genua Ein Unternehmen der Bundesdruckerei

Neuartige Anforderungen an IT-Sicherheit im Rahmen der digitalen Transformation der Energiebranche

Fachkongress AK Energie

Kai Dörnemann
28.6.2017

Wer bin ich?

genua Ein Unternehmen der Bundesdruckerei

- genua – 25 Jahre IT-Sicherheit

- **Produkte:** Firewalls, VPN, industrielle Fernwartung, mobile Sicherheit

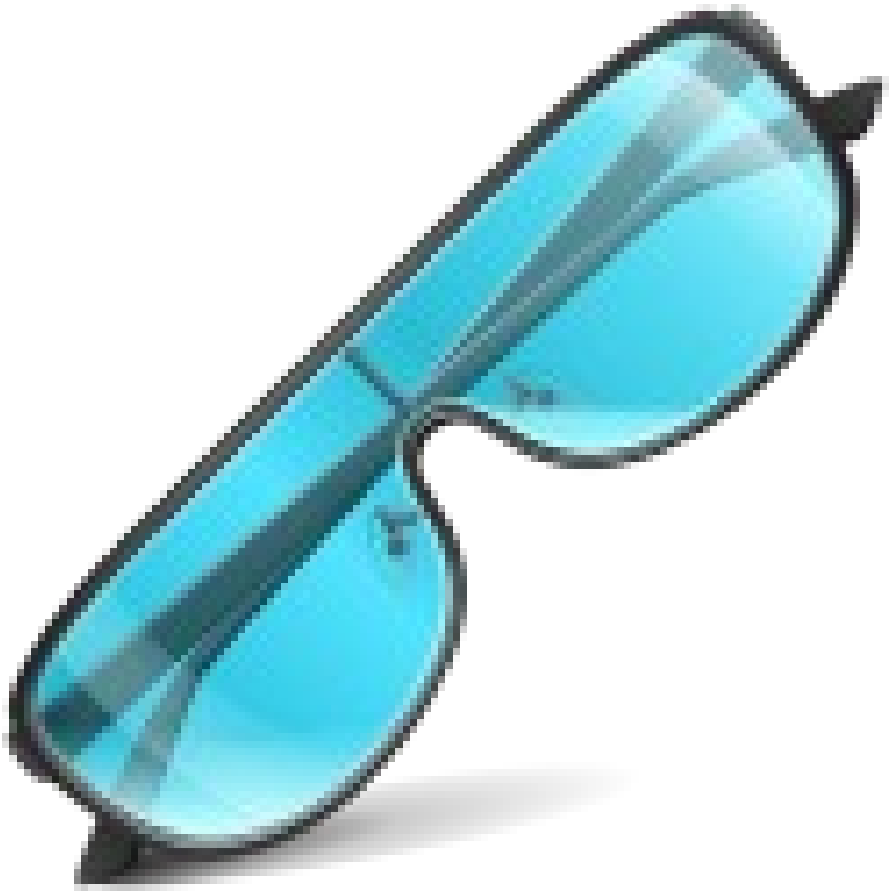



- meist zertifiziert nach CC EAL-4(+) / zugelassen für VS-NfD durch BSI

- **Unsere Kompetenzen:** Entwicklung sicherer Software, Betriebssysteme, Implementierung und Anwendung von Kryptografie, Netzwerke und Protokolle

genua Ein Unternehmen der Bundesdruckerei

IT-Security Brille



Warum Smart Grid?

