2009

STRATEGIEN ZUR SICHEREN BEREITSTELLUNG VON ENERGIEDATEN UND ZUM NACHWEIS VON INFORMATIONSWEITERGABEN GEMÄSS §9 ENWG

Petra Beenken
OFFIS

Sven Abels
Abelssoft

STRATEGIEN ZUR SICHEREN BEREITSTELLUNG VON ENERGIEDATEN UND ZUM NACHWEIS VON INFORMATIONSWEITERGABEN GEMÄSS §9 ENWG

Petra Beenken[1], Sven Abels[2]

Kurzfassung
Auflagen für die Informationsinfrastruktur von Energieversorgern durch das Energiewirtschaftsgesetz beeinflussen unternehmensinterne Prozesse und verlangen ein angemessenes Sicherheitsmanagement für Energiedaten. Im Bereich der Prozessleittechnik darf eine Ausweitung von Konzepten zur Vertraulichkeit jedoch nicht auf Kosten der Verfügbarkeit hinauslaufen, da hier teilweise hohe Echtzeitanforderungen beim Datentransfer bestehen. In diesem Beitrag wird eine Konzeption der sicheren Bereitstellung und Informationsweitergabe für die Energiedomäne skizziert, die den Echtzeitanforderungen in Zusammenhang mit hohem Schutzbedarf begegnet.

1. Einleitung

IT-Sicherheit im Energiedatenmanagement steht durch die Liberalisierung und aufgrund von domänenspezifischen Schutzzielen speziellen Herausforderungen gegenüber. Diese werden in diesem Beitrag beschrieben. Ferner wird kurz auf das Umfeld und verwandte Arbeiten eingegangen. Im Anschluss daran folgt die Beschreibung eines Sicherheitsmanagements, das den speziellen Herausforderungen begegnet. Das Konzept bezieht sich dabei auf die gesetzlichen Richtlinien der Europäischen Union und insbesondere der deutschen Gesetzeslage. Nach der Beschreibung eines Ansatzes für zeitkritische Sicherheitsprüfungen folgen ein Fazit sowie ein Ausblick.

2. Herausforderungen durch die Liberalisierung des Strommarktes

Die Liberalisierung in der Energiebranche durch die Elektrizitätsrichtlinie 1997 und das Energiewirtschaftsgesetz 1998 führte zur ersten Entflechtung der Netzbetreiber, sog. Unbundling. Somit ist es verschiedenen Energieerzeugern möglich, Energie in das Gesamtnetz einzuspeisen und zum Verkauf anzubieten.

Neben einer Energieinfrastruktur ist auch eine Informationsinfrastruktur bzw. ein Informationssystem notwendig, um zu erkennen, wer wie viel Energie einspeist respektive entnimmt. Durch das Unbundling steigt tendenziell die Anzahl der Beteiligten am Strommarkt, so dass es mehr Daten und mehr Zugreifende auf die Daten im Energiemanagementbereich gibt [16].

[1] OFFIS, Escherweg 2, 26121 Oldenburg
[2] Abelssoft GmbH, Langeooger Str. 2, 27755 Delmenhorst

Nach §9 EnWG (1) „[..] haben vertikal integrierte Energieversorgungsunternehmen und Netzbetreiber sicherzustellen, dass die Vertraulichkeit wirtschaftlich sensibler Informationen, von denen sie in Ausübung ihrer Geschäftstätigkeit als Netzbetreiber Kenntnis erlangen, gewahrt wird“. Im Rahmen dessen ist eine nachvollziehbare Dokumentation des Informationsflusses zu erstellen.

In einem liberalisierten Energiemarkt gibt es viele unterschiedliche Akteure. Um Sicherheit in einem dezentralen Netz zu gewährleisten sind Interoperabilität und IT-Standards notwendige Bestandteile. Zum Einen muss ein angemessenes, einheitliches Sicherheitsniveau für alle Beteiligten im Energiemarkt geschaffen werden, um den sicheren Austausch von Informationen zu ermöglichen; zum Anderen muss ein einheitliches Sicherheitskonzept mit bestehenden Lösungen kombiniert werden können.

