschäftigte zu manipulieren.

Das Verständnis für die Bedeutung der Cybersicherheit ist laut Müller-Lahn in den meisten Unternehmen der Energiebranche mittlerweile groß. Bei der Umsetzung gebe es allerdings in manchen Unternehmen Nachholbedarf: „Zum Beispiel arbeiten manche Systeme noch mit veralteter Software, weil versäumt wurde, regelmäßig Updates vorzunehmen.“ Auch die Systeme und Sicherheitsprotokolle selbst seien mitunter nicht auf dem neuesten Stand. Ähnlich beurteilt Giehl die Lage. „Das Thema ist angekommen, in der gesamten Energiewirtschaft“, sagt der Fraunhofer-Forscher. Gerade große Unternehmen hätten zuletzt viel für den Schutz ihrer Anlagen und Systeme getan. „Bei manch kleinen gibt es allerdings noch Defizite, vor allem weil ihnen dafür die nötigen Ressourcen fehlen“, sagt Giehl.

Verschärfte Meldepflichten

Angesichts der immer angespannteren geopolitischen Lage macht jetzt auch die Politik mehr Druck. Die EU hat mit der sogenannten NIS-2-Richtlinie die Anforderungen an die Cybersicherheit deutlich erhöht. Die Bundesregierung setzte die Vorgaben im Dezember in nationales Recht um. Das Gesetz verpflichtet die Netzbetreiber sowie viele Anlagenbetreiber und Anbieter digitaler Dienste, ihre Schutzmaßnahmen zu verstärken. Sie müssen ihre IT-Sicherheit prüfen und vertraglich absichern. Auch die Meldepflichten wurden verschärft. Das Gesetz nimmt die Geschäftsführer der Unternehmen persönlich in die Haftung, wenn sie die Maßnahmen in ihren Unternehmen nicht wie gefordert umsetzen. „NIS-2 ist ein sehr wichtiger, längst überfälliger Schritt für mehr Cybersicherheit in der kritischen Infrastruktur“, sagt Giehl. BSI-Präsidentin Claudia Plattner spricht gar von einem „Gamechanger für die Sicherheit und Stabilität unseres Landes“.

Die geplante Neufassung des Cybersecurity Act geht noch weiter. Laut einem Entwurf, den die EU-Kommission Mitte Januar vorgestellt hat, soll künftig auch potenziell sicherheitsgefährdende Technik verboten werden können. Damit zielt die EU vor allem auf Solar-Wechselrichter aus China, über die sich daran angeschlossene Photovoltaikanlagen fernsteuern lassen könnten. Wolfram Axthelm, Geschäftsführer des Bundesverbands Erneuerbare Energie (BEE), befürwortet die Pläne. „Angesichts der neuen geopolitischen Lage ist es sehr sinnvoll, dass die EU nun genauer hinschaut, ob wir uns mit den chinesischen Solar-Wechselrichtern nicht in eine gefährliche Abhängigkeit bewegen. Zumal wir in Europa eine eigene, starke Wechselrichter-Fertigung haben“, sagt er.

68

kritische Vorfälle meldete der Energiesektor in der ersten Jahreshälfte 2025.

Quelle: BSI

Allerdings hält er es für überzogen, auch bereits installierte Geräte austauschen zu lassen. „Ein etwaiges Verbot darf nur für neue Wechselrichter gelten.“

Sicherheitsexperte Müller-Lahn ist dagegen nicht überzeugt, ob ein reines Verbot von Wechselrichtern aus China sinnvoll ist. Attacken seien schließlich nicht nur über Wechselrichter, sondern auch über andere Hardware möglich. Er plädiert deshalb dafür, die Diskussion weiter zu fassen. Zudem stelle sich die Frage, ob man dann nicht konsequenterweise auch Produkte aus anderen Ländern vom europäischen Markt verbannen sollte, sagt Müller-Lahn: „China ist schließlich nicht der einzige Lieferant kritischer Energietechnik, bei dem wir uns fragen sollten, ob wir ihm voll und ganz vertrauen können.“