Energie: Cyber-Sicherheit ist entscheidend für die Abwehr von Gefahren für intelligente Stromnetze und damit wesentlich für die Energiesicherheit, so ein neuer Bericht der EU-Agentur für Cyber-Sicherheit.

Die EU Agentur für Netz- und Informationssicherheit, ENISA, weist darauf hin, dass die Einschätzung von Gefahren für Smart Grids wesentlich für den Schutz dieser ist und somit ein zentrales Element der Energiesicherheit darstellt.

Smart Grids sind komplexe „Systeme von Systemen", die Energie speichern, weiterleiten und die Versorgung von der Energieerzeugung bis zum Verbraucher steuern. Ein Smart Grid ist de facto kritische Infrastruktur, da Energie für die Gesellschaft und für das reibungslose Funktionieren der Wirtschaft von zentraler Bedeutung ist. Smart Grids kombinieren Energie- und Informationsinfrastrukturen und stellen somit eine kritische Infrastruktur dar, die sicher funktionieren und die Privatsphäre von Endverbrauchern wahren soll.

Der Geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, kommentierte den Bericht wie folgt: *„Ein Verständnis der Gefahrenlage von Bedrohungen im Internet ist unerlässlich, um die notwendigen Schutzmaßnahmen für Smart Grids zu ergreifen. Der Bericht ist die Antwort auf dringende Fragen von Energieversorgern und anderen Beteiligten: Er liefert das Instrumentarium, um die Risikolage für Smart Grids abzuschätzen. In Sachen Cybersicherheit müssen wir gemeinsame Anstrengungen unternehmen und unsere Aktivitäten koordinieren, um die Auswirkungen zu verringern."*

Der Bericht schildert die Risikolage für die Komponenten Smart Grids. Er unternimmt eine Bestandsaufnahme der verfügbaren Cybersicherheit und bisheriger Ansätze zur Absicherung und listet bewährte Verhaltensregeln auf. Die Studie verweist ebenso auf die internen Gefahren für IT-basierte Smart Grid Anlagen, darunter die unterschiedlichen Gefahren, die von Fehlern oder Insider-Angriffen ausgehen.

Wichtige Schlussfolgerungen: Einige Schlussfolgerungen sind:

- *Prüfen Sie externe und interne Gefahren:* In Sachen Cyber-Sicherheit stellen externe Cyber-Bedrohungen die wichtigste Quelle externer Gefahren dar. Dieses Gefahrenumfeld geht von Akteuren aus, die Online-Bedrohungen und Cyber-Angriffe starten.
- *Zerlegen und klassifizieren Sie die Elemente der Smart Grids, die potenziell Gefahren ausgesetzt sind*: von elektrischen Bestandteilen wie Kabeln, Schaltern, Routern,

Sensoren und Informationen bis hin zu Software wie Betriebssystemen, Services, Hardware, Infrastrukturen und diejenigen, die die Systeme bedienen.

- *Nutzen Sie das verfügbare Wissen*: Greifen Sie auf bewährte Verhaltensweisen zurück, nachdem Sie den gewünschten Sicherheitsgrad festgelegt haben.
- *Machen Sie eine Liste der **konkreten Cyberbedrohungen für Smart Grids** wie etwa:*
    - *Abhören/Abfangen/Übernahmen: z.B. Informationslecks, das Abfangen von elektromagnetischen oder Radiofrequenzen, Angriffe von Schnüfflern, der Ausfall von Geräten oder Systemen, Angriffe und tätliche Angriffe*
      *und derjenigen, von denen diese **Bedrohungen ausgehen** wie etwa Konzerne, Internetkriminelle, Angestellte, Hacktivisten, Nationalstaaten, Naturkatastrophen, Terroristen, das neue Phänomen der Cyber Fighter*
- *Erkennen Sie die Schwachstellen und Gefahren in Smart Grids.*
- *Einschätzung durch Netzeigentümer*: Die Agentur kommt zu dem Ergebnis, dass die Bewertung der Gefahren und Risiken eines Smart Grids nur durch den Netzeigentümer stattfinden kann, da er die Komplexität und Verflechtung der entsprechenden Infrastrukturen kennt.

Zum vollständigen Bericht

Hintergrund: ENISA-Bericht zu Smart Grids (Dezember 2012); Zehn Empfehlungen (Juli 2012) Die Cybersicherheits-Strategie der EU, der Vorschlag für eine EU-Richtlinie zur Cyber-Sicherheit

Für Interviews: Ulf Bergström, Pressesprecher, ulf.bergstrom@enisa.europa.eu, mobil: + 30 6948 460 143, Dr. Louis Marinos, ENISA-Experte, resilience@enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.

http://www.enisa.europa.eu/media/enisa-auf-deutsch/
www.enisa.europa.eu