01. Jul 2014

Werden Industrieumgebungen mit den IT (Informationstechnik)-Netzen ihrer Betreiber gekoppelt, werden sie jedoch auch anfällig für Angriffe aus dem Internet. ©Bild: Aka / pixelio.de

Cyberkriminalität: Hacker bedrohen das Stromnetz

(©SR) Viele Einrichtungen der Stromversorgung werden über das Internet gesteuert und sind somit leicht angreifbar. Mit dem Trend zu Smart Grids und Smart Metering erhöht sich die Anfälligkeit der IT-Systeme weiter. Wenn der Umbau zum intelligenten Netz gelingen soll, müssen die Einfallstore für Cyberkriminelle geschlossen werden.

Ein Windkraftbetreiber in Brandenburg: Als in der Leitwarte die Nachricht von einer brennenden Windturbine eintrifft, sind die Techniker geschockt. Bei der Überwachung der Anlagen war zuvor alles in Ordnung. Doch eine E-Mail, die kurz darauf eintrifft, zeigt: Erpresser haben sich in das Computer-Netzwerk des Unternehmens eingeschleust und die Anlage sabotiert. Wenn es in Brandenburg noch einen einzigen „Spargel“ aufstelle, so die Drohung, werden weitere Mühlen zerstört.

Längst Standard
Dieses Beispiel ist nur erfunden, aber nicht unrealistisch. Denn viele Industrieanlagen und Kraftwerke sind heute mit dem Internet verbunden. Für die Unternehmen bringt die Vernetzung mehr Komfort und spart Kosten, etwa weil Techniker Maschinen aus der Ferne steuern können. In der Windkraft ist die Fernüberwachung längst Standard. Über ein Onlineportal und eine Internetverbindung greifen Betreiber auf die Monitoring- und Steuerungssysteme ihrer Anlagen zu.

Werden Industrieumgebungen mit den IT (Informationstechnik)-Netzen ihrer Betreiber gekoppelt, werden sie jedoch auch anfällig für Angriffe aus dem Internet. Das Problem ist ein technologisches Erbe aus den achtziger Jahren. Seit Jahrzehnten setzt die Industrie so genannte ICS/Scada-Systeme (Industrial Control Systems/Security Control and Data Acquisition) ein, mit denen Anlagen und Prozesse gesteuert werden. Diese Systeme haben aber keine Schutzmechanismen gegen unbefugten Zugriff oder Manipulation, denn sie wurden nicht konzipiert, um über das Internet erreichbar zu sein. „Schutz vor Hackern bieten sie deshalb nicht“, erklärt der IT-Experte Udo Schneider vom Software-Entwickler Trend Micro.

Offen wie ein Scheunentor
Gerade die Stromversorgung bietet Cyberkriminellen eine immer grössere Angriffsfläche. „Mit dem Trend zu Smart Grids und Smart Metering erhöht sich die Anfälligkeit der IT-

Systeme weiter“, erklärt Hartmut Pohl, Chef der Firma Softscheck und Sprecher des Arbeitskreises Datenschutz und IT-Sicherheit der Gesellschaft für Informatik. Mit dem Ökostrom-Ausbau muss das Stromnetz komplett umstrukturiert werden. Es besteht nicht mehr aus einfachen Versorgungsnetzen, sondern die Marktteilnehmer müssen über den Marktmechanismus miteinander kommunizieren. Das kann nur gelingen, wenn Stromerzeuger, -verbraucher und -speicher sowie die für die Übertragung und Verteilung notwendige Infrastruktur intelligent über viele Schnittstellen miteinander vernetzt werden. „Jeder dieser Verknüpfungspunkte bietet Kriminellen ein Einfallstor“, sagt Pohl.

Ein Problem sind die intelligenten Stromzähler in den Privathaushalten. Sie hängen an einem Kommunikationsmodul, dem Smart Meter Gateway, das die Messwerte weiterreicht. Ein weiteres Einfallstor für Hacker bieten Energiemanagementsysteme, die in den Netzen und Umspannwerken installiert sind. Sie haben die Aufgabe, Kraftwerke und Verbraucher in kleinen und grösseren Netzen miteinander zu verknüpfen. „Die Systeme werden zum Beispiel eingesetzt, um die Leistung mehrerer Energieerzeuger zu bündeln und diese aggregiert an die nächste Spannungsebene weiterzureichen“, erklärt Michael Metzger, Smart Grid-Experte bei Siemens. Die Gefahr: Wenn es Hackern gelingt, sich über das Betriebssystem eines Netzbetreibers Zugang zur Verteil- und Kontrolltechnik zu verschaffen, könnten sie ganze Netzbereiche lahm legen.

