SecDER
Schutzsystem für Virtuelle Kraftwerke

[18.7.2024] Das Projekt SecDER hat ein Schutzsystem entwickelt, das Virtuelle Kraftwerke mithilfe Künstlicher Intelligenz vor Cyberangriffen und technischen Störungen bewahrt. Die Lösung funktioniert herstellerunabhängig und soll in Zusammenarbeit mit der Energiewirtschaft weiter optimiert werden.

Das Projekt "SecDER – KI-basierte Erkennung und resiliente Vermeidung von Cyber-Angriffen und technischen Störungen bei virtuellen Kraftwerken und dezentralen Energieanlagen" hat ein neuartiges Schutzsystem entwickelt, das Virtuelle Kraftwerke mit dezentralen Energieanlagen automatisiert vor Ausfällen schützt. Wie das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) mitteilt, nutzt das System Künstliche Intelligenz, um Cyberangriffe und Störungen zu erkennen. Anders als marktübliche Systeme arbeitet das neue System nur mit Daten der Kommunikation zwischen den Anlagen in Virtuellen Kraftwerken. Eine genaue Kenntnis der Energieanlagen und ihrer Messgrößen ist nicht notwendig. Damit ist die Lösung unabhängig von proprietärer Technologie der Anlagen und lässt sich herstellerunabhängig einsetzen. Die im Projekt prototypisch realisierte Lösung soll nun gemeinsam mit der Energiewirtschaft weiterentwickelt werden.

Was sind Virtuelle Kraftwerke?

Virtuelle Kraftwerke spielen eine wichtige Rolle bei der Nutzung erneuerbarer Energien. Sie bündeln, steuern und überwachen die Energieflüsse aus einer Vielzahl von unterschiedlichen dezentralen Energiequellen wie Windenergie-Anlagen, Photovoltaikanlagen und Wasserkraftwerken. Damit agieren sie wie ein Großkraftwerk, um die erforderliche Pool-Größe für die erfolgreiche Teilnahme an den Strommärkten zu erreichen. Der Betrieb eines solchen Anlagenparks ist technisch anspruchsvoll und lässt sich nur mittels moderner IT-Systeme bewältigen. Das vergrößert die Angriffsfläche Virtueller Kraftwerke für Cyberangriffe enorm, im Gegensatz zu klassischen Großkraftwerken.
Im Projekt SecDER wurde zunächst die Sicherheit Virtueller Kraftwerke untersucht und Cyberangriffe auf ein Modell eines Virtuellen Kraftwerks simuliert. Dabei stellten die Forschenden fest, dass selbst erfolgreiche Attacken auf einzelne Anlagen bislang nicht immer von Kraftwerks- oder Anlagenbetreibern bemerkt

werden. Denn herkömmliche Überwachungssysteme reagieren nicht unbedingt auf Ausfälle einzelner Anlagen. Doch verschiedene kleinere Ausfälle können in Summe die Sicherheit des Gesamtsystems gefährden und dazu führen, dass Virtuelle Kraftwerke keinen Strom mehr liefern.

Automatische Erkennung von Störungen

Das Projektkonsortium entwickelte daraufhin ein Intrusion-Detection-System, das mittels Machine Learning sowohl Cyberangriffe als auch technische Störungen automatisch erkennt und abwehrt. Es versetzt das gesamte System in eine passende Cybersafe-Position, sodass keine unsichere Steuerungsmaßnahme mehr ausgeführt werden kann. Dabei gibt es nicht nur eine Cybersafe-Position, sondern verschiedene, die dynamisch und passgenau auf unterschiedliche Gefahrenszenarien reagieren. Trotz laufender Angriffe und Störungen können Virtuelle Kraftwerke so zuverlässig weiter Strom erzeugen.
Das SecDER-Intrusion-Detection-System nutzt allgemeine Daten und Kommunikationskanäle, die jede Anlage mit ihrem Virtuellen Kraftwerk teilt, statt Daten aus einem spezifischen Netz und Systemen einer spezifischen Anlage. Dadurch ist die SecDER-Lösung unabhängig von spezieller proprietärer Technologie, spezifischer Netzwerkarchitektur oder -protokollen und abstrahiert von herstellerspezifischer Technik. Dennoch schafft es die Lösung nachweislich immer noch, Störungen zu finden.
Das Projekt SecDER wurde vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) mit insgesamt 2,7 Millionen Euro gefördert und vom Projektträger Jülich unterstützt. Das Projekt begann im April 2021 und dauerte 36 Monate. Beteiligt waren die Fraunhofer-Institute für Energiewirtschaft und Energiesystemtechnik (IEE) und SIT sowie die Hochschule Hannover, DECOIT, ENERTRAG und ANE. *(th)*

https://secder-project.de
https://www.sit.fraunhofer.de
https://www.iee.fraunhofer.de

Stichwörter: Informationstechnik, SecDER, Virtuelle Kraftwerke, Fraunhofer SIT, Fraunhofer IEE

Quelle: www.stadt-und-werk.de