
E-CONTROL
PROFITIEREN. WO IMMER SIE ENERGIE BRAUCHEN.

Cyber-Security in der E-Wirtschaft
Rahmenbedingungen und Diskussionsumfeld

Vorstand DI Walter Boltz

Energie-Control Austria (E-Control)

28. April 2014

Weltweit sind Betreiber kritischer Infrastruktur vermehrt Ziel von gezielten IKT- Attacken

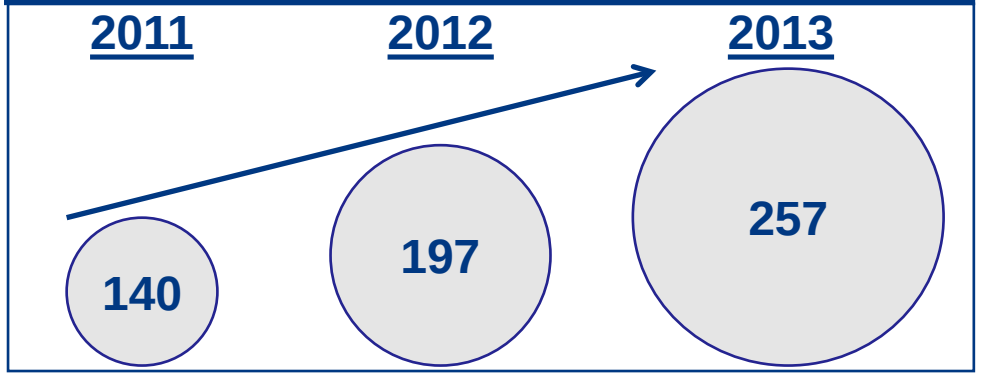
E-CONTROL

Sektoren mit Kritischer Infrastruktur

Globale Kosten für Cyber-Security Maßnahmen betrugen ~ **46 Mrd. USD in 2013** (+10% zu 2012).

Quelle: Wall Street Journal, 02/2014

Anzahl an gemeldeten Cyber-Zwischenfällen, USA



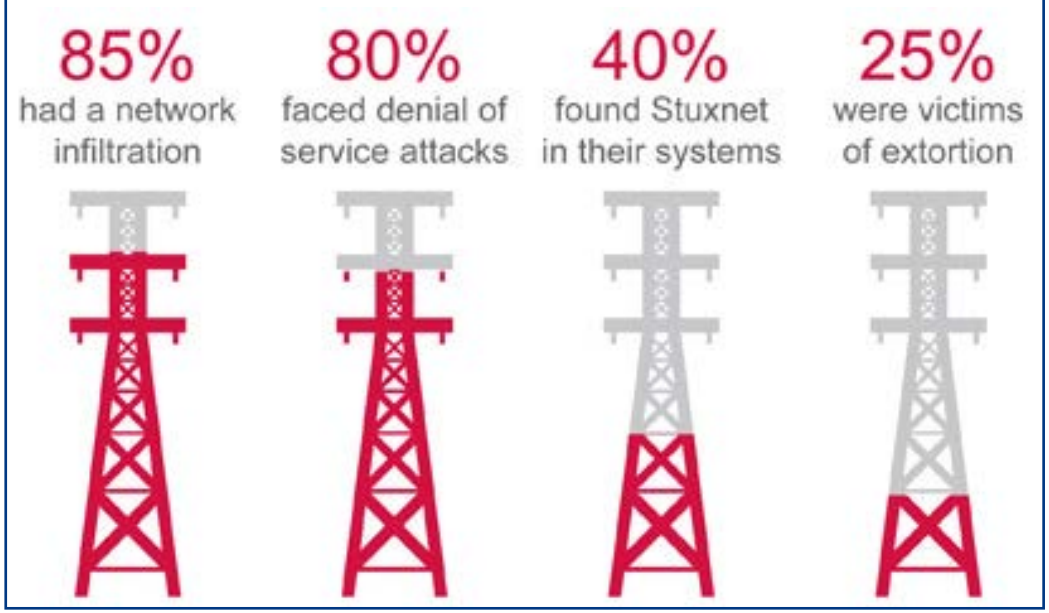
~ 56% aller schwerwiegenden Cyber-Zwischenfälle entfielen auf den **Energiesektor**

Quelle: US Department of Homeland Security, 2013

Intentionale Cyberattacken stellen eine neue Bedrohungssituation für die E-Wirtschaft dar

- **Stuxnet als „Weckruf“** für neue Bedrohungssituation: digitaler Softwarecode zerstört physische Infrastruktur
- digitale Sicherheit war früher kein wesentliches Design-Konzept von Steuerungs-anlagen (SCADA)