3. Anforderungen zur Datenbereitstellung für Prozessleitsysteme

Prozessleitsysteme dienen der Kontrolle und Regelung von Energiesystemen. Die Ansteuerung der Energieerzeugung wird beispielsweise durch so ein System geregelt [15]. Zunehmend wird in der Leittechnik Standard-IT wie in einem kaufmännischen Netzwerk eingesetzt, um Kosten zu senken und Interoperabilität zu anderen Systemen zu schaffen.

Alle Technologien der Standard-IT lassen sich für Leitsysteme nicht problemlos übernehmen. So ist der Einsatz gängiger Sicherheitsstrategien respektive Technologien aufgrund der Echtzeitanforderungen in Leitsystemen nur eingeschränkt anwendbar. Kontinuierliches Patch-Management ist bei kaufmännischen Servern problemlos möglich, indem diese Server über Nacht zwecks Aktualisierung vom Netz genommen werden. Bei Systemen der Leittechnik ist es nicht möglich Server über Nacht vom Netz zu nehmen, da sie i. d. R. durchgängig laufen müssen. Aktualisierungen sind nur bei redundant ausgelegten Systemen möglich, indem Patches auf Spiegelungen installiert werden. Nach einer Testphase kann die Leittechnik auf das Spiegelsystem umgeschaltet werden. Das Nicht-Einspielen oder nicht rechtzeitiges Einspielen von Patches hat einige Schadensfälle in der Vergangenheit nach sich gezogen [9,10,12].

