Cybersecurity bei kleinen und mittleren Elektrizitätswerken

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

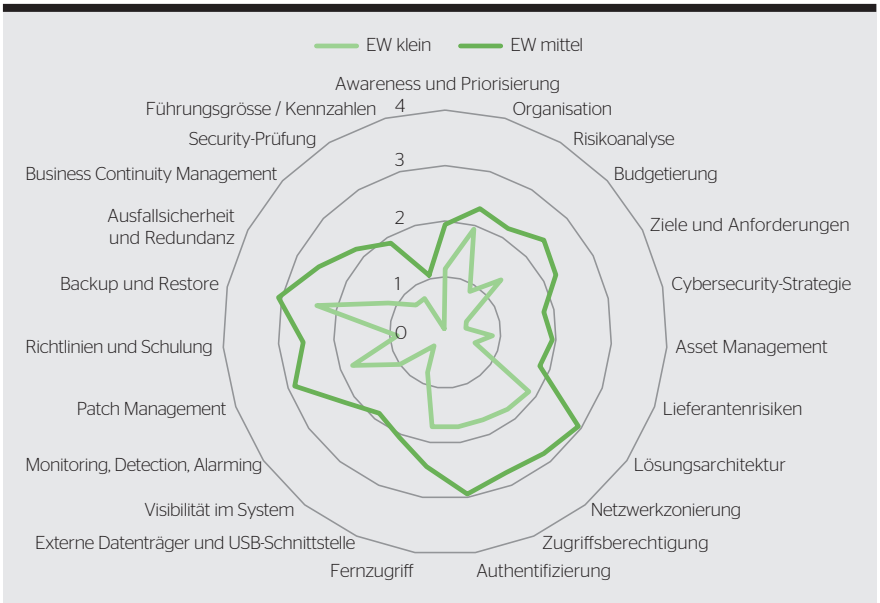
LEVENTE J. DOBSZAY

Die immer noch häufig anzutreffende Annahme, aus irgendwelchen Gründen nicht zum Ziel von Cyber-Attacken zu werden, macht Unternehmen zur besonders leichten Beute. Gerade bei Betrieben, die zur kritischen Infrastruktur gehören, kann dies verheerende Folgen haben. Der Hackerangriff auf die Betriebssteuerung der Wasserversorgung von Ebikon im November 2018 konnte glücklicherweise durch das im Herbst installierte Sicherheitssystem vereitelt werden. Der Systembetreiber registrierte die Angriffe und meldete sie der Gemeinde.

Aus der Tatsache, dass ein Unternehmen bisher keine Sicherheitsprobleme feststellen konnte, lässt sich vor allem in Anbetracht der oft weitgehend fehlenden Visibilität der Vorgänge im Netzwerk nicht automatisch darauf schliessen, dass es bisher alles richtig gemacht und noch nicht Opfer eines erfolgreichen Angriffs geworden ist. Es kann gut sein, dass der Feind sich bereits tief im System eingenistet hat und nur darauf wartet, loszuschlagen. Untersuchungen haben gezeigt, dass Infektionen mit Schadsoftware im Durchschnitt länger als ein Jahr unentdeckt bleiben. Davon zeugt auch der Spionagefall bei der Ruag. Immer mehr kleine und mittlere Unternehmen erkennen, dass auch sie für Cyber-Attacken weder zu klein noch zu wenig interessant sind.

Zunehmende Vernetzung führt neue Risiken ein

Im Zuge der fortschreitenden Digitalisierung sehen sich immer mehr Bereiche der «Operational Technology» (OT), das heisst der Informationstechnologie (IT) für die Steuerung von Maschinen in industriellen Herstellungs- und Logistikprozessen, mit den



Durchschnittliche Cybersecurity-Prozess-Maturität.

Herausforderungen der digitalen Sicherheit konfrontiert. Infrastrukturen, die ursprünglich nicht dafür konzipiert wurden, werden zunehmend mit der Aussenwelt vernetzt und sind dadurch auch entsprechenden digitalen Risiken ausgesetzt. Damit wird neben dem Nutzenpotenzial zugleich auch ein Gefahrenpotenzial erschlossen.

Bei der Konvergenz von OT und IT wachsen technisch verwandte Welten zusammen, die sich jedoch hinsichtlich der Sicherheitsprioritäten, Lebenszyklen und Sicherheitskulturen sowie auch in den aktuellen technischen Möglichkeiten für digitale Sicherheitsmassnahmen unterscheiden. Während die Schutzziele «Vertraulichkeit», «Integrität» und «Verfügbarkeit» in der Welt der klassischen IT in eben dieser Prioritätenfolge adressiert werden, sind die Prioritäten in der OT-Welt gerade umgekehrt. Hier steht in der Regel die Verfügbarkeit an oberster Stelle, während die Vertraulichkeit eine weit weniger wichtige Rolle spielt, weil die zu schützenden Daten sowie die diese Daten verarbeitende Hardware und Software nur einen geringen bis gar keinen Personenbezug aufweisen. Vertraulichkeit ist hier in erster Linie im Zusammenhang mit Industriespionage relevant.

