oesterreichs energie.

GENERALSEKRETARIAT

Herr
Dr. Po-Wen Liu
RTR-GmbH
Mariahilfer Straße 77 - 79
1060 Wien
Per E-Mail an: po-wen.liu@rtr.at

Kontakt	DW	Unser Zeichen	Ihr Zeichen	Datum
DI Armin Selhofer	232	ARS/Ha – 11/2013	-	27.02.2013

Stellungnahme Konsultationsdokument (RTR) IKT – Strategie für Österreich 2014 - 2018

Sehr geehrter Herr Doktor Liu,

Oesterreichs Energie bedankt sich für die Gelegenheit, an der Konsultation zur Entwicklung einer IKT-Strategie für Österreich Stellung nehmen zu dürfen. Wir beziehen uns in unserer Stellungnahme im Wesentlichen auf das Kapitel 6.3.

In diesem Kapitel werden Aussagen getroffen, die aus Sicht von Oesterreichs Energie deutlich differenzierter zu sehen sind.

Unsere wesentlichen Kritikpunkte sind:

- Zur effizienten Umsetzung gesetzlicher Vorschriften müssen entsprechende Ressourcen (z.B. Frequenzbereiche) den Energieversorgern zeitnahe bereitgestellt werden
- Zusätzlicher Einsatz von IKT führt nicht per se zu Energieeinsparungen
- Die Anforderungen der E-Wirtschaft an IKT unterscheiden sich von den Systemparametern und Anforderungen der Telekommunikationsanbieter
- Ein Zusammenführen von betrieblichen und kommerziellen Kommunikationsnetzen führt zu zusätzlichen Sicherheits- und Verfügbarkeitsrisiken sowie zusätzlichem personellen und finanziellen Aufwand.

Zu den weiteren Punkten aus Kapitel 6.3 nehmen wir im Detail wie folgt Stellung:

1. Einleitung

Die Energieversorger in Österreich sind durch die sich ändernde Leistungsaufbringung in den Energienetzen, durch die verstärkte Integration dezentraler Erzeugungsanlagen sowie

DVR 0422100, UID ATU37583307, ZVR 064107101; UniCredit Bank Austria AG, SWIFT/BIC: BKAUATWW, IBAN: AT 90 1100 0006 4204 1800

der E-Mobilität und die dadurch bedingte Stromnetzbelastung in den nächsten Jahren gefordert, neue Lösungen in Bezug auf Ökologie, Verfügbarkeit, Netzqualität, Ökonomie, gesetzlichen Anforderungen und Sicherheit dieser kritischen Infrastruktur bereitzustellen. Dabei liegt ein nicht unbeträchtlicher Anteil dieser Anforderung in der sich aus den neu entstehenden verteilten Erzeugungsanlagen ergebenden Strukturänderung der Energienetze. Bis vor wenigen Jahren wurde die Energieverteilung ausgehend von den vorhandenen meist großen Erzeugungsanlagen wie Wasser-, Kohle- und Gaskraftwerken in eine top-down-Energieflussrichtung betrieben. Dabei entstand über die Jahrzehnte eine vermaschte Struktur der Höchstspannungs- und Hochspannungsnetze überregional europaweit. Bei Ausfall einer großen Erzeugungsanlage (1000 bis 2000 MW) wurde durch das vermaschte Netz und die daran angebundenen Kraftwerke ein entsprechender Energieausgleich (Frequenzstützung) gewährleistet. Der Energiefluss von den Stromnetzen war ausgehend von diesen Hochspannungsnetzen auf die Mittelspannungsebene und weiter über die Niederspannungsverteilstationen zu den Verbrauchern. Das Energienetz der Zukunft wird durch das Wachstum der erneuerbaren Energieerzeuger und die daraus entstehende Energieeinspeisung direkt an den Niederspannungsnetzen die Struktur der Stromnetze der Zukunft ändern. Die dezentralisierte Energieerzeugung (Photovoltaik, Windenergie usw.) von kleinen oder mittleren erneuerbaren Energieversorgern wird die zur Verfügung gestellte Leistung, abhängig von den Gegebenheiten der Außenwelt wie Sonneneinstrahlung, Wind usw. zu unterschiedlichen Zeiten in die Niederspannungsnetze einbringen. Diese dezentrale von der Außenwelt abhängige Stromerzeugung erfordert von dem Stromnetzbetreiber die bestehende Netzstruktur entsprechend den sich neu ergebenden Anforderungen anzupassen. Diese neuen Anforderungen müssen in einem ökologischen und ökonomischen Umfeld betrachtet werden. Die Energieversorger haben ein bestehendes IKT-Netz zum Betrieb von Fernwirkanlagen, zur Datenübertragung, für die Telefonie usw. Dieses IKT-Netz ist bei kritischen Anwendungen redundant auf LWL-Basis (Lichtwellenleiter-Basis) vorhanden und über Jahrzehnte auf den sicheren Betrieb dieser Anlagen ausgerichtet.

