Smart Metering & IT-Sicherheit

Bedrohungsszenarien und Lösungsansätze

Hans G. Zeger, Michael Löffler, e-commerce monitoring gmbh

Wien, Österreichische Energieagentur, 28. Oktober 2010

- IT-Sicherheit bei SM
- Sicherheit gem. §14 DSG 2000
- Sonderbestimmungen zur IT-Sicherhheit
- Bedrohungsszenarien
- Lösungsansätze

Was ist Smart Metering?

Begriff hat in Öffentlichkeit sehr breite Ausdehnung - "alles was keine Ferraris-Zähler sind"

Smart Metering im Rahmen dieses Workshops:

- Elektronische Lastaufzeichnung
- Speicherkapazität für mehrere (viele) Datensätze
- zeitliche Synchronisation, frei wählbare Zeitintervalle und Preismodelle
- bidirektionaler Datenverkehr
- WAN - Anbindung, Bereitstellung verschiedener Kommunikationsschnittstellen
- Modular erweiterbar, inkl. Anschluss weiterer SM-tauglicher Geräte
- Möglichkeit Lastnutzung remote steuerbar

Die Funktionalität muss nicht zwangsläufig im Endgerät lokalisiert sein!

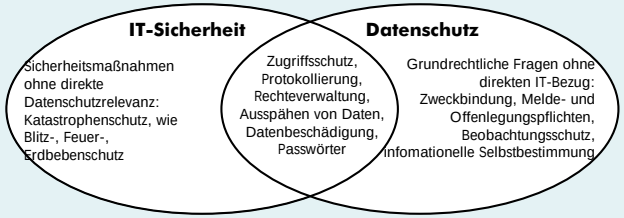
Was ist IT-Sicherheit?

- Sicherung der Authentizität
- Sicherung der Integrität
- Sicherung der Vertraulichkeit
- Sicherung der Verfügbarkeit
  - allgemeine Betriebssicherheit (OS, Applikationen, Geräte, Netzwerk, Operating, Prozesse, ...)
  - Katastrophenschutz

Deliktschutz: betrifft alle Sicherheitsbereiche
Delikte sind nur als ein Auslöser unter vielen anzusehen (andere sind etwa Fahrlässigkeiten, Unwissenheit der Mitarbeiter, Fehleinschätzungen der Geschäftsführung, technische Gebrechen, ...

IT-Sicherheit

Verhältnis von Datensicherheit (IT-Sicherheit) und Datenschutz (Privacy)



IT-Sicherheit behandelt vorrangig
technische Fragen
Was ist machbar? Was ist möglich?
Im Zentrum stehen Abwehrszenarien

Datenschutz behandelt vorrangig
(grund)rechtliche Fragen
Was ist erwünscht?
Im Zentrum stehen Gestaltungsszenarien

DSG 2000 - Sicherheitsbestimmungen

Sicherheitsbestimmungen (§14)

Sicherheitsmaßnahmen haben einen Ausgleich zwischen folgenden Punkten zu finden:

- Stand der Technik entsprechend
- wirtschaftlich vertretbar
- angemessenes Schutzniveau muss erreicht werden

In Österreich gibt es seit 2003 ein "offizielles" IT-Sicherheitshandbuch, das 2007 in Version 2.3 vom Ministerrat empfohlen wurde

DSG 2000 - Sicherheitsbestimmungen

rechtlich-organisatorische Sicherheitsmaßnahmen

- ausdrückliche Aufgabenverteilung
- ausschließlich auftragsgemäße Datenverwendung
- Belehrungspflicht der Mitarbeiter
- Regelung der Zugriffs- und Zutrittsberechtigungen
- Vorkehrungen gegen unberechtigte Inbetriebnahme von Geräten
- **Dokumentationspflicht zur Kontrolle und Beweissicherung**
- **Protokollierungspflicht**

Insgesamt können die Maßnahmen als Verpflichtung zu einer Security-Policy verstanden werden!
z.B. gemäß BSI M 2.192 Erstellung einer IT-Sicherheitsleitlinie

