Stromnetze unter Stress

Projekt CyberStress forscht für mehr Resilienz gegen IT-Angriffe

Dezentralisierung und Flexibilisierung der Energiesysteme sind zwei zentrale Konzepte der Energiewende. Damit einher geht ein erheblicher Bedarf an Automatisierungs- und Digitalisierungsmaßnahmen in den Verteilnetzen. Das bringt erhöhte Anforderungen an die IT-Sicherheit mit sich, da neue Schnittstellen und Zugangspunkte zum Netz entstehen, die geschützt werden müssen. Stromnetze gehören zur kritischen Infrastruktur und ein Versorgungsausfall kann weitreichende Folgen haben. Zur Stärkung der Versorgungssicherheit und des gesellschaftlichen Schutzes steht im Fokus des Projektes CyberStress deshalb die Entwicklung einer umfassenden Stresstestmethodik für Stromnetze.

Sicherheit im digitalen Raum ist vor allem für die kritische Infrastruktur unabdingbar. Die fortschreitende Digitalisierung und Dezentralisierung der Energiewende führen zu einer immer stärkeren Vernetzung von Stromnetzen und IT-Systemen. Damit vergrößert sich auch die Angriffsfläche für Cyberattacken auf kritische Infrastrukturen. Besonders die zunehmende Integration von Internet-of-Things-Geräten (IoT) wie Photovoltaikanlagen, Wallboxen oder Wärmepumpen stellt Netzbetreiber wie die e-netz Südhessen AG vor neue Herausforderungen. Angreifer könnten die Anlagen per Fernzugriff unter Kontrolle bringen, um beispielsweise falsche Steuerbefehle zu senden, Daten zu manipulieren oder ganze Anlagengruppen lahmzulegen. Manipulierte Messdaten oder eine gezielte Überlastung von Netzabschnitten könnten die Stabilität des Stromnetzes gefährden. Das durch das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) geförderte Projekt CyberStress entwickelt eine modellbasierte Stresstestmethodik, um die Resilienz der Stromnetze gegenüber Cyberangriffen systematisch zu bewerten und zu verbessern.

Ein zentrales Element ist dabei der Aufbau eines Realdemonstrators, der die Auswirkungen von Cyberangriffen unter realitätsnahen Bedingungen untersucht.

Projektüberblick und Zielsetzung

Im Projekt CyberStress arbeiten die Technische Universität Darmstadt und die e-netz Südhessen AG gemeinsam mit den Partnern Universität zu Köln (Lehrstuhl für das Recht der Digitalisierung) und QGroup GmbH an der Entwicklung und Erprobung eines Stresstests für Stromnetze. Die Bundesnetzagentur und die Amprion GmbH sind als assoziierte Partner ebenfalls involviert. Das Projekt startete im Mai 2023 und läuft bis Mitte 2026. Die Leitung des Projekts liegt bei der Technischen Universität Darmstadt. Deren Fachgebiet Energy Information Networks & Systems (EINS) entwickelt die grundlegende Methodik für den Stresstest und koordiniert die interdisziplinäre Zusammenarbeit im Konsortium. Die e-netz Südhessen bringt als Verteilnetzbetreiber umfassende Praxiserfahrung und reale Netzinfrastrukturen in das Projekt ein. Sie stellt einen geschützten Netzabschnitt als Testumgebung für den Realdemonstrator bereit und ermöglicht, dass die entwickelten Methoden und Maßnahmen anwendungsnah erprobt werden können.

Bild1. Bewertung der Anomalien

Ziel ist es, regulatorisch relevante Angriffsszenarien zu identifizieren, deren Auswirkungen zu simulieren und daraus konkrete Handlungsempfehlungen für Netzbetreiber und für die Regulierung abzuleiten.

