Neue ENISA-Studie: 10 Empfehlungen, um europäische intelligente Stromnetze sicherer zu machen

Die EU-Agentur ENISA hat einen neuen Bericht dazu veröffentlicht, wie intelligente Stromnetze (Smart Grids) und ihre Markteinführung erfolgreich gestaltet werden können, insbesondere durch Berücksichtigung von IT-Sicherheitsfragen von Beginn an.

Smart Grids sind spezielle Elektrizitätsnetze mit wechselseitiger digitaler Kommunikation zwischen Anbieter und Verbraucher. Die Einführung von intelligenten Stromnetzen wird die Verteilung und Kontrolle von Energie für Solaranlagen, kleinen Windturbinen, elektrischen Fahrzeugen, etc. dramatisch verändern. Durch ihre effizientere Energieversorgung bieten intelligente Stromnetze Verbrauchern, Stromanbietern, Netzbetreibern und der Gesellschaft als ganzer klare Vorteile. Gleichzeitig macht die Abhängigkeit von Computernetzwerken und Internet unsere Gesellschaft anfälliger für Cyber-Angriffe, mit potentiell verheerenden Folgen. Um eine erfolgreiche Markteinführung von intelligenten Stromnetzen vorzubereiten, schlägt die ENISA-Studie daher aus mehr als 100 Erkenntnissen zehn Sicherheitsmaßnahmen für den öffentlichen und privaten Sektor vor. Zu den wichtigsten Empfehlungen gehören:

- ***Die Europäische Kommission (EC) und die verantwortlichen Behörden der Mitgliedsstaaten (MS) müssen ein klares Regelwerk und einen Politikrahmen zur Cybersicherheit von intelligenten Stromnetzen auf nationalem und EU-Level aufstellen, die derzeit noch fehlen.***
- ***Die EC sollte in Zusammenarbeit mit der ENISA, den MS und dem Privatsektor eine Mindestanzahl an Sicherheitsmaßnahmen ausarbeiten, entsprechend den vorhandenen Standards und Leitlinien.***
- ***Sowohl die EC-, als auch die MS-Behörden sollten Sicherheitszertifizierungsverfahren für die komplette Wertschöpfungskette von Bestandteilen der Smart Grids fördern, einschließlich der Organisationssicherheit.***
- ***Die MS-Behörden sollten Computer Emergency Response Teams miteinbeziehen, damit diese eine beratende Rolle bei der Sicherheit von Stromnetzen spielen können.***

Der Geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, bemerkte dazu:

„Unsere Studie zeigt, dass die zwei „getrennten Welten" von Energiesektor und IT-Sicherheitssektors bei der Sicherheit von intelligenten Stromnetzen miteinander abgestimmt werden müssen. Wir befürchten, dass sich intelligente Stromnetze ohne die Berücksichtigung von Cybersicherheit unkoordiniert entwickeln werden. Ich empfehle daher, dass die Sicherheit von Smart Grids Teil der künftigen EU-Internetsicherheitsstrategie werden sollte."

Internetsicherheitsaspekte von intelligenten Stromnetzen

Intelligente Stromnetze erzeugen neue Herausforderungen an die Informationssicherheit für Elektrizitätsnetzwerke. Die Angreifbarkeit von Informationssystemen kann in Cyberattacken aus wirtschaftlicher oder politischer Motivation dazu genutzt werden, um Kraftwerke abzuschalten. Im Jahr 2009 gaben US-Behörden zu, dass sich Cyber-Spione ins amerikanische Stromnetz eingehackt hatten (Quelle: DowJones/*The Wall Street Journal*). Software und Hardware für die Infrastruktur der intelligenten Stromnetze sind daher starke Risikoziele. Deshalb ist der freie Zugang zu Informationen vital für den Erfolg von intelligenten Stromnetzen.

Vollständiger Bericht

Hintergrund:

EU Smart Grids Communication

EU Critical Information Infrastructure Protection- CIIP Communication

European Commission Initiative on Smart Cities

Für Interviews: Ulf Bergstrom, Pressesprecher, ENISA, press@enisa.europa.eu, Mobil: + 30 6948 460 143, oder Konstantinos Moulinos, Smart Grids Project Manager, ENISA, Konstantinos.Moulinos@enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.
http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch
www.enisa.europa.eu