

SIDATE – Sichere Informationsnetze bei kleinen und mittleren Energieversorgern

Julian Dax, Daniel Hamburg, Sebastian Pape, Volkmar Pipek, Kai Rannenber, Christopher Schmitz, André Sekulla, Frank Terhaag

Forschungsprojekt:
SIDATE



Im Fokus des Forschungsprojekts SIDATE steht die technische Unterstützung kleiner und mittelgroßer Energieversorger bei der Selbsteinschätzung und Verbesserung ihrer IT-Sicherheit.

Motivation

Eine reibungslos und sicher funktionierende Energieinfrastruktur ist für fast alle Lebensbereiche der heutigen Gesellschaft grundlegend. Der Schutz dieser Infrastrukturen liegt dementsprechend im Interesse der Allgemeinheit. Um den Anforderungen an eine sichere und nachhaltige Energieversorgung im Rahmen der Energiewende gerecht zu werden, wird auch im Energiesektor immer mehr Informations- und Kommunikationstechnik (IKT) eingesetzt. Durch die Entwicklung neuer Ansätze zur Steigerung von Effektivität und Effizienz unterliegt diese ständigen Veränderungen. Die Abwehr von Angriffen auf diese Kritischen Infrastrukturen ist darum eine ständig wachsende Herausforderung. Die meist privatwirtschaftlichen Betreiber stehen dabei vor einer schwierigen Aufgabe: Sie müssen sowohl den Schutz als auch die Wirtschaftlichkeit ihrer Infrastrukturen sicherstellen. Speziell kleine Betreiber mit kleinen IKT-Abteilungen, die dann oft auch eher kleine IT-Sicherheitsabteilungen mit sich bringen, sind hier besonders herausgefordert. Ziel des Projektes ist es, hier Lösungsansätze aufzuzeigen.

Ziele und Vorgehen

Im Forschungsprojekt SIDATE werden Werkzeuge und Konzepte entwickelt, die eine bessere Einschätzung des vorhandenen Sicherheitsniveaus ermöglichen und damit gleichzeitig helfen, die Sicherheit der Infrastrukturen kleiner und mittlerer Betreiberfirmen zu verbessern. Dabei liegt ein besonderes Augenmerk auf der Praxis-tauglichkeit der Werkzeuge und Konzepte, die auch für Betreiber mit wirtschaftlichen, organisatorischen und personellen Besonderheiten anwendbar sein sollen. Erarbeitet werden unter anderem Metriken zur Erfassung des Sicherheitsniveaus, eine Beschreibungssprache zur Abbildung der grundlegenden Elemente und Abhängigkeiten der Infrastruktur sowie eine Wissensdatenbank und eine Kooperationsplattform zur Unterstützung organisationsinterner sowie überorganisationaler Kollaborations- und Austauschprozesse. Um eine möglichst

große Anwenderfreundlichkeit, auch für Anwender mit verschiedenen Anwendungs- und Kompetenzprofilen, zu erreichen, werden dabei verschiedene Stakeholder und speziell kleine und mittlere Betreiber sowie Hersteller von Fernwirkssystemen in den Prozess mit eingebunden.

Innovationen und Perspektiven

Neu an diesem Ansatz ist – neben der Fokussierung auf kleine und mittlere Unternehmen – dass Selbsteinschätzungen eine entscheidende Rolle spielen. Mit dem Werkzeugkasten sollen Betreiber deutlich schneller und zuverlässiger feststellen können, ob alle gesetzlichen Auflagen und Richtlinien zur Absicherung der kritischen Versorgungsinfrastrukturen erfüllt sind. Ob die Umsetzung auch effektiv und wirtschaftlich erfolgt, lässt sich mithilfe von Best- bzw. Good-Practice-Sammlungen beantworten.

Förderkennzeichen:

16KIS0239K, 16KIS0240 bis 16KIS0243

- Universität Siegen
- Goethe-Universität Frankfurt am Main
- TÜV Rheinland i-sec GmbH
- regio iT gesellschaft für informationstechnologie mbH
- Arbeitsgemeinschaft für sparsame Energie- und Wasserverwendung im VKU