Ergebnisse Cyber-Sicherheitsreport E-Wirtschaft, 2011

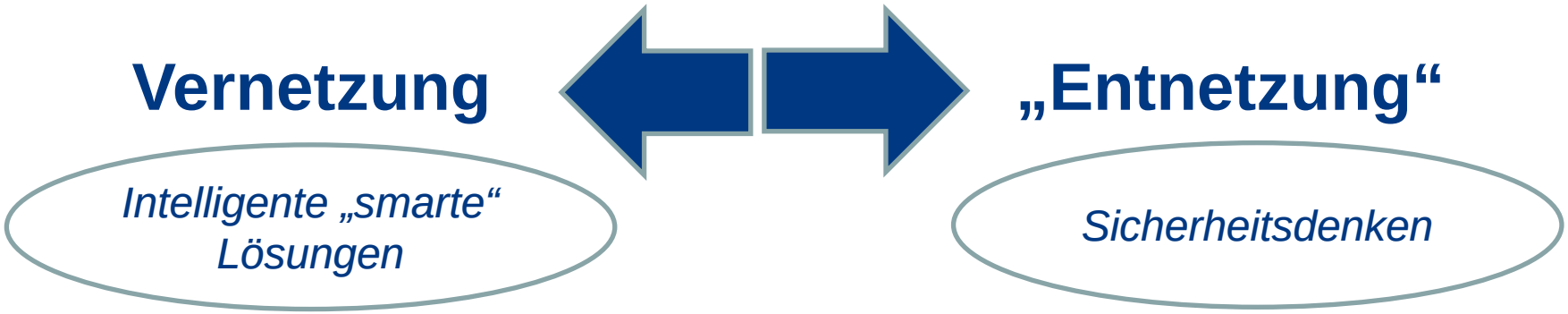


- Weltweite Umfrage in 14 Staaten (USA, Europa, Asien)
- Sektor: E-Wirtschaft
- Zeitraum: 2011
- 200 IT-Sicherheits-verantwortliche (C-Level)
- McAfee und Center for Strategic and International Studies

Quelle: McAfee, CSIS, 04/2011

Der Einsatz von „intelligenten“ Lösungen und Sicherheitsdenken als Balanceakt

- Marktveränderungen, eine steigende Anzahl an Marktakteuren sowie deren Vernetzung untereinander führen zu einer **Zunahme an Komplexität.**
- Unternehmen reagieren auf diese Veränderung mit der zunehmenden **Automatisierung** von Prozessen. Aufgaben werden an Systemdienstleister ausgelagert.
- Der **Einsatz von „intelligenten“ IKT-Lösungen** in der Energiewirtschaft zur Steuerung und Regelung von Erzeugung und Verbrauch **nimmt zu**.
- Exogene sowie systemimmanenten Faktoren führen zu neuen Bedrohungssituationen, die eine strukturierte End-2-End Betrachtung und Analyse aller Komponenten und Schnittstellen erfordern.



Das Diskussionsumfeld in Österreich

- **Start der flächendeckenden Einführung von Smart Meter** (2015) als eines der wichtigsten Projekte der österreichischen Energie- und Wirtschaftspolitik

- **Emotional geführte öffentliche Debatte** zu den Risiken von Smart Meter und dem Bedrohungspotential durch Cyber-Attacken

- **Zusammenwirken verschiedener nationaler und internationaler Prozesse:**
  - „Roll-Out“ von Smart Meter
  - Gesamtstaatlicher Lagebildprozess
  - Nationale Cyberstrategie (ÖSCS)
  - APCIP-Prozess zur Identifikation der ACI-Betreiber („*critical infrastructure*“)
  - Prozess zur Definition und Umsetzung von Sicherheitsvorsorgemaßnahmen durch IKT-Betreiber
  - Aufbau des European Cybercrime Center (EC3)
  - Etablierung eines europäischen Meldewesens (NIS-Richtlinie der EK)

- **Nutzung von Synergien** zur realistischen Analyse und Bewertung von potentiellen Bedrohungen durch den zunehmenden Einsatz von IKT Systemen im Energiebereich

Ziele und Inhalte des durchgeführten Cyber-Security Projektes der E-Wirtschaft

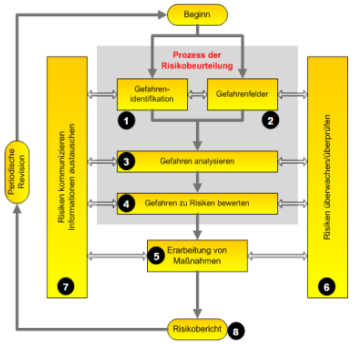
- **Projekt:**
  - Multidisziplinäres Public-Private Partnership (Regulator, Branche, Ministerien)
  - Prinzip der Freiwilligkeit
  - Projekt basierend auf international anerkannten Risikomanagement Standards (ISO 31.000, ONR 49.002-1-3, ÖNORM S2410)

