Mit einem ISMS dem Blackout entgegentreten

Noch vor wenigen Jahren sprach keiner von Cyber Attacken – auch wenn es sie damals schon gab – heute sind sie in aller Munde. Die Bedrohung ist real und die Angreifer professionell, motiviert und leider auch erfolgreich. Ein Szenario wie im Technologie-Thriller «Blackout» beschrieben, ist durchaus denkbar. Um möglichen Sicherheitslücken wirksam zu begegnen, drängt sich ein strukturierter Sicherheitsansatz in Form eines Informationssicherheits-Managementsystems (ISMS) auch im Energiesektor auf.

von Markus Limacher, Senior Security Consultant, InfoGuard AG

Die Bedrohung der IT-Sicherheit für Unternehmen durch gezielte Cyber Attacken hat in den letzten fünf Jahren weltweit massiv zugenommen und längst ist nicht mehr nur der Finanz-Sektor betroffen. Treffen gezielte Attacken die Betreiber von kritischen Infrastrukturen, wie Energieversorgungsunternehmen (EVU), Wasserversorgung, Banken, Transport- und Logistikunternehmen), können sich mögliche Schäden massiv auf die betroffenen Unternehmen sowie auf nationaler und internationaler Ebene auswirken und eine Kettenreaktion verursachen. Welche Auswirkungen ein Energieausfall haben kann, hat im November 2014 auch die schweizweit angelegte Krisenübung aufgezeigt, bei welcher den Beteiligten die Konsequenzen eines plötzlichen Energiemangels eindrücklich vor Augen geführt wurden.

Komplexität mit erheblichem Risikopotential

Energieversorgungsunternehmen betreiben eine hochkomplexe und fragile IT-Infrastruktur, welche weit über die eigenen Unternehmensgrenzen hinausgeht und teilweise durch intelligente und miteinander kommunizierende Netzwerke verbunden ist. Viele Prozesse werden dabei durch Steuerungssoftware automatisiert und sind untereinander eng verzahnt. Dabei gelten gerade die SCADA-Netzwerke als besonders gefährdet. Bislang existierten die ICS-/SCADA-Systeme in einer eigenen isolierten Welt, proprietärer Protokolle auf speziellen Plattformen und einer darauf zugeschnittenen Kommunikationsinfrastruktur. Diese vermeintlich isolierte Welt ist jedoch selten so isoliert wie angenommen und wird mit Standard Komponenten und Applikationen ergänzt. Zudem werden diese Systeme zukünftig noch stärker mit externen Netzwerken und Cloud Services verbunden – und sei es «nur» um Lieferanten einen Remotezugang für Wartungsarbeiten zur Verfügung zu stellen. Damit sind sie auch den aus dem Internet bekannten Gefahren ausgesetzt. Datenschutz, Anlagen- und Informationssicherheit stellen somit wesentliche Faktoren für den Betrieb und den wirtschaftlichen Erfolg dar. Die technischen Innovationen im Stromnetz bringen Fortschritt, gleichzeitig neue oder gar zusätzliche Angriffsoptionen und Herausforderungen. Internationale Standards wie der ISO/IEC 27001 bietet ein Modell für die Einrichtung, Umsetzung, Überprüfung und Verbesserung auf der Basis eines Informationssicherheits-Managementsystems (ISMS) im systematischen Umgang mit bestehenden und neuen Herausforderungen.

EVU im Fokus von Hackern und Cyber Kriminellen

Die Gefahr von Angriffen ist real und Hacker führen zunehmend gezielt Angriffe auf Energieversorgungsunternehmen aus. Dabei fokussieren sie sich häufig auf existierende Schwachstellen in den Systemen und Prozessen oder auf den Menschen. Einige der bekanntesten Angriffe wie bei Stuxnet, Shamoon und dem jüngsten Nachfolger Dragonfly/Havex konzentrierten sich die Angreifer darauf,

SCADA-Systeme und andere industrielle Kontroll-Systeme indirekt anzugreifen. Dabei platzierten die Angreifer beispielsweise einen Trojaner auf einer Webseite eines ICS-Herstellers, darüber werden die Computer der Mitarbeiter infiziert, welche an die ICS-Umgebungen angebunden sind – Konsequenzen können Betriebsstörungen, Erpressungen, Informationsabfluss, Kontroll-Verlust der Systeme uvm. sein.

Solche «Watering-Hole»-Methoden, bei der die Opfer in Analogie zu Wildtieren an die «Wasserstelle» gelockt werden, wo der Feind lauert, werden oft angewendet. Die Angreifer missbrauchen dabei Schwachstellen in Web-Plattformen, um zum Download bereitgestellte Software-Installer durch infizierte zu ersetzen. Auf diese Weise gelang es mehrere Systeme auch von Schweizer EVU zu kompromittieren.

Mit System zu mehr Sicherheit

Energieversorgungsunternehmen sind gut beraten, wenn sie sich konsequent mit diesen neuen Risiken auseinandersetzen und der Informationssicherheit das nötige Gewicht beimessen. Dabei gilt es, das Rad nicht neu zu erfinden. Existierende, anerkannte Sicherheitsstandards, wie ISO/IEC 27001, welcher sowohl die organisatorischen als auch technischen Aspekte berücksichtigt, ohne dabei den Menschen ausser Acht zu lassen, können genutzt werden. Informationssicherheit lässt sich nicht durch technische Massnahmen alleine erreichen. Sie sind ganz sicher unabdingbar, sollten aber immer Mittel zum Zweck sein und sich in ein Gesamtsystem einbinden.

Genau hier setzt auch ein ISMS nach ISO/IEC 27001 an. Die Einführung eines ISMS ist gerade für Energieversorgungsunternehmen sehr hilfreich, aus zweierlei Gründen:

- Hinter der IT-Sicherheit stehen sehr komplexe Anforderungen, beginnend bei der klaren Definition der individuellen Sicherheitsanforderungen bis zum ständigen Monitoring und kontinuierlichen Verbesserung.
- Von den Unternehmen werden bereits viele Security-Massnahmen genutzt. Vielfach sind diese jedoch nicht aufeinander abgestimmt, weil sie einen anderen Fokus haben.

Diese Punkte können in einem konzertierten ISMS am effizientesten adressiert werden. Zu ihren Schlüsselelementen zählen Sicherheitsrichtlinien und -prozesse, welche den Security-Massnahmen (sowohl technischer wie organisatorischer Art) eine Ordnung und Führung verleihen. Zudem geht es auch darum, das Bewusstsein bei den Mitarbeitenden, den Sicherheitsverantwortlichen und dem Management gezielt zu fördern. Denn nach wie vor ist der Mensch einer der wichtigsten Eckpfeiler in einer Sicherheitsstrategie und viele erfolgreiche Angriffe haben ihren Ursprung beim Fehlverhalten (aus Unwissenheit oder manchmal auch Nachlässigkeit) von Menschen.

Auf der technischen Seite wird die Informationssicherheit durch die Umsetzung einer angemessenen Systemarchitektur massgeblich bestimmt. Es gilt verschiedene Verteidigungslinien (Lines of Defence) 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. Zudem ist die System- und Software-Wartung, mit einem entsprechenden Patch-Management unerlässlich und muss alle Systeme, Betriebssysteme und Applikationen berück-

ISMS nach ISO/IEC 27001

Mit ISO 27001 steht ein bewährter, global anerkannter und zertifizierbarer Standard zur Verfügung. Zentrales Merkmal ist das Verständnis der Informationssicherheit als geplanter, gelebter, überwachter und sich kontinuierlich verbessernder Prozess. Ein wesentliches Element des ISMS ist das Risikomanagement. Systematisch werden die wichtigen Informationswerte des Unternehmens und die damit verbundenen Risiken identifiziert, analysiert und der angemessene Schutz durch Massnahmen definiert.

Die regelmässige Überprüfung der Wirksamkeit ist ein weiterer wichtiger Bestandteil des Systems. Dadurch wird es «lernfähig» und passt sich wechselnden Bedingungen an. Der Standard lässt bei der Implementierung grosse Flexibilität zur individuellen Adaption. Es wird festgelegt, was unter bestimmten Rahmenbedingungen getan werden muss, jedoch nicht, wie es getan werden muss. Dies hat den Vorteil, dass schlanke, pragmatische Massnahmen definiert werden können; ein wichtiges Kriterium, um eine effektive Informationssicherheit zu erzielen. Dank der Skalierbarkeit des Standards könne vom KMU bis zu grossen Konzernen alle unterstützt werden.

sichtigen. Was schlussendlich nie vergessen werden darf, ist die periodische Überprüfung der gesamten Infrastruktur auf Schwachstellen und mögliche Angriffspunkte.

Die Einführung eines ISMS nach ISO/IEC 27001 Standard hilft Energieversorgungsunternehmen das Sicherheitsniveau systematisch zu steigern und dabei von Best Practice-Ansätzen zu profitieren.

Sicherheit kommt aus der Schweiz

Der Informationssicherheits-Experte InfoGuard bietet die ganze Palette an geeigneten Massnahmen zum Schutz der Informationen und Systeme im Energieumfeld. Dazu zählen der Aufbau eines ISMS, Risiko Optimierung in Form eines CISO as a Service Mandats, die gezielte Sensibilisierung der Mitarbeitenden, Sicherheitsaudits und Penetration Tests, aber auch Massnahmen zur Implementierung einer greifenden organisatorischen Sicherheit sowie technologische Massnahmen. Des weiteren Managed Services aus der Schweiz – angefangen von der Erstellung eines Zonenkonzeptes über den Perimeter Schutz bis hin zur Real Time Überwachung mittels eines Security Information and Event Management Systems (SIEM) zur frühzeitigen Erkennung und Abwehr von Angriffen auf die Infrastruktur.