Realdemonstrator

Der Realdemonstrator wurde in einer typischen Verteilnetzumgebung der e-netz Südhessen AG aufgebaut. Diese

Umgebung umfasst einen E-Auto-Ladepark mit einer Vielzahl von IoT-fähigen Verbrauchsanlagen. Da der Ladevorgang eines E-Autos aus der Ferne gestartet und beendet wird und bei Vehicle-to-Grid-Fähigkeit Strom aus dem Auto ins Netz eingespeist werden kann, könnte diese Fernsteuerbarkeit als Einfallstor für Cyberangriffe auf das Netz ausgenutzt werden.

Um Cyberangriffe auf das Netz durch IoT-fähige Anlagen zu erkennen, wurde in der verbundenen Ortsnetzstation (ONS) ein umfassender Netzanalysator installiert. Dieser misst und analysiert kontinuierlich den Leistungsfluss (Bild 1). Die Messdaten werden an einen lokalen Computer in der ONS weitergeleitet (Bild 2).

Angriffsszenario: IT-Angriff auf verteilte Geräte

Im Mittelpunkt des Demonstrators steht das Szenario eines koordinierten Cyberangriffs auf eine Vielzahl dezentraler, leistungsstarker IoT-Geräte. Angreifer könnten durch die Kompromittierung der Ladeinfrastruktur, aber beispielsweise auch per unberechtigtem Zugriff auf PV-Anlagen, Wallboxen oder Wärmepumpen eine synchrone Laständerung im Netz auslösen.

Solche Laständerungen können zu verschiedenen Schadwirkungen im Verteil- und Übertragungsnetz führen. Auf Verteilnetzebene können Spannungsbandverletzungen und ausgeprägte Oberwellen in einer schlechten Spannungsqualität resultieren. Diese kann wiederum nicht kompromittierte Anlagen negativ beeinflussen und ihre Abschaltung bewirken. Das würde die Schadwirkung des Angriffs verstärken. Im Realdemonstrator spielt die Verteilnetzebene eine zentrale Rolle, da die verteilten IoT-Geräte, über die der Angriff erfolgt, auf dieser Netzebene angeschlossen sind. Dadurch eignet sie sich besonders gut für die Entwicklung von Identifikations- und Gegenmaßnahmen.

CyberStress hat sich auch mit möglichen Auswirkungen auf das Übertragungsnetz beschäftigt. Hier wären Spannungsprobleme, überlastete Leitungen, eine destabilisierte Netzfrequenz und – im schlimmsten Fall – die Erschöpfung der Regelreserven mögliche Folgen einer solchen adversen Laständerung. Für die Versorgungssicherheit hätte das potenziell gravierende Konsequenzen.

Methodik und Umsetzung im Realdemonstrator

Die Umsetzung im Realdemonstrator erfolgt in mehreren Schritten:

- Begonnen wurde mit der Auswahl eines geeigneten Standorts für den Realdemonstrator.
- Basierend auf dem definierten Angriffsszenario wurde eine entsprechende Mess- und Analyseinfrastruktur (Netzanalysator und PC) ausgewählt, um die relevanten Parameter der verschiedenen Schadwirkungen messen zu können.
- Danach erfolgte die Erfassung der regulären Lastflüsse und die Entwicklung eines Anomalie-Erkennungsverfahrens zur Identifikation von Cyberangriffen.
- Daraus werden in der aktuellen Projektphase Gegenmaßnahmen abgeleitet sowie Tests verschiedener technischer und organisatorischer Maßnahmen erarbeitet, zum Beispiel gezielte Netztrennung und Nutzung der CLS-Schnittstelle zur anlagenspezifischen Fernabschaltung.

Besonders wichtig ist die enge Verzahnung von IT- und Netzbetrieb, um sowohl die technischen als auch die prozessualen Aspekte der Resilienz zu beleuchten. Die Durchführung von Versuchen am Realdemonstrator der Stresstests erfolgt in enger Abstimmung mit den Netzexperten der e-netz Südhessen. Sie übernehmen das Monitoring der Netzparameter, die Umsetzung der Gegenmaßnahmen im Betrieb und die Bewertung der Ergebnisse hinsichtlich der Versorgungssicherheit und der betrieblichen Abläufe.

