MEDIT

Methoden für Energienetzakteure zur Detektion, Prävention und Reaktion bei IT-Angriffen und IT-Ausfällen

Fraunhofer
Fraunhofer-Zentrum Digitale Energie

Projektziele

Die Elektrizitätsversorgung steht durch die Energiewende und der damit einhergehenden Digitalisierung vor großen Herausforderungen. Benötigt werden unter anderem speziell angepasste IT-Sicherheitstechnologien. Die beteiligten Partner des Fraunhofer-Zentrums Digitale Energie, die Schleswig-Holstein Netz AG, die devolo AG, die P3 Energy & Storage GmbH, die KISTERS AG und die Hochschule Bremen entwickeln im Rahmen des vom BMWK geförderten Projektes »MEDIT« Methoden für Energienetzakteure zur Detektion, Prävention und Reaktion bei IT-Angriffen und IT-Ausfällen.

Nutzen

Der Wandel in der Stromerzeugung bringt den vermehrten Einsatz von Informations- und Kommunikationstechnik (IKT) auch auf Verteilungsnetzebene mit sich. Dies stellt den Netzbetrieb vor allem auch im Bereich der IT-Sicherheit vor neue Herausforderungen, da Ausfälle oder Eingriffe auf IKT-Ebene direkte, schwerwiegende Auswirkungen für den sicheren Netzbetrieb haben können. Der Untersuchung der IT-Sicherheit und der Entwicklung von IT-Sicherheitstechnologien speziell für elektrische Netze kommt demnach eine hohe Bedeutung zu. Hierbei wird im Rahmen des Projekts ein ganzheitlicher Ansatz verfolgt, der gleichermaßen die Bereiche Prävention, Detektion und Reaktion adressiert und Besonderheiten in der Energiebranche berücksichtigt.

Ergebnisse

Es wurde eine Forschungs- und Validierungsumgebung zur Entwicklung neuer IT-Sicherheitstechnologien aufgebaut. Hierzu zählen u.a. eine Co-Simulation für Energie- und IKT-Netze, sowie die Erweiterung des Labors der RWTH Aachen um IKT für Prozessnetze.

Fraunhofer FIT entwickelte zudem einen mehrstufigen Ansatz zur Detektion von Cyberangriffen im Prozessnetz auf der Basis von energietechnischem sowie informationstechnischem Wissen. Ein Schwerpunkt von Fraunhofer FKIE im Projekt lag in der Entwicklung eines Leitfadens für technisches Personal zum Vorgehen bei IT-Sicherheitsvorfällen und einer Übungsumgebung, in der diverse Störungs- und Angriffsszenarien abgebildet werden und somit die Anwendung des Leitfadens ermöglicht.

Konsortium

- devolo AG
- Hochschule Bremen
- KISTERS AG
- RWTH Aachen
- Schleswig-Holstein Netz AG
- umlaut energy GmbH

Projektlaufzeit

01/2018 – 01/2022

Gefördert durch

Das Bundesministerium für Wirtschaft und Klimaschutz - BMWK

Fragen zum Projekt?

Schreiben Sie uns, oder besuchen Sie die Projekt-Webseite.