SIEM-Sensor für Virtuelle Kraftwerke

Bachelor-/Masterarbeit

Kontakt: Prof. Dr.-Ing. G. Dartmann
Prof. Dr.-Ing. G. Ascheid

Motivation

Hintergrund

- Beitrag für den **nationalen IT-Gipfel**
- Projektgruppe M2M (Internet der Dinge) der AG2 im nationalen IT-Gipfel
- Umsetzung von Handlungsempfehlungen: Monitoringsystem für die M2M-Cybersicherheit (M2M-CERT)

Bundesministerium für Wirtschaft und Energie

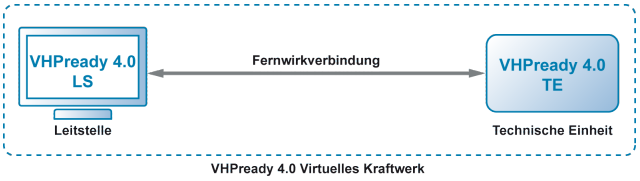
Anwendungsszenario

Regenerative Energieerzeugung verlangt die Entwicklung sogenannter virtueller Kraftwerke. Aufgrund der digitalen Vernetzung solcher Anlagen, gibt es vielfältige Möglichkeiten diese Anlagen zu attackieren. Cyberattacken können bei virtuellen Kraftwerken immense Schäden anrichten. Ein Monitoringsystem, das Meldungen auf freiwilliger Basis entgegennimmt und einer breiten Öffentlichkeit zur Verfügung stellt, hilft erkannte Schwachstellen zu beseitigen und das Sicherheitsniveau der virtuellen Kraftwerke insgesamt zu verbessern.

Vernetztes IT-System

Industriestandard für virtuelle Kraftwerke

- **VHPready**: Virtual Heat and Power Ready
  - Offener Industriestandard zur Steuerung von Anlagen und zur Energieerzeugung
  - Dezentrale Anlagen: notwendig bei regenerativen Energiequellen



VHPready 4.0 Virtuelles Kraftwerk

Sicherheit in Vernetzen Systemen

SIEM: Security Information & Event Management

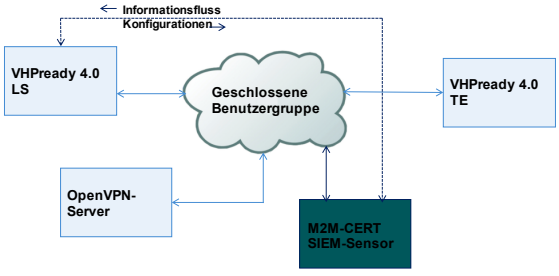
- Echtzeitanalyse von Sicherheitsalarmen in Netzwerken
- Langzeitspeicherung und Reporting von Log-Dateien
- Identity- und Zugangsmanagement

Fähigkeiten des Systems:

- **Data-Aggregation:** Log-Management sammelt Daten von vielen Quellen: Netzwerk, Server, Anwendungen…
- **Korrelation:** Sucht nach Verbindungen zwischen verschiedenen Ereignissen
- **Warnung:** Automatische Korrelationsauswertung und Warnung

Aufgabenstellung

Integration konfigurierbare SIEM-Sensoren



Anforderungen

Zielgruppe

- Studierende des Masters und Bachelors ET/IT mit guten Programmierkenntnissen

Kooperationspartner

- SSV Software Systems GmbH
- RWTH Aachen University

Prof. Dr.-Ing. Guido Dartmann
E-Mail: guido.dartmann@rwth-aachen.de
Raum: 401

Bundesministerium für Wirtschaft und Energie

RWTH AACHEN UNIVERSITY