BEDEUTUNG DES RISIKOMANAGEMENTS FÜR DIE SICHERHEIT VON SMART GRIDS

Johannes GÖLLNER[1], Christian MEURERS[1], Andreas PEER[1]

Lucie LANGER[2]

Markus KAMMERSTETTER[3]

Einleitung

Die Energieversorgung der Zukunft wird sich fundamental auf den Einsatz von IKT-Systemen stützen. Die damit verbundenen Risiken wirken sich unmittelbar auf die Sicherheit der Energieversorgung aus und stellen neue Bedrohungsbilder in diesem Bereich dar. Im Rahmen des KIRAS-Sicherheitsforschungsprogramms beschäftigt sich das Projekt *Smart Grid Security Guidance (SG)²*, basierend auf einer fundierten Bedrohungs- und Risikoanalyse aus einer gesamtstaatlichen Sicht sowie auf Sicherheitsanalysen von Smart-Grid-Komponenten, mit einer systematischen Untersuchung von Smart-Grid-Technologien in Bezug auf IKT-Aspekte und der Erforschung von entsprechenden Gegenmaßnahmen zur Erhöhung der Sicherheit von IKT-Systemen in der kritischen Infrastruktur „Energie".

Existierende Ansätze

Als Basis für die Bedrohungs- und Risikoanalyse dienen zunächst State-of-the-Art-Risikomodelle wie die BSI-Standards und IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik, die in den Bereichen der Informationstechnik und Risikoanalyse bereits ein weites Spektrum an Gefährdungen abdecken. Weiters werden Ergebnisse und Ansätze aus bereits durchgeführten Forschungsprojekten, wie beispielsweise das Doppelvektorenmodell [1], berücksichtigt. Dieses wurde im Rahmen des BMLVS-internen Forschungsprojektes „Szenarioplanung und Wissensmanagement im ÖBH" in mehreren Anwendungsfällen erarbeitet, weiterentwickelt sowie getestet und stellt die Möglichkeit dar, ereignisrelevanten Inhalt zu dokumentieren und für weitere Analysen abrufbar zur Verfügung zu stellen. Die Kategorisierung basiert auf der Unterscheidung eines Ereignisses hinsichtlich:

- der Organisation,
- des Verursachers sowie
- der Art des Ereignisses.

Weiters erfolgt die Kategorisierung bezüglich:

- des Zeitrahmens,
- der räumlichen Ausdehnung/Einflussnahme sowie
- des erforderlichen Abstraktionslevels.

Dadurch lässt sich grundsätzlich jedes Ereignis entsprechend kategorisieren und dokumentieren. In Verbindung mit diversen Akteuren und Wissensrollen lassen sich daraus Zusammenhänge und Wechselwirkungen erkennen und ableiten. Ein zusätzlicher Mehrwert ergeht auch aus der Möglichkeit, Muster von Ereignissen in den diversen Kategorien zu erkennen. Dies dient nicht nur Analysten, sondern kann auch für die Beurteilung von zusätzlich erforderlichem Informationsbedarf zweckmäßig sein.

Der (SG)²-Risikokatalog

Im Rahmen des Projekts wurde ein Risikokatalog für Smart Grids in Österreich entwickelt, welcher Energieversorgungsunternehmen dabei unterstützen soll, eine Risikoanalyse für ihr System durchzuführen. Ausgehend von der durch CEN-CENELEC-ETSI entwickelten Referenzarchitektur (*Smart Grid Architecture Model*) [2] wurde zunächst ein IKT-Architekturmodell für österreichische

[1] Landesverteidigungsakademie Wien des Bundesministeriums für Landesverteidigung und Sport, Roßauer Lände 1, 1090 Wien
[2] AIT Austrian Institute of Technology GmbH, Donau-City-Straße 1, 1220 Wien
[3] Technische Universität Wien, Institute of Computer Aided Automation, Treitlstraße 1-3, 1040 Wien

Smart Grids definiert, welches als Grundlage für den Risikokatalog diente. Dazu wurden die im Architekturmodell dargestellten Komponenten und Kommunikationsverbindungen zu Domänen (z.B. Netzbetrieb, Metering, Erzeugungsanlagen) gebündelt. Anschließend wurden, ausgehend von den IT-Grundschutz-Bedrohungskatalogen [3] sowie ergänzenden Dokumenten wie z.B. den einschlägigen BSI-Schutzprofilen [4,5], relevante Bedrohungen identifiziert. Auf diese Weise entstand eine Liste von etwa 250 Bedrohungen, die jedoch zum Teil unterschiedliche Detaillierungsgrade aufwiesen.