Anforderungen für den Stromnetzbetreiber sind:

- Sicherheit der Energieversorgung gewährleisten
- Qualität der Energieversorgung garantieren (Spannungswert +- 10 % des Grundwertes laut Norm ÖVE EN 50160)
- Frequenzstabilität
- Einspeisemöglichkeit für erneuerbare Energien
- Vermeiden von Spannungsspitzen
- Schutzeinrichtungen für Personen und Anlagen
- Rücksicht auf die ökologischen Argumente bei der Energieverteilung
- Wirtschaftlichkeit der Anlagen und des Betriebes
- Ausfallsicherheit und kurze Wiederherstellzeiten bei höherer Gewalt (Sturm, Schnee usw.)
- Notstromversorgung bei Netzbauten

usw.

1.1 Kurzbeschreibung Green & Energie

Der intelligente Einsatz von IKT per se wird zu keiner Reduktion des Energieverbrauchs führen. Diese ist nur insoweit möglich, als die Bevölkerung selbst Maßnahmen dazu setzt, wie zum Beispiel die Verwendung von IKT zur Steuerung der Haushaltsverbraucher. Ein größeres Einsparungspotential liegt hingegen in der ökologischen Herausforderung des Austausches der Energieverbraucher auf weniger energiehungrige und die sparsame Verwendung der Energie. Als Beispiele dazu sind die heute schon auf dem Markt erhältlichen Produkte der Smart-Home-Automatisierung vorhanden.

Bestehende und zukünftige Smart Grids und Smart-Metering-Anwendungen in der Energiewirtschaft bieten die Chance, die räumlich dislozierte Erzeugung und den Verbrauch von Energie besser als bisher aufeinander abzustimmen. Der innovatorische Gehalt dieses Konzeptes besteht darin, dass auch Privathaushalte und Kleinunternehmen als Verbraucher sowie dezentrale, verbrauchsnahe Erzeugungseinheiten zeitnahe Informationen erhalten, die direkt ihr Energieverbrauchsverhalten beeinflussen können. Dabei ist jedoch das Verbrauchsverhalten der Konsumenten und Betriebe an die gesellschaftlichen und sozialen Gegebenheiten gebunden. Die Mehrzahl der Haushalte sind kinderlos (72 %) und ein Drittel der Haushalte sind Singlehaushalte (Studie der AK Wien Mietenbelastung 2009. Archivnummer 21.917.026). Ausgehend von dieser Studie kann angenommen werden, dass am Tag nur ein Drittel der Haushalte die in einem Haushalt anfallenden Arbeiten erledigen wird. Die anderen zwei Drittel der Haushalte werden ihr Verbrauchsverhalten in erster Linie auf die Abende oder das Wochenende verlegen. Gerade zu den Tageszeiten, an welchen erneuerbare Energie (Photovoltaik) Strom in das Leitungsnetz einbringt, wird es je nach im Niederspannungsnetz vorhandenen Energieverbrauchern schwierig, diese Energie im Umfeld der Erzeugung zu nutzen. Eine höhere Transparenz des tatsächlichen Verbrauchs und der anfallenden Kosten könnte längerfristig zu einer stärkeren Sensibilisierung des Energiekonsums und damit zu einem bewussteren Umgang mit Energie führen, soweit die Energieeinsparung einen bestimmten für den Nutzer wirtschaftlichen Wert überschreitet.

Der weitere Einsatz von IKT in anderen Wirtschaftssektoren wie Gebäudemanagement, Verkehr und Produktion würde ebenfalls zu einer Reduktion des Energieverbrauchs führen. Durch intelligente Lösungen, die flexibel auf das sich ändernde Umfeld reagieren, kann die Energie durch bessere Steuerung effizienter genutzt werden. Hingegen sind Einsparungspotentiale in den Unternehmen meist nur soweit schwer umsetzbar, als die Produktion immer mehr in eine „Just in Time"-Produktion übergeht. Die Einsparungspotentiale in der Lagerhaltung und in der Logistik stehen hier den Energieeinsparungspotentialen entgegen. Mit Maßnahmen aus erneuerbaren Energieträgern lässt sich der CO_2-Ausstoß reduzieren. Der Energieverbrauch hingegen lässt sich durch diese Maßnahmen nur marginal reduzieren. In Förderungen für erneuerbare Energien müsste auf die Netztopologie der Energienetzbetreiber und die vorhandenen Verbraucher Rücksicht genommen werden. Wenn es gelingt, die Energieaufbringung durch erneuerbare Energien zeitkritisch und räumlich begrenzt mit dem Energieverbrauch von Haushalten und Unternehmen abzustimmen, wäre der größte wirtschaftliche, ökonomische und ökologische Nutzen vorhanden.

Ausgehend von den vorhin genannten Punkten ist es für die Energieversorger sinnvoll, unterschiedliche IKT-Netzstrukturen zu schaffen, deren Übergänge oder Zusammenschlüsse nur mit speziellen Schutzeinrichtungen gewährleistet werden dürfen. Ein Beispiel hierfür ist der von der NIST (National Institute of Standards and Technology) kommunizierte Einsatz komplexer IT-Architekturen im Smart-Grid-Bereich. Österreichs Energie hat in Security-Arbeitsgruppen ein ähnliches Architekturmodell zusammengestellt. Dabei gibt es verschiedene in sich geschlossene Bereiche, wie den Betrieb des Energienetzes, den Smart Meter als dem Haushalt zugewiesenem Gerät, dem Internet, den Abrechnungs- und Informationsplattformen für Energievertrieb/Markt. Der überwiegende Teil dieser IKT-Netzstrukturen ist bereits bei den Energieversorgern vorhanden und der neue erforderliche zusätzliche sollte sich in die bestehende gut funktionierende IKT-Netzstruktur der Energienetzbetreiber einfügen. Ein Zusammenführen dieser IKT-Netzstrukturen sollte den bis heute hohen Verfügbarkeitsstandard der Energienetze Rechnung tragen sowie die vorhandenen IKT-Netzstrukturen der Energienetzbetreiber weiter nutzen und somit zu einer Synergie beitragen.

2. Eingrenzung Smart Grids, Smart Meter

Österreich steht wie viele andere Länder in Europa am Anfang bei der Umstellung der Energienetze auf Smart Energy. Unternehmen wie die Energie AG Oberösterreich mit mehr als 100.000 Smart Metern bei den Haushalten und die Linz Strom AG mit mehr als 60.000 Smart Metern bei den Haushalten haben eine Vorreiterrolle in der Umsetzung der IME-Verordnung. In der IME-Verordnung hat das BMWFJ den Energienetzbetreiber verpflichtet, bis zum Jahr 2017 mindestens 70 % und bis 2019 mindestens 95 % der Haushalte mit intelligenten Messgeräten auszustatten [vgl. (BMWFJ - Bundesministerium für Wirtschaft, Familie und Jugend, 2012)].
Die Energieversorger führen schon seit Jahren in entsprechenden Testregionen unterschiedliche Smart-Grid-Projekte durch. Dabei sind die Energie AG Oberösterreich mit dem Projekt Energieaufbringung durch dezentrale Photovoltaikanlagen unter dem Einsatz von regelbaren Trafostationen in Eberstallzell, die VKW mit dem Projekt der Cos-phi-Regelung dezentraler Einspeiser im Klein Walsertal, die Salzburg AG mit dem Pilotprojekt in der Gemeinde Köstendorf und die Linz AG mit dem Projekt Solarenergie und Stromtankstellen als Beispiele zu nennen.

2.1 Smart Grids

Die Europäische Richtlinie aus dem EPCIP-Programm und daraus abgeleitet das Österreichische APCIP-Programm finden vermehrt Einzug in den Smart-Grids-Programmen.
Derzeit sind verschiedene Untersuchungen auf ministerialer Ebene und Projekte der unterschiedlichen Unternehmen, Hochschulen und Infrastrukturbetreiber abgeschlossen, in Arbeit oder in der Genehmigungsphase.

Einige aktuelle Projekte in Österreich sind:

- Das BMVIT untersucht derzeit die institutionellen Rahmenbedingungen für Smart Energy, diese Studie soll Ende des Jahres 2012 vorliegen
- Unter dem BMF erheben die IV, das FEEI und das BRZ erstmals Zahlen und Potenziale zur CO2-Reduktion sowie der volkswirtschaftlichen Auswirkungen in verschiedenen nachhaltigen Bereichen wie Smart Grids, Endgeräte, Telekommunikation und Rechenzentren
- Smart Grid Security Guidance. Sicherheitsfragen bezüglich von Cyber Security Risiken für den Betrieb der Energieversorgungsnetze aus den neuen IKT-Anforderungen durch Smart Grids und Smart Meter
- Nationale Technologie-Plattform Smart Grids.

2.2 Smart Meter

Smart Meter sind in Europa im Rollout. Österreich ist im Verhältnis zu den anderen Märkten für Smart-Meter-Hersteller ein relativ kleiner Markt. Die technischen Anforderungen und die Sicherheitsanforderungen an die Smart-Meter-Hersteller sollten einen bestimmten Grundlevel an Sicherheitsstandards enthalten. Dazu hat Oesterreichs Energie Arbeitsgruppen für Security-Anforderungen an Smart-Meter-Schnittstellen und Smart Meter, Smart-Grid-Security u.a. eingerichtet. Diese Arbeitsgruppen bestehen aus IKT-Technikern und Security-Spezialisten. Durch die enge Zusammenarbeit dieser Spezialisten und den Informationsaustausch zwischen den Unternehmen von Österreichs E-Wirtschaft erfolgt eine regelmäßige zum Teil anlassbezogene Abstimmung der Arbeitsdokumente dieser Arbeitskreise. Die Unternehmen von Österreichs E-Wirtschaft betreiben seit ihrem Bestehen ein Metering-System und sind daher in der Lage, die gesetzlichen Anforderungen, auch wenn diese sich ändern, am besten zu gewährleisten. Großes Know-how ist hier bei den zertifizierten Eichstellen, den Managementsystemen für Zählerinstallation, Zählerwechsel usw. vorhanden. Zudem sind die Abrechnungssysteme erprobt und funktionieren zur vollsten Zufriedenheit der Kunden. Die Energie AG Oberösterreich und die Linz Strom AG sind seit Jahren mit der Einführung von Smart Metern befasst. Dazu wurden Logistik, Technik und Security-Anforderungen an die Systeme vor der Einführung dieser Systeme ausführlich den gesetzlichen Anforderungen entsprechend getestet. Zur Gewährleistung der Funktionalität und Sicherheit der Systeme erfolgen jährliche Qualitäts- und Sicherheitstests bei den einzelnen Energieversorgern.

