

06.03.2019 - 09:15 Uhr

Studie Electrosuisse zu Cybersecurity bei kleineren und mittleren Elektrizitätswerken



Cybersecurity

bei kleinen und mittleren Elektrizitätsversorgungsunternehmen



Fehrltorf (ots) -

Electrosuisse hat bei kleinen und mittleren Elektrizitätswerken untersucht, wie es um deren Fähigkeit steht, den Bedrohungen des digitalen, global vernetzten Zeitalters zu begegnen.

Immer mehr KMUs erkennen, dass auch sie für Cyberattacken weder zu klein noch zu wenig interessant sind. Vor allem für Unternehmen der kritischen Infrastrukturen wie Energie- und Wasserversorgung ist das Management der digitalen Risiken von ganz besonderer und zunehmend existenzieller Bedeutung. Electrosuisse wollte wissen, wie es um die «Cyber-Resilienz» bei kleinen und mittleren Elektrizitätswerken steht, und hat diese mit einem Cybersecurity Quick Assessment erhoben. Es wurden die Betriebsleiter und IT- und OT- beziehungsweise Cybersecurity-Verantwortlichen von 30 Werken mit 4 bis 600 Mitarbeitern befragt.

Cybersecurity ist in der Branche ein Thema

Erfreulich war festzustellen, dass Cybersecurity bei allen Elektrizitätswerken mehr oder weniger thematisiert wird, auch wenn die Aufgabe bei den kleineren noch wenig systematisch angegangen wird. Während die mittleren Elektrizitätswerke im Hinblick auf die Cybersecurity mehrheitlich relativ gut bis in einzelnen Bereichen sehr gut unterwegs sind, zeigt sich besonders bei den kleinen, lokalen Elektrizitätsversorgungsunternehmen in vielen Disziplinen ein erheblicher Nachholbedarf.

Vor allem bei kleineren Werken wird dem Schutz mehr Aufmerksamkeit geschenkt als der Entdeckung von digitalen Sicherheitsvorfällen und der Fähigkeit und Bereitschaft zu einer raschen und angemessenen Reaktion auf diese. Werke mit mehr als 60 Mitarbeitern haben zu einem grossen Teil erkannt, dass neben mehrstufigen Schutzmassnahmen auch ein wirkungsvolles und verzögerungsfreies Erkennen von Sicherheitsvorfällen, eine zeitnahe und angemessene Reaktion auf diese sowie die Wiedererlangung der sicheren Operabilität innert nützlicher Frist wichtige Elemente einer ganzheitlichen Cybersecurity-Strategie sind.

Es braucht eine Sicherheitskultur

Dabei sollte dem Faktor Mensch als grösste Schwachstelle auch eine entsprechende Rolle zukommen. Eine vermehrte Investition in verständliche und praktikable Richtlinien sowie die regelmässige, systematische Schulung von Mitarbeitern sollte nicht als Luxus betrachtet werden. Sicherheit braucht nicht nur technische Lösungen sondern vor allem auch eine Sicherheitskultur.

Kontakt:

Electrosuisse, Luppenstrasse 1, 8320 Fehraltorf

Weitere Informationen zur Studie:

Levente Dobszay, dobszay.levente@electrosuisse.ch,
T +41 44 956 13 03

Christine Andres, PR-Verantwortliche,
christine.andres@electrosuisse.ch,
T +41 44 956 11 23

Medieninhalte

Cybersecurity

bei kleinen und mittleren Elektrizitätsversorgungsunternehmen



Electrosuisse hat bei kleinen und mittleren Elektrizitätswerken untersucht, wie es um deren Fähigkeit steht, den Bedrohungen des digitalen, global vernetzten Zeitalters zu begegnen. Weiterer Text über ots und www.presseportal.ch/de/nr/100005499 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/Electrosuisse"

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100005499/100825580> abgerufen werden.