Um eine konsistente Darstellung zu erreichen, wurden diese Bedrohungen in weiteren Iterationen teils zusammengefasst und auf den Smart-Grid-spezifischen Kontext zugeschnitten. So entstand letztendlich ein Katalog von 31 Bedrohungen, welche verschiedenen Kategorien zugeordnet wurden. Diese Bedrohungen wurden anschließend im Rahmen des vorhandenen IKT-Architekturmodells evaluiert, d.h. es wurde untersucht, inwieweit die Bedrohungen auf die einzelnen Domänen zutreffen. Anschließend wurde das Risikopotential dieser Bedrohungen bewertet, indem die Eintrittswahrscheinlichkeit und die Auswirkungen eines erfolgreichen Angriffs geschätzt wurden. Die Einschätzung erfolgte jeweils auf einer Skala von 1 (sehr gering) bis 5 (sehr hoch). Durch Multiplikation der beiden Werte ergibt sich das zu der jeweiligen Gefährdung gehörige Risikopotential. Das Ergebnis, der $(SG)^2$-Risikokatalog, zeigt in einer Matrix-Darstellung die für die Architekturkomponenten relevanten Risiken, und kann von Energieversorgern als Hilfestellung genutzt werden, um eine konkrete Risikoanalyse des bei ihnen implementierten Systems durchzuführen.

Auswertung & Ausblick

Vor allem durch die fortschreitende Transformation bestehender Energienetze zu Smart Grids und der damit verbundenen massiven Integration von Informations- und Kommunikationstechnologien (IKT) stehen Netzbetreiber heute vor der Herausforderung, die dadurch entstehenden Risiken adäquat zu bewerten. Erst durch die Risikobewertung können kritische Bereiche identifiziert und in weiterer Folge besser geschützt werden. Diese Risikobewertung kann allerdings nur mittels Detailbetrachtung der bei den Netzbetreibern umgesetzten Systemlandschaft erfolgen. Eine auf die Gesamtarchitektur bezogene Risikobewertung fehlt jedoch häufig. Viele Netzbetreiber stehen daher heute vor dem Problem, zum einen auf keine geeigneten Risikomanagement-Methoden im Smart-Grid-Bereich zurückgreifen zu können, und zum anderen Risiken in der Smart Grid Gesamtarchitektur nicht erfassen zu können.

Im Gegensatz zu den im EURACOM FP7 Projekt analysierten bestehenden Methoden [6], verfolgt der im Projekt entstandene Risikokatalog einen durch die Gesamtarchitektur getriebenen Ansatz. Durch die architekturelle Bewertung in Bezug auf Risikopotential und Eintrittswahrscheinlichkeit erfolgt für die Netzbetreiber eine innerhalb des Smart Grids architekturbezogene Vorauswahl der bestehenden Risiken. Durch Kombination der Gesamtarchitektur-Risikobewertung mit der detailbezogenen individuellen Risikobewertung ermöglicht die Anwendung des $(SG)^2$ Risikokatalogs einen gesamtheitlichen Ansatz.

Referenzen

[1] Göllner, Meurers, Peer, Povoden, paper-presentation: „Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria", -accepted paper at the 7th Social Network Conference 07/2011, University of Greenwich, London, accepted: 13.05.2011 by Programme Committee und nach: Göllner, Vorlesungspräsentation an der Donau Universität Krems iRd LVA Risikomanagement des ULG Risk Management, 2009

[2] CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture, Document for the M/490 Mandate, Version 3.0, 2012

[3] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standards 100-1 bis 100-4, 2008, aktuelle Version erhältlich unter https://www.bsi.bund.de/

[4] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0073), Version 1.2, 2013

[5] Bundesamt für Sicherheit in der Informationstechnik: Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (BSI-CC-PP-0077), Version 1.0, 2013

[6] FP7 project EURACOM, URL: http://www.eos-eu.com/?Page=euracom