



Sicherheit und Datenschutz Voraussetzung für erfolgreiches Smart Metering.

Frankfurt, Juni 2010

Erleben, was verbindet.



Smart Metering & Home Management.

Abgrenzung Datenschutz und IT-Sicherheit.



Im Gegensatz zu anderen Rechtsprinzipien gilt beim Datenschutz:
„Was nicht erlaubt ist, ist verboten!“

Wie bei allen Innovationen muss ein Smart Metering Markt erst einmal entwickelt werden, d.h. Vertrauen in Lösungen aufbauen.

Daher stellt sich auch die Frage der Informationssicherheit sehr früh.

Am meisten überzeugt es daher, wenn man „privacy by design“ praktiziert, also Datensicherheit und Datenschutz in den Designprozess der Produkte und Dienstleistungen einfließen zu lassen.



Smart Metering & Home Management.

Datensicherheit – Die konkreten Herausforderungen.



Smart Metering & Home Management.

Datenintegrität.

Veränderung

- Schutz vor Manipulation von Daten durch interne und externe Angreifer.
- Verbrauchsdaten dürfen bei der Übertragung zwischen Zähler und Auslesegerät bzw. Zähler und Leistungsanbieter nicht manipuliert werden können.

Beschädigung

- Korrekte Übermittlung der Daten vom Zähler über den Multi Utility Server und das Smart Metering System zum Leistungsanbieter.
- Daten müssen auch bei schlechter Leitungsqualität korrekt übertragen werden können. Prüfziffern zur Kontrolle und Verifikation nach Übertragung. Validation vor der weiteren Verarbeitung

Zerstörung

- Verhinderung des Datenverlustes
- durch ein örtlich getrennte Speicherorte (MUS und zentrales System)
- Sicherungskopien relevanter Verbrauchsdaten nach erfolgreicher Übertragung an Auftraggeber für 30 Tage.



Smart Metering & Home Management.

Vertraulichkeit

Alle Komponenten und „Rollen“ müssen im System authentifizierbar sein.

Zähler in Verbindung mit einer eindeutigen Identität. Nutzer, Administrator, Provider 1..n, Zentrale, etc. über Rollen-Zertifikate

Unterbindung eines unbefugten Fernsteuerns von Hausfunktionen.

Zu keinem Zeitpunkt darf ein unbefugtes Fernsteuern von Hausfunktionen möglich sein (Gefahr für Leib und Leben).

Datensparsamkeit.

Daten, die nicht definitiv zum Zweck der Weiterverarbeitung benötigt werden bzw. vom Endverbraucher dazu frei gegeben wurden, werden nicht in das zentrale System übertragen.



Smart Metering & Home Management.

Verfügbarkeit

Für alle in der Prozesskette eingebundenen IV-Systeme besteht ein durch den Datenschutz der Telekom freigegebenes Datenschutzkonzept, in dem u.a. die technischen und organisatorischen Maßnahmen zum Datenschutz detailliert beschrieben werden.

Bezogen auf Verfügbarkeit sind dies:

- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Getrennte Verarbeitung



Die Umsetzung der Datenschutzvorgaben innerhalb der Deutschen Telekom wird regelmäßig überprüft.



Smart Metering & Home Management.

Schutz von personenbezogenen Daten und von Verbrauchsdaten

Der Datenschutz schützt jeden Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informelle Selbstbestimmung beeinträchtigt wird.

Schutz personenbezogener Daten.

Unbefugte dürfen niemals Zugang zu personenbezogenen Daten erhalten.

Schutz von Verbrauchsdaten.

Eine unbefugte Überwachung und Auswertung des Nutzungsverhaltens darf zu keinem Zeitpunkt möglich sein.

Stufe A: frei zugängliche Daten, sobald sie einmal veröffentlicht wurden

Stufe B: personenbezogene Daten, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist

Stufe C: personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann (Stichwort: Beeinträchtigung des Ansehens)

Stufe D: personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann (Stichwort: soziale Existenz)

Stufe E: Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann (Stichwort: physische Existenz)



Penetrationstests

Anforderungen der Telekom Security und empfohlene Maßnahmen für den MUS.