3. Ist – Analyse

3.1 Bestehende IKT-Infrastruktur der Energienetzbetreiber

Die Energienetzbetreiber verfügen über eine bestehende IKT-Netzinfrastruktur für den Betrieb der Erzeugungsanlagen, der Energienetze, der Messeinrichtungen, der Schutzeinrichtungen, der Datenkommunikation, der Telefonie, des Notfallfunkes usw. Die bestehenden IKT-Netze sind mit den Anforderungen des Betriebes, der Sicherheit, der Verfügbarkeit der

Energienetze, entstanden. Dabei wurden von den Energieversorgern entsprechende Investitionen getätigt, welche die Gewährleistung der Einhaltung dieser Anforderungen sicherstellt. Der Notfallfunk hat auch bei einem großflächigen Ausfall des Stromversorgungsnetzes über einen Zeitraum von mindestens 72 Stunden zu funktionieren. Die erforderliche Bandbreite für die Kommunikation und den sich aus einem solchen Krisenfall ergebenden Anforderungen an ein breites Spektrum von Nutzern wurde ebenfalls Folge getragen, wie die Erreichbarkeit an den für die Stromversorgung notwendigen neuralgischen Punkten. Die Anforderung der Kommunikation von Schutz, Steuer, und Regelbefehlen zu den Leitstellen der Energieversorger verlangt ebenfalls eine hohe Verfügbarkeit. Die Verbindungen der Schutzeinrichtungen in den einzelnen Stromnetzebenen sind zeit- und verfügbarkeitskritisch. Dabei ist es erforderlich, dass das zwischen den einzelnen Leistungsschaltern liegende Stromnetzsegment Schutzinformationen im Millisekunden-Bereich erhält. Diese Schutzeinrichtungen dienen nicht nur dem Schutz der Anlagen sondern auch dem Schutz der an den Anlagen arbeitenden Mitarbeitern und dem Schutz der Bevölkerung (z.B. bei Erdschluss durch einen Kran in Stromnetz). Aus diesem Grunde wurden LWL-Verbindungen wegeredundant zwischen den einzelnen Anlagen aufgebaut. Von den bestehenden IKT-Netzbetreibern konnte bis heute ein Teil dieser Anforderung nicht erfüllt werden oder hätte einen enormen zusätzlichen finanziellen Mehraufwand für die Energienetzbetreiber bedeutet.

3.2 Risiken und Anforderungen, welche sich durch die Nutzung einer fremden IKT-Infrastruktur für die Branche ergeben würden

Das von öffentlichen Mobilfunkbetreibern angebotene GSM-Netz ist seit 2008 gehackt und bietet für die Energieversorgungsunternehmen einen eher geringeren Sicherheitslevel für betriebliche Anwendungen. Die weitere Übertragung der Kommunikationsdaten von der BTS (Base Transceiver Station) zur BSC (Base Station Controller) und weiter zum MSC (Mobileservices Switching Centre) erfolgt unverschlüsselt. Zudem ist die Verfügbarkeit einer Mobilfunkanbindung nicht flächendeckend an allen strategisch wichtigen Verteil- und Versorgungsstandorten der Energieversorger gegeben.

Ein Verbindungsaufbau bei GSM-Verbindungen erfolgt durch eine anforderungsbezogene Einwahl auf das bestehende IKT-System des entsprechenden Mobilfunkbetreibers, wodurch es zu Zeitverzögerungen (ca. 10 s) bei kritischen Anwendungen (Schutz usw.) kommt.

Die von den Mobilfunkbetreibern verwendeten Mobilfunkverbindungen sind ein sogenanntes Shared Medium. Hier kann es bei punktuellen Überlastungen zu Abbrüchen der Verbindungen kommen. Ein weiterer Schwachpunkt sind die Übertragungseinrichtungen der Mobilfunk- und Festnetzbetreiber. Diese Übertragungseinrichtungen verfügen größtenteils über keine oder nur mit einer geringen Standzeit versehene Notstromversorgung. Hier würde beim Ausfall des Stromnetzes auch die Verbindung zu dezentralen Inselanlagen, welche ein wesentlicher Vorteil bei einem Netzwiederaufbau sind, fehlen. Damit würden Regelungen, Steuerungen, Messungen und Kommunikationseinrichtungen zu der Netzleitstelle nicht mehr funktionieren.