DSG 2000 - Sicherheitsbestimmungen

Protokollierung des IT-Betriebs (§ 14 DSG 2000)

- Protokolldaten dürfen nur eingeschränkt verwendet werden (zur Kontrolle der Zulässigkeit der Verwendung)
- zulässig ist die Verwendung zur Aufklärung von Straftaten, die mit mehr als fünfjähriger Freiheitsstrafe bedroht sind
- Aufbewahrungsdauer ist drei Jahre, sofern gesetzliche Bestimmungen nichts anderes vorsehen
- Frühere Löschung zulässig, wenn betroffener Datenbestand ebenfalls gelöscht ist

DSG 2000 - Verschwiegenheitsverpflichtung

Verpflichtung zum Datengeheimnis (§ 15)

Mitarbeiter sind - sofern nicht andere berufliche Verschwiegenheitspflichten gelten - vertraglich zu binden.

Mitarbeiter dürfen Daten nur aufgrund einer ausdrücklichen Anordnung übermitteln.

Mitarbeiter sind über die Folgen der Verletzung des Datengeheimnisses zu belehren.

Mitarbeitern darf aus der Verweigerung der Befolgung einer Anordnung einer rechtswidrigen Datenübermittlung kein Nachteil erwachsen.

Bereitstellungspflicht der Datensicherheitsmaßnahmen (§ 14 Abs. 6)

spezifische Sicherheitsbestimmungen

Bestehende Sicherheitsanforderungen in Ö

- Verschlüsselung bei Webapplikationen / in der Datenübertragung
  Grundlage: ePrivacy-RL 2002/58/EG
- Besondere Sicherheitsmaßnahmen bei Gesundheitsdaten
  Grundlage: GTelG + GTelVO
- Sicherheit in der elektronischen Rechnungslegung
  Grundlage: EG-RL 2001/115/EG, BMF-Verordnung BGBl 583/2003
- Sicherheitsbestimmungen + Genehmigungsverfahren bei Digitaler Signatur
  Grundlage: EG-RL 1999/93/EG, SigG, SigV
- Einsatz der Bürgerkarte
  Grundlage: E-GovG

spezifische Sicherheitsbestimmungen

Bestehende Sicherheitsanforderungen in Ö II

- Medikamentenabrechnung der Apotheken, Videoüberwachung
  Grundlage: StMV 2004 des Bundeskanzleramtes
- Webapplikationen der Behörden
  Grundlage: Portalverbundprotokoll pvp 1.8.9, eine privatrechtliche Vereinbarung
- Bankomatkassen
  Grundlage: privatrechtliche Vorgaben des Betreibers
- e-card/GINA-Box + Peering-Point der Ärzte
  Grundlage: privatrechtliche Vereinbarungen
- ??????????
  Grundlage: ??????????

Online - Sicherheit

Datenverschlüsselung von Webapplikationen

Keine ausdrückliche Anordnung, jedoch gilt: Stand der Technik, Wirtschaftlichkeit, Angemessenheit (siehe 2002/58/EG Kommunikations-Datenschutz-RL, EG 20, Art. 4)

128bit-SSL/TLS-Verschlüsselung kann heute als defacto-Standard / Stand der Technik angesehen werden, die DSK schreibt ihn in mehreren Fällen vor)

Verwendung von verschlüsselter Datenübertragung bei Webformularen (Analyse 03/2009)

- Webseiten österreichische Anbieter: 6%(II) [ausgewertet: 944 Server]
- Webseiten internationale Anbieter: 15% [ausgewertet:120 Server]

Server in ausgewählten Bereichen:

- Finanzdienstleister (73): verschlüsselt 11 (15%), unverschlüsselt kritisch 13 (18%), unverschlüsselt sonstige 49 (67%)
- Gesundheit (46): V 4 (9%), uV kritisch 7 (15%), uV sonstige 35 (76%)
- Telekom/IT-Dienstleister (729): V 51 (6%), uV kritisch 159 (19%), uV sonstige 591 (75%)

