# Presse

Forum für Zukunftsenergien

## Nr. 16/7 vom 08.04.2016

**„Regionales Forum für Zukunftsenergien“**

# Sicherheit der kritischen Infrastruktur im Zeitalter der Digitalisierung

Köln. **Die Digitalisierung kritischer Infrastrukturen wie der Energieversorgung verspricht Effizienzsteigerungen, mehr Komfort und stellt eine Schlüsseltechnologie für die Energiewende dar. Gleichzeitig beinhaltet sie jedoch auch neue Anforderungen an den Datenschutz und die Gewährung der Sicherheit der Systeme vor Angriffen. Welche Risiken sich daraus ergeben und wie diese minimiert werden können, diskutierte das Forum für Zukunftsenergien in Kooperation mit RheinEnergie im Rahmen des „Regionalen Forum für Zukunftsenergien“ am 4. April 2016.**

Der Mensch sei immer noch der größte Unsicherheitsfaktor, argumentierte der Innenminister von Nordrhein-Westphalen Ralf Jäger. Sorglosigkeit mache jede noch so gute Firewall, jedes Schutzprofil und alle hohen Standards obsolet. Das gelte sowohl für die Bürger, vor allem aber auch für Netzbetreiber und Energieversorger. Eine wichtige Maßnahme gegen Cyber-Kriminalität sei daher, auf allen Ebenen ein Bewusstsein für potenzielle Angriffspunkte und ihre Vermeidung zu schaffen. Sollte es dennoch zu einem Angriff kommen, sollten die Unternehmen sich unmittelbar an das Cybercrime-Kompetenzzentrum wenden und mit den Behörden zusammenarbeiten, denn Cyber-Kriminalität sei nur mit vereinten Kräften zu bekämpfen. Ebenso müssten Schutzstandards in Kooperation entwickelt werden.

Die Digitalisierung stelle jedoch nicht nur eine Bedrohung, sondern auch eine große Chance dar, die es zu nutzen gelte. Der steigende Anteil an erneuerbaren Energien erfordere beispielsweise eine effiziente Analyse und Koordination von Stromproduktion und Stromverbrauch, bei der die Digitalisierung in Form von intelligenten Zählern (*Smart Meter*) eine Schlüsseltechnologie bildet.

Die in jüngster Zeit erfolgreichen Hackerangriffe auf den Deutschen Bundestag und Unternehmen wie Sony sowie die versuchten Angriffe auf belgische Kernkraftwerke zeigten auf, wie groß die Gefahr durch Cyber-Attacken sei, berichtete Thomas Haldenwang, Vizepräsident des Bundesamtes für Verfassungsschutz. Angreifer müssten nicht unbedingt über die Fähigkeiten, sondern lediglich über die finanziellen Mittel verfügen, um einen Angriff durchführen zu lassen.

Der Verfassungsschutz setze zur Bekämpfung von Cyber-Attacken nicht nur auf die Erkennung von Angriffen, sondern auch auf deren Prävention. So werden regelmäßig Info-Briefe herausgegeben, um über aktuelle Gefahren zu warnen und Fortbildungen zum sicheren Umgang mit IT-Systemen angeboten. Fortschritte seien auch durch das am 25. Juli 2015 in Kraft getretene „IT-Sicherheitsgesetz“ erzielt worden. Darin werden Betreiber von kritischen Infrastrukturen verpflichtet, mit ihren Infrastrukturen Mindeststandards bei der IT-Sicherheit zu erfüllen und eventuelle Vorfälle zu melden. Außerdem sollen innerhalb der Branchen Standards entwickelt werden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) genehmigt werden müssen. Die Kooperation mit den Unternehmen gestalte sich bislang jedoch schwierig, da diese sich nicht gerne „in ihre Arbeit hereinreden“ ließen. Im Falle eines Angriffs biete sich der Verfassungsschutz als diskreter Partner an, da dieser im Gegensatz beispielsweise zur Polizei keine Strafverfolgung betreibe.

Dr. Andreas Cerbe, Mitglied des Vorstands der RheinEnergie AG, betonte, dass

neben der Kundennähe für Stadtwerke wie die RheinEnegie das Kundenvertrauen von höchster Bedeutung sei. Daher stehe man einer übereilten Einführung von neuen Technologien, wie „*Smart Meter",* kritisch gegenüber, soweit dadurch Sicherheitsstandards herabgesetzt würden. Problematisch sei insbesondere, dass jeder Kontaktpunkt zu Daten auch einen Angriffspunkt auf selbige darstelle. Dabei hätte die Zahl der Kontaktpunkte im Zuge der Dezentralisierung der Stromnetze bereits stark zugenommen, da sich diese von unidirektionalen in bidirektionale Netze wandeln, um die vielen verschiedenen Erzeugungsanlagen zu integrieren und zu koordinieren. Während man sich gegen Ausfälle in bidirektionalen Netzen mit redundanten Kommunikationsinfrastrukturen absichern könne, erhöhten Technologien wie „*Smart Meter"* die Komplexität der Systeme in beträchtlichem Maße. Um die Folgen von Angriffen möglichst gering zu halten, seien die Systeme (Prozesssteuerung, Büro-IT, Kundenkommunikation, usw.) in Zonen aufgeteilt. Diese Zonen seien nur über Umwege und in Teilbereichen gekoppelt. Mit Blick auf die Komplexität des Themas appellierte Dr. Cerbe daran, Kräfte und Systeme auch unternehmensübergreifend zu bündeln, um ein hohes Sicherheitsniveau zu gewährleisten.

An der anschließenden Podiumsdiskussion, die von Dr. Annette Nietfeld, Geschäftsführerin des Forum für Zukunftsenergien, moderiert wurde, beteiligten sich neben Dr. Andreas Cerbe Dr. Frank Schmidt, Leiter Energy bei T-Systems International, Udo Sieverding, Mitglied der Geschäftsleitung und Bereichsleiter Energie bei der Verbraucherzentrale Nordrhein-Westfalen und Joachim Vanzetta, Leiter Systemführung Netze Brauweiler bei Amprion.

Zum Thema „*Smart Meter*" führte Dr. Cerbe an, dass nur solche Geräte eingesetzt würden, die das vom Gesetzgeber geforderte Schutzprofil aufweisen. Probleme könnten jedoch entstehen, wenn Nutzer sich *Smart Home*-Lösungen selbst zusammenstellten, für die diese dann selbst verantwortlich sind. Daher müssten sichere Komplettsysteme angeboten werden. Dr. Schmidt betonte, dass der als Ergebnis aus einer langen Diskussion hervorgegangene BSI-Standard kaum sicherer zu gestalten sei. Sieverding stellte den für die Zukunft geplanten Zwangseinsatz von „*Smart Meter"* generell in Frage, da sich für Haushalte (ausgenommen *Prosumer* mit eigenen Erzeugungsanlagen), die nur 25 Prozent des Stromverbrauchs ausmachten, kein finanzieller Nutzen ergebe.

Die Diskussionsteilnehmer waren sich einig, dass Kunden zwar achtsam mit ihren Daten umgehen sollten, die Versorgungsunternehmen jedoch in der Pflicht stünden, – wie bisher – eine zuverlässige Energieversorgung zu gewährleisten. Dazu würden auf Netzebene laut Vanzetta zum Beispiel separate Kommunikationsnetze betrieben. Sieverding argumentierte, dass eventuelle Mehrausgaben zur Verbesserung der Sicherheitsstandards von Netzen nicht zu Kostensteigerungen für die Endverbraucher führen dürften. Diese Kostensteigerungen würden durch Effizienzsteigerungen, die durch die Digitalisierung zu erzielen seien, kompensiert.

Vanzetta wies auf die Verlagerung von Verantwortung für die Systemsicherheit auf die Verteilnetzbetreiber (VNB) hin. Unabhängig davon gelte es, die Zusammenarbeit von VNB und Übertragungsnetzbetreibern (ÜNB) zu vertiefen, was im Netz von Amprion sehr gut funktioniere, bestätigte Dr. Cerbe.

Außerdem problematisierte Vanzetta das Dilemma welches sich durch die gewünschte Onlineoffenlegung von Lastflüssen zwischen Transparenz- und Sicherheitsstrebens ergibt. Potentiellen Angreifern würden dadurch die Schwachstellen des Systems präsentiert.

Zum Thema *Cloud-D*ienste unterstrich Dr. Schmidt, dass sie großen Nutzen böten. Durch sie könne die Aktualisierung von Schutzmechanismen einfacher gewährleistet werden. Dabei seien gewerbliche *Cloud*-Dienste von öffentlichen Diensten zu unterscheiden, die mit der Auswertung der Kundendaten Geld verdienten. Mit Blick auf Zugriffsrechte müsse jedoch bedacht werden, in welchem Land die Datenhaltung erfolge.

Das Forum für Zukunftsenergien bedankt sich bei RheinEnergie für die Unterstützung.

## Über das Forum für Zukunftsenergien e.V.

Das Forum für Zukunftsenergien engagiert sich als einzige branchenneutrale und parteipolitisch unabhängige Institution der Energiewirtschaft im vorparlamentarischen Raum in Deutschland. Der eingetragene Verein setzt sich für erneuerbare und nicht-erneuerbare Energien sowie rationelle und sparsame Energieverwendung ein. Ziel ist die Förderung einer sicheren, preisgünstigen, ressourcen- und umweltschonenden Energieversorgung. Dem Verein gehören ca. 250 Mitglieder aus der Industrie, der Energiewirtschaft, Verbänden, Forschungs- und Dienstleistungseinrichtungen sowie Persönlichkeiten aus Politik, Wirtschaft, Wissenschaft und Verwaltung an.

**Kontakt:**


Gregor J. Weber M.A.
Referent
Forum für Zukunftsenergien e.V.
Reinhardtstr. 3
10117 Berlin

Tel.: 030 / 72 61 59 98 - 5
Fax: 030 / 72 61 59 98 - 9
weber@zukunftsenergien.de
www.zukunftsenergien.de