Die Qualität der Dienstleistung der Mobilfunkbetreiber ergibt bei den heute verwendeten Lastprofilzählern der Energieversorger einen hohen personellen Aufwand für den Betrieb und

die Überprüfung dieser Verbindungen. Bei Störungen kommt es vermehrt zu einer verlängerten Fehlersuche, da zuerst bei den Kunden der Fehler gesucht werden muss (Fehlersuche an den Netzen der Mobilfunkbetreiber, obwohl die Fehlerursache nicht bei den Mobilfunkbetreibern liegt). Dadurch entsteht für die Energienetzbetreiber ein erhöhter Personal- und Finanzaufwand.
Die Datenübertragung vom Zähler in den Zähleinrichtungen ergab aus eigenen Tests mit den in Österreich anbietenden drei Mobilfunknetzbetreibern (A1, T-Mobile, H3G) im Versorgungsgebiet der Energie AG Oberösterreich eine durchschnittliche Erreichbarkeit von 60 %. Ein Grund dafür ist, dass seit Mitte der 70er-Jahre eine ÖVE-Vorschrift für Energieverteilsysteme mit Zähleinrichtung aus technischen und brandschutztechnischen Gründen die Verwendung einer Metalleinhausung für die Zähleinrichtungen fordert. Kunststoffkästen sind erst seit einigen Jahren qualitativ in der Lage, diese Metallkästen zu ersetzen.
Die heutigen Smart Meter sind zum Teil eine Basisinfrastruktur für Smart Grid und die daraus erforderliche Netzautomatisierung und Netzinformation für die Verfügbarkeit und Sicherheit dieser Netze. Diese Netzautomatisierung und Sicherheit muss auch bei großflächigen und längerfristigen Störungen im Stromnetz sichergestellt werden können, was zum Beispiel bei GPRS nicht der Fall wäre. Auch im Falle eines Blackouts ist für den Netzwiederaufbau eine gesicherte Datenverbindung zu den Verteilstationen der Stromnetze erforderlich. Das Zuschalten der wichtigsten Netznutzer, z.B. Polizei, Ärzte, Krankenhäuser usw., zur Gewährleistung der Sicherheit hat in einem solchen Szenario Vorrang.
Die Engpassmanagementfunktionalität (Adressierung aller LSG (Lastschaltgeräte) innerhalb von 20 Sekunden) mit höchster Priorität im Kommunikationsnetz benötigt Zugriff auf hoch verfügbare Datenleitungen zwischen den LSG und über die Bundesgrenzen hinaus zu anderen Stromnetzbetreibern (EU VO 1228/2003). Vorhandene oder vorgesehene Schaltfunktionen in Zählern z. B. für Home Automation usw. dürfen Hackern auf keinen Fall zugänglich gemacht werden. Für Energienetzbetreiber ist daher eine Absicherung dieser durch eine entsprechenden IKT-Netztrennung (eigene Netze ohne Verbindung zum Internet) eine der wesentlichen Voraussetzungen (IKT-Security).

3.3 Smart Grids

Smart-Grid-Tests werden in erster Linie auf Stromnetzebene durchgeführt. Dabei wird auf Schutzeinrichtungen, Frequenzstabilität, Spannungsqualität, Netzbelastung und zusätzliche Speichereinrichtungen in den Niederspannungsnetzen Augenmerk gelegt. Die Informationen zwischen den einzelnen Systemen werden über eine eigene Infrastruktur bis zu einer Stufenregelung auf den entsprechenden Ortsnetztransformatoren geführt. Einige Systeme regeln den Cos-Phi-Faktor an den Einspeisestellen, um die erforderliche Spannungs- und Frequenzstabilität zu gewährleisten. Damit werden in erster Linie Blindleistungsverluste des Niederspannungsnetzes und der angeschlossenen Verbraucher optimiert.
Die Energieversorger betreiben unterschiedliche Netzwerke für den Betrieb der Netzverteilstellen, der Verfügbarkeit des Anlagen- und Personenschutzes, des Smart-Metering-Netzes, der Messwerte aus den einzelnen Erzeugungsanlagen, dem allgemeinen Kommunikationsnetz und dem für den Notbetrieb ausgelegten Funknetz. Dazu sind in allen Verteilstationen

und Endgerätestationen USV-Anlagen installiert, welche eine Mindestnotstromversorgung der vorhandenen technischen Anlagen von 72 Stunden gewährleisten. Die von den Unternehmen von Österreichs E-Wirtschaft für die einzelnen technischen Anforderungen betriebenen Netzsysteme sind gewährleistet durch: am Festnetzsektor zwei getrennte IKT-Netze mit Netzwerkkomponenten von zwei unterschiedlichen Geräteerzeugern, ein Datenfunknetz, ein Betriebsfunknetz, direkte LWL-Verbindungen für Schutz sowie ein DWDM-Netz (Dense Wavelength Division Multiplexing).
Diese Vielfalt der Netze, die Trennung dieser von den kommerziellen Netzen und der eigene Betrieb mit Überwachung der IKT-Infrastruktur und Technik ist ein äußerst wertvoller, schwer finanziell darstellbarer Vorteil beim Betrieb von Energienetzen.

