FORSCHUNGSPROJEKT

CyberStress – Modellbasierte Stresstests für cybersichere Energienetze

AUGSGANGSLAGE

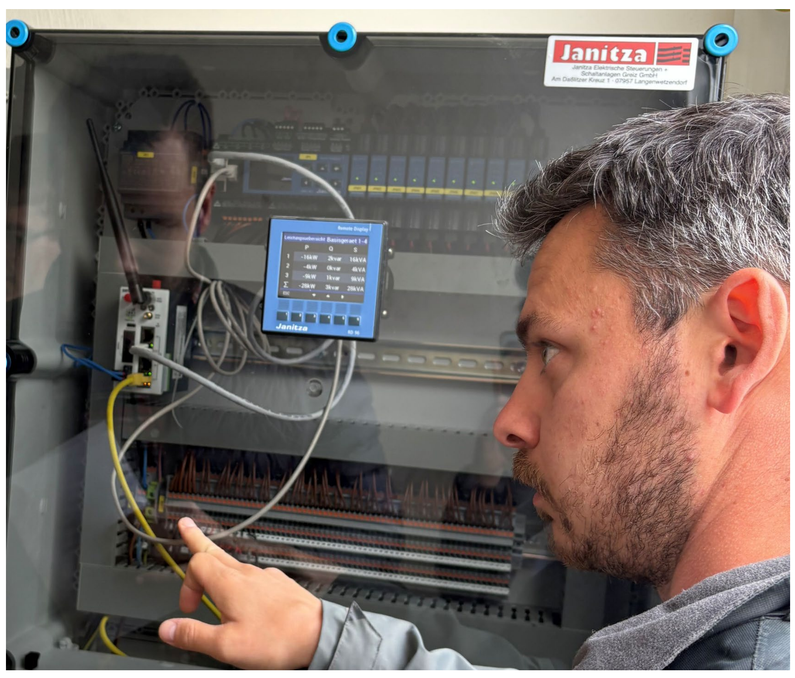
Die Energiewende bringt viele dezentrale, IoT-fähige Anlagen ins Stromnetz – etwa PV-Anlagen, Wärmepumpen und Ladeinfrastruktur. Dadurch wächst die Angriffsfläche für Cyberangriffe auf kritische Infrastrukturen deutlich. Die e-netz Südhessen betreibt bereits eine große Anzahl an dezentralen Erzeugungs-anlagen und steuerbaren Lasten, die zunehmend vernetzt und damit potenziell angreifbar sind.

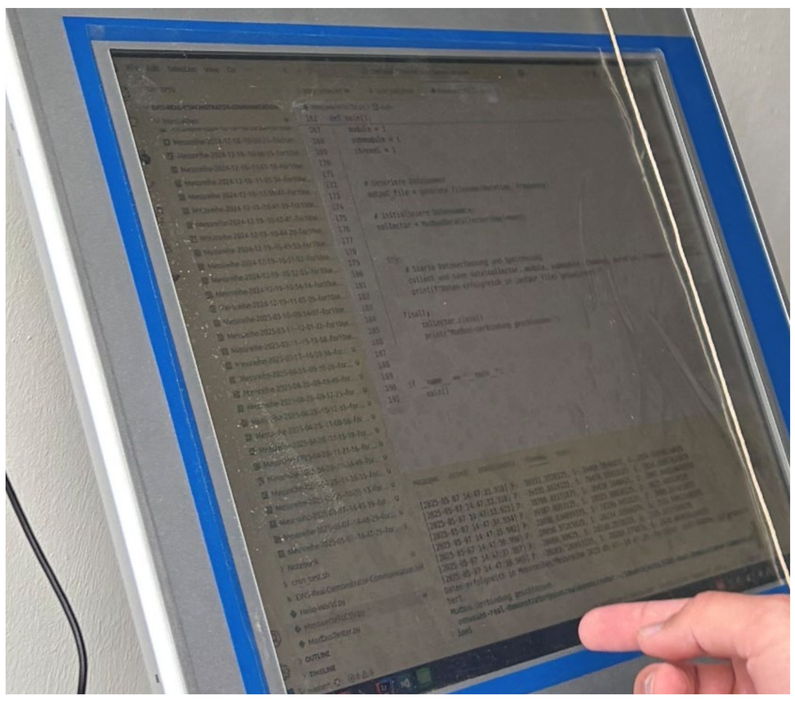
PROJEKTZIEL

Im Projekt wurde das Prinzip von Stresstests – bekannt aus dem Bankensektor – auf Stromnetze übertragen.

Im Fokus standen:

- Identifikation und Bewertung neuer Bedrohungen durch koordinierte Angriffe auf verteilte IoT-Geräte
- Aufbau eines Realdemonstrators in einem typischen Verteilnetz
- Konzeption eines dezentralen Edge-Frühwarnsystems zur Anomalieerkennung
- Konzeptentwicklung modellbasierter Stresstests





ERGEBNISSE

- Koordinierte Cyberangriffe über dezentrale, fernsteuerbare Anlagen sind realistisch und können kritische Netzzustände verursachen
- Intelligente Ortsnetzstationen mit Edge-Anomaliedetektion erkennen solche Angriffe früh und lokalisieren betroffene Bereiche
- Selektive Abschaltung, gezielte Netzschaltungen und Smart Meter Gateway/CLS-Einsatz begrenzen die Auswirkungen wirksam.

LEARNINGS & AUSBLICK

CyberStress zeigt: Cyberangriffe auf dezentrale IoT-Geräte sind realistisch, lassen sich aber durch intelligente Ortsnetzstationen, Anomaliedetektion und klare Melde- und Notfallprozesse beherrschbar machen. Die Ergebnisse sollten nun in den IT-Sicherheitskatalog, Netzbetriebsprozesse und den Ausbau intelligenter Ortsnetzstationen einfließen.

Gefördert vom

Bundesministerium für Forschung, Technologie und Raumfahrt

Förderkennzeichen 13N16628

VDI Technologiezentrum

PROJEKTPARTNER

TECHNISCHE UNIVERSITÄT DARMSTADT

UNIVERSITÄT ZU KÖLN

e·netz südhessen

QGROUP GMBH

amprion verbindet

Bundesnetzagentur