Besondere Sicherheitsmaßnahmen bei Gesundheitsdaten

- Regelung im Gesundheitstelematikgesetz GTelG (2005)
- Umfasst Gesundheitsdaten inkl. Abrechnungsdaten und soziale Daten
- Datenaustausch durch Serverzertifikate abgesichert
- Identitätsnachweis durch Zertifikate oder Zugangsberechtigung
- Datenübertragung im Internet muß verschlüsselt erfolgen
- Dateien sind zu signieren (Integritätsnachweis)

Umsetzung derzeit (Ende 2010) de facto nicht gegeben, da viele Ausnahmen und GTelVO aus 2008 erlaubt Abweichen

Sicherheit in der elektronischen Rechnungslegung

- 2001: EU-RL 2001/115/EG (Mehrwertsteuerrichtlinie)
- 2003: Verordnung 583/2003 des BMF zur elektronischen Rechnungslegung
  - ⇨ elektronische Rechnungen sind fortgeschritten zu signieren oder
  - ⇨ falls mittels EDI-Verfahren übermittelt, ist Sammelrechnung ebenfalls zu signieren oder ausgedruckt zu übermiteln
- 2005: Erlass des BMF zur Verordnung
  - ⇨ regelt u.a. Gültigkeit von Massensignatur, automatisierte Signatur, Signatur durch Dienstleister, ...
- 20??: Ende der unsignierten Fax-Rechnung
- 2011: Ende spezifischer Sicherheitsanforderungen in der Rechnungslegung??

Digitale Signatur

Rechtsgrundlagen:
EG-RL 1999/93/EG "Rahmenbedingungen für elektronische Signaturen"
SigG BGBl. I Nr. 190/1999 + SigVO BGBl. II Nr. 3/2008
E-GovG BGBl. I Nr. 10/2004 "Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen"

Zielsetzung:
Regelt Rechtswirksamkeit digitaler Signaturen:
grundsätzliche Zulässigkeit aller technischer Verfahren,
besondere Rechtswirkung bestimmter Verfahren (§ 3)

Inhalt:
Genehmigungspflicht und Aufsicht durch Behörde bei bestimmten Verfahren ("qualifiziertes Zertifikat"),
Verordnung schreibt bestimmte Techniken vor (Hashfunktionen, Signaturalgorithmen, Erzeugung von Zufallszahlen)

Einsatz der Bürgerkarte

Rechtsgrundlagen:
E-GovG BGBl. I Nr. 10/2004 "Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen"

Zielsetzung:
Regelt Form der "rechtserheblichen" elektronischen Kommunikation (vorrangig mit Behörden)

Inhalt:
Bürgerkarte als "digitaler Ausweis": verknüpft Identitätsdaten, Sicehrheitsdaten und "qualifizierte" digitale Signatur
mit besonderen Bestimmungen der Prüfung des Antragstellers ("Stammregisterbehörde", "Personenbindung")
jedoch: kein Sicherheitskonzept in der Anwendung!
Anwendung der Bürgerkarte nicht geregelt!

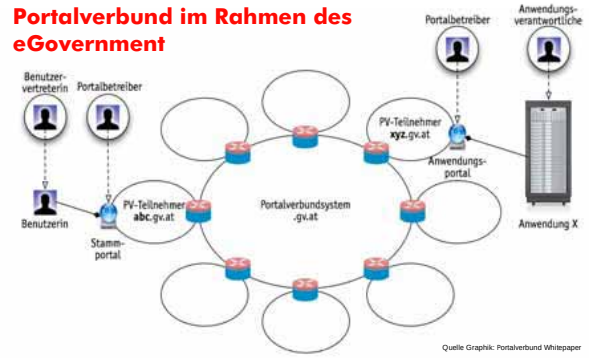
Medikamentenabrechnung der Apotheken / Videoüberwachung - Verschlüsselung

Rechtsgrundlagen:
StMV 2004 des Bundeskanzleramts
(BGBl. II Nr. 312/2004 idgF)

Zielsetzung:
Einhaltung der Sicherheitsbestimmungen gem. § 14 DSG 2000

Inhalt:
SA026 "Verrechnung ärztlicher Verschreibungen für Rechnung begünstigter Bezieher durch Apotheken": Übermittlung der Datensätze an den Empfänger in sicherer, verschlüsselter Form
SA032 "Videoüberwachung": Verschlüsselte Videoüberwachung [gemeint wohl: verschlüsselte Aufbewahrung]

Portalverbund im Rahmen des eGovernment



Viele Anwendungen können über eine einheitliche Schnittstelle benutzt werden.

