Petra Beenken

**Schutz sicherheitsrelevanter Informationen**

**in verteilten Energieinformationssystemen**

Im Bereich der Energiewirtschaft vollzieht sich durch die im EnWG geforderte Liberlisierung seit einigen Jahren ein struktureller Wandel, der u.a. eine strikte Trennung bzw. Entflechtung von Aufgabenbereichen wie Transport, Lieferung und Umwandlung von Energie vorsieht. Neue Herausforderungen für die Energiewirtschaft bestehen ferner durch Klima - und Umweltschutz sowie Kostentransparenz und Energieeinsparungen bei gleichzeitiger Ressourcenschonung. Die Vision des Smart Grid und der damit verbundene Aufbau eines intelligenten Energienetzes soll helfen, diese Ziele zu erreichen, indem verstärkt regenerative Energien eingebunden, Einsparungen bei fossilen Energieträgern gemacht und eine höhere Energieeffizienz erreicht werden. Die hierfür notwendige Koordination benötigt Informationen über Energieerzeugungsanlagen, -speicher und -verbraucher. Durch Vernetzung und schnellen Informationsaustausch mit Hilfe eines intelligenten Energienetzes kann eine effiziente Energienutzung erreicht werden. Die verstärkte informatorische Vernetzung durch intelligente Energienetze kann aber auch zu Schwachstellen i.S.d. Informationssicherheit für die Energiewirtschaft führen. Die erhöhte Anzahl an Beteiligten sowie an Datenübertragungen wird eine größere Angriffsfläche bieten als bisher, daher ist ein angemessener Schutz des intelligenten Energienetzes wichtig. Insbesondere durch den §9 EnWG genießt das Schutzziel der Vertraulichkeit besondere Bedeutung. Eine Realisierung dieses Schutzziels darf aber nicht auf Kosten der Verfügbarkeitsanforderungen gehen, die in vielen Bereichen der Energiewirtschaft existieren. Neben der Feststellung solcher Seiteneffekte ist auch die Etablierung der Vertraulichkeit im Hinblick auf verteilte, dezentrale Systeme eine Herausforderung. Das ENERTRUST-Sicherheitsmodell sieht den Aufbau einer Wissensbasis vor, anhand derer über ontologiebasiertes Inferieren Konflikte bzw. Seiteneffekte von Schutzmaßnahmen für die Domäne der Energiewirtschaft erkannt werden können. Des Weiteren ermöglicht ENERTRUST die Etablierung eines Vertraulichkeitsschutzes von dezentralen Positionen aus durch den Einsatz und die Kombination von Kryptosystemen und ein zugehöriges separates und dezentral verwaltetes Schlüsselmanagement. Durch den Einsatz dieses Sicherheitsmodells können Datenbesitzer sicherheitsrelevante Daten und deren Schutzbedarf über eine Inferenzierung identifizieren und eine angemessene, d.h. konfliktfreie Schutzmaßnahme in Form eines Kryptosystems spezifizieren. Dabei werden auch mögliche Authentifikationsverfahren zur sicheren Schlüsselübertragung vom Modell betrachtet und es besteht die Möglichkeit, die Notwendigkeit eines Zugriffs auf Energiedaten durch Subjekte mit Hilfe von definierten Geschäftsprozessen festzustellen.