Defending the European Energy Infrastructures

DEFENDER befasst sich mit den neu auftretenden Herausforderungen bezüglich des proaktiven Schutzes und der schnellen Wiederherstellung bei physischen und Cyberangriffen - oder Kombinationen dieser - auf die Infrastruktur der Übertragungs- und Verteilnetze. Solche Herausforderungen liegen prinzipiell jeglicher kritischer Energie-Infrastruktur zugrunde.

STRATEGISCHE HERAUSFORDERUNGEN

DEFENDER schützt die existierende kritische Energie-Infrastruktur und entwirft eine neue Generation einer Europäischen Energieinfrastruktur, die eine höhere Widerstandsfähigkeit mit der Möglichkeit zur Selbstheilung aufweist. Diese Energieinfrastruktur ist fähig:

- Große, kombinierte cyber-physisch-soziale Angriffe und Störfälle zu verkraften
- Den fortlaufenden Betrieb zu gewährleisten, während Kaskadeneffekte auf die Infrastruktur, die Umwelt, die Bürger in der unmittelbaren Umgebung sowie die Endabnehmer der Energie minimiert werden.

VISION

DEFENDER wird eine Reihe von unterschiedlichen Technologien und operativen Entwürfen anpassen, einbinden, hochskalieren, realisieren und validieren. Das Ziel ist es, einen neuen Ansatz zum Schutz des Betriebs der bestehenden und zukünftigen europäischen kritischen Energie-Infrastrukturen vor cyber-physisch-sozialen Bedrohungen zu entwickeln, basierend auf:

- Neuartigen Schutzkonzepte für die Lebenszyklusanalyse, Resilienz und Selbstheilung, wobei beim Design insbesondere der Aspekt der Sicherheit betrachtet wurde
- Fortschrittlichen Werkzeugen zur Verringerung der Auswirkung von Angriffen
- Sicherheitsvorkehrungen, bei denen vertrauliche Informationen zwischen geschulten Mitarbeitern und Freiwilligen ausgetauscht werden, den cyber-physischen Schutz ergänzen, während die Privatsphäre der beteiligten Bürger gewahrt bleibt.

PILOTANLAGE

Die Ergebnisse aus DEFENDER werden mittels des hochmodernen Laboremulators für kritische Energie-Infrastrukturen (RWTH, Deutschland) sowie der vier realen Pilotanlagen (Belgien, Italien und Slowenien) validiert. Dies dient der Auswertung, Validierung und Veranschaulichung, in welchem Ausmaß das DEFENDER Konzept eine effektive, ganzheitliche cyber-physische Sicherheit erlaubt. Die betrachteten kritischen Energie-Infrastrukturen bestehen dabei aus Kraftwerken, dem Übertragungsnetz, dem Verteilnetz und industriellen Prosumern.

HERANGEHENSWEISE

DEFENDER setzt zur Erreichung seiner Ziele vier Strategien um:

- ***Risikobeurteilung.*** Bereitstellung eines vollständigen Verständnisses der aktuellen Sicherheitslage für die Interessenvertreter kritischer Energie-Infrastrukturen. Außerdem wird eine kontinuierliche Bewertung sich entwickelnder Gefahren und Angriffs-möglichkeiten, ihrer Risiken und möglicher Gegenmaßnahmen ermöglicht.
- ***Schutzmaßnahmen.*** Entwicklung neuer, proaktiver Schutzmaßnahmen um Systemrisiken wie beispielsweise Angriffsmöglichkeiten und aufkommende Gefahren zu reduzieren.
- ***Bewältigung von Zwischenfällen.*** Bei einem möglichen Versagen der Schutz-maßnahmen minimieren Gegenmaßnahmen die Auswirkung des Zwischenfalls.
- ***Aufbau einer Sicherheitskultur.*** Interessenvertreter kritischer Energie-Infrastrukturen nutzen nachträgliche Analysen und forensische Methoden um aus Zwischenfällen zu lernen.

Projektkoordinator:

Dr. **Massimo Bertoncini** - Engineering

Weitere Informationen:

www.defender-project.eu

Kontakt:

info@defender-project.eu

Partner: