Sind Smart Meters und ihre Umgebung sicher?

Chancen & Risiken

Dr. Jens Oberender

22. August 2018

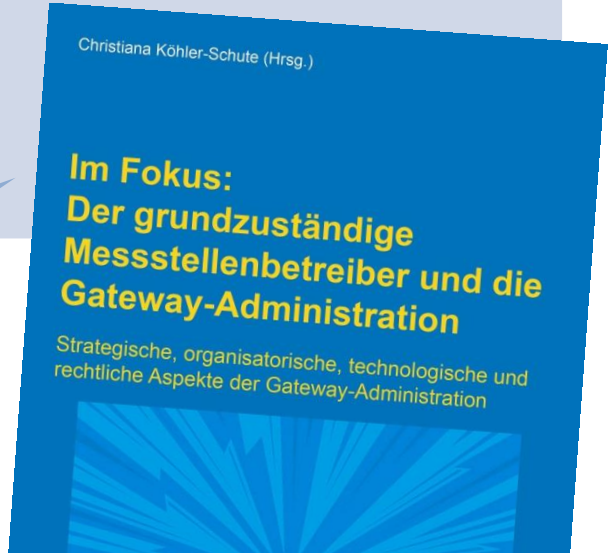
Sind Smart Meters und ihre Umgebung sicher?

- **Perspektive Sicherheit & Bedrohungen**
- **Risk Breakdown**
- **Chancen & Risiken**
  - **Vorgaben**
  - **Common Criteria Zertifizierung**
  - **Ökonomie**
- **Ausblick**

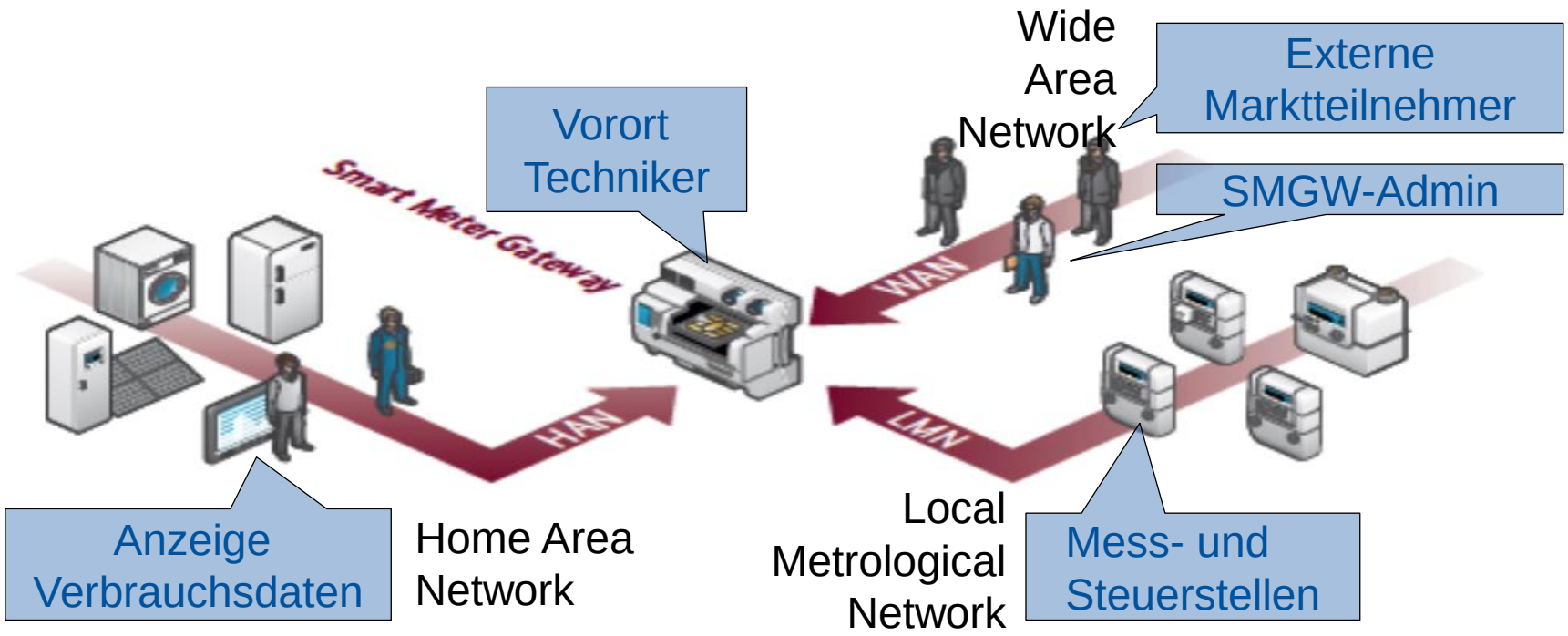
Kurzvorstellung

Jens Oberender	SRC Security Research & Consulting GmbH
• Leitung ‚Evaluation kommerzielle Produkte‘ Hintergrund • Dipl.-Informatik • Promotion: Privacy in Netzwerken	Common Criteria • Angriffsbewertung AVA_VAN.5 gegen Security Modules • Öffnen von Siegeln und SMGW Gehäusen ISMS Beratung TR-Prüfungen

