«Ein Cyber-Angriff verursacht Vertrauensverlust»

Cyber-Attacken | Die fortschreitende Digitalisierung macht Energieversorgungsunternehmen verwundbar gegen Attacken aus dem Netz. Sicherheitsexperte Roman Haltinner erklärt, wie gut die Schweizer EVU gegen solche Attacken abgesichert sind und welche Faktoren absolute Sicherheit verunmöglichen.

Zur Person
Roman Haltinner ist Partner | Cybersecurity | EMEIA GSA (Germany Switzerland Austria) bei EY.
→ EY, 4051 Basel
→ roman.haltinner@ch.ey.com

Bulletin: Roman Haltinner, als wie hoch schätzen Sie das Risiko ein, dass Schweizer Energieversorger Opfer einer Cyber-Attacke werden könnten?
Roman Haltinner: Die Bedrohung für Unternehmen durch Cyber-Attacken hat stark zugenommen. Cyber-Angriffe richten sich gegen Unternehmen aller Industrien weltweit. Laut verschiedenen Befragungen und unserer EY-Studie wurde mehr als die Hälfte der befragten Schweizer Unternehmen in den letzten zwölf Monaten Opfer von Cyberangriffen. Durch unsere tägliche Arbeit haben wir auch Kenntnisse von aktuellen Fällen, die Schweizer Energieversorger betreffen.

Wie gut sind die Schweizer Energieversorger gegen solche Attacken und digitale Intrusion gerüstet?
Je stärker die Digitalisierung fortschreitet, je mehr sie die Geschäftsprozesse der Energieversorger durchdringt, desto grösser ist die Gefahr, dass Unternehmen Opfer von Cyber-Attacken werden. Das Management von Cyber-Risiken ist daher ein kontinuierlicher Prozess. Die Schweizer Energieversorger haben dafür ein Bewusstsein entwickelt und Massnahmen auf allen Ebenen ergriffen. Zudem steht die Branche vor spezifischen Herausforderungen bezüglich der Sicherheit, weil die klassische Büroinformatik und die operationelle Technologie aufgrund des technologischen Fortschritts immer mehr zusammenwachsen.

Im Dezember 2015 führte eine Cyber-Attacke zu einem Blackout in der Ukraine. Allerdings geschah dies vor dem Hintergrund des Konflikts zwischen der Ukraine und Russland. Wäre eine solche Attacke auch in der Schweiz denkbar? Oder gab es sogar schon solche Fälle?
Unter Blackout versteht man einen grossräumigen Stromausfall, von dem eine sehr grosse Zahl von Menschen betroffen ist. Auch wenn sich ein solcher Vorfall meines Wissens in der Schweiz im Zusammenhang mit einem Cyber-Angriff noch nie ereignet hat, stellt er doch ein Risiko dar, das die Energiebranche nicht unterschätzen darf. Tatsächlich müssen solche Szenarien in Betracht gezogen und die zu ergreifenden Massnahmen vorausschauend geplant werden. Cyber-Angriffe stellen neben operativen auch rechtliche Risiken dar. Zu nennen sind der Verlust von geistigem Eigentum, Bussen aufgrund von Datenschutzverletzungen oder Schadenersatzforderungen wegen Vertragsverletzungen. Für kritische Infrastrukturen führt ein Cyber-Angriff zu Untersuchungen durch Behörden. Dies bindet administrative Ressourcen, verursacht Kosten und führt zu einem Vertrauensverlust.

Wäre es möglich, dass sich ein solcher – womöglich lokal begrenzter – Blackout bereits ereignet hat, ohne dass er als Cyber-Attacke erkannt worden wäre? Quasi als Testlauf für eine grössere Attacke?
Akteure, die sich ein Blackout einer Region oder gar eines Landes zum Ziel setzen, werden dies tun. Militärische Operationen im Cyberspace beinhalten in der Regel «Testläufe», also vorbereitende oder täuschende Massnahmen, die verschiedene Angriffsvektoren beinhalten. Das «Wall Street Journal» hat im Januar in einer aufwendigen Recherche minuziös beschrieben, wie sich Angreifer Zugang zu den Schaltstellen der amerikanischen Stromversorgung zu verschaffen suchen.[1] Im vergangenen Juli wurde bekannt, dass es Hackern schon gelang, an die Schalthebel einiger Produktionsanlagen heranzukommen. **INTERVIEW: RALPH MÖLL**

Die Fortsetzung dieses Interviews finden Sie auf www.bulletin.ch

Referenz
[1] «America's Electric Grid Has a Vulnerable Back Door – and Russia Walked Through It», www.wsj.com, 10. Januar 2019 (der Artikel ist kostenpflichtig).