— Business —

Leichtes Ziel für Hacker

Versorgungssicherheit | Viele Einrichtungen der Stromversorgung werden über das Internet gesteuert und sind damit einfach zu attackieren. 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 ein einziger „Spargel" aufstellt, so die Drohung, werden weitere Mühlen zerstört.

Dieses Beispiel ist 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. Auch Dienstleister, die für die Wartung und Instandhaltung oder die Vermarktung des Windstroms zuständig sind, kommunizieren mit den Turbinen.

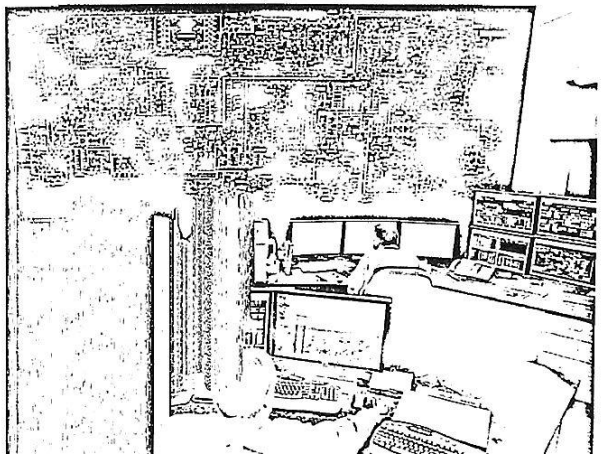
Werden Industrieumgebungen mit den IT (Informationstechnik)-Netzen ihrer Betreiber gekoppelt, dann werden sie aber auch anfällig für Angriffe aus dem Internet. Das Problem ist ein technologisches Erbe aus den achtziger Jahren. Seit Jahrzehnten setzt die Industrie so genannte ICS/Scada-Systeme (Industrial 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", sagt der IT-Experte Udo Schneider vom Software-Entwickler Trend Micro.

Tausende ungesicherte Industrieanlagen

Das Bedrohungspotenzial ist immens. Trend Micro hat einen Monat lang eine virtuelle Attrappe eines Wasserwerks aufgestellt und die Attacken auf die mit dem Internet verbundenen ICS/Scada-Systeme untersucht. Die Experten zählten in dieser Zeit 39 Angriffe auf Geräte-Protokolle und Server der Werksattrappe. „Alles, was mit dem Internet verbunden ist, wird wahrscheinlich angegriffen", schlussfolgert Schneider. Ein beängstigendes Fazit, wenn man bedenkt, dass nach einer aktuellen Erhebung der Freien Universität Berlin weltweit tausende Industrieanlagen, darunter Chemiefabriken, Kraftwerke und Pipelines, mit ungesicherten ICS/Scada-Systemen betrieben werden.

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", sagt 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 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. In den vergangenen Monaten wurden solche Stromzähler mehrfach geknackt. Auf der Insel Malta haben Kriminelle rund 1.000 Smart Meter so manipuliert, dass sie bei einigen stromintensiven Unternehmen im Land bis zu 75 % weniger Verbrauch erfassten. Der Betrug soll im Jahr 2012 zehn Prozent des maltesischen Stromverbrauchs ausgemacht haben. 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.



Das IBM-Programm „Hyref" will mit Hilfe von Messdaten aus Wind- und Solarkraftwerken und der Analyse von Wettermodellen kurzfristige Vorhersagen über die Ökostrom-Produktion etablieren. Doch die Sicherheitsfragen bei dieser internetbasierten Vorgehensweise sind noch nicht beantwortet.

Risiko „Big Data"

Risiken birgt auch der Ansatz, Massendaten aus dem Smart Grid in hoher Geschwindigkeit mit so genannten Big Data-Programmen zu analysieren. Der amerikanische Computerkonzern IBM zum Beispiel will mit dieser neuartigen Methode exakte, kurzfristige Vorhersagen der Ökostrom-Produktion ermöglichen. Sein Programm „Hyref" (Hybrid Renewable Energy Forecasting) verbindet eine Big-Data-Analysetechnik mit Wettermodellen, aktuellen Wetterdaten und Messdaten, die Windturbinen oder Solarkraftwerke liefern. Je größer der Anlagenpool und die Datenmenge ist, desto präziser die Vorhersage, heißt es. Doch wie sicher sind die Datenquellen bei diesem neuen Geschäftsmodell? Lassen sich aus Massendaten überhaupt eindeutige Zusammenhänge ableiten? Falsche Energieprognosen haben zur Folge, dass teure Regelenergie bereitgestellt werden muss.

Aufgrund der hohen Risiken plant die 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 6.000 kWh pro Jahr den Einbau von intelligenten Messsystemen verpflichtend vorschreibt. Die Einbaupflicht gilt, sobald die Smart Meter das so genannte Schutzprofil des 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 Sicherheitsmodul installiert sein, das sämtliche Messwerte signiert und kryptografisch verschlüsselt. Parallel prescht auch die 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.

Steuern über die Wolke

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 Cloudlösungen werden immer wichtiger", sagt Albert Hold, Sprecher der Telekom-Tochter T-Systems. So arbeitet die Telekom 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, will die Telekom ab 2015 so genanntes Cloud Computing anbieten. 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 Web-Oberfläche oder eine passende Schnittstelle. Eigene Programme für die Smart Meter-Kommunikation müssen sie nicht pflegen. Denkbar sei, dass künftig etwa auch virtuelle Kraftwerke über die Cloud gesteuert werden, sagt Hold.

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 Anspruch gegenüber der Wartungsfirma, sagt Schneider.

Auch T-Systems-Experte Jörg Benze glaubt, dass der Weg zu einem sicheren Stromnetz arbeitsreich werden könnte. Er leitet das Fokusprojekt „Energieinformationsnetze und -Systeme" der Informationstechnischen Gesellschaft im Verband VDE, im Rahmen dessen Experten aus den Sparten Energieversorgung, Automatisierung und Telekommunikation Normen und Standards zum Thema Smart Grid entwickeln. Die Herausforderung dabei: „Es müssen verschiedene Welten zusammengebracht werden. Anlagenbauer und Automatisierer gewichten Schutzziele anders als die Informations- und Kommunikationstechnologie." Bevor Sicherheitsregeln für das Smart Grid definiert werden könnten, müsse zunächst eine gemeinsame Fachsprache geschaffen werden, sagt Benze. Ein Schutzkonzept für das Stromnetz der Zukunft sei eine lösbare, aber schwierige Aufgabe. (rz) Sascha Rentzing