- **Projektziele:**
  - Versachlichung der öffentlichen Diskussion
  - Sensibilisierung und Ausbildung von Sicherheitsbewusstsein
  - Schaffung von inhaltlichem Mehrwert durch internationale „Best Practices“ und branchenübergreifenden Informationsaustausch zwischen Beteiligten
  - Förderung von Interoperabilität zwischen Komponenten und Netzen durch gemeinsame Zusammenarbeit und technischen Diskurs
  - Erstellung einer umfassenden Risikoanalyse mit End-2-End Betrachtung und Priorisierung der identifizierten Risiken für die flächendeckende Stromversorgung
  - Entwicklung und Formulierung von Mindestsicherheitsstandards und detailliertem Umsetzungsplan
  - Freiwillige Selbstverpflichtung der Branche

Das Projektergebnis war eine umfassende IKT-Risikoanalyse und ein Maßnahmenplan

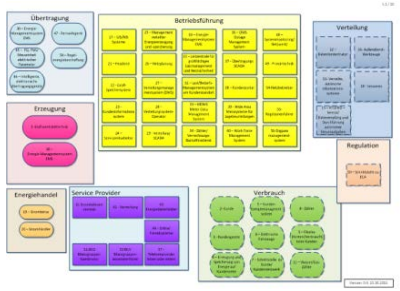
E-CONTROL

Literaturanalyse



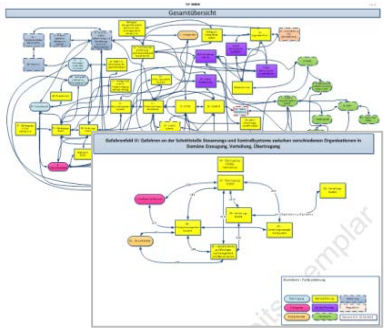
1

Domänenmodell



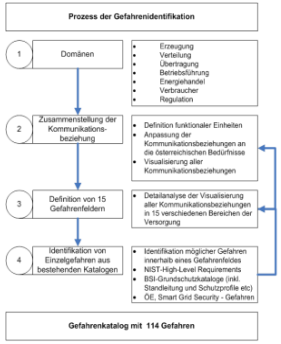
2

Risiko-Identifizierung



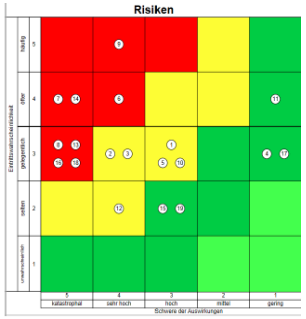
3

Risiko-Bewertung



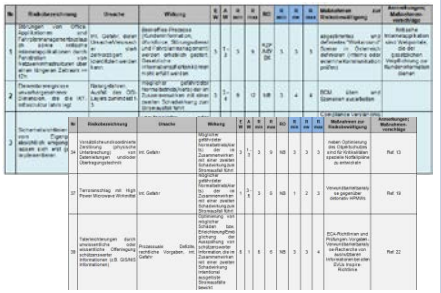
4

5x5 Risiko Matrix



5

Maßnahmenplan



6

Key Learnings und nächste Schritte

- Trotz traditionell gut ausgeprägtem Sicherheitsbewusstsein sind viele Unternehmen noch nicht ausreichend auf IKT-Risiken vorbereitet
- Public-Private Partnerships eignen sich um den Informationsaustausch und die Zusammenarbeit zwischen öffentlichen und privaten Stakeholdern zu erhöhen
- Freiwillige Selbstverpflichtungen von Unternehmen zu Mindestsicherheitsstandards sind eine Alternative zu gesetzlichen Vorgaben
- Die Einbeziehung der Gaswirtschaft ist sinnvoll um eine gesamthafte Betrachtung der Energiewirtschaft zu gewährleisten und Interdependenzen zu adressieren
- Ein zwischen allen Akteuren abgestimmter und institutionalisierter Kommunikations- und Alarmierungsprozess in Ergänzung zur bestehenden Energielenkung ist notwendig um über kurzfristig auftretende Störungen zu informieren und Maßnahmen zu koordinieren
- Die Vereinheitlichung von Sicherheitsstandards und –anforderungen auf europäischer Ebene ist notwendig um Synergien zu heben.

Kontakt

Vorstand DI Walter Boltz

+431 24724

walter.boltz@e-control.at

www.e-control.at


E-CONTROL
PROFITIEREN. WO IMMER SIE ENERGIE BRAUCHEN.