Cybersecurity gewinnt zunehmend an Bedeutung

Vor allem für Unternehmen der kritischen Infrastrukturen wie Energie- und Wasserversorgung ist das Management der digitalen Risiken von ganz besonderer und zunehmend existenzieller Bedeutung. Mit der Umsetzung der Energiestrategie 2050 wird durch den flächendeckenden Einsatz von «Smart Metern» das Thema Cybersecurity bis in die Haushalte und Betriebe der Stromkunden und

Bild: Electrosuisse

der Betreiber von Photovoltaikanlagen getragen. Aber auch Fertigungsanlagen sowie Gebäudetechnik und -automation sind immer mehr den Bedrohungen der vernetzten digitalen Welt ausgesetzt.

Auch kleinere Elektrizitätswerke werden sich zunehmend bewusst, dass auch sie in den Fokus von Cyber-Attacken geraten und zum Zielobjekt in der globalen, digitalen Kriegsführung werden können. Ein einzelnes Werk für sich mag kein strategisches Ziel sein, aber alle auch noch so kleinen Werke in der Summe sind es sehr wohl. Entsprechend ist kein Werk zu klein, um sich nicht mit mehrstufigen Schutzmassnahmen auf allen Ebenen gegen Cyber-Attacken zu schützen. Cybersecurity gehört daher auf die Liste der Top-Prioritäten von Unternehmen der kritischen Infrastruktur. Und dies völlig unabhängig von ihrer Grösse.

«Cyber-Resilienz»-Umfrage bei KMU-Elektrizitätswerken

Electrosuisse wollte wissen, wie es um die «Cyber-Resilienz» bei kleinen und mittleren Elektrizitätswerken steht, und hat diese im Zeitraum vom September bis Dezember 2018 mit einem Cybersecurity Quick Assessment erhoben. Dafür wurden die einzelnen Themen des NIST-Cybersecurity-Frameworks zu Schlüsselelementen verdichtet und mit zusätzlichen Aspekten zu Budgetierung und Führungskennzahlen ergänzt.

In einem rund zweistündigen Interview wurden die Betriebsleiter und IT- und OT- beziehungsweise Cybersecurity-Verantwortlichen von 30 Werken mit 4 bis 600 Mitarbeitenden befragt. Nachweise wurden keine gefordert. Daher ist davon auszugehen, dass die Selbsteinschätzung der Teilnehmer als eher zu optimistisch einzustufen ist. Trotzdem kann angenommen werden, dass die Verteilung der Maturitätsstufen der Realität entspricht, auch wenn die effektive Maturität tendenziell tiefer liegen dürfte. Die Unterscheidung zwischen kleinen und mittleren Werken wurde anhand der Anzahl Mitarbeitenden vorgenommen, wobei Werke mit 60 Mitarbeitenden und weniger als klein eingestuft wurden.

Das Thema ist in der Branche angekommen

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

Es braucht eine Sicherheitskultur

Informationssicherheitsvorfälle können mit radioaktiver Strahlung verglichen werden: Ohne die richtigen Schutz- und Erkennungsmassnahmen bemerkt man sie erst, wenn es schon zu spät ist. Trotzdem wird vor allem bei kleineren Werken 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 Mitarbeitenden 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. Dabei sollte dem Faktor Mensch als grösster Schwachstelle auch eine entsprechende Rolle zukommen. Eine vermehrte Investition in verständliche und praktikable Richtlinien sowie die regelmässige, systematische Schulung von Mitarbeitenden sollten nicht als Luxus betrachtet werden, denn Sicherheit erfordert nicht nur technische Lösungen, sondern vor allem auch eine von allen Beteiligten gelebte Sicherheitskultur.

Return on Investment schlecht messbar

Investitionen in Cybersecurity werden oft zu zögerlich getätigt, weil für die Budgetallokation ohne einen messbaren «Return on Investment» eine Argumentation meist schwierig ist. Kritische Infrastrukturen haben ungleich längere Lebenszyklen als die Technologien der Cyber-Welt. Für die Infrastrukturbetreiber gilt es, Fähigkeiten zu entwickeln, um die Verschmelzung der OT- und IT-Welt und die damit verbundenen neuen Bedrohungen zu bewältigen.

Die identifizierten Defizite sind einerseits auf das zu wenig als Führungsaufgabe wahrgenommene Thema und die beschränkten personellen sowie auch finanziellen Ressourcen und andererseits auf die fehlende Verfügbarkeit der nötigen Fachkompetenz zurückzuführen. Während die ganz grossen Unternehmen Chief Information Security Officers und spezifische Abteilungen haben, die sich dediziert mit dem Thema Cybersecurity befassen, wird dessen Relevanz in vielen kleinen und mittleren Unternehmen noch oft unterschätzt. Unternehmen, welche die Herausforderungen nicht aus eigener Kraft stemmen können, sind gut beraten, sich fachkompetente Hilfe ins Haus zu holen oder einzelne Dienste an entsprechende Dienstleister auszulagern. Und nicht zuletzt sollte auch die Fachkompetenz auf der Führungsebene verstärkt werden.

Angebote

Als Fachverband möchte Electrosuisse zur Stärkung der «Cyber-Resilienz» beitragen. Mit Angeboten zu Prüfungen, Zertifizierungen, Schulungen und Beratungen sollen besonders jene Unternehmen unterstützt werden, die nicht über die personellen Ressourcen und das Fachwissen verfügen, um eine ausreichende Cybersecurity sicherzustellen. Zudem arbeitet Electrosuisse an der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) mit.

Link
www.electrosuisse.ch/cybersecurity

Autor
Levente J. Dobszay ist Cybersecurity-Specialist bei Electrosuisse.
→ Electrosuisse, 8320 Fehraltorf
→ levente.dobszay@electrosuisse.ch