Neues Netz gegen Hacker

Je stärker sich die Akteure des Energiemarkts kommunikativ miteinander vernetzen, desto anfälliger wird das Stromnetz für Cyberattacken. Die Energiebranche braucht dringend ein Schutzkonzept für das Smart Grid.

Helle Aufregung im Kontrollzentrum von Bajupower: Soeben sind im Allgäu drei Solarkraftwerke des bayerischen Energieversorgers mit fünf Megawatt Gesamtleistung ausgefallen. Dabei war den Technikern zuvor nichts Ungewöhnliches aufgefallen. Als sich etwas später ein anonymer Anrufer meldet, erfahren sie, was schiefgelaufen ist: Solargegner haben sich in das System des Unternehmens gehackt und die Kraftwerke lahmgelegt. Sollte Bajupower die bayerische Landschaft mit weiteren Solarparks verschandeln, so die Warnung, werde die Gruppe künftig regelmäßig Kraftwerke des Unternehmens manipulieren.

Zwar sind Bajupower und die Erpressung frei erfunden, doch unrealistisch ist das Szenario nicht. In der Industrie ist die Fernüberwachung von Anlagen mittlerweile Standard. Fast alle Solarkraftwerke und Windturbinen werden heute über das Internet von einer zentralen Leitwarte aus gesteuert, weil Betreiber auf diese Weise lange Wege und Kosten sparen können. Koppeln die Unternehmen ihre Anlagen mit ihrer Informationstechnik (IT), sind sie aber auch leicht über das Internet attackierbar. „Es gibt keine absolute IT-Sicherheit. Deshalb kann auch das Energienetz angegriffen werden", sagt Prof. Jörn Müller-Quade, Leiter der Arbeitsgruppe Kryptographie und Sicherheit am Karlsruher Institut für Technologie (KIT).

Die Gefahr ist nicht bloß herbeigeredet. Die Softwarefirma Trend Micro hat einen Monat lang eine virtuelle Attrappe eines Wasserwerks aufgestellt und die Attacken auf die mit dem Internet verbundenen Anlagensteuerungssysteme untersucht. Die Experten zählten in dieser Zeit insgesamt 39 Angriffe auf die Geräte-Protokolle und Server der Werksattrappe. Ihr Fazit: Alles, was mit dem Internet verbunden ist, wird wahrscheinlich angegriffen.

Mit dem Aufbau des Smart Grids, des intelligenten Stromnetzes, steigt die Zahl möglicher Angriffspunkte weiter. Um eine dezentrale Versorgung mit erneuerbaren Energien zu ermöglichen, müssen Stromerzeuger, -verbraucher und -speicher sowie die für die Übertragung und Verteilung notwendigen Anlagen flexibel und über viele Schnittstellen miteinander vernetzt werden. „Wenn es um bewusste Manipulation geht, dann sind die Hauptangriffspunkte die Schnittstellen zwischen den Akteuren im Energiesystem", erklärt der Wirtschaftsingenieur Mathias Dalheimer vom Chaos Computer Club in Kaiserslautern.

Das Problem beginnt bei den Smart Metern, die nach und nach in allen deutschen Privathaushalten installiert werden sollen. Die intelligenten Stromzähler sind mit einem Smart-Meter-Gateway-Administrator verbunden, der die Messwerte über das Stromkabel oder per Mobilfunk an die Energieversorger weiterreicht. So entsteht in jedem Haus ein Einfallstor, das für Anschlussnutzer frei zugänglich ist. „Dass eine Plombe davor hängt, heißt nicht, dass die Leute nicht trotzdem versuchen werden, das System zu knacken", so Dalheimer. Ein noch gefährlicheres Einfallstor bietet aus seiner Sicht die gesamte Verteil- und Kontrolltechnik, die im Feld, also in den Netzen und bei den Energieerzeugern, installiert ist. „Ein Zugang ist die Prozessleittechnik der Energieversorger, um Windparks abzuregeln, die oft über einen Rückkanal mit den Steuerungssystemen des Verteilnetzes gekoppelt ist. Das ist alles extrem kompliziert gestrickt, und es lässt sich nicht generell sagen, welcher Angriffspunkt wie am besten geschützt werden sollte", erklärt der IT-Experte.