System Plattform

- Die Anwendung muss auf einer 3-Schicht Architektur basieren (Präsentationsschicht, Anwendungsschicht, Datenbankschicht).
- Die verschiedenen Schichten der Anwendung müssen in getrennten Netzwerken mit dazwischengeschalteten Firewalls realisiert werden.
- Die Präsentationsschicht muss in einer physikalisch getrennten DMZ umgesetzt werden (Hintergrund: Bedrohungslage vgl. Internet).

Multi Utility Server

- Erhöhung des baulich technischen Schutzes
Meldekontakt bei Gehäuseöffnung, Vergiessen des Gerätes, Verklebtes bruchfestes Gehäuse
- Architektur-Änderung
Implementation eines Speichers der die sichere Speicherung von Zertifikaten / Schlüsseln (PKI) erlaubt
- Funktionsänderung
Update der Firmware nur durch vom Hersteller signierte Firmwarepakete möglich, Härtung von Betriebssystem und Applikationen (z.B. Buffer Overflow Protection, Patchlevel der Applikationen, Sichere Konfiguration), Absicherung des Bootloaders
- Kommunikation zwischen MUS und Smart Metering System Plattform über einen geschützten Kanal (Verhinderung von Man in the Middle Attacks)



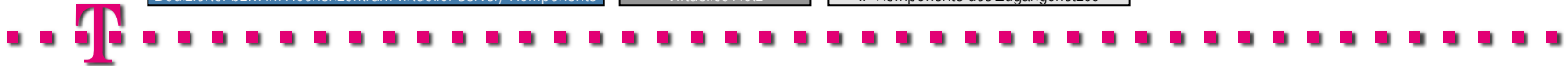
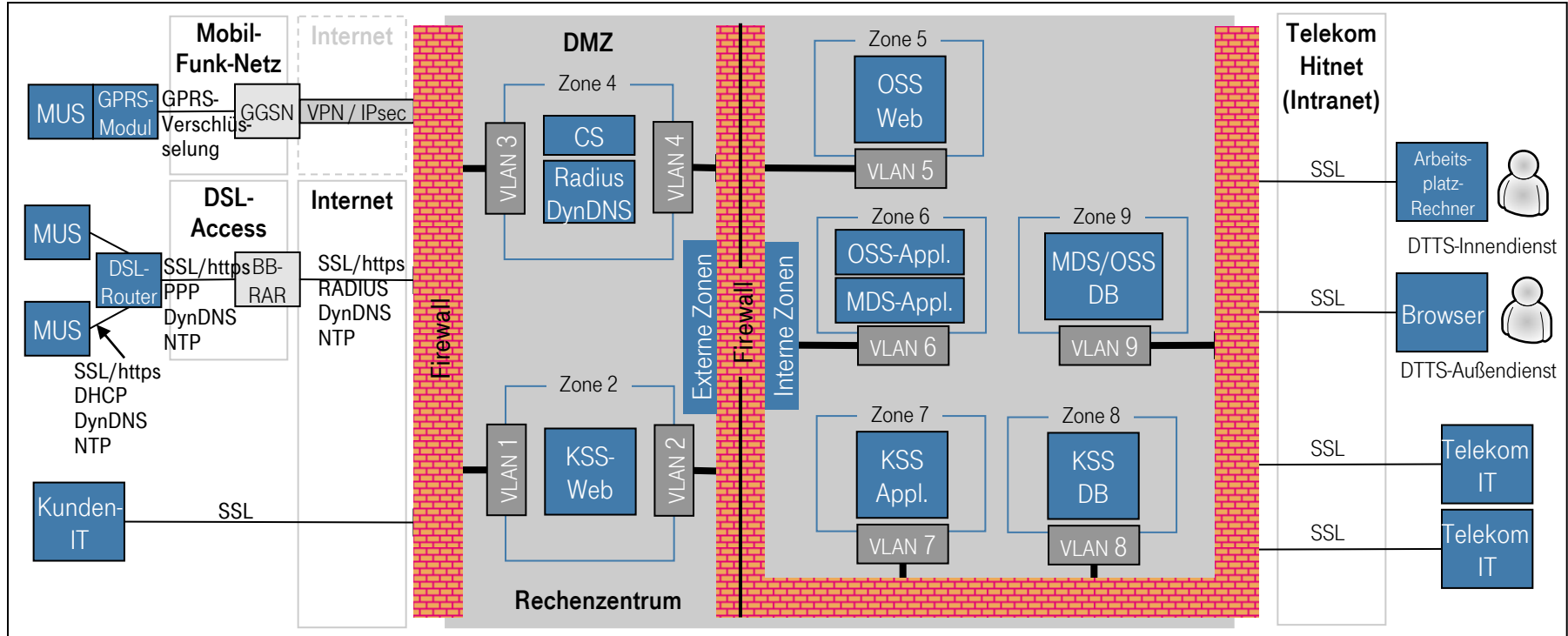
Systemplattform und Netzarchitektur.