3.3.1 Smart Meter

Zurzeit sind in Oberösterreich mehr als 160.000 Smart Meter im Einsatz. Das dabei verwendete technische Equipment entspricht einem Mindeststandard an Sicherheitsanforderungen nach ISO 27001. Die neue IMA- und IME-Verordnung erfordert den Ausbau und eine weitere Verbesserung der technischen Anforderungen an die dabei verwendeten Anlagen und zusätzliche Sicherheitsanforderungen an letztere.
Die beiden derzeit in Österreich einen Smart-Meter-Rollout durchführenden Unternehmen von Österreichs E-Wirtschaft sind beide ISO 27001 zertifiziert. Andere weitere Unternehmen in Österreich sind dabei, eine entsprechende Zertifizierung nach ISO 27001 durchzuführen.
Die Smart-Metering-Datenübertragung erfolgt von den Kundenanlagen zu den Niederspannungsverteilstationen leitungsgebunden mittels Powerline. Bei den Niederspannungsverteilstationen werden die Daten durch einen Datenkonzentrator jeweils anforderungsbezogen abgerufen und dann gesammelt über die IKT-Infrastruktur der Netzbetreiber zu den Transaktionsservern und von diesen in das entsprechende Meter-Data-Management-System (MDM) eingebunden. Der Zugriff der Kunden erfolgt über das Internet auf einen entsprechenden Webserver über eine Firewall in einer DMZ. Damit ist eine weitere Trennung der Netze gegeben. Die dabei verwendete Dreifachstufung der Netze gewährleistet ein Mindestmaß an Sicherheit und beinhaltet die Bereitstellung der Meterdaten in das MDM-System, die Verarbeitung und Bereitstellung der jeweils kundenbezogenen relevanten Daten weiter in die DMZ und den Zugriff der Kunden auf ihre jeweiligen Daten aus dem Internet. Anbindungen über die Funkschnittstelle mittels eines Shared Mediums (GSM, UMTS, GPRS usw.), welches anforderungsbezogen sich neu verbindet, führt zu zusätzlichen Sicherheits- und Verfügbarkeitsrisiken, welche in die Sicherheitsüberlegungen der Smart Meter miteinzubeziehen ist.

4. Antworten zu den folgenden Fragestellungen

4.1 Welche Initiativen gibt es derzeit noch zu diesem Themenfeld?

Derzeitige Initiativen der Unternehmen von Österreichs Energie sind der Ausbau mit IMA-konformen Smart Metern in Österreich sowie der Aufbau eines Smart Grad und Smart-Meter-Security-Testlabors in Wegscheid. Die Erweiterung der Smart-Grid- und Smart-Meter-

Security in den bestehenden IKT-Netzen und die Gewährleistung dieser Security-Anforderungen und die Einbeziehung späterer Sicherheitsanforderungen in die Planung und die Erweiterung der bestehenden IKT-Netze. Die Mitarbeit in den in Österreich bestehenden und geplanten Projekten für die Erweiterung und der notwendigen Sicherheit von Smart-Grid- und Smart-Meter-Netzen zum Betrieb der kritischen Strominfrastruktur. Aktuelle Projekte sind PRECYSE, Smart Grid Security Guidance (SG²) und Reference Architecture for Secure Smart Grids in Austria (RASSA), Einbringen der Energieversorger von Sicherheitsüberlegungen für kritische Infrastrukturplanung in die Vorgaben des BKA zum Schutz kritischer Infrastruktur sowie in die nationale IKT-Sicherheitsstrategie vom BKA, BM.I und BMF.

4.2 Wie lassen sich Ziele bis 2018 verwirklichen?

Einbringen und Umsetzen der Erkenntnisse aus den Ergebnissen der geplanten, der laufenden und der abgeschlossenen Projekte in Bezug auf den Betrieb kritischer Infrastruktur. Weiterer Rollout der Smart Meter und Einbinden dieser in die bestehende IKT-Infrastruktur. Die Entwicklung der nationalen IKT, welche als Strategiegrundlage den Breitbandausbau im Telekommunikationsbereich hat, darf nicht mit der IKT-Strategie der Energienetzbetreiber vermischt werden. Bei letzterem liegt das Hauptaugenmerk in der Gewährleistung der Versorgungssicherheit und des Betriebs der kritischen Infrastruktur der Energienetze. Der Ausbau der internen energiespezifischen IKT-Infrastruktur zum Betrieb der Energienetze muss beim Bau der Energienetze in einer gemeinsamen Infrastrukturverlegung der Energienetz und der energiespezifischen IKT-Netz des Energieversorgers zum sicheren Betrieb des Energienetzes seinen Einfluss finden. Dabei ist keinesfalls die Mitverlegung der öffentlichen Telekommunikationsnetze angedacht. Hierbei besteht das Risiko, dass bei Störungen an den öffentlichen Telekommunikationsnetzen der Energieversorger nicht mehr an die Infrastruktur des mit dem Energienetz mitverlegten Telekommunikationsnetzes gelangt (Grabungsarbeiten in der Nähe beschalteter Hochspannungsleitungen, in der Nähe von in Betrieb befindlichen Gasleitungen). Zudem gestaltet sich die Mitverlegung mit anderen Infrastrukturen ebenfalls als schwierig. Als Beispiel sei hier eine Mitverlegung mit Nah-Wärmeerzeugern genannt. Sind an den bestehenden Nah-Wärmenetzen neue Kunden anzubinden oder Reparaturen durchzuführen, besteht die Gefahr der Beschädigung der mitverlegten IKT-Infrastruktur. Zudem ist ein zusätzlicher Aufwand in der Grabung bei diesen Arbeiten durch den erschwerten Einsatz von Baumaschinen und den daraus notwendigen manuell erfolgten Grabungsarbeiten festzustellen. Die Infrastrukturtopologie der Energieerzeuger und -verteiler ist eine andere als die der Telekommunikationsnetzbetreiber, weswegen eine gemeinsame Nutzung beider Infrastrukturen wenig Kostenvorteile bringen würde. Als Beispiel dazu ist anzuführen, dass das Stromnetz anders aufgebaut ist als das bereits bestehende öffentliche Telekommunikationsnetz. Leerrohre der Stromnetzbetreiber würden bei der Verwendung für die öffentliche Telekommunikation an vielen Stellen unterbrochen und eine spätere Nutzung durch die Stromnetzbetreiber wäre mit erhöhten Kosten für die Wiederherstellung verbunden.

