Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 110 (2019)
Heft: 1-2

Artikel: «Ein Cyber-Angriff verursacht Vertrauensverlust»
Autor: Haltinner, Roman / Möll, Ralph
DOI: https://doi.org/10.5169/seals-855921

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 09.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

«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).