secunet Security Networks AG

Projekt Sichere Informations- und Kommunikationstechnologien für ein intelligentes Energienetz

Salzburg, 14.05.2013

Steffen Heyde

Agenda

1. **Projektorganisation**
2. Projektziel
3. Projektinhalte

Konsortium

- Interdisziplinäre Zusammensetzung
  - Energiewirtschaft
  - Standardisierung
  - IT- bzw. IT-Sicherheits-Wirtschaft
  - Forschung
- Zusätzliche Einbindung eines wissenschaftlichen Beirats

Agenda

1. Projektorganisation
2. **Projektziel**
3. Projektinhalte

Ziel der Studie

- Erstellung einer Studie zur IT-Sicherheit im Smart Grid
- Ableitung sicherheitsrelevanter Anforderungen
- Analyse von potenziellen Bedrohungen und Bewertung von Risiken auf Basis einer abstrakten Referenzarchitektur und primären Use Cases

Agenda

1. Projektorganisation
2. Projektziel
3. **Projektinhalte**

Schwerpunkte der Studie

- Erfassung und Auswertung wesentlicher Aktivitäten / Normen / Studien
- Smart Grid Architektur (Strukturanalyse und Referenzarchitektur mit ausgewählten Use Cases)
- IT-Sicherheitsspezifische Betrachtung

Auswahlkriterien für die betrachteten Use Cases

- Abdeckung möglichst vieler Domänen im Bereich der Verteilnetze
  - Markt
  - Customer Premises Network
  - IT Service Providing
  - Leittechnik
  - Netzbetrieb
- Unterschiedliche adressierte Schutzziele
- Unterschiedliche Einordnung in Risikoklassen
- Abbildung von unterschiedlichen Arten von IT-sicherheitsspezifischen Anforderungen

Adressierte Schutzziele, z.B.

- Vertraulichkeit

  z.B. Abrechnungsdaten, Vertragsdaten, Messdaten (im Sinne Datenschutz)

- Integrität

  z.B. Abrechnungsdaten, Mess- und Steuerdaten

- Verfügbarkeit

  z.B. Ausfall Kommunikationsnetze, Systemkomponenten

IT-Sicherheitsspezifische Betrachtung

Grundlage: UseCase-Abbildungen

- Definition von allgemeinen Risikoklassen
- Bedrohungsanalyse für einzelne Angriffsziele
  - Beispiele: Angriff auf Verfügbarkeit, Manipulation von Daten / Dienste / Komponenten
- Risikobewertung
- Ableitung von sicherheitsspezifischen Anforderungen

360° Betrachtung IT-Sicherheitsanforderungen

- Sicherheitstechnologien
- Sichere Architektur und Prozesse
- Organisatorische Prozesse
- Notfallmanagement inkl. Schwarzstartfähigkeit
- Physikalische / Bauliche Sicherheit
- Vertrauenswürdiges und fachkundiges Personal
- IT-Sicherheits-Awareness: Aufklärung / Beratung
- Test, Auditierung und Zertifizierung
- Übergreifende IT-Sicherheitsanforderungen

- Sicherer Betrieb und stetige Neubewertung von Risiken und Maßnahmen, Restrisiken

- techn. Normungsbedarf bzw. Normenüberarbeitungsbedarf

Vielen Dank!

secunet Security Networks AG

Steffen Heyde
Telefon +49 201 5454-2025
steffen.heyde@secunet.com