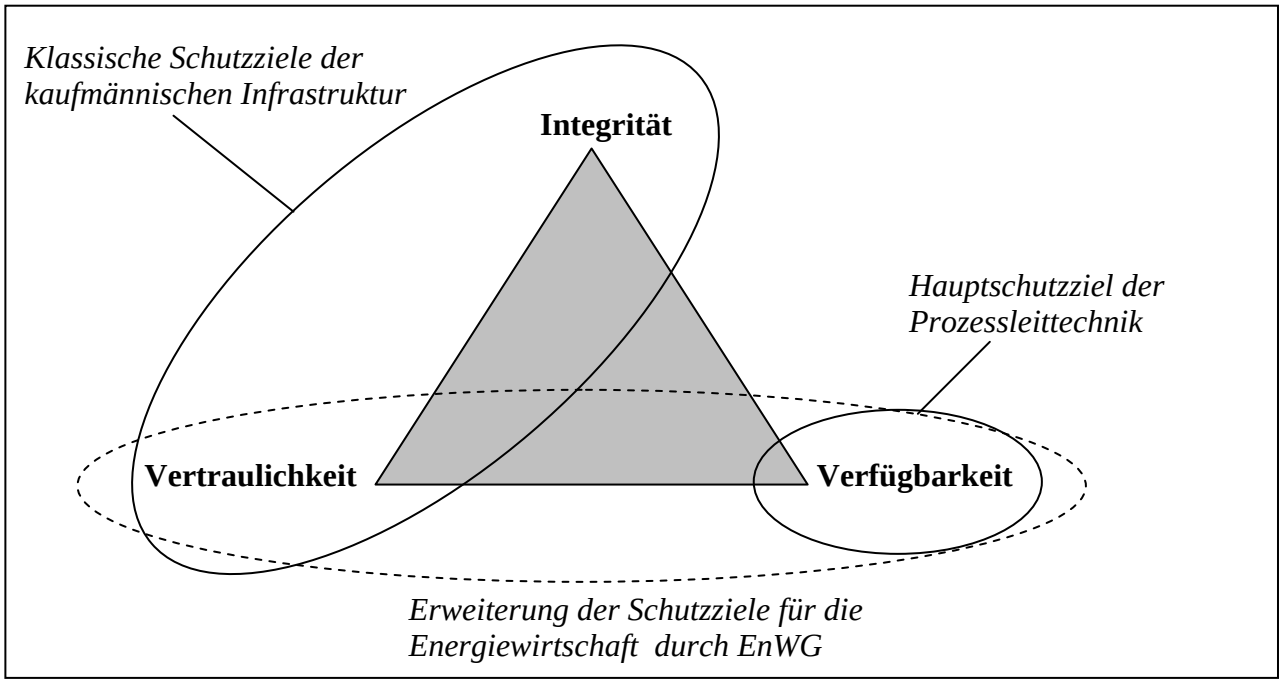

Abbildung 1 Schutzzieledreieck

Auch die Verschlüsselung sämtlicher Daten ist in der Leittechnik teilweise schwer anwendbar, da die eingesetzten, eingebetteten Systeme nicht immer über ausreichend Prozessorkapazität verfügen, um die Entschlüsselung in der erforderlichen Zeit durchzuführen. Die Datenbereitstellung in Prozessleitsystemen unterliegt somit oft hohen Anforderungen an das Schutzziel Verfügbarkeit.

Abbildung 1 skizziert die Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit in einem Dreieck [3]. Alle drei Schutzziele sind sowohl für das kaufmännische als auch für das Leittechnik-Netzwerk wichtig, es existiert jedoch eine unterschiedliche Priorisierung. Wie beschrieben existieren in der Leittechnik oft hohe Echtzeitanforderungen. Das wichtigste Schutzziel in der Leittechnik ist somit die Verfügbarkeit. Im kaufmännischen Netzwerk sind die Schutzziele gegenüber dem Leittechnik-Netzwerk umgekehrt priorisiert [5]. Das Schutzziel der Verfügbarkeit liegt dort hinter den Schutzzielen der Vertraulichkeit und Integrität. Durch den §9EnWG gewinnt das Schutzziel Vertraulichkeit für die Energiewirtschaft an Gewichtung.

4. Umfeld und verwandte Ansätze

Der Austausch von Informationen ist nicht einheitlich geregelt und wird i. d. R. bilateral festgesetzt [2, 3]. Der Bundesverband der Energie- und Wasserwirtschaft e.V (BDEW) empfiehlt zum Austausch das EDIFACT-Format. Ein Datenaustausch zwischen zwei Parteien ist bspw. notwendig, wenn ein Anschlussnehmer seinen Messstellenbetreiber wechselt. In diesem Fall liegen sogar personenbezogene Daten vor. Bei personenbezogenen Daten kann in Deutschland Bundesdatenschutzgesetz Anwendung finden. Dann sind beim Datenaustausch insbesondere die technisch-organisatorischen Maßnahmen nach §9 BDSG zu beachten.

Aktuelle Ansätze zum sicheren Datenaustausch setzen auf vor allem auf Technologie-orientierte Schutzmaßnahmen. So ist der Einsatz von Firewall-Systemen bspw. eine Selbstverständlichkeit. Die Projekte SELMA[3] und VEDIS[4] befassen sich mit der Sicherheit von Datenaustausch im Energiedatenmanagement. Beide empfehlen den Einsatz von Kryptologie zum sicheren Datenaustausch. So kann durch asymmetrische Verschlüsselung respektive digitale Signaturen die Echtheit der Daten und die Authentizität der Beteiligten festgestellt werden. Der Einsatz von so genannten qualifizierten Signaturen erfordert bei Signaturerstellung ein gültiges und qualifiziertes Zertifikat wie das X.509-Zertifikat. Zudem muss die Signatur mit einer sicheren Signaturerstellungseinheit gem. §§17 und 23 SigG erzeugt werden. Hier hilft der Aufbau einer Public-Key-Infrastruktur (PKI).

