Bundesministerium
für Bildung
und Forschung

Modellbasierte Stresstests für Cybersichere Energienetze (CyberStress)

Motivation

Mit der zunehmenden Nutzung erneuerbarer Energiequellen kommt es zu einer fortschreitenden Dezentralisierung der Stromerzeugung. Damit Strom bedarfsgerecht bereitgestellt werden kann, nimmt auch der Grad der Vernetzung und Automatisierung zu, was wiederum die Anfälligkeit des Stromnetzes für sog. verteilte Cyberangriffe erhöht. Wie die Widerstandsfähigkeit von Stromnetzen gegen solche Angriffe ohne größere Nutzungseinschränkungen ausreichend sicher und wirtschaftlich erreicht werden kann, ist mit komplexen Herausforderungen verbunden. So fehlt es beispielsweise den Netzbetreibern bisher an Erkenntnissen und Erfahrungen über modellbasierte Stresstests bei verteilten IT-Angriffen.

Ziele und Vorgehen

Das Projekt CyberStress zielt darauf ab, diese Wissenslücken zu schließen. Basierend auf Konzepten aus dem Finanzsektor für systemkritische Banken soll eine allgemeine Stresstest-Methodik entwickelt werden. Ein weiterer Schritt ist die Simulation von Stresstestmodellen für verschiedene Angriffsszenarien. Für das Szenario des verteilten Cyberangriffs werden auch aktive Gegenmaßnahmen untersucht und in die Simulation einbezogen. Neben den IT-technischen Problemstellungen werden auch wirtschaftliche Schadensfälle analysiert, die zum Beispiel durch Marktmanipulationen verursacht werden. Zum Abschluss werden die Simulationen an einem Beispielnetz getestet und ausgewertet. Mit Hilfe solcher Stresstests können mögliche Sicherheitslücken im Energiesystem frühzeitig identifiziert, das System gehärtet und die Versorgungssicherheit langfristig sichergestellt werden.

Innovationen und Perspektiven

Durch das Projekt wird die Widerstandsfähigkeit von Stromnetzen gegenüber Cyberangriffen erhöht. Der Bundesnetzagentur wird eine wissenschaftlich fundierte und wirtschaftlich einsetzbare Methodik für die Konzeptionierung und Durchführung von Stresstests im nationalen Energiesystem bereitgestellt, um auf zukünftige Angriffsszenarien besser vorbereitet zu sein.

Die fortscheitende Digitalisierung und Vernetzung halten auch bei der Stromversorgung Einzug.

Programm
Forschung für die zivile Sicherheit
Bekanntmachung: Zivile Sicherheit – Bedrohungen aus dem digitalen Raum.

Gesamtzuwendung
1,77 Mio. Euro

Projektlaufzeit
Mai 2023 – Apri 2026

Projektpartner
- Technische Universität Darmstadt – Energy Information Networks and Systems, Darmstadt
- Johann Wolfgang Goethe-Universität Frankfurt am Main – FB 01 Rechtswissenschaften, Frankfurt am Main
- e-netz Südhessen AG, Darmstadt
- QGroup GmbH, Wehrheim

Assoziierte Partner
- Bundesnetzagentur
- Amprion GmbH

Verbundkoordinator
Prof. Dr. Florian Steinke
Technische Universität Darmstadt
E-Mail: florian.steinke@eins.tu-darmstadt.de

Impressum
Herausgeber Bundesministerium für Bildung und Forschung (BMBF), Referat Zivile Sicherheitsforschung, 53170 Bonn;
Stand August 2023; **Text** VDI Technologiezentrum GmbH; **Gestaltung** neues handeln AG; **Bildnachweis** stock.adobe.de/zoteva87

↗ bmbf.de ↗ sifo.de