Verhinderung des Total-Ausfalls

«Blackout». So lautet der Titel eines der erfolgreichsten Technologie-Thriller der letzten Jahre. Die europäischen Stromnetze werden von Hackern attackiert, sensible Punkte der Stromversorgung werden angegriffen. Der darauf folgende wochenlange Blackout führt in einigen Ländern zum Super-GAU. Was in der Fiktion ein gutes Ende findet, wurde von der Realität bereits überholt. Deshalb gilt: Gerade bei kritischen Infrastruktur ist die Informationssicherheit unerlässlich und darf nicht vernachlässigt werden.

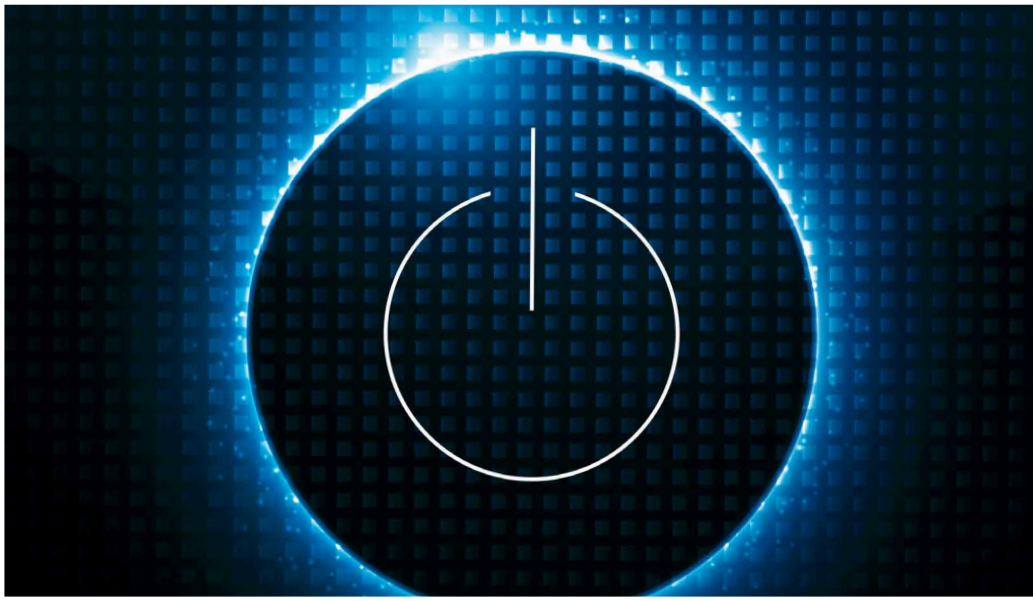
von Markus Limacher, Senior Security Consultant, InfoGuard AG

Stuxnet, Shamoon, Dragonfly: Wir befinden uns nicht im Biologieunterricht, sondern bei den gefährlichsten bekannten Attacken auf Energieversorger der letzten Jahre. Stuxnet ist ein Schadprogramm, welches speziell für SCADA Systeme (Supervisory Control and Data Acquisition) zur Überwachung und Steuerung technischer Prozesse entwickelt wurde. Dies führte zu Störungen im iranischen Atomprogramm (in der Urananreicherungsanlage). Der Computerwurm Shamoon führte bei Energieunternehmen im Nahen Osten (z. B. Saudi Aramco, Qatar's RasGas) zu einer plötzlichen Betriebsstörung und die Libelle (Dragonfly, ein Trojaner) ist ein Cyber-Spionagering, der hauptsächlich den nordamerikanischen und europäischen Energiesektor bedroht.

Das Feld potenzieller Bedrohungen ist gross und reicht von Naturkatastrophen bis hin zu human induzierten Krisen wie Erpressung, Wirtschaftsspionage oder Terrorismus. Auch in der Schweiz geht nach den oben erwähnten Vorfällen bei Energiedienstleistern die Besorgnis vor Cyberangriffen um. Gerade die Vorfälle im Iran zeigen deutlich auf, was passieren kann, wenn die Steuerungssysteme von den falschen Händen angefasst werden. Wie die Stromnetzbetreiber-Gesellschaft Swissgrid in einem Interview gegenüber SRF ausführte, sind die Hacker den Angegriffenen immer mindestens einen Schritt voraus. Zwar würden viele Spezialisten an der Verhinderung eines Blackouts arbeiten, gerade aber kleinere und mittlere Kraftwerkbetreiber mit wenig Ressourcen in punkto Sicherheitsmassnahmen wären eine einfache Beute. Und würden zu einem Kaskadeneffekt führen, welcher sich dann in einem gewaltigen «Knall» entladen und zum Ausgehen der Lichter führen könnte.