4.3 Besteht Handlungsbedarf bei diesem Themenfeld?

Beim Ausbau und/oder Umbau der bestehenden Energienetze sollte eine IKT-Infrastruktur zum Betrieb der Energienetze miteingeplant werden. Dabei ist auf eine für den Betrieb und die Sicherheit dieser Netze erforderliche Qualität der Verlegung und Schutz der Dokumentation Bedacht zu nehmen. GIS-Daten sollten nur räumlich begrenzt auf Anfragen zur Verfügung gestellt werden und die Verpflichtung zur Einhaltung der Vertraulichkeit dieser Daten muss gewährleistet sein. Nicht mehr notwendige Informationen sind den Informationseignern zurückzugeben oder zu löschen. Eine Verflechtung der kritischen Betriebsinfrastruktur mit der Telekommunikationsinfrastruktur sollte weitgehend vermieden werden und Übergänge der beiden Infrastrukturen gehören dementsprechend geschützt. Eine breite Diskussion in der Öffentlichkeit wird die kritische Infrastruktur und die Anlagen zum Betrieb dieser weiter in den Blickpunkt der Öffentlichkeit bringen und die Gefahr des Zugriffes Fremder, nicht dem Schutz der Allgemeinheit dienender Personen, erhöhen (d.h. deren Interesse wecken). Eine Vermischung der Investitionen aus dem Energieinfrastrukturbereich und dem öffentlichen Telekommunikationsinfrastrukturbereich könnte zu Querfinanzierungen der beiden Infrastrukturen führen. Der Energieversorger hat die gesetzliche Verantwortung, Energie mit einer hohen Verfügbarkeit und Sicherheit bereitzustellen. Dazu ist es notwendig, die erforderliche Infrastruktur und Ressourcen im gleichen Maße bereitzustellen.

4.4 Was wäre bis 2018 realisierbar?

Ein mindestens 50 % flächendeckender Ausbau des Smart-Metering-Systems in Österreich und einen Teil der für die Zukunft notwendigen Smart-Grid-Infrastruktur vorzubereiten. Die Sicherheit der Smart Meter und Smart-Grid-Systeme weiter voranzutreiben und in einzelnen Projekten wie SG² und RASSA Möglichkeiten sicherer Referenzarchitekturen zu entwickeln. In einzelnen Projekten sind die Smart-Grid-Infrastrukturen auf die sich neu ergebenden Anforderungen der dezentralen erneuerbaren Energieeinspeisung, der Energiespeicherung und der sich daraus ergebenden Anforderungen bezüglich Netzqualität, Sicherheit und Verfügbarkeit weiter zu entwickeln.

4.5 Welche Schritte wären zu setzen, um das Themenfeld voranzutreiben?

Eine klare Unterstützung des Gesetzgebers beim Smart-Meter-Rollout für die Netzbetreiber sowie klare gesetzliche Regelungen für Smart Meter und Smart-Grid-Systeme beim Datenschutz, dem Telekommunikationsgesetz, dem Energiegesetz usw. wäre wünschenswert. Vernetzen der technischen Spezialisten und der Sicherheitsspezialisten der Unternehmen von Österreichs E-Wirtschaft mit den Anforderungen, die sich aus dem APCIP-Programm ergeben, und das Einrichten einer Expertengruppe für die Betreiber kritischer Energie-Infrastrukturen in enger Zusammenarbeit mit der E-Control wäre vorteilhaft. Weiters wäre ein Forcieren und die Förderung von Projekten zwischen Hochschulen, AIT, Hersteller und Energienetzbetreibern für Netzbetreiber und für Österreich als Wirtschaftsstandort von Interesse.

4.6 In welcher Zeit lassen sie sich umsetzen?
Die Umsetzung der Ziele ist von der Entwicklung der Gesellschaft und der Wirtschaft stark abhängig. Man darf davon ausgehen, dass Smart-Grid-Systeme in den nächsten Jahren in sogenannten Pilotgebieten entstehen. Der Zeitraum für ein vorhandenes österreichweites Smart Grid wird noch mindestens 20 Jahre dauern. Der Bau von erneuerbaren Energieträgern, die Integration von Home-Automation-Systemen in den Haushalten, die Bereitstellung von dezentralen Speichereinheiten, der Ausbau der Energienetze und Systeme für die Sicherheit (Schutzeinrichtungen Energienetz, IKT-Schutz), die Netzqualität und Verfügbarkeit sowie viele andere Anforderungen des Umfeldes (gesetzliche, ökologische, ökonomische usw.) lassen auch keine grobe Einschätzung einer Zielerreichungszeit zu.

