Cyberabwehr - Stromnetze im Visier von Hackern

Essen (APA/dpa) - Die Angriffe von Hackern auf die deutsche Stromversorgung nehmen zu und werden immer ausgefeilter. Die Versorger ziehen ihre Abwehrmauern höher. Der Netzbetreiber Innogy will nun in einem Trainingszentrum die richtige Reaktion auf Angriffe üben. Hacker kapern ein Stromnetz, legen Umspannwerke und Schaltanlagen lahm.

In der Ukraine ist das im Dezember 2015 passiert - stundenlang fiel der Strom aus. In Deutschland undenkbar? Nein, sagt Florian Haacke. Er ist Leiter der Konzernsicherheit bei Deutschlands größtem Stromnetzbetreiber Innogy in Essen. "Die Cyberattacken zeigen, dass es Angreifer gibt, die ein Interesse haben, so etwas durchzuführen - und es können. Wir sollten nicht annehmen, dass dies in Deutschland nicht möglich ist."

Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat erst am vergangenen Mittwoch erneut vor einer Angriffswelle auf die deutschen Energieversorger gewarnt. In die Büro-Netzwerke einiger Unternehmen seien Angreifer bereits eingedrungen. In zentrale Bereiche der Stromversorgung hätten es die Hacker noch nicht geschafft, aber das sei "womöglich nur eine Frage der Zeit", warnte BSI-Chef Arne Schönbohm.

Der Schutz vor schwerwiegenden Cyber-Angriffen ist nach Einschätzung von Norbert Pohlmann, Professor am Institut für Internet-Sicherheit der Westfälischen Hochschule in Gelsenkirchen, bisher auch deshalb gelungen, weil viele Stromnetze noch voneinander abgeschottet sind. Die Wahrscheinlichkeit solcher Angriffe werde mit der Digitalisierung aber steigen. "Der Schutz der Netze wird zu einer Herkulesaufgabe, denn die Angreifer werden immer intelligenter", warnt er.

Damit es nicht zu einem Blackout kommt, bauen die Stromkonzerne ihre Sicherheitskonzepte ständig aus. Bei Innogy kümmern sich in der Konzernzentrale rund 130 Spezialisten um die Sicherheit im mehr als 460.000 Kilometer langen Innogy-Stromnetz in Deutschland und Osteuropa. Sie werden schon misstrauisch, wenn einer der rund 40.000 Innogy-Mitarbeiter innerhalb kurzer Zeit mehrfach ein neues Passwort anfordert. "Da schauen wir nach, ob es den wirklich gibt und was der

Grund ist", sagt Haacke. Fälle dieser und ähnlicher Art gibt es bei Innogy etwa 1.000 pro Quartal. Mit schwerwiegenderen Störungen und Bedrohungen, die genau unter die Lupe genommen werden, haben es die Experten aus seinem Team fünf bis zehn Mal in einem Quartal zu tun.

Das neueste Projekt von Innogy: Ein Trainingszentrum, in dem Mitarbeiter aus den Leitstellen der Netze im Erkennen und Abwehren von digitalen Angriffen geschult werden. Gemeinsam mit der israelischen Firma Cybergym baut Innogy in Frankfurt ein solches Schulungszentrum auf. Komplexe Cyber-Angriffe sollen dort nachgeahmt werden. "Die Teilnehmer werden dabei auch real unter Stress gesetzt, um die physikalischen Auswirkungen von Cyber-Angriffen deutlich zu machen. Die Heizung geht beispielsweise an, ein Pumpensystem lässt sich nicht mehr abschalten", beschreibt Haacke die Übungen.

Der Schutz der Energienetze durch technische Mittel wie Datenverschlüsselung, Firewalls und Virenscanner reicht nach Einschätzung des IT-Branchenverbands Bikom allein nicht mehr aus. Die Netze müssten "resilient" werden, also bei Störungen ihre grundlegenden Funktionsfähigkeit erhalten oder zumindest eigenständig wiederlangen können, heißt es in einem Bitkom-Papier. "Wenn ein Cyberangriff erfolgreich ist, droht im traditionellen System eine Ausbreitung in der Fläche. Ein resilientes System erkennt einen Cyberangriff rasch, verhindert die Ausbreitung und behebt die Störung schnell", sagte Hauptgeschäftsführer Bernhard Rohleder bei der Vorstellung des Papiers. Durch eine Echtzeitanalyse aller Datenströme in den digitalisierten Netzen werde das möglich sein.

Und noch eine Schwachstelle müsste nach Ansicht von Haacke schnell abgestellt werden: Die oft zu späte Information durch die Hersteller von Soft- und Hardware über Sicherheitslücken in ihren Produkten. "Sie müssten gesetzlich verpflichtet werden, ihre Erkenntnisse unverzüglich an ihre Kunden weiterzugeben", fordert der Innogy-Sicherheitschef.

(Schluss) pat

ITM0001 2018-06-15/11:14

151114 Jun 18

Link zur Aussendung:
https://www.it-press.at/presseaussendung/ITM_20180615_ITM29510717542826048