Was ist der Portalverbund?

- **Zusammenschluss verschiedenster eGovernmentanwendungen**
- **Betreiber: Länder, Ministerien, Körperschaften, ...**
- **Vorteile:**
  - Single Point of Administration: zentrale Verwaltung der Benutzerrechte
  - Single Sign On (SSO): ein Benutzerkennzeichen für alle Anwendungen
  - einheitliches technisches Konzept und einheitliche Betreuung, vereinfachter Betrieb
- **angebotene Dienste (Beispiele):**
  - BMI/ZMR, EKIS, BRZ/Führerscheinregister, Firmenbuch, BMWA/Gewerberegister

Was ist der Portalverbund? II

konzeptionell: "Web of Trust"

technisch: ein Extranet, Umsetzung durch das Portalverbundsprotokoll (derzeit pvp 1.8.9)

datenschutzrechtlich:
- Datenübermittlung im Sinne des §4 Z12
- Informationsverbundsystem gem. § 50 DSG 2000

Rechtsgrundlage: privatrechtliche Vereinbarung

Vereinbarung pvv 1.0 sieht im §9 Sicherheitsbestimmungen vor, insbeondere Konzept der Sicherheitsklassen

Besonderheiten von Smart Meter

- SM ist grundsätzlich ein IT-System, wie viele andere
- muss wartungs- und bedienungsfrei sein
- extrem hohe Zuverlässigkeitsanforderungen, da Fehler-/Ausfall weitreichende Konsequenzen hat
- nicht bloß passives Zähl- und Messsystem, sondern interaktives Steuersystem
- im Gegensatz zum Ferraris-Zähler (keine Datenübertragung) findet bei SM bidirektionale Datenübertragung statt
- Millionenfache Verbreitung praktisch identer Geräte ("Monokultur"), siehe GSM, Satelliten-Dekoder, Spielkonsolen

- Unterschiedliche Interessenslage von Benutzer und Betreiber

Unzureichende technische Verfügbarkeit

- **Defekt des Smart Meters:**
  Ausfall einzelner Komponenten, mangelnde Stromversorgung, Kurzschluss, sonstige elektromagnetische Störungen, ...
- **Probleme bei Datenübertragung:**
  Powerline-Kommunikation (PLC): Entfernung zur Trafostation (300m), Funkstörung
  Festnetz (POTS, xDSL, ISDN): Verfügbarkeit einer fixen Anbindung, Abhängigkeit von Dritt-Betreiber
  Mobilnetz (GSM, GPRS, UMTS): Funkstörungen, "Funklöcher", Abhängigkeit von Dritt-Betreiber
- **Datenverlust bei der Weiterverarbeitung:**
  Absturz/Ausfälle der Webapplikationen/Hardware, Bedienfehler der Mitarbeiter (z.B. Löschung von Datensätzen, ...),

[- **Kommunikation von Endgeräten mit Smartmeter:**
Funkstörungen]

Manipulationen durch den Benutzer

Ziel(e): Manipulation (Senkung) des Stromverbrauchs, Wiedereinschaltung von Geräten, Erhöhung des zulässigen Verbrauchs, Veränderungen der Verbrauchsmuster (Blindstromanteil), Vortäuschen einer Rückspeisung

- hardwartechnische Manipulationen
  Beispiele: Kurzschluss des Zählers mit Besteck, Kabel
- softwaretechnische Manipulationen
  Beispiele: Abfangen von übermittelten Zählerständen, Rücksetzen von Zählerständen
- energietechnische Manipulationen
  Beispiele: Absenken der Versorgungsspannung des SM auf 160-180V (Manipulationen der Zuleitungen)

Manipulationen durch Betreiber (Mitarbeiter)

Ziel(e): Ausgleich von Verbrauchsschwund, Frustabbau, Optimierung von Erlösen, ...

