Bundesamt
für Sicherheit in der
Informationstechnik

Aktuelles zu Kritischen Infrastrukturen

Marc Schober

Bundesamt für Sicherheit in der Informationstechnik

Referat 112 – Kritische Infrastrukturen und IT-Sicherheitsrevision

GI SECMGT Workshop, 2011-06-10

KRITische InfraStrukturen

Kritische Infrastrukturen sind

Organisationen und Einrichtungen
mit wichtiger Bedeutung für das staatliche Gemeinwesen,

bei deren Ausfall oder Beeinträchtigung

- nachhaltig wirkende Versorgungsengpässe,
- erhebliche Störungen der öffentlichen Sicherheit,
- oder andere dramatische Folgen

eintreten würden.

KRITIS Sektor-Einteilung 2011

Energie
Elektrizität, Gas, Mineralöl

Informationstechnik und Telekommunikation
Telekommunikation, Informationstechnik

Transport und Verkehr
Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, **Logistik**

Gesundheit (aus „Versorgung“)
Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore

Wasser (aus „Versorgung“)
Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung

Ernährung (aus „Versorgung“)
Ernährungswirtschaft, Lebensmittelhandel

Finanz- und Versicherungswesen
Banken, Börsen, Versicherungen, Finanzdienstleister

Staat und Verwaltung
Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/ Rettungswesen einschl. Katastrophenschutz

Medien und Kultur (aus „Sonstiges“)
Rundfunk, gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke

KRITische Informations InfraStrukturen

Kritische Informations-Infrastrukturen sind diejenigen

IuK / IT Systeme & Anwendungen

von deren Verfügbarkeit die **kritischen Prozesse** innerhalb des Betriebs der Kritischer Infrastrukturen un/mittelbar abhängig sind.

(noch) keine offizielle Definition für KRITIIS!

KRITIS Sektor-Zuständigkeiten

Energie ← **IKT Anteil**

Informationstechnik und Telekommunikation

Transport und Verkehr ← **IKT Anteil**

Gesundheit ← **IKT Anteil**

Wasser ← **IKT Anteil**

Ernährung ← **IKT Anteil**

Finanz- und Versicherungswesen

Staat und Verwaltung ← **IKT Anteil**

Medien und Kultur ← **IKT Anteil**

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BBK

Bundesamt für Bevölkerungs-
schutz und Katastrophenhilfe

Herausforderungen

- Zunehmende – **heute schon sehr starke** – Abhängigkeit der KRITIS bzw. kritischen Prozessen von internen wie externen IKT Anteilen
- In Zukunft noch weit stärker → Smart Grid, VoIP, …
- Zunehmende **Interdependenzen** zwischen KRITIS Sektoren
  - Vernetzung in/zwischen Sektoren durch IKT
  - Zusammenarbeit bei der Bereitstellung von Dienstleistungen
  - Berücksichtigung von Abhängigkeiten im Krisenfall

  ➔ **Alle Sektoren abhängig von Energie** (Strom) **und IKT!**
- Auch internationale Abhängigkeiten sind zu berücksichtigen
  - wird bereits behandelt! - z.B. auf Europäischer Ebene (EPSKI,...)

Aktuelle Vorfälle

„Abhängigkeiten“ zwischen KRITIS müssen nicht immer beabsichtigt, bekannt und/oder geplant sein...

- **Brandanschlag auf Berliner S-Bahn (23.5.2011)**
  - Brandanschlag auf eine Kabelbrücke im Bereich Berlin Ostkreuz
  - Bahnverkehr stark gestört
  - Ausfall verschiedener IT-Dienstleistungen der Bahn (Reiseauskunft)
  - **ABER AUCH:** Ausfälle bei Mobilfunkanbietern

➔ **Durch räumliche Nähe und/oder die Nutzung von SharedMedia** (Kabelstrecken, Netze) **und SharedServices** (Cloud Computing) **können auch „Abhängigkeiten“** (von Dritten) **entstehen!**

Aktuelle Bedrohungen

„**Stuxnet** – *Ein Warnsignal für die IT-Sicherheit*“ KES 2011/1

- Stuxnet hat die „Sichtbarkeit“ von SCADA Systemen und deren Bedeutung für die Wirtschaft (und KRITIS) stark erhöht
- Laufend werden neue SCADA Schwachstellen gefunden (es wird auch intensiver gesucht...)