Digitales Rechtemanagement wurde entwickelt um urheberrechtlich geschützte Daten, vor allem Audio- oder Videodaten, vor einer nicht autorisierten respektive nicht erlaubten Nutzung zu schützen [3]. Im Gegensatz zum Data Leakage Prevention verhindert Digital Rights Management nicht den Abfluss von Daten, lediglich die unautorisierte Nutzung.

5. Energiedatenmanagement mit dem Enertrust-Ansatz

Im Gegensatz zu bisherigen Ansätzen konzentriert sich der hier vorgestellte Ansatz nicht auf rein technologieorientierte Schutzmaßnahmen. Der Faktor Mensch wird durch in Schutzprofilen definierten Sicherheitsrichtlinien mit berücksichtigt. Zudem setzt der Ansatz einen Fokus auf Objekt- statt Subjekt-Gebundenheit.

---

3 http://www.selma-project.de/

4 http://www.vdew.net/bdew.nsf/id/3DDD6E8DCA1B22EDC125728E004AE896/$file/Energie_Info_Studie_SichererGesch%C3%A4ftsverkehr.pdf

Anwendungstypen sind in diesem Zusammenhang Subjekte, d.h. Personen oder Prozesse, die auf Objekte zugreifen. Dateitypen sind passive Objekte, also Daten oder Inhalte, die von Anwendungstypen genutzt werden. Kommunikationstypen stellen das Bindeglied zwischen Subjekten und Objekten dar. Sie definieren die Art des Datentransports.

5.1 Schutzprofile

Schutzprofile sind Informationen zum Schutzbedarf von Objekten. Der Begriff stammt ursprünglich aus den Common Criteria [6]. Im Rahmen dieses Ansatzes sind Schutzprofile spezielle Metadaten, die an ausgewählten Energiedaten gelinkt bzw. ihnen umgeben werden wie in Abbildung 2 angedeutet. Schutzprofile setzen Angemessenheit von Sicherheitsinformationen um. Für sicherheitsrelevante Energiedaten wird ein Schutzprofil definiert, das den Schutzbedarf im Rahmen einer Sicherheitsrichtlinie darlegt. Was mit einem Objekt getan werden darf und was nicht wird somit im Schutzprofil definiert. Die Verlinkung zum Objekt gleicht einem traditionellen Objektschutz und nimmt Abstand von Subjekt-zentrierten Ansätzen wie der rollenbasierten Zugriffskontrolle. Schutzprofile stellen die Wissensbasis für eine nachfolgende Sicherheitsprüfung dar.

Auf Basis von Referenzmodell und Normen ist bereits ein ontologiebasiertes Energiedatenmodell vorhanden und wird in [14] detailliert beschrieben. Auch im Bereich der Sicherheitskonzepte existieren Ontologien, die Sicherheitsmaßnahmen beschreiben, wie in [7,13] aufgezeigt. An diese Arbeiten wird angeknüpft indem Schutzprofilmodelle ebenfalls in Form einer Ontologie beschrieben werden. Die Integration respektive Vernetzung von Daten und Prozessen mit zugehörigen Schutzprofilen erfolgt durch die Vernetzung zweier existierender Ontologien, nämlich des ontologiebasierten Energiedatenmodells und der Sicherheitskonzepte. Eine Erweiterbarkeit für unternehmensspezifische Konzepte wird dabei sichergestellt, da sich die gewählten Ontologien jederzeit um weitere Konzepte und Relationen erweitern lassen (Open World Assumption). Zur Modellierung der Verknüpfung von Energiedaten- und Sicherheits-Ontologien können Frameworks wie FOAM der Universität Karlsruhe eingesetzt werden [4].