© IAEA Imagebank, flickr

- viele kleine Erzeuger
- Dezentralisierung
- Wetterbedingte Schwankungen
- Einbindung externer Datenquellen und Sensoren
- → Exaktere Steuerung via IP-Netzwerk notwendig

- wenige große Erzeuger
- einfache Steuerung über z.B. Netzfrequenz
- Schwankungen vorhersehbar und leicht auszugleichen

© www.CGPGrey.com

Smart Grid → Smart Problems?

genua Ein Unternehmen der Bundesdruckerei

- viel IT ausserhalb des Rechenzentrums, hohe „Angriffsfläche“
- großes Meß-/Steuer-/Regelnetzwerk
- Mehr Komplexität
  → mehr Angriffsmöglichkeiten
  → mehr Fehlerquellen
  → Fehler werden durch „Schlamperei“ eines Teilnehmers möglich

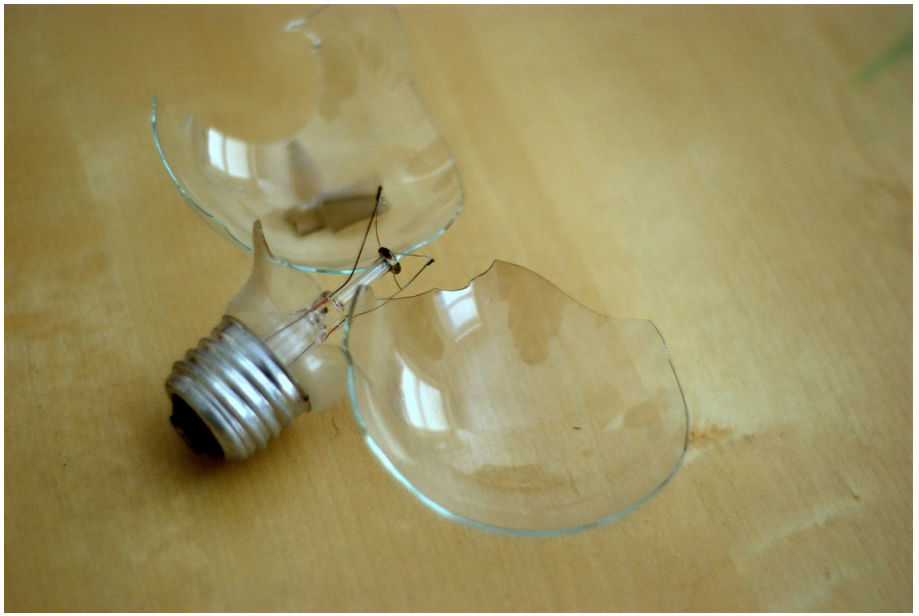
© jrladia, flickr.com

- Verbindung mit Internet ist kostengünstig, lädt aber neue Angreifer ein. Zudem gibt es immer wieder Ausfälle/Missgeschicke.
- Kommunikation via IP
  → es wird viel Software benötigt (OS, IP-Stack, httpd, App-Srv, …)
  → Systeme sind anfällig für CVEs etc.
- Datenschutz und Sicherheit sind schwerer herzustellen
- IT-Sicherheit ist Top-3-Thema der Digitalisierung [1]
- DE: KRITIS-Gesetz (BMI), Smart-Meter TR-3109 (BSI), ...

Wird etwas schiefgehen?

genua Ein Unternehmen der Bundesdruckerei

- Ja.
- Komplexität ist der Feind von Security.
- SmartGrid für Hacker attraktiv:
  - Dinge kaputtmachen
  - Geld verdienen durch Abrechnungsbetrug, Erpressung etc.
  - Kritische Infrastruktur
    → dafür wird man bezahlen



- „cyberwar“ ist kein Witz mehr.
- Smart Meter
  - hohe Anforderungen durch BSI (in Deutschland)
  - aber: viele gleichartige Geräte, Monokultur, einfach zugänglich, hoher Kosten+Zeitdruck vs. hohe benötigte Software-Qualität
- Industrie-Steuerungen & Leitstände
  - meist schlecht gewartete PCs mit veralteter und ungepatchter Software.
  - Anwendungen aus der „Vor-Internet-Zeit“

4 Hacks der vergangenen 5 Jahre

genua Ein Unternehmen der Bundesdruckerei

- Stadtwerke Ettlingen (2014, Pen Testing) [3]

  physischer Anschluss an Verwaltungsnetz
  Ausspähen von Informationen
  Bequemlichkeit der Admins ausgenutzt
  Zugriff auf den Leitstand innerhalb von 2 Tagen