Die Bundesregierung plant deshalb nun strengere Regeln im Energienetz. Ein neues IT-Sicherheitsgesetz soll Energieversorger künftig zu Mindeststandards bei der Sicherheit ihrer Computersysteme verpflichten. Außerdem sollen die Unternehmen Angriffe auf ihre Netze an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden, damit die Behörden Gefahren besser einschätzen können. Schließlich müssen Smart Meter in Zukunft das sogenannte BSI-Schutzprofil erfüllen. Dieses schreibt ein zusätzliches Sicherheitsmodul für die Geräte vor, das alle Messwerte signiert und kryptografisch ver-

„Es gibt keine absolute IT-Sicherheit. Deshalb kann auch das Energienetz angegriffen werden."

schlüsselt. So kann kein Unbefugter die Kommunikation zwischen dem Smart Meter, dem Endkunden und externen Marktteilnehmern anzapfen.

Gleichzeitig treibt die Bundesnetzagentur ein neues Regulierungsvorhaben voran. Die Behörde will Energieversorger verpflichten, ein Informationssicherheits-Managementsystem einzuführen, um ihre IT-Systeme fortlaufend auf dem neuesten Stand der Sicherheitstechnik zu halten. Für Softwarefirmen öffnet sich damit ein riesiger neuer Markt. Die Energiebranche dürfte in den kommenden Jahren verstärkt Sicherheitstechnologien und Analysemethoden nachfragen, um Angriffe aus dem Internet abwehren zu können.

Die Telekom setzt dabei unter anderem auf die Cloud. Damit Smart-Meter-Betreiber Smart-Metering-Daten nicht aufwendig selbst verwalten müssen, bietet sie ihnen externe Rechenleistung an, auf die sie ihre Informationen und Anwendungen auslagern und über die sie alle Dienstleistungen laufen lassen können. Zugriff auf die Cloud haben die Betreiber entweder über eine Weboberfläche oder eine passende Schnittstelle. Eigene Software benötigen sie nicht.

In eine ähnliche Richtung geht der Ansatz des Kommunikationsspezialisten mdex. Er unterhält für Betreiber von Regenerativkraftwerken geschlossene Rechnernetze, sogenannte Virtual Privat Networks, mit denen sie ihre Anlagen sicher an ihre Leitstellen anbinden können. Über eine als Tunnel bezeichnete verschlüsselte Verbindung schickt der Kraftwerksbetreiber seine Anfragen über das mdex-Rechenzentrum an seine Anlagen. Dabei weist mdex dem Nutzer eine neue IP-Adresse zu. So sind die Mess- und Steuerungswerte, die durch den sicheren Tunnel gehen, von außen nicht einsehbar.

Prof. Hartmut Pohl, Chef des Softwareentwicklers Softscheck, glaubt, dass sich das Smart Grid aber auch mit relativ einfachen Methoden der klassischen IT schützen lässt. Die Firma nutzt verschiedene Verfahren, um Sicherheitslücken in den Betriebssystemen von Unternehmen zu identifizieren und so einer Manipulation vorzubeugen. „Wir simulieren Angriffe. Sind die Angriffe erfolgreich, ist ein Software-Update nötig“, erklärt Softscheck-Chef Hartmut Pohl. Neben diesem „Security Testing“ bieten laut Trend-Micro-Experte Udo Schneider auch sogenannte Intrusion Detection Systeme wirkungsvollen Schutz vor Angriffen auf ein Computernetzwerk. „Diese Systeme horchen am Internetübergang den Netzwerkverkehr ab und melden verdächtige Aktivitäten.

Doch Schneider befürchtet, dass sich Sicherheitstechnologien in der Energiebranche nur schleppend durchsetzen werden: „Kraftwerke und Industrieanlagen müssten dafür heruntergefahren und überprüft werden – das verursacht Kosten.“ Außerdem bestünden Wartungs- und Supportverträge. Würden fremde Firmen in ein Supportsystem eingreifen, würde der Kunde seinen Support verlieren, so Schneider. KIT-Forscher Müller-Quade ergänzt, dass die Energiebranche Sicherheitsbedenken derzeit noch nicht richtig ernst nehme. Um das zu ändern, müsse man den Unternehmen die neuralgischen Punkte aufzeigen. „Dafür ist vorab eine Modellbildung zur Analyse und Beschreibung des Smart Grids Voraussetzung“, so der Wissenschaftler. Bis zu einem Schutzkonzept für das Energienetz ist es noch ein weiter Weg. *Sascha Rentzing*

„Sicherheitsbedenken werden noch nicht richtig ernst genommen.“