Wie in der Schweiz und Deutschland können in jedem Land jederzeit die kritischen Infrastrukturen und allen voran die Energieerzeuger von (Cyber-) Angriffen getroffen werden. Die Zahl der Cyber-Attacken wächst seit Jahren exponentiell. Attraktive Ziele für Hacker sind vor allem kritische Infrastrukturen wie Energie, Kommunikation und Verkehr. Diese sind aber oft nur rudimentär geschützt: Entweder wird Informationssicherheit nicht

systematisch betrieben oder die technische Umgebung wird noch getrennt von der IT betrachtet. Da heute Energie- und Datennetze vornehmlich digital gesteuert werden und Vernetzungsgrad und Datenflut ständig steigen, wächst auch die Verwundbarkeit der Infrastrukturen durch Cyber-Attacken. Die grössten Gefahren lauern in einer Infektion durch Schadsoftware über das Internet, deren Einschleusen mittels Wechseldatenträgern wie USB-Sticks, Social Engineering, mit dem Internet verbundene Steuerungskomponenten oder DDoS-An-griffen. Wichtig ist, die erforderlichen Sicherheitssysteme durchgängig zu implementieren, erst dann wird ein wirksamer Schutz gegenüber Cyber-Angriffen möglich.



Die Prozesse Im Energiesektor sind heute durch Steuerungssoftware vielfach automatisiert und hochgradig vernetzt. Dabei gelten gerade die SCADA-Netzwerke als besonders gefährdet. Bislang existierten die ICS-/SCADA-Systeme in einer eigenen Welt, proprietärer Protokolle auf speziellen Plattformen und einer darauf zugeschnittenen Kommunikationsinfrastruktur. Sie waren von anderen Netzwerken – einschliesslich Internet – weitgehend isoliert. Doch nun wird immer häufiger Standard-Hard- und Software (beispielsweise Microsoft Windows) eingesetzt und die Systeme werden mit externen Netzwerken und Cloud Services verbunden. Damit sind sie auch den aus der IT bekannten Gefahren ausgesetzt. Darum sind auch Hackerangriffe auf Energieversorger keine Seltenheit mehr, wie zahlreiche Pressemeldungen belegen. Das halbjährlich erscheinende ZEW Energiebarometer (Zentrum für Europäische Wirtschaftsforschung GmbH in Mannheim) hat im ersten Halbjahr 2014 eine Befragung der deutschen Energieversorger-Branche (ohne IT-Spezialisten) zur IT-Sicherheit durchgeführt. Dabei wurde insbesondere bei der Übertragungsnetz- und Verteilnetzinfrastruktur sowie bei der die Kraftwerksteuerung zum Teil erheblicher Nachholbedarf aufgedeckt.

So Smart die Grids, so komplex deren Schutz

Der Siegeszug der Vernetzung scheint unaufhaltsam. Bis 2020 wird sich die Zahl der «Networked Connections» – also der Internet-Zugänge, die mit anderen Stationen im globalen Netz Informationen austauschen – fast verzehnfachen (von jetzt 7 Mrd. auf 50 bis 70 Mrd.). Die Ursache für den rasanten Anstieg: In der jetzigen Phase der digitalen Revolution werden elektronische Geräte in das weltweite Netz integriert. Diese tauschen Informationen mit anderen Stellen im Netz aus. Das Internet der Dinge entsteht: «The Internet of Things». Ein wesentlicher Anwendungsfall im Internet der Dinge wird SmartGrid sein. Denn in einer Zeit, in der alternative Energien im Vormarsch sind, wird sich das Energiemanagement grundlegend wandeln. Ansonsten klaffen Verbrauchs- und Produktionsspitzen zeitlich auseinander. Dann drohen grossflächige Stromausfälle – Blackouts. Bereits aktuell ist unübersehbar, dass die Zahl der stabilisierenden Eingriffe in das Netz deutlich gestiegen ist. Beispielsweise registrierte der Energieversorger EWE im norddeutschen Gebiet im ersten Halbjahr 2013 insgesamt 350 solche Situationen. Doppelt so viele wie ein Jahr zuvor. Noch vor vier Jahren waren dort ein- bis zweimal wöchentlich solche Lenkungsmassnahmen nötig, heute oft mehrmals täglich.