- teilw. Blackout in der Ukraine (23.12.2015, ~3h) [2]

  (russische?) Hacker bringen Malware „BlackEnergy“ auf >= 3 Steuerungsrechner auf
  Angriff durch gezielt infizierte Emails („Spear-Phishing“)
  Verwaltungs- und Steuerungsnetz nicht hinreichend getrennt

- Aramco Saudi Arabien (2012) [4]

  ca. 30.000 Rechner durch Shamoon Virus infiziert
  85% der Hardware wurde zerstört / entsorgt
  Systeme waren bis zu 10 Tage offline
  Ölförderung massiv beeinträchtigt
  Pech oder gezielter Angriff?

- Gehackte Smart Meter machen Lichter aus (Black Hat Europe 2014) [5]

  Sicherheitsexperten ist es gelungen, in Spanien eingesetzte intelligente Stromzähler zu hacken. Damit könnten sie den Strom abschalten, den Zähler manipulieren oder dort Malware installieren.

Software allein reicht nicht …

genua Ein Unternehmen der Bundesdruckerei

- Die beste Software hilft nicht gegen Bequemlichkeit oder Dummheit
- Niedriges Sicherheits-bewusstsein macht Phishing & Co. erst möglich

http://files.idg.co.kr/itworld/image/avatar/article/2014/June/dylee1999@gmail.com/parking_system.jpg

- Vermutlich wird sich auch jemand finden, der einen ungeprüften USB-Stick in den Kontrollrechner einsteckt ...

Was tun?

genua Ein Unternehmen der Bundesdruckerei

- Nutzer und Admins schulen
- Patches überall schnell einspielen!
- ISMS nach ISO 27001
- Notfallpläne aufstellen
- „cyberwehr“-Übungen abhalten und Schadensauswirkungen kennenlernen
- Am Ball bleiben und alle Massnahmen periodisch auf den Prüfstand stellen!
- Austausch über aktuelle Bedrohungen etablieren

organisatorisch

- Netzwerk segmentieren und minimal mögliche Privilegien vergeben
- Firewalls, IDS/IPS, … an neuralgischen Punkten einsetzen
- Komplexität senken!
- Standardprotokolle statt exotischer Eigenentwicklungen nutzen
- Eingesetzte Systeme testen (lassen): Funktion, Inter-Op, Pen
- Zertifizierte Systeme nutzen, falls möglich (CC, NERC-CIP, ...)

technologisch

[6,7]

„Wir müssen aber auch selber Software entwickeln …“

genua Ein Unternehmen der Bundesdruckerei

- Softwaresysteme segmentieren und minimalisieren (analog Netzwerk)
- „richtig“ entwickeln: Review-Prozess, Pen-Test/Security Audit, automatisches Testen
- KISS: Keep it super simple. Komplexität ist der Feind von Sicherheit.
- Kryptografie nicht selber entwickeln, wenn man kein Experte ist.
- Sicherheit herstellen = Verantwortung für ganzen Software-Stack
  - 3rd Party Software (Betriebssystem, Libraries, Compiler, …)
  - Open-Source Komponenten
  - eigene Software
  - ...

Vielen Dank!

genua Ein Unternehmen der Bundesdruckerei

https://9gag.com/gag/2011364

Quellen und weiterführende Artikel

- [1] https://www.q-perior.com/wp-content/uploads/2016/06/Q_PERIOR_Experteninterviews_Digitale-Transformation_Energie.pdf
- [2] https://www.heise.de/tp/features/Ukraine-Hackerangriff-verursachte-Blackout-3377593.html
- [3] http://www.zeit.de/2014/16/blackout-energiehacker-stadtwerk-ettlingen
- [4] https://www.welt.de/wirtschaft/article158440599/So-fatal-waere-ein-Cyberangriff-auf-die-globale-Stromversorgung.html
- [5] https://www.golem.de/news/intelligente-stromzaehler-gehackte-smart-meter-machen-lichter-aus-1410-109923.html
- [6] http://www.zdnet.com/article/smart-meter-hacking-tool-released/
- [7] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide