Dieser Artikel ist in leicht gekürzter Form in der Fachzeitschrift
IT Security 4/2008 (Juli/August), S. 32-35 erschienen.

Informationssicherheit in der Marktkommunikation

Effektivität optimieren, Missbrauch minimieren

Die Bundesnetzagentur hat die Standardisierung der Datenübermittlung und Geschäftsprozesse zur Anbahnung und Abwicklung der Belieferung von Kunden mit Elektrizität forciert.

Einleitung

Intention des Beschlusses BK6-06-009 ist die inhaltliche, formale und zeitliche Vereinfachung der Prozesse. Insbesondere sollen die Vorgänge des Lieferantenwechsels transparenter und beschleunigt werden, was durch ein hohes Maß an Automatisierung ermöglicht wird.

Fristsetzung für die Umsetzung war der 1. August 2007, wobei verschiedene Fristeneinhaltungen zum Teil auf Basis zu veröffentlichender Begründungen gewährt werden. Gleichwohl ist ein erheblicher Zeitdruck in den Umsetzungsprojekten entstanden. Die zu verwendenden Formatversionen, die Releases der Abrechnungslösungen aber auch die Komplexität des Vorhabens haben dafür gesorgt, dass die Umsetzungsfristen flexibel ausgelegt worden sind und werden. Bis heute haben nach wie vor nicht alle betroffenen Marktteilnehmer alle Vorgaben umgesetzt beziehungsweise bestehen Probleme in der Interoperabilität.

Dieser Artikel beschreibt ein Gemeinschaftsprojekt des IT-Dienstleisters prego services GmbH und des Informationssicherheitsspezialisten TTS Trusted Technologies and Solutions GmbH. In diesem Projekt wurde für einen Energieversorger eine Anwendungs- und Systemlandschaft konzipiert und umgesetzt, die geeignet ist, den Anforderungen an die Marktkommunikation zu genügen.

Neben den Aspekten der Effizienz und Effektivität ist dabei ein besonderes Augenmerk auf die Informationssicherheit gelegt worden – ein Aspekt, der in den Diskussionen um die Umsetzung der Marktkommunikation wenig Präsenz zeigt und auch von der Bundesnetzagentur kaum adressiert wird. Die Vorkehrungen zur Wahrung der Authentizität, Integrität, Vertraulichkeit und Verfügbarkeit der auszutauschenden Informationen sind jedoch eine Voraussetzung für eine ordnungsgemäße Abwicklung der Marktkommuni-

Dieser Artikel ist in leicht gekürzter Form in der Fachzeitschrift IT Security 4/2008 (Juli/August), S. 32-35 erschienen.

kation und letztlich auch die Voraussetzung für eine Automatisierung der Abläufe. Ohne erweiterte Sicherheitsmaßnahmen besteht daher die Gefahr, dass die angestrebten Effizienz- und Effektivitätsziele verfehlt werden und genauso ärgerliche wie kostspielige Missbräuche der Marktkommunikationsprozesse auftreten werden.

Problemstellungen

Datenschutz

Der Austausch der Nachrichten im EDIFACT-Format erfolgt in der Regel per E-Mail oder über das Datentransferprotokoll FTP, zukünftig wohl auch vermehrt als AS2-Nachricht (http). Dabei findet in vielen Fällen auch eine Datenübertragung über unsichere Netze, meist das Internet statt. Ein sehr offensichtliches Problem ist darin zu sehen, dass im Rahmen des Lieferantenwechselprozesses personenbezogene Daten übermittelt werden. Diese unterliegen dem Bundesdatenschutzgesetz und sind entsprechend durch Maßnahmen der Verschlüsselung abzusichern.

Angreifbarkeit

Auch wenn derartige Vorfälle noch nicht bekannt geworden sind: Die Kommunikation zwischen den Marktteilnehmern ist standardisiert und ohne zusätzliche Maßnahmen recht einfach angreifbar. Trotz zahlreicher Plausibilitätsprüfungen in den nachgelagerten Anwendungssystemen lassen sich Angriffsszenarien entwickeln, die zum Beispiel zu unrechtmäßigen An- und Abmeldungen beziehungsweise Netznutzungsabrechnungen führen.

Archivierung

Eine etwa in einer E-Mail enthaltene Erklärung beziehungsweise Information ist rechtsrelevant und hat im Geschäftsverkehr dieselbe rechtliche Bedeutung wie ihr Pendant in Papierform (gem. HGB, AO, …). Alle steuerrechtlich relevanten eingehenden und ausgehenden E-Mails müssen daher im Original archiviert werden, um einen revisionssicheren Prozessablauf zu gewährleisten.