Netz- und Übertragungssicherheit.

Öffentliche bzw. Fremdschnittstellen

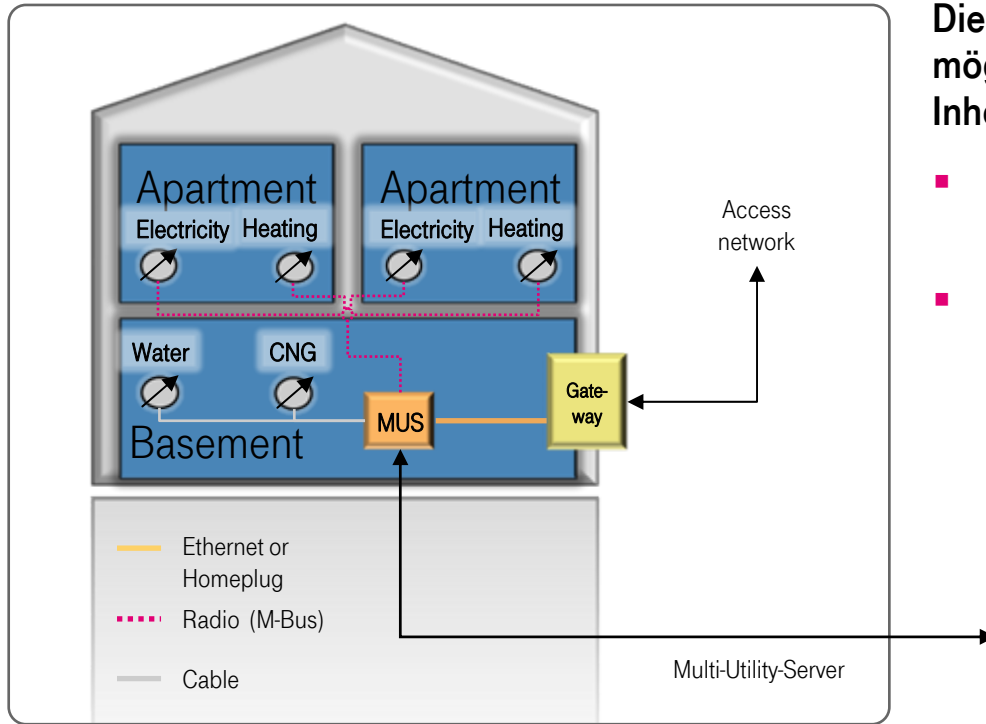
Smart Metering Core System

Allgem. Telekom Systemwelt



Das Inhaus - Konzept.

Sowohl der MUC, als auch der Multi-Utility-Server erfordert in der Informationskette besondere Beachtung



Die folgenden Angriffs-Vektoren sind theoretisch möglich und werden daher in die Betrachtung des Inhouse Konzeptes einbezogen:

- Angriff auf den MUS mit dem Ziel der Datenmanipulation / Informationsgewinn
- Angriff auf den MUS mit dem Ziel die Metering Plattform zu attackieren



Vielen Dank für Ihre Aufmerksamkeit.
Besuchen Sie uns am Stand oder im Internet
www.telekom.de/smartmetering.





Peter H. Wiesner
Leiter
Technik und Betrieb Smart Metering

Deutsche Telekom Technischer Service GmbH

Hausanschrift Bernkasteler Str. 8, 53175 Bonn
Telekontakte Telefon +49 228 181 65328
E-Mail peter-heinz.wiesner@telekom.de