- unberechtigte Abschaltungen/SM-Eingriffe
- Manipulationen an den übermittelten Datensätzen
- Manipulation an den Systemzeiten

Manipulationen durch Dritte

Ziel(e): Störung der Verfügbarkeit der Energieversorgung allgemein, Vertrauensverlust gegenüber Stromlieferanten, gezielte Schädigung "unliebsamer" Personen

- DoS- oder DDoS-Attacken gegen SM-Geräte
  Risiko/Relevanz: hoch (bisher keine direkten Erfahrungen)
- direkte Manipulation der Software des SM-Geräts
  Risiko/Relevanz: hoch (vergleichbare Systeme werden durch Ausspähen hardcodierter Passwörter geknackt)
- Unterdrücken der Datenübertragung vom SM-Gerät
  Risiko/Relevanz: hoch (bisher keine Erfahrungen, Konsequenz? Stromabschaltung?)
- Wurm-/Trojaner-Angriffe auf SM-Steuerung (SCADA-Schnittstelle)
  Risiko/Relevanz: hoch (mit STUXNET seit 7/2010 erste Erfahrungen, Gegenmaßnahmen derzeit schwer zu implementieren)

Manipulationen durch Dritte II

- Ausspähen/Manipulieren der Kommunikation zwischen Endgeräten und SM-Gerät
  ZigBee-Standard ähnlich leicht zu knacken wie WLAN-WEP
  Risiko/Relevanz: hoch
- Manipulation der übertragenen Daten
  Risiko/Relevanz: derzeit gering (keine Vorfälle bekannt, ist technisch gut beherrschbar)
- DoS- oder DDoS-Attacken gegen Web-Portale / Weiterverarbeitung der Daten
  Risiko/Relevanz: hoch (häufiges Phänomen, kann durch technische Maßnahmen gut abgefangen werden)
- SQL Injection
  Risiko/Relevanz: hoch (häufiges Phänomen, kann durch Softwareengineering vermieden werden)

Manipulationen durch Dritte III

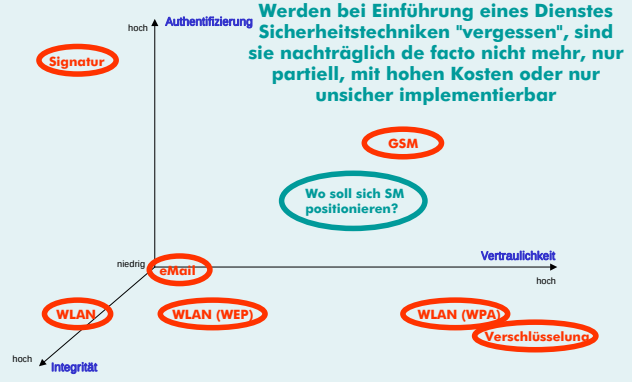
- Phishing-Attacken gegen Infoportale
  Risiko/Relevanz: hoch (häufiges Phänomen, kann durch organisatorische Maßnahmen vermieden werden)
- Spam-Attacken über Infoschnittstellen
  Risiko/Relevanz: hoch (kann durch geeignete Protokolle/Signaturen vermieden werden)

Beobachtungen bei Einführung vergleichbarer Techniken

- GSM-Daten mithören
  Schwachstelle: verwendete A5/1-Verschlüsselung kann vorberechnet werden (2 TB-große Tabelle mit allen Schlüsseln)
- WLAN
  Schwachstelle: WEP schwache Verschlüsselungsverfahren
- eMail
  Schwachstelle: keinerlei Authentifizierungs-, Integritäts- und Vertraulichkeitsmechanismen
- Bluetooth
  Schwachstelle: Session-Schlüssel kann angestoßen / mitgeschnitten werden, Brutforce-Attacke besonders bei Handys mit bloß 4-Ziffern-Passwort leicht; Handys von Nokia, Panasonic, Siemens und Sony Ericsson wiesen Sicherheitslücken auf