Verfügbarkeit

Bisher unterschätzt wird, dass Informationen diskriminierungsfrei zur Verfügung gestellt werden müssen. So steht ein Netzbetreiber in der Pflicht, die mit seinem assoziierten Vertrieb ausgetauschten Informationen auch allen anderen in seinem Netzgebiet tätigen Lieferanten zu vergleichbaren Zeitpunkten, in vergleichbarer Geschwin-

Rechtliche Grundlagen

Das Gesetz über die Elektrizitäts- und Gasversorgung (EnWG) legt die rechtliche Basis für die Verordnungen über den Zugang zu Elektrizitäts- beziehungsweise Gasversorgungsnetzen (StromNZV, GasNZV). Die StromNZV ermächtigt die Bundesnetzagentur zur Durchsetzung eines bundesweit einheitlichen elektronischen Datenaustauschformats sowie einheitlicher Prozesse mit größtmöglicher Automatisierung. Dem gegenüber fordert die GasNZV die Entwicklung einheitlicher Regeln und Verfahren zu Datenaustausch, Überwachung und Steuerung sowie die Entwicklung eines einheitlichen Verfahrens zum vereinfachten Lieferantenwechsel.

Durch den Beschluss „Festlegung einheitlicher Geschäftsprozesse und Datenformate zur Abwicklung der Belieferung von Kunden mit Elektrizität (BK6-06-009) sind Energieversorgungsunternehmen verpflichtet, alle Prozesse der Elektrizitätsversorgung einheitlich und auf Basis des Datenformats Edifact abzuwickeln. Davon betroffen sind die Geschäftsprozesse Lieferantenwechsel, Lieferende/-beginn, Ersatzversorgung, Zählerstand-/Zählerwertübermittlung, Stammdatenänderung, Geschäftsdatenabfrage und Netznutzungsabrechnung. Dabei gelten folgende Fristen:

- Seit 1. August 2007 gilt Edifact für die Übermittlung von Zählerständen (MSCons), An- und Abmeldungen (UtilMD)
- Seit 1.Oktober 2007 ist Edifact bindend für die Übermittlung von Netznutzungs- und Verbrauchsabrechnungen (Invoic) sowie Zahlungsavisen (RemaDV)
- Seit 1. Februar 2008 sind Bestätigungsanmeldungen der Anwendung (Aperak), Übertragungsprotokollnachrichten wie Empfangsbestätigungen (Contrl) und Dokumentenanforderungen (ReqDoc) ausschließlich in Edifact auszutauschen
- Ab 1. Oktober 2009 sind alle Prozesse mit nicht integrierten Lieferanten genauso abzuwickeln wie mit dem vertikal integrierten Lieferanten

Eine entsprechende Festlegung zur Abwicklung des Wechsels von Lieferanten bei der leitungsgebundenen Versorgung von Letztverbrauchern mit Gas (BK7-06-067: „Geschäftsprozesse Lieferantenwechsel Gas, GeLiGas“) ist am 20.08.2007 erfolgt. Die Festlegung ist bis zum 01. August 2008 von den Marktteilnehmern umzusetzen.

Dieser Artikel ist in leicht gekürzter Form in der Fachzeitschrift IT Security 4/2008 (Juli/August), S. 32-35 erschienen.

digkeit und vergleichbarer Qualität zur Verfügung zu stellen. Letztlich bedeutet dies, dass erhebliche Anforderungen insbesondere an die Hochverfügbarkeit von Kommunikationsschnittstellen und deren Anwendungsprogramme gestellt werden. Dies betrifft das ERP-System genauso wie die E-Mail-Infrastruktur, das Archivierungssystem und den Internet-Zugang. Für all diese Systeme sind Betriebsprozesse erforderlich, die eine Hochverfügbarkeit der Systeme erfordern. Übliche Office-SLA für den E-Mail-Server mit Servicezeiten von 7–18 Uhr oder Wiederherstellungszeiten im Bereich von zwei bis drei Werktagen kommen da wohl kaum noch in Betracht.

Denial-of-service

Die Betreiber von E-Mail-Systemen sind seit langem mit Denial-of-Service Attacken konfrontiert. Im Bereich Spam und Viren besteht ein Wettrüsten, das zu immer neuen Bedrohungsszenarien führt. Während die Spam-Problematik derzeit einigermaßen beherrscht wird, wächst die Anzahl der Kollateral-Spams im Jahr 2008 ganz erheblich. An dem Bewusstsein, dass Spammer Adressen Dritter als Absenderadresse missbrauchen und für die betroffenen Absender eine automatisierte Antwort unerwünscht ist, mangelt es offenbar. Als Resultat entsteht eine wahre Rückläuferplage, die zu einer Verstopfung von E-Mail-Konten oder gar –Servern führt, was wiederum einem Totalausfall der Marktkommunikation gleichkommt.

Automatisierung

Effizienz und Effektivität sind treibende Faktoren der Marktkommunikation. Diese sollen durch einen hohen Automatisierungsgrad erreicht werden. Als Zielsetzung sicherlich richtig - die Automatisierung macht aber erst dann Sinn, wenn eine Gewissheit besteht, dass die zum Einsatz kommenden Anwendungssysteme das tun, was von ihnen erwartet wird. Der Realisierungstand und Reifegrad der Umsetzungen bei den verschiedenen Marktteilnehmern ist sehr unterschiedlich und noch fehleranfällig, so dass noch weitgehend auf eine automatisierte Versendung von Nachrichten verzichtet wird. Da die Geschäftsvorfälle über eine Vielzahl von Kommunikationsvorgängen abgewickelt werden, müssen die einzelnen Vorgänge händisch anhand mehrerer E-Mail-Nachrichten bewertet und gegebenenfalls nachgesteuert werden müssen.

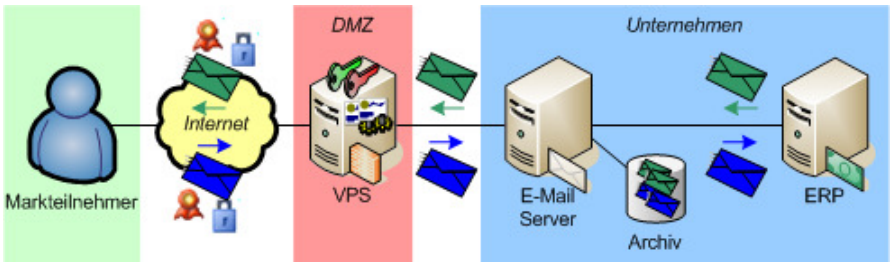
Lösungsansatz

Die prego services ist beauftragt worden, eine Systemlandschaft zur Unterstützung der Marktkommunikation gemäß BK6-06-009 zu entwickeln und umzusetzen. In Zusammenarbeit mit der TTS GmbH wurden die relevanten Geschäftsprozesse des Kunden analysiert und eine Schutzbedarfsfeststellung für die zu verarbeitenden Informationsbestände durchgeführt. Die ermittelten Schutzbedürfnisse sind danach den IT-Komponenten zugeordnet worden, die zum Einsatz kommen, um die jeweiligen Informationen zu verarbeiten, zukommunizieren oder zu speichern. Auf diese Weise ist zum Beispiel der Schutzbedarf des E-Mail-Servers über die Schutzbedürfnisse der Informationen definiert, die über ihn kommuniziert werden. Im Nachgang wurden durch eine Gefährdungsanalyse Risiken für die einzelnen Systemkomponenten ermittelt. Dedizierte Maßnahmenempfehlungen zur Erreichung eines akzeptablen Restrisikos wurden ausgesprochen.

Aus der Vielzahl der Maßnahmenempfehlungen wurde eine Sicherheitsarchitektur entwickelt. Ein Großteil der erforderlichen Maßnahmen konnte geeignet durch die Einbringung einer zentralen Virtuellen Poststelle praktisch umgesetzt werden.

Virtuelle Poststelle

Eine Virtuelle Poststelle (VPS) bietet die Möglichkeit, ausgehende und eingehende E-Mails automatisch zu Ver- oder Entschlüsseln sowie elektronische Signaturen zu erzeugen oder zu prüfen. Dabei lässt sich eine VPS transparent in die vorhandene E-Mail-Architektur eines Unternehmens einbinden. Sie eignet sich damit zur automatischen Umsetzung von Regeln sowohl für die Bearbeitung manuell erzeugter als auch für automatisch generierte E-Mails. Abhängig von verschiedenen Merkmalen der Nachricht (Sender, Empfänger, Betreff) können verschiede-



Dieser Artikel ist in leicht gekürzter Form in der Fachzeitschrift IT Security 4/2008 (Juli/August), S. 32-35 erschienen.

ne Varianten der Verschlüsselung und Signatur gewählt werden. So können zum Beispiel Rechnungsnachrichten mit einer qualifizierten elektronischen Signatur versehen werden, andere Nachrichten werden dagegen mit einer normalen Signatur geschützt beziehungsweise diese geprüft oder Daten lediglich verbeziehungsweise entschlüsselt. Über eine Schnittstelle zu einem Archivierungssystem können unabhängig von der Archivierung in den Endsystemen zudem alle E-Mail-Nachrichten an zentraler Stelle archiviert werden.

