Cyber Threats im Energiesektor – die Energiewende der anderen Art

Ohne sie geht gar nichts mehr: Kritische Infrastrukturen stellen die grundlegende Versorgung von Wirtschaft und Gesellschaft sicher. Deren Steuerung erfolgt zunehmend unter Einbezug von vernetzten ICT-Systemen. Damit ist der Schutz vor Cyber Angriffen zu einer täglich neuen Herausforderung geworden. Insbesondere ICS- und SCADA-Systeme benötigen durch die Zunahme der Cyber Bedrohung und Vernetzung in der Wertschöpfungskette einen noch umfassenderen Schutz. Datenkompromittierung, Kontrolle durch Dritte oder Ausfälle hätten kaum abschätzbaren Folgen und könnten zu einem Dominoeffekt führen. Solche Dominoeffekte in der Energieversorgung hätten weitreichende Folgen.

von Markus Limacher, Senior Security Consultant, InfoGuard AG

Normalerweise tritt der Name «Norwegian Pearl» im Zusammenhang mit idyllischen Fjorden und nie enden wollenden Sommernächten auf. Dies änderte sich vor ein paar Jahren schlagartig, als dieser Begriff plötzlich im gleichen Atemzug mit einem der grössten Stromausfälle in Europa in Verbindung gebracht wurde. Es wird vermutet, dass die Überführung eines gleichnamigen Kreuzfahrtschiffes auf dem deutschen Fluss Ems und die damit verbundene Abschaltung zweier über den Fluss führenden Hochspannungsleitungen eine Kettenreaktion auslöste und binnen Sekunden zur Netzüberlastung und schlussendlich zu Stromausfällen im ganzen Euro-Raum führte. Die Folgen waren verheerend – in ganz Europa sassen rund 10 Millionen Menschen fast anderthalb Stunden im Dunkeln – und dennoch nur die Spitze möglicher Folgen. Der Ausfall von Energieerzeugern und der nachfolgenden Stromknappheit führten ebenso drastisch vor Augen, wie abhängig wir von kritischen Infrastrukturen sind. Aber auch ein einzelner Mitarbeiter oder ehemaliger Arbeitskollege kann grossen Schaden anrichten, wie ein Beispiel aus dem australischen Queensland zeigt: Mittels einer drahtlosen Verbindung drang dieser in das Wasserkontrollsystems seines Ex-Arbeitgebers ein und öffnete buchstäblich alle Schleusen, woraufhin sich Unmengen an Abwasser in die Flüsse ergossen.

Das Mittelalter ist näher, als man denkt

So weit, so schlecht. Neue Bedrohungen ergeben sich aber auch aus der ICT-Infrastruktur sowie der zugrunde liegenden Steuerungstechnik ICS- (Industrielle Kontrollsysteme) und SCADA-Systeme (Supervisory Control and Data Acquisition). Die Energie produzierende Branche ist zunehmend vernetzt und damit von einer funktionierenden ICT-Infrastruktur abhängig. Durch diese Vernetzung sind Energieproduzenten tagtäglich Angriffen aus dem Cyberspace ausgesetzt und stellen heute grosse Herausforderungen an die Produzenten dar. Die kleinste Störung und Abweichung vom «courant normal» hat

schnell überregionale Auswirkungen, weil Energie ein systemrelevanter Faktor ist.

Es ist essentiell die Energiebranche und -versorgung mit ihren Industrieanlagen, Informations – und Kommunikationssystemen als wichtigen Teil der kritischen Infrastrukturen zu schützen. Dass der Schutz kritischer Infrastrukturen jeweils weiter als nur bis an die Landesgrenzen geht, verdeutlichen die publik gewordenen Attacken der jüngsten Zeit. Stuxnet – ein Schadprogramm, welches speziell für SCADA Systeme zur Überwachung und Steuerung technischer Prozesse entwickelt wurde, hat immense Schäden bspw. an der iranischen Urananreicherungsanlage verursacht. Der Computerwurm Shamoon führte bei Energieunternehmen im Nahen Osten zu einer plötzlichen Betriebsstörung und Dragonfly ist ein Cyber-Spionagering, der hauptsächlich den nordamerikanischen und europäischen Energiesektor bedroht. Das Feld von Bedrohungen ist bunter, als nur Naturkatastrophen und menschliches Versagen, sondern betrifft immer mehr auch gezielt herbeigeführte Katastrophen, welche eine Zivilisation innert Kürze in das Mittelalter zurückversetzen können.

ICS- und SCADA-Sicherheit mit System

Betreiber kritischer Infrastrukturen sind gut beraten sich konsequent mit aktuellen und neuen Bedrohungen und Risiken auseinandersetzen und der Informationssicherheit das nötige Gewicht beizumessen. Dabei gilt es, das Rad nicht neu zu erfinden. Internationale Standards (beispielsweise die ISO/IEC 270xx Familie) bieten ein anerkanntes Modell für die Einrichtung, Umsetzung, Überprüfung und kontinuierlichen Verbesserung auf der Basis eines Informationssicherheits-Management-Systems (ISMS).