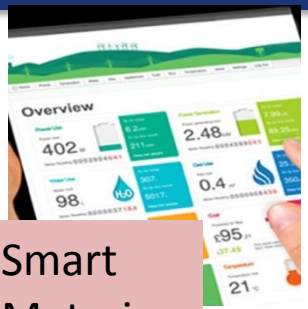
mit Beitrag von Dr. Deniz Ulucay/SRC
08/2018 erschienen



Das Smart Meter Gateway im **Einsatz**



Was bedroht den Einsatz von Smart Metering?



Smart Metering

Smart Meter Gateway

Security Module

Infrastruktur SMGW-Admin

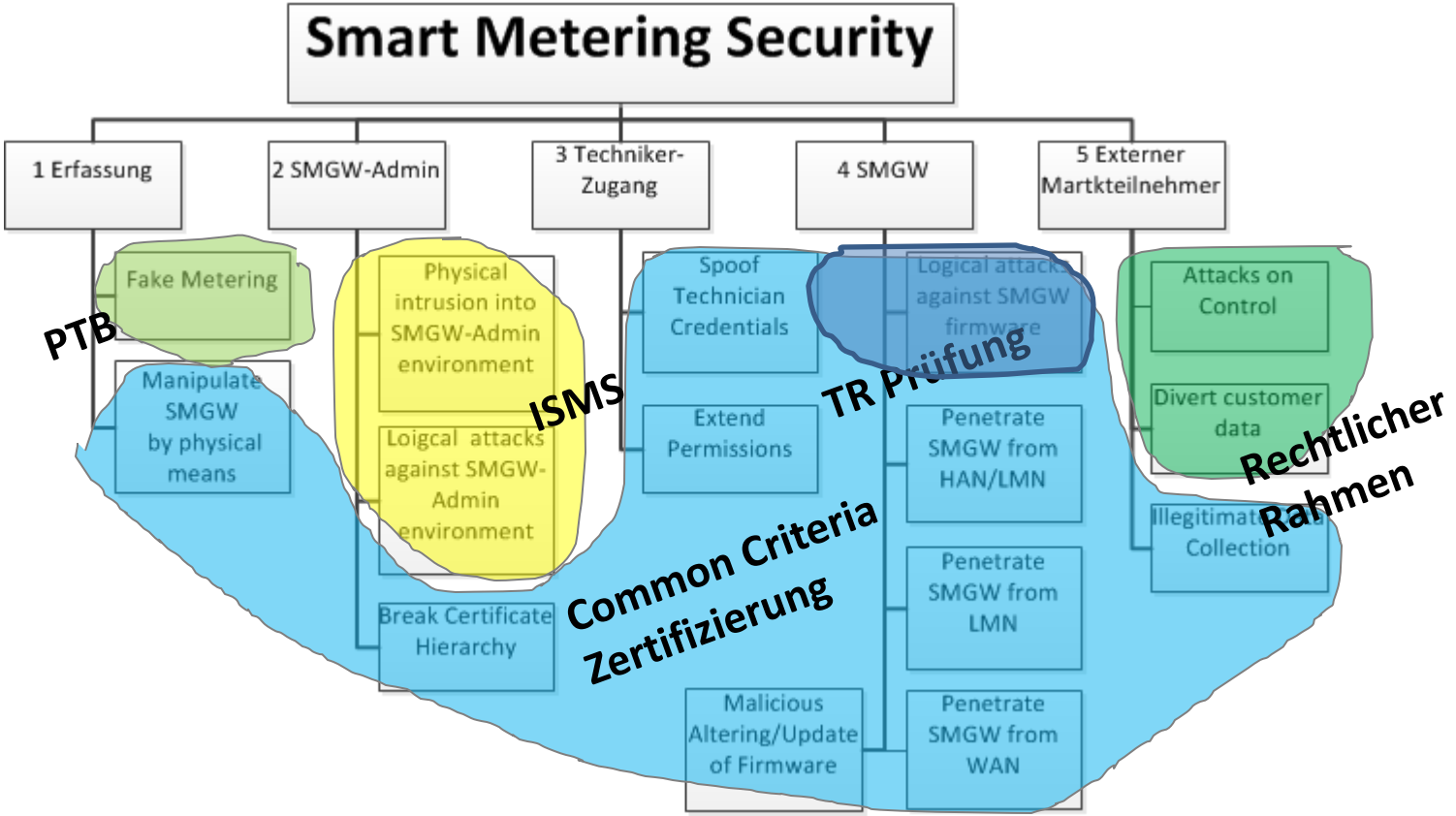
- **Verletzung der Privatsphäre**
  - **Auslesen des Stromverbrauchs**
- **Missbrauch per Fernverwaltung**
  - **Stromabschaltung**
  - **Sabotage SMGW-Admin**
- **Verfälschte Abrechnungsdaten**