Angriffserkennung

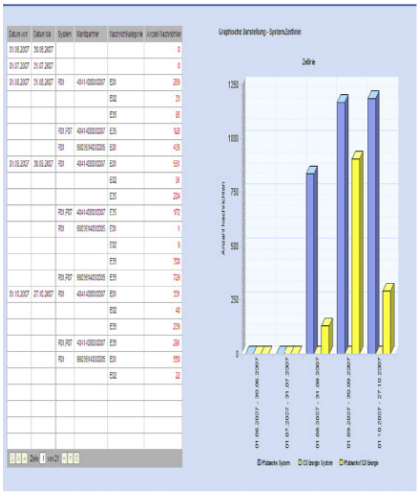
Um das Angriffspotential auf die Marktkommunikationsprozesse zu senken, sollten alle Teilnehmer elektronische Signaturen verwenden, um dadurch die Prüfung der Authentizität des Senders zu ermöglichen. Dies ist heute noch nicht der Fall, jedoch ist klar zu erkennen, dass immer mehr Marktteilnehmer auf die kryptographische Absicherung setzen. So wurden in den ersten vier bis fünf Monaten des Betriebs der Virtuellen Poststelle ca. 500 Benutzerzertifikate importiert beziehungsweise ermittelt. Diese stammen zwar nicht ausnahmslos von Marktteilnehmern, trotzdem ist aber der Anteil der empfangenen signierten E-Mails in der Marktkommunikation stetig gestiegen.

Trotz des Einsatzes der modernsten Spam-Abwehrtechniken bleibt die Gefährdung durch Kollateral-Spam bestehen. Die möglichen Gegenmaßnahmen unterscheiden sich grundlegend von denen gegen allgemeinen Spam, da der Charakter der Nachrichten ein gänzlich anderer ist. Es handelt sich um legitime Nachrichten, die auf Basis einer nichtlegitimen E-Mail generiert oder geschrieben wurden. Während man auf persönliche Antworten gegebenenfalls reagieren sollte oder gar muss, können automatische Antworten wie Unzustellbarkeitsnachrichten oder Abwesenheitsnotizen verworfen werden. Besonders problematisch ist dabei, dass das Ausfiltern der Rückläufernachrichten schwierig ist, da es kein Standardformat für Bounces, Abwesenheitsnachrichten und ähnliches gibt. Solange sich hier kein Best Practice entwickelt, wird es eine Herausforderung bleiben, zwischen erwünschten und unerwünschten E-Mails zu unterscheiden. Ungeachtet dessen besteht hier zusätzlich das Problem, dass der Betreiber der E-Mail-Infrastruktur durch eine automatische Löschung in rechtliche Schwierigkeiten geraten kann.

Verfügbarkeit

Auch wenn die Bundesnetzagentur derzeit noch keine expliziten Aussagen zu der Verfügbarkeit der Geschäftsprozesse getroffen hat, zeichnet sich ab, dass hier hohe Anforderungen gestellt werden. Gerade die Wiederherstellung von komplexen IT-Systemen, wie etwa der E-Mail-Architektur eines Unternehmens, ist zeitlich kritisch zu sehen. Allein die Wiederherstellung eines Information Store kann durchaus mehr als 24 Stunden beanspruchen, zusätzlich sind weitere Systeme zur Absicherung des E-Mail Aufkommens wiederherzustellen.

Im oben erwähnten Projekt ist entsprechend empfohlen worden, die E-Mail-Kommunikation für die Marktkommunikation durch einen dedizierten E-Mail-Server zu unterstützen, um dadurch eine schnelle Wiederherstellung der wenigen E-Mail-Postfächer zu ermöglichen. Ein weiterer Aspekt, der zu dieser Entscheidung beigetragen hat, liegt an der Häufung des E-Mail-Verkehrs zu bestimmten Zeitpunkten. Die Spitzenlast liegt Mitte des Monats (13. – 15.), weitere erhöhte Aufkommen zu Monatsbeginn (2. – 5.) und –ende (29. – 31.).