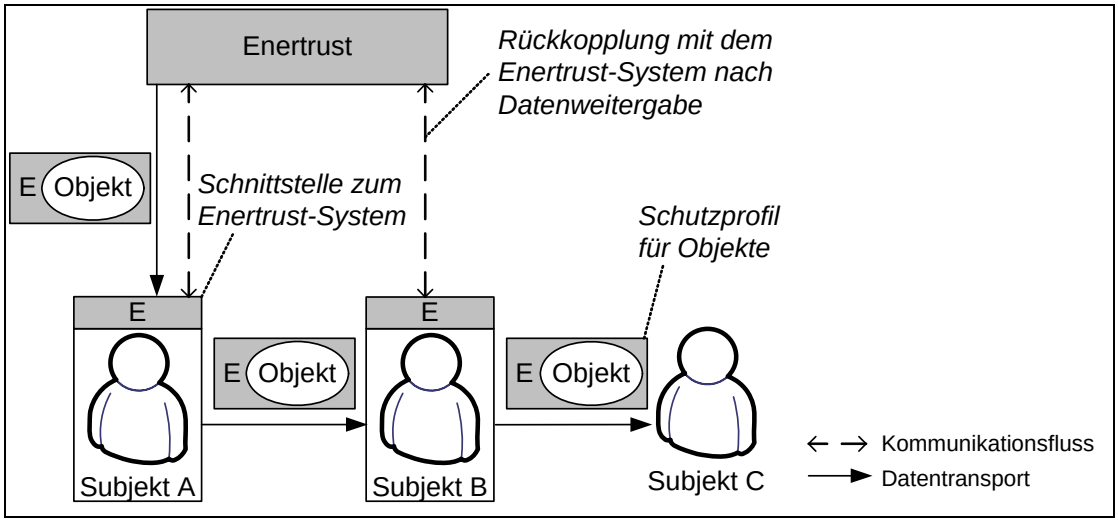

Abbildung 2 Sicherheitsstrategien für die Datenweitergabe

5.2 Semiautomatisierte Sicherheitsprüfung

Mit einem Katalog an definierten Schutzprofilen als Grundlage kann eine Sicherheitsprüfung semiautomatisch erfolgen. Die Einhaltung der Schutzprofile wird in den jeweiligen Prozessen beobachtet und kontrolliert. Verbotene Aktionen werden dabei soweit möglich unterbunden. Dies kann bspw. eine Unterbindung der Veränderung des Energiedatums sein. Falls eine Aktion zwar verbo-

ten ist, aber nicht verhindert werden kann, so wird ein Alarm mit einem entsprechenden Hinweis gegeben. Dies könnte bspw. ein unerlaubter Kopiervorgang sein. In diesem Fall greift bei versiertem IT-Personal eine automatische Sicherheitsprüfung oft nicht, daher wird hier ein semiautomatisierter Ansatz verfolgt.

Die semiautomatische Sicherheitsprüfung kann in einem zentralen System bspw. innerhalb eines Unternehmens erfolgen. Dann erfolgt die Prüfung direkt in einem Netzwerk. Zudem besteht die Möglichkeit die semiautomatische Prüfung in dezentralen Systemen durchzuführen.

5.2.1 Schnittstelle zum Enertrust-System

Zur Prüfung in dezentralen Systemen sieht dieser Ansatz eine Schnittstelle für interessierte Subjekte vor. Die Subjekte, die auf die Objekte geschützt durch das Enertrust-System zugreifen möchten, können eine Enertrust-Schnittstelle nutzen. In Abbildung 2 nutzen die Subjekte A und B eine solche Schnittstelle „E“. Damit erkennen Sie die definierten Schutzprofile an.

5.2.2 Datenbesitzer

Die Schutzprofile werden in einem solchen dezentralen System in der Regel vom Datenbesitzer definiert. Ist Subjekt A Datenbesitzer der Daten a sowie Subjekt B Datenbesitzer von b und nutzen beide das Enertrust-System, so können sie sich sicher sein, dass ihre Schutzprofile für a und b untereinander Geltung haben. Somit ist ein wechselseitiger Austausch von Informationen unter vielen Beteiligten möglich, die den Sicherheitsvorgaben des jeweiligen Datenbesitzers entsprechen. Auf diese Weise wird ein übergreifender Schutz der Energiedaten angemessen realisiert. Da in die Schutzprofile aktuelle IT-Standards aus dem Energiebereich einfließen, wird somit auch ein einheitlicher Sicherheitsstandard der Energiedaten unterstützt.