Bei einem so umfassenden Informationsaustausch spielen Interoperabilität und Sicherheitsaspekt eine zentrale Rolle. Daten müssen immer häufiger über Unternehmensgrenzen hinweg ausgetauscht werden, weil eine Vielzahl verschiedener Unternehmen Teiltätigkeiten im Energie-Sektor übernommen haben, die früher an einer Stelle gebündelt wa-

ren. Unter diesen Voraussetzungen ist das SmartGrid ein starker Treiber der Sicherheitsthematik. Grundsätzlich gibt es (auch) im SmartGrid fünf essentielle Schutzziele:

- es muss einen Schutz vor Daten-Manipulation geben (Integrität)
- die Vernetzung muss stabil und verlässlich sein. Verlorene oder nicht erhaltene Informationen müssen identifiziert werden können, um bei Bedarf entsprechende Gegenmassnahmen zu treffen. (Verfügbarkeit)
- kein Unbefugter darf Zugriff auf Daten haben (Vertraulichkeit)
- die dauerhafte Energieversorgung ist zu gewährleisten (Versorgungssicherheit)
- die Herkunft von Daten muss nach vollziehbar sein (Nicht-Abstreitbarkeit)

Das Schutzziel der Versorgungssicherheit ist eng mit den Zielen Integrität und Verfügbarkeit verknüpft. Ein Mehr an Sicherheit in all diesen Bereichen umzusetzen ist umso wichtiger, weil die Sensibilität für das Thema Sicherheit in der öffentlichen Wahrnehmung sehr hoch ist. Die alarmierenden Berichte aus der Presse (bis hin zu Kühlschränken, deren Vernetzung für Spam-Attacken missbraucht wird) haben die Diskussion weiter befeuert. Somit ist ein vernünftiges Sicherheitskonzept zu einem zentralen Kriterium geworden.

Strategisches Vorgehen zur Sicherstellung der ununterbrochenen Stromversorgung

Zu diesem Zweck empfiehlt sich die Durchführung eines IT Security Audits, um mögliche Risiken auch aus dem Sichtwinkel eines externen aber auch eines internen Angreifers zu lokalisieren, einzuordnen und mögliche Lösungen zur Schliessung der Sicherheitsrisiken aufzuzeigen. Ziel ist es, für die Energiedienstleister eine ganzheitliche Sicherheit des Informationsflusses zu gewährleisten. Zur Kontrolle werden regelmässige System Audits, Penetration Tests und Vulnerability Scans durchgeführt. Gleichzeitig muss die Sicherheit aber auch auf der organisatorischen Ebene berücksichtigt werden. So müssen u. a. ein stringentes Berechtigungsmanagement, ein Datenschutz-Management System und ein Konzept zur Wahrung der organisatorischen Sicherheit (Need-to-Know-Prinzip) wichtige Eckpfeiler im Sicherheitsdispositiv von Energiedienstleistern sein.

In technologischer Hinsicht ist auf verschiedene Verteidigungslinien (Lines of Defence) zu setzen. Die Informationssicherheit wird durch den Entwurf der Systemarchitektur massgeblich bestimmt. Zu den Verteidigungswällen zählen die Verbindung von der kritischen Infrastruktur und der ICT mit einer End-zu-End-Sicherheit, ein umfassender Malware-Schutz auf vernetzten und geschlossenen Systemen, einem Perimeter Schutz bestehend aus einer Firewall, einem Intrusion Detection/Prevention System, einem VPN und einer Demilitarisierten Zone. Zudem ist der System- und Software-Update, mit einem entsprechenden Patch-Management unerlässlich. Dieser muss dabei alle Systeme, Betriebssysteme und Applikationen umfassen.

Grundsätzlich gilt auch im Energiesektor: Denken Sie im Rahmen der Strategiefindung auch an die Sicherheit der Informationen!

InfoGuard AG sichert die Energieversorgung

Der Schweizer Informationssicherheits-Experte InfoGuard bietet die ganze Palette an geeigneten Massnahmen zum Schutz der Daten und Systeme im SmartGrid. Dazu zählen CISO as a Service, Sicherheitsaudits und Penetration Testing, aber auch Massnahmen zur Implementierung einer greifenden organisatorischen Sicherheit sowie technologische Massnahmen und Managed Services aus der Schweiz – angefangen von der Erstellung eines Zonenkonzeptes über den Perimeter Schutz bis hin zur Real Time Überwachung mittels eines SIEM Security Information and Event Management Systems SIEM.

Kontakt
InfoGuard AG
Lindenstrasse 10
CH-6340 Baar
Telefon +41 (0) 41 749 19 00
info@infoguard.ch
www.infoguard.ch

Markus Limacher ist Senior Security Consultant bei der InfoGuard AG.