Cyberangriffe auf Stromversorgung

Wenn ein Land in der Dunkelheit versinkt

Stromerzeuger und Netzbetreiber werden zunehmend zur Zielscheibe von Hackerangriffen. Aufgrund der sich häufenden Vorfälle sind IT- und Cybersecurity-Spezialisten im Energiesektor gefragter denn je.

Erst bei einem Stromausfall wird uns bewusst, wie abhängig wir im alltäglichen Leben von elektrischer Energie sind und wie selbstverständlich die konstante Versorgung mit Strom für uns ist Quelle: Pixabay

Stellen Sie sich vor, plötzlich ist es dunkel und nichts funktioniert mehr: Die Lichtschalter streiken, aus der Leitung fließt kein Wasser mehr, die Internetverbindung bricht ab, das Licht der Straßenlaternen erlischt, Ampeln fallen aus, Aufzüge bleiben stecken und der Bahnverkehr kommt zum Erliegen. Totaler Stromausfall. Auf den Straßen bricht Chaos aus. In den Krankenhäusern springen die Notstromaggregate an. Erst in diesem Moment wird uns bewusst, wie abhängig wir im alltäglichen Leben von elektrischer Energie sind und wie selbstverständlich die konstante Versorgung mit Strom für uns ist.

Einen Stromausfall hat jeder schon einmal erlebt. Meist sind die Probleme lokal begrenzt und innerhalb weniger Minuten oder einer Stunde wieder behoben – aber was, wenn dieser Zustand ein ganzes Land betrifft und über längere Zeit hinweg anhält? Ein Szenario, das Marc Elsberg in seinem Buch »Blackout – Morgen ist es zu spät« sehr anschaulich beschreibt: Nach einem Hackerangriff bricht das europäische Stromnetz innerhalb kurzer Zeit zusammen, Millionen von Menschen sind plötzlich ohne Strom. Damit greift der Autor ein Thema auf, das die Energiebranche bereits seit einigen Jahren beschäftigt.

Mehr Angriffsfläche durch Digitalisierung und Dezentralisierung

Der Energiesektor zählt zu den sog. kritischen Infrastrukturen. Per Definition zählen hierzu alle Organisationen oder Einrichtungen, die für das staatliche Gemeinwesen wichtig sind und deren Ausfall oder Beeinträchtigung zu Engpässen bei der Versorgung, Schwierigkeiten bei der Wahrung der öffentlichen Sicherheit und anderen verheerenden Folgen führen würde. Wie ein Dominoeffekt wirkt sich die Unterbrechung der Energieversorgung auf andere Bereiche aus und bringt

Thomas Hoppe, Business Unit Manager für die Branche Energy & Utility, Hager Unternehmensberatung GmbH, Frankfurt (Main)

nach und nach die einzelnen Spielsteine im Zusammenwirken von Staat, Wirtschaft und Gesellschaft zu Fall.

Durch die fortschreitende Digitalisierung der Energiewirtschaft, die Verkettung von Stromleitungen und dem Datenverkehr sowie die Dezentralisierung der Netze im Zuge der Energiewende nehmen die Sicherheitsschwachstellen zu. Auch in den privaten Haushalten werden analoge Stromzähler mehr und mehr durch digitale Smart Meter ersetzt. Die Angriffsfläche für Hacker wächst also stetig und die Stromversorgung wird anfälliger für Cyberattacken. Immer wieder beobachten große Versorger und Netzbetreiber Angriffsversuche. Im Rahmen des G20-Gipfels in Hamburg im Juli 2017 verzeichnete der örtliche Stromnetzbetreiber der Hansestadt beispielsweise unmittelbar vor und während des Gipfeltreffens über 20 Mal so viele Netzzugriffsversuche wie normal.

IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen

Durch eine Cyberattacke, bei der es sich IT-Spezialisten zufolge um einen Sabotage-Akt russischer Hacker gehandelt hat, wurde 2015 das ukrainische Stromnetz lahmgelegt. Der Angriff betraf 27 Umspannwerke und führte zu erheblichen Stromausfällen, so dass etwa 700 000 Haushalte mehrere Stunden ohne Strom waren. Eingeschleust wurde die Schadsoftware lt. Medienberichten als Anhang in gefälschten E-Mails an die Mitarbeiter des Energieversorgers. Sobald die Dateien im Anhang geöffnet wurden, erhielten die Hacker Zugriff auf das System.

Trotz des hohen Sicherheitsstandards in Deutschland sind solche Vorfälle auch hier nicht ausgeschlossen. Deshalb hat der Deutsche Bundestag bereits im Mai 2016 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) beschlossen. Die Richtlinie verpflichtet die Betreiber kritischer Infrastrukturen dazu, Attacken auf ihre Systeme dem Bundesamt für Sicherheit in der Informationstechnik zu melden, ihre eigenen IT-Standards zu erhöhen und ein Information Security Management System (ISMS) einzurichten.

Fazit

Dennoch ist die Energiebranche in Deutschland (noch) nicht ausreichend auf die Gefahren und mögliche Folgen eines Angriffs vorbereitet. Netzbetreiber müssen ihre Konzepte zur IT-Sicherheit überarbeiten und Schwachstellen sowie daraus resultierende Angriffspunkte identifizieren. Der Bedarf an IT- und Cyber-Security Managern zur Besetzung von Positionen wie der des CISO (Chief Information Security Officer) steigt. Aufgrund der großen Nachfrage sind hoch qualifizierte Experten immer schwerer zu bekommen und werden folglich auch immer teurer. Klar ist: Ohne geht es nicht. Die Investition in kluge Köpfe zur Stärkung der IT- und Cybersicherheit ist heute unabdingbar.

thomas.hoppe@hager-ub.de

www.hager-ub.de