5.2.3 Rückkopplung

Vor der Einsicht von Energiedaten wird vom Enertrust-System das definierte Schutzprofil eines Energiedatums, falls vorhanden, überprüft. Dabei werden Anwendungs-, Datei- und Kommunikationstyp überprüft. Bei der semiautomatisierten Sicherheitsprüfung wird somit überwacht wer welche Information auf welchem Wege abholen möchte. Ferner werden die im Rahmen der Schutzprofile gestatten Aktionen überprüft. Über die Schnittstelle erfolgt die Rückkopplung zum Enertrust-System.

5.2.4 Prüfung nach Datenweitergabe

Die Energiedaten werden in der Form abgegeben, so dass sie nach einer Datenweitergabe überprüft werden können. Dies kann beispielsweise dadurch realisiert werden, dass die Anwendungstypen für die abgegebenen Objekte durch ein entsprechendes Plugin erweitert werden, so dass vor Aktivierung respektive Öffnung durch die Anwendung die Schutzprofile überprüft werden können. Auf diese Weise kann der Schutz auch nach einem transitiven Informationsfluss gewährleistet werden. Beziehen die Subjekte A und B Objekte vom System, kann es bei sehr großen Daten der Fall sein, dass sie die Daten untereinander austauschen möchten (transitiver Informationsfluss). Wenn die Daten nicht zentral über einen Server bezogen werden, sondern ein wechselseitiger Austausch von Daten und den Subjekten erfolgt, ist es schwer den Überblick „wer welche Daten hat“ zu behalten.

Je mehr Beteiligte an den Daten interessiert sind und die Daten untereinander wechselseitig austauschen, desto komplexer ist die Datenweitergabe zu überblicken. In einem gängigen Client-Server-System ist eine Überwachung nach Datenweitergabe in der Regel nicht vorgesehen. Durch die

Schnittstelle zum Prüfungssystem ist eine solche Kontrolle auch nach Datenweitergabe möglich. Wenn Subjekt A durch Schutzprofile geschützte Energiedaten vom zentralen Enertrust-System bezieht, wird zunächst die Einhaltung der Sicherheitsvorgaben selbst überprüft wie in Abbildung 2 skizziert. Falls nun A die Daten an ein Subjekt B direkt weiterleitet, bleibt der Profilschutz weiter bestehen. Ist B an die Enertrust-Schnittstelle angeschlossen, so erfolgt auch bei dem transitiven Informationsfluss eine Überprüfung der definierten Schutzprofile durch das zentrale Enertrust-System. Sendet B wiederum die Daten an ein Subjekt C, das nicht an das Enertrust-System angeschlossen ist, so wird – falls möglich – automatisiert die Dateneinsicht verhindert. Ist eine Verhinderung nicht möglich, wird der Missbrauch protokolliert.

5.2.5 Sicherheit nach Datenweitergabe

Eine Möglichkeit einen solchen unautorisierten Datenabfluss zu verhindern, ist die grundsätzliche Übertragung von verschlüsselten Daten, wobei eine Entschlüsselung der Daten erst nach einer Überprüfung der definierten Schutzprofile erfolgt. Ein weiterer Ansatz ist das Energiedatum mit einem Kopierschutz zu umgeben.

5.2.6 Zeitlich befristete Dateneinsicht und Datensperrung

Falls ein Datenzugang zeitlich befristet für Subjekte in den Schutzprofilen definiert wird, kann dies ebenfalls durch die Rückkopplung umgesetzt werden. In wahlweise regelmäßigen Abständen oder beim jeweiligen Öffnen, überprüft das Enertrust-System den Status der Energiedaten. Ist ein Einsichtszeitraum verstrichen, wird das entsprechende Energiedatum angewiesen sich zu sperren. Das heißt das Energiedatum wird nicht mehr entschlüsselt, unleserlich gemacht oder im härtesten Fall wird eine Löschung angewiesen. Dies greift auch wenn eine Rückkopplung zum System unterbunden wird. Dann kann nämlich der Fall eintreten, dass absichtlich nachträglich geänderte Schutzprofile missachtet werden sollen.