Beobachtungen bei Einführung vergleichbarer Techniken II

- TV-/Satelliten-Decoder/Spielkonsolen/Kopierschutz
  Schwachstelle(n): hardcodierte Schlüssel/Passwörter, zu kurze Passwörter, zu viele Passwörter, Insiderinformationen, umgehen des Passwortschutzes
- DVD: 40-bit Schlüssel aller Hersteller auf allen DVDs vorhanden, 1. Schlüssel durch Insiderinformationen bekannt, Gesamtsystem wegen unverschlüsselter Abspeicherung auf Software eines DVD-Players (Dauer: einige Wochen nach Markteinführung)
  Siehe auch Siemens SCADA-System: hardcodiertes PSW im Internet jahrelang veröffentlicht
- iPhone: (starke) 256-Bit-AES-Verschlüsselung kann umgangen werden, wen iPhone vorab mit Ubuntu-Linux-Distribution hochgefahren wird
- digitale Signatur nach X.509v3, Verschlüsselung RSA, EC
  Schwachstelle: bisher keine bekannt



Sicherheitsstandards (IT-seitig)

- Kryptographische Verfahren (Bauteile)
  Standard (Beispiel): NIST FIPS 140-2 (Level 2)
  Beschreibt soft- und hardwaretechnische Anforderungen beim Erzeugen, Verwalten und Verwenden von kryptographischen Systemen (Level 2 = geeigneter Algorithmus + manipulationsgeschützte Hardware)
- Gerätesicherheit
  Standard (Beispiel): CommonCriteria V3.1 (EAL 4)
  Bewertet die Qualität und Funktionalität eines IT-Systems, wobei verschiedene Prüftiefen definiert werden (EAL 4 = System wurde methodisch entwickelt, getestet und durchgesehen)

Sicherheitsstandards (IT-seitig) II

- Betriebssicherheit
  Standard (Beispiel): ISO 27001
  Beschreibt ein Sicherheitsmanagementsystem und umfasst sowohl technische, als auch organisatorische Aspekte
- Kommunikations-/Übertragungssicherheit
  Standard (Beispiel): SSL/TLS (rfc2818), WPA/WPA2 (IEEE 802.11i), ...
  SSL/TLS beschreibt auf Transportebene Sicherheitsanforderungen und dient zur Absicherung der Datenübertragung, heute bei Internetverbindung "defacto"-Standard
  WPA/WPA2 beschreibt die Übertragungssicherheit in WLAN-Netzen

Sicherheitsstandards (IT-seitig) III
Sicherheit von Web Applikation

ÖNORM A 7700 ("Sicherheitstechnische Anforderungen an Webapplikationen")

Regelt unter anderem
- Architektur der Web-Applikation
- Authentisierung und Sitzungsmanagement
- Formulare und andere Benutzereingaben
- Ausführung externer Programme
- Datenbanken
- System-/Fehlermeldungen
- Kryptographie

ÖNORM A 7700 ist Nachfolge der ONR 17700

Es kann auch ein staatlich anerkanntes Zertifikat erlangt werden derzeit sind drei Anwendungen nach ONR 17700 und zwei nach ÖNORM A 7700 zertifiziert (Stand FJ 2010)

Sicherheit und Smart-Meter im Blickwinkel bestehender Regelungen

Regelungen:
- Richtlinie 2009/72/EG - gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt
- Elektrizitätswirtschafts- und –organisationsgesetz - ElWOG - StF: BGBl. I Nr. 143/1998 (inkl. Entwurf 2010)
- Maß- und Eichgesetz - MEG - StF: BGBl. Nr. 152/1950

Sicherheitshinweise:
- Sicherheit meist auf Versorgungssicherheit reduziert
- sonstige Sicherheit abstrakt beschrieben: Art. 2 Z 28 2009/72/EG bzw. § 7 Z 35b ElWOG „Sicherheit“ sowohl die Sicherheit der Elektrizitätsversorgung und -bereitstellung als auch die Betriebssicherheit;"
- 2009/72/EG Art. 42 Ermächtigung für nationale Sicherheitsmaßnahmen