Abwesenheit, Fernsehkanal, Lebensgewohnheiten

Deutschlandweiter Blackout

Eichrecht, Abrechnungen anfechtbar

Risk Breakdown Structure



Chance & Risiko I
Vorgaben

Chance/Risiko	Eintrittswahr-scheinlichkeit	Auswirkung	Sensibilität der Stakeholder	Maßnahmen
Manipulation Messeinrichtung / intelligentes Messsystem	Gering	Gering	Gering	PTB fordert **Verplombung**
PKI	Gering	Sehr hoch	Hoch	kryptographischen Anforderungen
Missbrauch SMGW-Admin	Gering	Hoch	Hoch	**ISMS** gefordert

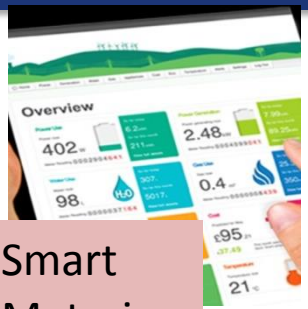
Chance & Risiko II
Common Criteria Zertifizierung

Chance/Risiko	Eintrittswahr-scheinlichkeit	Auswirkung	Sensibilität der Stakeholder	Maßnahme: Common Criteria Zertifizierung
Verwundbare Implementierung	Mittel	Gering	Mittel	**Schwachstellenbewertung**
Sichere Produktionskette	Gering	Hoch	Gering	**Sicherheitsaudits** bei der Einbringung des Sicherheitsmoduls
Missbrauch Technikerzugang	Mittel	Gering	Gering	**Berechtigung**skonzept
Angriffe auf SMGW	Mittel	Gering	Hoch	Schlüssel in ein hochsicheres **Security Modul** ausgelagert; Untersuchung berücksichtigt alle Schnittstellen
SMGW interner Webserver	Hoch	Gering	Mittel	**Unumgehbarkeit**; begrenzte Scripting-Fähigkeit Client/SMGW
Datenschutzverstöße	Mittel	Hoch	Mittel	zulässige **Aggregation** (Vorgabe TR)

Chance & Risiko III
Ökonomische Perspektive

Chance/Risiko	Eintrittswahr-scheinlichkeit	Auswirkung	Sensibilität der Stakeholder	Maßnahmen
Erschließung neuen Marktes	Hoch	Hoch	Hoch	Wettbewerb forciert
Einhaltung Liefertermine	Mittel	Hoch	Hoch	zusätzliche Ressourcen im BSI
Gesteigerte Produktattraktivität	Hoch	Gering	Gering	Enge Vorgaben
Fortschritte Netzsteuerung	Gering	Hoch	Mittel	Rollout bereitet Boden für **zukünftige Funktionalität**

Quo vadis SMGW Sicherheit?



Smart Metering

Smart Meter Gateway

Security Module

Infrastruktur SMGW-Admin

- Komplexes Konstrukt für Politik, Behörden und Industrie
  - Änderungen für Prüfspezifikation erfordern Re-Zertifizierung
  - Schwieriges Umfeld für Innovation
- **Zertifizierte Sicherheit**
  - Begrenzte Gültigkeit des Zertifikats; Klärung zur Nutzung darüber hinaus
  - Bewertung **neuester Kenntnisse und Angriffsmethoden**

Danke für Ihre Aufmerksamkeit!

SRC
Dr. Jens Oberender
Security Research & Consulting GmbH
Emil-Nolde-Straße 7
53113 Bonn

Tel. +49-(0)228-2806-100
Fax: +49-(0)228-2806-199
E-mail: jens.oberender@src-gmbh.de
WWW: www.src-gmbh.de