Im Fall von Subjekt C aus Abbildung 2 ist eine Rückkopplung aufgrund der fehlenden Schnittstelle nicht möglich, so dass hier eine automatische Datensperrung erfolgt. Falls ein sehr hoher Schutz für ein Energiedatum definiert wurde, kann auch eine sofortige Datenlöschung ohne Rückkopplung zum System erfolgen.

Durch den Mechanismus der Rückkopplung mit anschließender Datensperrung wird das Gedächtnis des Internets abgemildert, d.h. in einem dezentralen Netz verteilte Daten können auch nach einer komplexen Datenweitergabe nicht mehr genutzt werden. Durch den hier dargelegten Ansatz ist es möglich Kontrolle in die dezentrale Datenverteilung zu bringen.

5.2.7 Nachträgliche geänderte Schutzprofile

Eine regelmäßige Rückkopplung zum Prüfungssystem bietet einen weiteren Vorteil: Sollte sich Subjekt B entschließen, die für seine Daten b definierten Sicherheitsrichtlinien zu ändern, greifen diese Änderungen nicht nur für vom zentralen System abgegebene Daten, die Änderungen haben auch für bereits abgegebene Daten Gültigkeit.

6. Ontologiebasierte Schutzprofile für zeitkritische Sicherheitsprüfungen

Um den in Abschnitt 5 beschriebenen Ansatz durchzuführen ist eine Wissensbasis in Form von Schutzprofilen von Energiedaten nötig. Die Sicherheitsprüfung erfolgt für an das Enertrust-System registrierte Energiedaten, die als besonders sicherheitsrelevant eingestuft werden. Das Enertrust-System enthält eine Wissensbasis, die Datenmodelle, Sicherheitskonzepte und eine Verbindung

dieser beiden in Form von Schutzprofilen. Die beschriebene Wissensbasis des Enertrust-Systems liegt als Ontologie in einer Datenbank. Semantische Anfragen auf die Ontologien können beispielsweise mit der W3C-Empfehlung SPARQL erfolgen.

Um den Echtzeitanforderungen Rechnung zu tragen, werden Anfragen zur Sicherheitsprüfung einer Klassifizierung unterzogen. Diese hat die Aufgabe die Anfragen nach Dringlichkeit zu priorisieren. Bei Zeitkritikalität können auch niedrig priorisierte, vorgeschriebene Schutzmaßnahmen zeitweise ausgekoppelt werden, damit die Prozesse der Leittechnik nicht beeinträchtigt werden und um angemessene Verfügbarkeit zu garantieren.

Zur Erzielung einer gewissen Ausfallsicherheit für das zentrale Prüfungssystem Enertrust, wird es redundant ausgelegt. Es wird ein Peer-to-Peer-System aufgebaut in dem das System und die ontologiebasierte Wissensbasis dezentral verteilt sind. Auf diese Weise ist auch ein *Load Balancing* möglich, um eine mögliche Anfragelast zu verteilen.

7. Fazit und Ausblick

Der vorgestellte Ansatz liefert Sicherheitskonzepte mit denen der zunehmenden Dezentralisierung in der Energiedomäne begegnet werden kann. Durch einheitlich definierte Schutzprofile, die internationale Sicherheitsstandards beachten, wird dem Datenbesitzer ein Format gegeben, um seine Sicherheitsrichtlinien für verteilte Beteiligte, die Dateneinsicht benötigen könnten, zu definieren. Diese Sicherheitsprofile werden von zentraler Stelle überprüft. Durch eine Rückkopplung zum System kann die Sicherheitsprüfung bei der Datenbereitstellung vom zentralen Server als auch bei Datenweitergabe unter den Beteiligten erfolgen. Dies bietet die Möglichkeit ungewollte Datenweitergabe zu verhindern. Eine Datensperrung nach einer zeitlichen Frist oder ohne Rückkopplung zum System ermöglicht es, abgegebene Daten aus den dezentralen Systemen zurückzuziehen.