Sicherheit und Smart-Meter im Blickwinkel bestehender Regelungen II

Sicherheitshinweise:
- ElWOG neu: Verordnungsermächtigung (§ 19, jedoch ohne Informationssicherheit)

Smart-Meter:
- ElWOG neu: SM als bidirektionales System definiert (§ 7 Z 33)
- ElWOG neu: Verordnungsermächtigung der Regulierungsbehörde bei SM-Einsatz + Vorgaben zur Ausstatung (§ 83, jedoch keine Hinweise auf IT-Sicherheitsvorgaben)
- ElWOG neu: Informationsverpflichtung bei SM-Einsatz über das Internet (§ 84, jedoch keine Sicherheitsvorgaben)

Berichtspflicht & Messdaten:
- ElWOG neu: Mindestverpflichtung in Ablese + Plausibilitätskontrolle bei Benutzerablesung (§ 57 Abs. 4, jedoch keine Sicherheitsmaßnahmen bei elektronischer Übertragung)
- ElWOG neu: Bereitstellung von Angaben zur Datenqualität (§ 40 Z 17, jedoch keine Vorgaben zur Mindestqualität)

Derzeit existiert keine Gesamtkonzeption zur IT-Sicherheit bei Smart Meter

Geregelt ist etwa die Mess- und die Störungssicherheit bei PLC

Rahmen einer rechtliche Regelung
- grundsätzliche Regelung des SM-Einsatzes im ElWOG
- laufende Anpassung der technischen Sicherheitsanforderungen durch Verordnung (analog SigV oder GTelVO)
- Verpflichtung zu bestimmten organisatorischen Maßnahmen (2 * 4-Augen-Prinzip bei zentralen Verarbeitungsbereichen)
- Typisierung und Zulassung der Systeme durch Aufsichtsstelle (analog: Signaturerstellungseinheiten und Zertifizierungsdienstanbieter)

Mögliche sonstige Problemstellungen
- Vertragsprobleme bei Nutzung des Internetanschlusses des Strombeziehers für Übertragung der SM-Daten

Alternative zu Smartmeter?

- Verwendung "einfacher"/"halb"intelligenter elektronischer Zähler
- Beispiel: Zähler modular konzipiert, Basis ist der "EDL21"-Zähler gemäß Spezifikation EnWG § 21b (D)

reduzierte Funktionalität:

- beschränkte Aufzeichnungsmöglichkeiten (im Stundentakt), Summierungsmöglichkeiten (1 Tag, 1 Woche, 30 Tage, 1 Jahr)
- vereinfachte Tarifmodelle (nur zwei möglich)
- keine Zeitsynchronisation
- keine Anbindung an Datenleitungen

jedoch:

- HMI-Interface für PIN-Eingabe, Sperren usw ("optischer" Taster)
- maschinelles Auslesen der Daten möglich (Infrarot-Schnittstelle)
- Integrität wird durch Signaturverfahren gesichert (asymetrisch, ECC192Bit)
- 2 getrennte Schnittstellen (für Betreiber und für Kunden)

Konsequenzen mangelhafter SM-Sicherheit

- Verwaltungsstrafe: nach DSG §52 Abs. 2 Verwaltungsübertretung mit Strafe bis 10.000 Euro
- Zivilrechtliche Haftung: Unternehmen bzw. Dienstnehmer könnten für Folgeschäden haften, auch Gehilfenhaftung
- UWG-Verfahren: Mitbewerber könnten fehlende Sicherheitsmaßnahmen als Versuch eines unlauteren Wettbewerbsvorteils einklagen
- immaterieller Schadenersatz: bei prangerartigen oder bloßstellenden Folgen §33 DSG, §1328a ABGB, Medienrecht
- Strafrecht: bei vorsätzlichen Handlungen (es genügt Schaden wird bewusst in Kauf genommen), z.B. §51 DSG, §§ 302/310 StGB, §§ 119/a StGB
- Imageschaden: Vertrauensverlust von Kunden und Öffentlichkeit

Ich danke für Ihre Aufmerksamkeit