Ergebnisse und Erkenntnisse

Die bisherigen Tests am Realdemonstrator zeigen, dass koordinierte Angriffe auf verteilte IoT-Geräte erhebliche Auswirkungen auf die Netzstabilität

haben könnten. Bereits eine kleine Anzahl synchron agierender Geräte kann kritische Schwellenwerte überschreiten lassen und die Regelreserven des Netzes stark belasten. Im nächsten Schritt werden verschiedene Gegenmaßnahmen bewertet. Noch tiefgehender geprüft werden soll die Eignung einer gezielten Identifikation von Cyberangriffen und die Abschaltung kompromittierter Anlagen über die Smart-Meter-Gateway-Infrastruktur, um die Auswirkungen eines Angriffs zu begrenzen.

Ein zentrales Ergebnis ist bereits jetzt die Erkenntnis, dass die Resilienz des Netzes nicht nur von der technischen Ausstattung, sondern auch von der organisatorischen Vorbereitung und der schnellen Reaktionsfähigkeit der Netzbetreiber abhängt.

Bild 2. Netzanalysator in der Ortsnetzstation

Ausblick

Die im Realdemonstrator gewonnenen Erkenntnisse sind auf andere Netzbetreiber übertragbar und bieten eine wichtige Grundlage für die Weiterentwicklung von Sicherheitsstandards und regulatorischen Vorgaben – auch für die Bundesnetzagentur. Die enge Zusammenarbeit zwischen Wissenschaft und Praxis hat sich als entscheidender Faktor erwiesen, um realistische und umsetzbare Lösungen zu entwickeln.

CyberStress strebt an, die entwickelten Methoden in die Praxis zu überführen und einen Beitrag zur Erhöhung der Cybersicherheit in der Energiewirtschaft zu leisten.

Bild 3. Edge Computing zur Anomalieerkennung in der Ortsnetzstation

Fazit

Der Realdemonstrator im Projekt CyberStress zeigt, wie sich die Resilienz von Stromnetzen gegenüber Cyberangriffen praxisnah testen und verbessern lässt. Die Kombination aus realen Netzkomponenten, moderner IT-Infrastruktur und enger Zusammenarbeit zwischen Forschung und Praxis ermöglicht es, sowohl technische als auch organisatorische Schwachstellen zu identifizieren und gezielt zu beheben. Die Projektergebnisse leisten einen wichtigen Beitrag zur sicheren Energieversorgung im Zeitalter digitalisierter Netze.

Danksagung

Das Projekt CyberStress wird durch das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) unter dem Kennzeichen 13N16628 gefördert. Wir danken allen beteiligten Kolleginnen und Kollegen der Projektpartner für die engagierte Zusammenarbeit.

>> **David Petermann**,
Leiter Forschung und Entwicklung,
e-netz Südhessen AG, Darmstadt

Karsten Hayn,
Leiter Netzinformationssysteme,
e-netz Südhessen AG, Darmstadt

Nicole Büchau,
Projektmanagerin Forschung und Entwicklung,
e-netz Südhessen AG, Darmstadt

Kirill Kuroptev,
Wissenschaftlicher Mitarbeiter,
Fachgebiet Energy Information Networks & Systems,
Technische Universität Darmstadt

Prof. Dr. **Florian Steinke**,
Leiter des Fachgebiets Energy Information Networks & Systems,
Technische Universität Darmstadt

>> david.petermann@e-netz-suedhessen.de
karsten.hayn@e-netz-suedhessen.de
nicole.buechau@e-netz-suedhessen.de
kirill.kuroptev@eins.tu-darmstadt.de
florian.steinke@eins.tu-darmstadt.de

>> www.e-netz-suedhessen.de
www.eins.tu-darmstadt.de