Die Auslegung des Enertrust-Systems als Peer-to-Peer-System garantiert eine gewisse Ausfallsicherheit. Diese ist wichtig, um die geschützten Prozesse respektive die zugehörigen semantischen Anfragen zur Sicherheitsprüfung zeitnah und unterbrechungsfrei zu beantworten. Eine Klassifizierung von semantischen Anfragen im Rahmen der Sicherheitsprüfung ermöglicht das Schutzziel Vertraulichkeit angemessen zusammen mit dem Schutzziel Verfügbarkeit umzusetzen.

8. Literaturangaben

[1] Bundesverband der Energie- und Wasserwirtschaft e.V., Richtlinie Datenaustausch und Mengenbilanzierung (DuM), 2007

[2] Bundesverband der Energie- und Wasserwirtschaft e.V., Nachrichtentyp zur Übermittlung von Stammdaten zu Kunden, Verträgen und Zählpunkten UTILMD Stand: 4.1a (19.05.2008), Berlin, 2008

[3] Eckert, C.., IT-Sicherheit, Oldenbourg Verlag 2008.

[4] EUZENAT, J., SHVAIKO, P., Ontology Matching, Springer 2007

[5] GRUNER, D.: IT-Security in Leit- und Automatisierungssystemen in der elektrischen Energieversorgung. Internationaler ETG-Kongress 2007, 2007

[6] Internationale Organisation für Normung: ISO 15408 - Common Criteria Version 3.1, 2006

[7] KIM, A., LUO, J., KANG, M., Security Ontology for Annotating Resources, 4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE'05), Agia Napa, Cyprus.

[8] KOCH, M; BAIER, D., Handel im liberalisierten Strommarkt. Erschienen im Jahrbuch der FfH Institut für Markt- und Wirtschaftsforschung GmbH Berlin 2003

[9] KREBS, B., Cyber Incident Blamed for Nuclear Power Plant Shutdown, Washington Post, Ausgabe vom 5. Juni 2008, URL: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html [Stand: 31.07.2008]

[10] KUHN, J., Der Schutz kritischer Infrastrukturen. Unter besonderer Berücksichtigung von kritischen Informationsinfrastrukturen, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, Juni 2005

[11] PFEIFFER, N, SELMA - Sicherer Elektronischer Messdaten Austausch, gat 2003, München 2003

[12] POULSEN, K., Slammer worm crashed Ohio nuke plant network, Security Focus 2003-08-19, URL: http://www.securityfocus.com/news/6767 [Stand: 31.07.2008]

[13] SURE, Y., HALLER, J., Towards Cross-domain Security Properties supported by Ontologies, In: Christoph Bussler, Sukki Hong, Woochun Jun, et al., Web Information Systems Engineering -- Workshop Proceedings, November 22nd, 2004, Brisbane, Australia, volume 3307 of LNCS, pp. 58-72. Springer-Verlag GmbH, 2004.

[14] USLAR, M., GRÜNING, F., Zur semantischen Interoperabilität in der Energiebranche: CIM IEC 61970, In: Wirtschaftsinformatik, 49(4), Vieweg Verlag, S.295-303, 9 (2007)

[15] WANG, Y., SHAHIDEHPOUR, M., Communication and Control in Electric Power Systems. IEEE Press, 2003

[16] WINKELS, L., SCHMEDES, T., APPELRATH, H.-J., Dezentrale Energiemanagementsysteme. In: Wirtschaftsinformatik, 49(5), Vieweg Verlag, S.386--390, (10) 2007