Mindeststandards-Verpflichtung
Aufgrund der hohen Risiken plant die deutsche Bundesregierung strengere Sicherheitsregeln im Energienetz. So kündigte sie noch für dieses Jahr den ersten Entwurf für ein IT-Sicherheitsgesetz an, das Betreiber wichtiger Infrastrukturen wie Energieversorger zu Mindeststandards bei der Sicherheit ihrer Computersysteme verpflichten soll.

Zudem will Berlin bis Ende des Jahres das Verordnungspaket „Intelligente Energienetze“ verabschieden. Wesentlicher Teil ist die Rollout-Verordnung, die für Haushalte und Gewerbebetriebe mit einem Jahresstromverbrauch von mehr als 6000 Kilowattstunden pro Jahr den Einbau von intelligenten Messsystemen verpflichtend vorschreibt. Die Einbaupflicht gilt, sobald die Smart Meter das so genannte Schutzprofil des deutschen Bundesamts für Sicherheit in der Informationstechnik erfüllen. Es sieht vor, dass das Gateway der Geräte drei Netzwerk-Domänen sicher miteinander verbinden kann, des Endkunden, des Zählers und externer Akteure. Dafür muss am Gateway ein zusätzliches Sicherheitsmodul installiert sein, das sämtliche Messwerte signiert und kryptografisch verschlüsselt.

Parallel prescht auch die deutsche Bundesnetzagentur mit einem neuen Regulierungsvorhaben vor. Die Behörde hat Energieanlagen- und Netze als kritische Infrastrukturen eingestuft und will die Unternehmen deshalb verpflichten, ein so genanntes Informationssicherheits-Managementsystem einzuführen. Kern dieser Systeme sind Regeln und Verfahren, die nötige Sicherheitstools definieren, steuern und kontrollieren und fortlaufend verbessern.

Smart Metering in der Cloud
Für Softwarefirmen öffnet sich mit den neuen Anforderungen ein gewaltiger Markt. Sie entwickeln deshalb auf breiter Front Sicherheitstechnologien und Analysemethoden, die Cyberattacken erkennen und stoppen können. „Firewalls und Antivirenprogramme allein reichen künftig nicht mehr aus. Verschlüsselung und Sicherheitslösungen werden immer wichtiger“, erklärt Albert Hold, Sprecher für Energiethemen bei der deutschen Telekom. So arbeitet das Unternehmen derzeit mit Projektpartnern an einem Smart Meter Gateway mit integriertem Kryptochip, der Daten verschlüsselt und die Zertifikate für das jeweilige Smart Meter verwaltet. Die ersten Geräte, die das Schutzprofil des BSI erfüllen, sollen diesen

Sommer für Feldversuche an Energieversorger geliefert werden.

Damit die Unternehmen die Smart Metering-Daten nicht aufwendig selbst verwalten müssen, bietet die Telekom ihnen so genanntes Cloud Computing an. Die Cloud ist vereinfacht gesagt ein riesiger Rechner, auf den die Smart Meter-Betreiber Informationen und Anwendungen auslagern und über den sie sämtliche Dienstleistungen laufen lassen können. Zugriff auf die Cloud haben sie über eine spezielle Web-Oberfläche oder eine passende Schnittstelle.

Security Testing fehlt oft

Softscheck-Experte Pohl ist überzeugt, dass sich das Smart Grid auch mit klassischen IT-Techniken vor Cyberangriffen schützen lässt. „Die Unternehmen überprüfen zwar regelmässig die Funktionalität ihrer Anlagen, aber eine Überprüfung der Sicherheitsfunktionen, ein Security Testing, fehlt oft." Softscheck hat verschiedene Verfahren entwickelt, um Sicherheitslücken in den Betriebssystemen von Unternehmen zu identifizieren und so einer Manipulation von ICS/Scada-Systemen vorzubeugen. „Wir simulieren Angriffe. Sind die Attacken erfolgreich, ist ein Software-Update nötig", erklärt Pohl.

Eine relativ einfache, aber wirkungsvolle Schutzmöglichkeit sieht Trend Micro-Experte Schneider in so genannten Intrusion Detection Systemen, die Angriffe auf ein Computernetzwerk frühzeitig erkennen. „Sie horchen am Internetübergang den Netzwerkverkehr ab und melden verdächtige Aktivitäten." Schneider befürchtet jedoch, dass sich Sicherheitschecks und -technologien nur schleppend durchsetzen werden. „Kraftwerke und Industrieanlagen müssten dafür heruntergefahren und überprüft werden – das verursacht Kosten." Ausserdem bestünden Wartungs- und Supportverträge. Griffen fremde Firmen in ein Gesamtsystem ein, verliere der Kunde seinen Support, so Schneider. Ein Schutzkonzept für das Stromnetz der Zukunft ist eine lösbare, aber schwierige Aufgabe.

Quelle: http://www.ee-news.ch/de/article/29016/cyberkriminalitaet-hacker-bedrohen-das-stromnetz