Automatisierung

Die Abläufe der Marktkommunikation sind standardisiert und erfordern jeweils das Versenden/den Empfang mehrerer E-Mail-Nachrichten, die im Format Edifact kaum noch lesbar sind. Die Vielzahl der E-Mails, die teilweise automatisiert über eine Kommunikationsschnittstelle (XI) des SAP-ISU Systems, verschickt werden, lassen den Aufwand erheblich ansteigen.

Gerade in der Einführungsphase der Marktkommunikationsprozesse hat es sich als sehr vorteilhaft erwiesen, eine Monitoringsoftware einzusetzen, die eine Zuordnung von Geschäftsvorgängen zu beteiligten E-Mails vornimmt, ein Fristenmanagement realisiert, Berichte liefert und vielfältige Such- und Filterfunktionen anbietet.

Ohne diese Zusatzsoftware ist der Verlauf der Geschäftsabläufe größtenteils intransparent und stellt ein nicht unerhebliches Risiko für den Prozessverantwortlichen dar.

Dieser Artikel ist in leicht gekürzter Form in der Fachzeitschrift IT Security 4/2008 (Juli/August), S. 32-35 erschienen.

Ein unerwartetes Problem entstand durch die automatische LDAP-Abfrage nach Zertifikaten in der Virtuellen Poststelle. Auf diese Weise wurden Zertifikate gefunden, die bereits ausgestellt und gültig waren, die der Kommunikationspartner aber noch nicht im Einsatz hatte. Andere Marktpartner haben im ERP-System statisch festgelegt, mit welchen Teilnehmern sie verschlüsselt kommunizieren und ignorieren die Bekanntgabe von Zertifikaten. Durch dieses unterschiedliche Verhalten sind in der Anfangsphase einige händische Anpassungen im Regelwerk der Virtuellen Poststelle notwendig geworden, um entsprechende Ausnahmebehandlungen vorzusehen.

Fazit

Die Umsetzung der Marktkommunikationsprozesse ist allein schon aus fachlicher Sicht eine Herausforderung, die erhebliche Ressourcen erfordert hat und noch heute bindet. Das erhöhte E-Mail Aufkommen stellt zudem neue Anforderungen an die Firewall-, Virenscan- und E-Mail-Architektur eines Unternehmens. Das Mailaufkommen durch diese Prozesse macht gegenwärtig schon einen Anteil von 15 – 30 Prozent des Gesamtverkehrs aus – Tendenz steigend.

Dieser Artikel hat ein Projekt zur Absicherung der Marktkommunikation vorgestellt. Die Erfahrungen aus gut einem halben Jahr sind weitestgehend positiv, auch wenn es nach wie vor Probleme in der Interoperabilität der Kommunikation mit neuen Marktteilnehmern gibt. Ohne eine Integration von Sicherheitsmaßnahmen besteht die Gefahr, dass ein Missbrauch der Marktkommunikationsprozesse erfolgt. Um dies abwehren zu können, sollten alle Marktteilnehmer elektronische Signaturen und Verschlüsselung realisieren – dies erspart aufwändige manuelle Plausibilitätsprüfungen und rechtliche Auseinandersetzungen. Wesentliche Erfolgskomponenten für die Gewährleistung einer sicheren Marktkommunikation sind im Einsatz des XI-Monitors und in der Virtuellen Poststelle zu sehen.

Den Verantwortlichen aus den Häusern der anderen Marktteilnehmer kann nur nachhaltig empfohlen werden, die hier beschriebenen Sicherheitsüberlegungen anzustellen und sich ganzheitlich um eine Absicherung der Marktkommunikation zu kümmern.

Dr. Jörg Cordsen, *TTS Trusted Technologies and Solutions GmbH*, Geschäftsführer

(joerg.cordsen@tts-security.com)

Rudolf Sichler, *prego services GmbH*, Geschäftsbereichsleiter Informationstechnologie

(rudolf.sichler@prego-services.de)

Die TTS Trusted Technologies and Solutions GmbH (www.tts-security.com) ist ein erfahrener und unabhängiger Dienstleister im Bereich der Informationssicherheit. Das Dienstleistungsportfolio besteht aus methodischen Lösungsansätzen, die dem Kunden helfen, seine Geschäftsprozesse sicher, vertrauenswürdig und effizient zu betreiben.

Die prego services GmbH (www.prego-services.de) ist ein Dienstleister in den Bereichen Informationstechnologie, Personaldienstleistungen, Materialwirtschaft und Abrechnungsdienstleistung mit umfassender Branchenkompetenz in der Industrie, Verwaltung und Energie.