Die Einführung eines solchen ISMS hilft Betreibern von kritischen Infrastrukturen das Sicherheitsniveau systematisch zu steigern und dabei von Good und Best Practice-Ansätzen zu profitieren. Es hat sich gezeigt, dass das systematische Vorgehen durch ein ISMS einen erheblichen Mehrwert bietet. Dazu zählen unter anderen, eine gezielte Risikobetrachtung und -bewertung, der Aufbau eines angemessenen Sicherheitskonzeptes und einer geeigneten Sicherheitsarchitektur, die Definition von Sicherheitsrichtlinien sowie der Aufbau einer Notfallplanung und Sicherheitssensibilisierung der Mitarbeitenden.

Aus Einzelelementen wird ein System

Die komplette Isolierung von ICS- und SCADA-Systemen, also ohne Verbindung zu externen Netzwerken, wäre aus Sicherheitsüberlegungen eine erstrebenswerte Situation. Doch im alltäglichen Betrieb ist dieses Szenario nicht realistisch, weil etwa Abrechnungssysteme, Fernmessungen oder organisatorische Funktionen Schnittstellen zu ICS- und SCADA-Netzwerken haben um Daten auszutauschen oder darauf zuzugreifen. Die Architektur von ICS- und SCADA-Systemen innerhalb des Unternehmensnetzwerks ist somit ein Schlüssel zur Sicherheit. Es gilt verschiedene Verteidigungslinien (Lines of Defense) aufzubauen. Zu diesen zählen die Verbindung der kritischen Infrastrukturen und der ICT mit einer End-zu-End-Sicherheit, kontrollierte Remote-Zugänge für Lieferanten und Partner, einem Perimeter-Schutz bestehend u.a. aus einer Firewall, einem Intrusion Detection/Prevention System, einem VPN und geschützte Netzwerk- und Zonenübergänge sowie einem umfassenden Malware-Schutz auf vernetzten und geschlossenen Systemen. Eine weitere Schlüsselkomponente für die Sicherheit ist die Authentisierung. Dabei gilt es zu beachten, dass die Authentisierungsinfrastruktur für das Unternehmensnetzwerk von ICS- und SCADA-Systemen separiert wird. Der Grund: Ist ein Konto im organisatorischen Netzwerk kompromittiert, so können sich die Angreifer einen nicht autorisierten Zugriff auf die Ressourcen im ICS- oder SCADA-System verschaffen.

Permanente Bedrohungsanalyse und Angriffserkennung

Die Risikosituation und Bedrohungslage ändert sich stetig. Aus diesem Grund sind regelmässige Überprüfungen des Sicherheitsdispositivs nach neuen Bedrohungen, Verwundbarkeiten und Schwachstellen unerlässlich. Zur Kontrolle sollten regelmässig System Audits, Penetration Tests und Vulnerability Scans durchgeführt werden, nur so kann die Sicherheit an die aktuelle Risikosituation angepasst und optimiert werden. Zur Erkennung möglicher komplexerer Angriffe eignen sich Security Information & Event Management Systeme, kurz SIEM genannt. Dabei werden Logs und Alerts von praktisch allen Komponenten und Systemen auf eine zentrale Plattform übermittelt und in Echtzeit analysiert. Das Ziel ist, verdächtiges Verhalten im auf allen Layern aufzuspüren und besser zu verstehen und entsprechende Aktionen einleiten zu können. Dazu gehören Authentisierungsfehler, Verstösse gegen die Firewall-Regeln, Zugriffs-Logs, IDS-Logs oder jede andere Art von Informationen, die dazu beitragen, ein umfassendes Bild von sicherheitsrelevanten Vorfällen, Zugangsübertretungen usw. zu erhalten.

Smart Energy Security aus der Schweiz

ICS- und SCADA-Systeme sind unentbehrlich – die Absicherung dieser ist aber eine sehr komplexe Aufgabe. Der Schweizer Informationssicherheitsexperte InfoGuard bietet dazu eine ganze Palette an geeigneten Massnahmen. Diese umfassen den Aufbau eines ISMS, die Umsetzung von Governance- und Compliance-Vorgaben sowie die Definition und Umsetzung einer geeigneten Netzwerk-Architektur und Sicherheits-Komponenten. Gleichzeitig unterstützt InfoGuard ihre Kunden bei der Integration angemessener ICT-Sicherheitsmassnahmen, welche auch in Form von Managed Security Services aus dem ISO/IEC 27001 zertifizierten Security Operation Center (SOC) zur Verfügung stehen. Periodische Audits der Infrastruktur und Sicherheitsprozesse sowie die permanente Überwachung der Infrastruktur komplettieren das Angebot.

Kontakt
InfoGuard AG
Lindenstrasse 10
CH-6340 Baar

www.infoguard.ch