Cyber-Notstand bei Atomkraftwerken

Der europäische Innovationsführer in Sachen Cybersicherheit, Blue Shield Security, warnt vor Sicherheitslücken bei Atomkraftwerken. „Es droht ein europaweiter Stromausfall bis hin zu einem atomaren Supergau, wenn nicht schnellstmöglich europaweit gehandelt und jedes Kernkraftwerk regelmäßigen Cyber-Stresstests unterzogen wird", so Blue Shield Gründer Alois Kobler.

Das Atomkraftwerk Mochovce, 200 Kilometer vor Wien.

Foto: honorarfrei

Mit der geplanten Inbetriebnahme des slowakischen Kernkraftwerks Mochovce, unweit der österreichischen Grenze, legt die österreichische Bundesregierung aktuell den Finger in jene Wunde, die die Sicherheit Europas nachhaltig bedrohen könnte. Umweltministerin Elisabeth Köstinger spricht über die Sicherheitsmängel bei Mochovce von „sehr besorgniserregenden Berichten" und verspricht „auf höchster EU-Ebene zu intervenieren."

„Bei der EU liegt der Kern des Problems", so Kobler. „Europäische Kernkraftwerke wurden nämlich zuletzt 2012 einem EU-Stresstest unterzogen, wobei gerade das Thema Cybersicherheit fatalerweise nicht Teil des Tests war. Der Druck der Atomlobby etwa aus Großbritannien und Frankreich war zu groß." Kobler weiß auch warum: „Sie wären alle durchgefallen!" Die marode finanzielle Situation der europäischen Kraftwerksbetreiber ist Fakt. Kobler führt weitere Gründe ins Treffen: „Bei Nuklearanlagen haben Sie Genehmigungsprozesse, die viele Jahre in Anspruch nehmen. Da haben Sie schnell 40 oder 50 Sicherheitsupdates versäumt. Die lange Dauer, bis dann ein Atomkraftwerk rentabel ist, führt die Betreiber in die Risikofalle, kaum etwas inIT und ihre Sicherheit zu investieren. Ein Teufelskreis".

Häufige Attacken auf Kraftwerke

Der Chef der Internationalen Atomenergiebehörde (IAEA) mit Sitz in Wien, der Japaner Yukiya Amano, warnt: „Cyberangriffe, die zu Störungen der Abläufe in Kernkraftwerken führen, sind keine imaginäre Gefahr, sondern längst Realität", und führt weiter aus: „Bislang werden Cyberangriffe auf Kernkraftwerke in der Regel nicht öffentlich gemacht." Das, was an die Öffentlichkeit gedrungen ist, erscheint schon bedrohlich genug zu sein. Ein kurzer Auszug: „Im bayrischen Atomkraftwerk Gundremmingen wurde 2016 ein Computervirus entdeckt", „Hacker erbeuteten 2018 in Frankreich Pläne von Atomanlagen des Kraftwerksbauers Ingérop" und „2019 berichtet ein Whistleblower über Sicherheitsmängel und Korruption beim Kernkraftwerk Mochovce".

Szenarien bei einem Angriff

„Wenn ein Atomkraftwerk gehackt wird, kann etwa über die Verwaltungsnetzwerke Schadsoftware auf die Leitrechner kommen und die Anlage herunterfahren, die Reaktorsteuerung würde manipuliert, die Kühlkreisläufe würden ausgeschalten und letztlich würde sogar der Gau, also die Kernschmelze, herbeigeführt werden", verdeutlicht Cybersecurity-Experte Alois Kobler den Ernst eines derartigen Szenarios. „Da die Energieversorger in Europa alle miteinander vernetzt sind, könnte eine Art Domino-Effekt eintreten, mit dem fatalen Resultat eines europaweiten Blackouts", skizziert Kobler den Ernstfall.

KI und europaweite Standards

Ein internationales Forschungsteam ist beim europäischen Innovationsführer in Sachen Cybersicherheit, Blue Shield Security, an der ständigen Weiterentwicklung von Abwehrmaßnahmen zum Schutz von kritischer Infrastruktur beschäftigt. Die neuesten Forschungsergebnisse in den Bereichen künstlicher Intelligenz und selbstlernender Algorithmen werden für die Kunden europaweit zur Abwehr von Cyberangriffen eingesetzt. „Als führendes Cybersecurity-Unternehmen könnten wir die nötigen Maßnahmen ergreifen, um auch Atomkraftwerke nachhaltig zu schützen. Die EU ist nun gefordert, verpflichtende regelmäßige Stresstests für alle Kraftwerke vorzuschreiben und gemeinsam mit IT-Experten europaweite Standards für den Schutz der Anlagen und somit für den Schutz der Bevölkerung einzuführen", betont Kobler mit Nachdruck.

Das Blue Shield Führungsduo COO Stefanie Kaiser und Alois Kobler warnen vor Mochovce.

Foto: Klaczak

„Herzstück der Wirtschaft"

Stefanie Kaiser, COO der Blue Shield Security und zuständig für das operative Geschäft, warnt vor Auswirkungen für die Gesamtwirtschaft: „Der Energiesektor ist das Herzstück für Wirtschaft und Gesellschaft eines Landes. Wer ihn lahmlegt, legt ein ganzes Land lahm." Das gelte, so Kaiser, nicht nur für die Atomkraftwerke direkt, sondern auch für Unternehmen und kritische Infrastruktur, die mit den Anlagen in Verbindung stünden. Sie fordert daher die Politik zum Handeln auf: „Ein Experte als EU-Kommissar für Cybersicherheit wäre ein wichtiger Schritt in die richtige Richtung. Auf dieser elementaren Ebene soll die Politik den Fachleuten Platz machen."