4.7 Welche Begleitmaßnahmen wären dazu erforderlich?
Die gesetzlichen Rahmenbedingungen für den Ausbau von Smart Grid und Smart-Meter-Systemen müssen als Basis geschaffen werden. Sicherheitsanforderungen für den Betrieb von kritischen Infrastrukturen in Abstimmung zwischen Gesetzgeber und kritischen Infrastrukturbetreibern müssen erarbeitet und in die entsprechenden Gesetze eingebracht werden. Weiters wäre die Bereitstellung von Fördermitteln für Testregionen und Projekten in enger Zusammenarbeit von kritischen Infrastrukturnetzbetreibern, Hochschulen, AIT und Herstellern wünschenswert.

4.8 Welche Ressourcen wären zur Zielerreichung erforderlich?
Der Ressourcenbedarf hängt von den jeweiligen gesetzlichen Anforderungen, den vorhandenen Mitteln, den gewährten Förderungen, der Mitarbeit einzelner Behörden und der Mitarbeit für die einzelnen Programme erforderlichen Unternehmen ab.

4.9 Wer wäre einzubinden?
Smart Meter und Smart Grid sind Anlagenteile für den Betrieb von kritischer Infrastruktur, welche einen für die Bevölkerung hohen Schutzbedarf und eine hohe Verfügbarkeit erfordert. Alleine aus diesem Grunde ist die Einbindung der folgenden Behörden, Institutionen und Unternehmen unerlässlich: BKA, E-Control, BMI, BMVIT, BMWFJ, Österreichs Energie, Energieversorger, KSÖ, Behörden aus dem Kiras-Programm, RTR und Hersteller.

4.10 Wer könnte die Trägerschaft übernehmen?
Die Trägerschaft für den Ausbau und die Schaffung der erforderlichen Rahmenbedingungen für den Betrieb der kritischen Infrastruktur der Energienetze sollte die E-Control als Energieregulator in Zusammenarbeit mit dem BKA und Österreichs Energie übernehmen. Die Aufgaben der E-Control decken einen großen Teil der Anforderungen an Smart Meter und

Smart-Grid-Systeme, wie Förderung nachhaltiger Energieerzeugung, Wettbewerb, Marktregeln (technisch und organisatorisch) schaffen, Versorgungssicherheit gewährleisten und eine Krisenvorsorge treffen, ab. Die Kompetenzzuteilung des Gesetzgebers an die E-Control (Versorgungssicherheit, Nachhaltigkeit, Endkundenservice, Wettbewerb, Netzregulierung, Marktintegration) prädestinieren diese, die Trägerschaft zu übernehmen.

5. Abschlussbemerkung

Eine Verflechtung der beiden Technologien Fernwirktechnik und Internet birgt zusätzliche Gefahren. Der Ausgang der Bedrohung für Smart-Grid-Systeme würde sich durch die Vernetzung in den Haushalt verlagern. Derzeit sind die unterschiedlichen Systeme wie Metering, Fernwirken, Energieaufbringung und Internet getrennt. Ein Übergang zwischen den einzelnen Netzsegmenten und Systemen ist aus sicherheitstechnischen Überlegungen nur durch dafür vorgesehene DMZs möglich. Diese Übergänge (< 1 s) sind meist nicht zeitkritisch, wodurch ein ausreichend schnelles Ansprechen von Schutz, Regelungs- und Steuereinrichtungen gewährleistet ist. Je komplexer Systeme durch Vernetzungen werden, desto größer wird hier die Gefahr von Manipulationen, welche zu einem Black Out führen könnten. Als Ergänzung muss angefügt werden, dass kein System völlig sicher sein kann. Die Übertragungssysteme der Energieversorger sind auf den Notbetrieb und die Wiederherstellung des Energienetzes ausgelegt und erfüllen dadurch die Anforderungen für den Betrieb von kritischer Infrastruktur. Die heute eingesetzten kommerziellen Telekommunikationseinrichtungen hatten in der Vergangenheit keine derartigen Anforderungen, auf Grund dessen der Wirtschaftlichkeit entsprechend, nicht nach diesen Standards gebaut wurde. Eine Umstellung oder Aufrüstung dieser kommerziellen Telekommunikationseinrichtungen würde eine enorme Investition bedeuten, welche aufgrund der bereits vorhandenen sicheren IKT-Infrastruktur der Energienetzbetreiber nicht notwendig ist.

Mit freundlichen Grüßen

DI Dr. Peter Layr
Präsident

Dr. Barbara Schmidt
Generalsekretärin

Österreichs E-Wirtschaft

Brahmsplatz 3
1040 Wien

Tel +43 1 501 98-0
Fax +43 1 501 98-900

info@oesterreichsenergie.at
www.oesterreichsenergie.at

DVR 0422100, UID ATU37583307, ZVR 064107101; UniCredit Bank Austria AG, SWIFT/BIC: BKAUATWW, IBAN: AT 90 1100 0006 4204 1800