Nationale Aktivitäten bis 2011

Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland (NPSI)

- Umfassende Dachstrategie zur IT-Sicherheit
- Der NPSI adressiert drei Aufgabenbereiche:
  - **Prävention** Angemessener Schutz der IIS in D
  - **Reaktion** Bei IT-Vorfällen wirkungsvoll handeln
  - **Nachhaltigkeit** IT-Sicherheitskompetenz in D stärken

- Konkretisierung des NPSI in 2 Umsetzungsplänen
  - Für die Bundesverwaltung (UP Bund)
  - Für die „nicht staatlichen“ KRITIIS (UP KRITIS)

UP KRITIS

Umsetzungsplan KRITIS

- Zielsetzung: Schutz der IT-Infrastrukturen in D
- Im September 2007 verabschiedet
- Entwicklung in Kooperation mit einer Vielzahl von KRITIS Betreibern - inkl. öffentl. Verwaltung

- Zielgruppe:
  Privatwirtschaftliche KRITIS Betreiber
  ➔ Gemeinsame Verantwortung von Staat & KRITIS Wirtschaft für die Informationssicherheit in den Kritischen Infrastrukturen

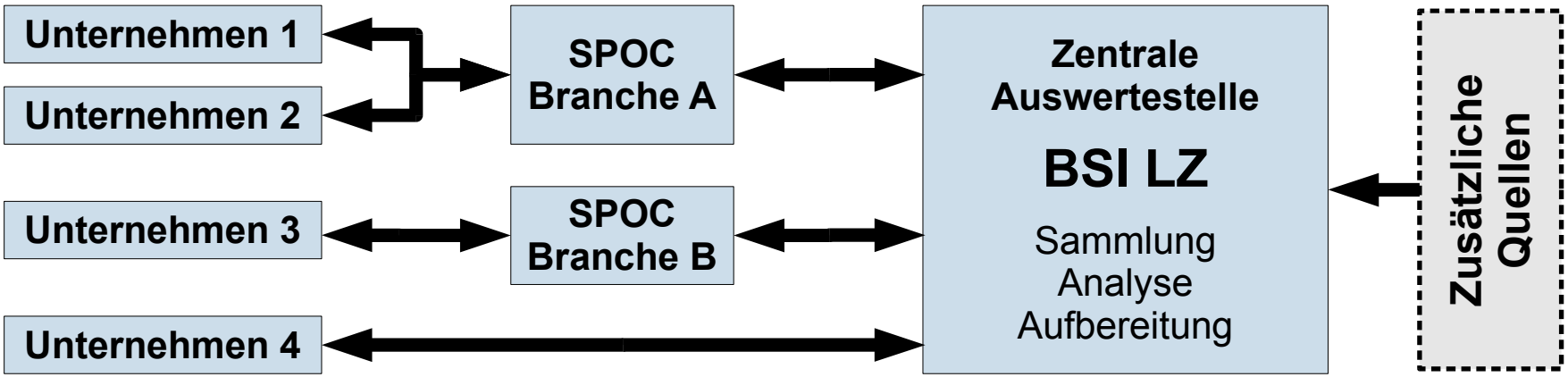
UP KRITIS Arbeitsgruppen

04/2007 → Gründung von **4 Arbeitsgruppen** unter Federführung des BMI

- **AG1: „Notfall und Krisenübungen“**
  - u.a.: Identifikation branchen- und sektorübergreifender Abhängigkeiten
- **AG2: „Krisenreaktion und Bewältigung“**
  - u.a.: Aufbau von Kommunikationsstrukturen für den Krisenfall als **eine** Grundlage des Krisenmanagements
- **AG3: „Aufrechterhaltung kritischer Infrastrukturdienstleistungen“**
  - u.a.: Verfügbarkeit, Aufrechterhaltung, schneller Wiederanlauf von kritischen Prozessen
- **AG4: „ Nationale und Internationale Zusammenarbeit“**
  - u.a.: Schaffung internationaler Mindestniveaus von IT-Sicherheit in KRITIS

UP KRITIS - Kommunikation

Kommunikation im UP KRITIS als wichtiges Mittel zur **Vermeidung**, (früh)**Erkennung** und **Bewältigung** von Krisen



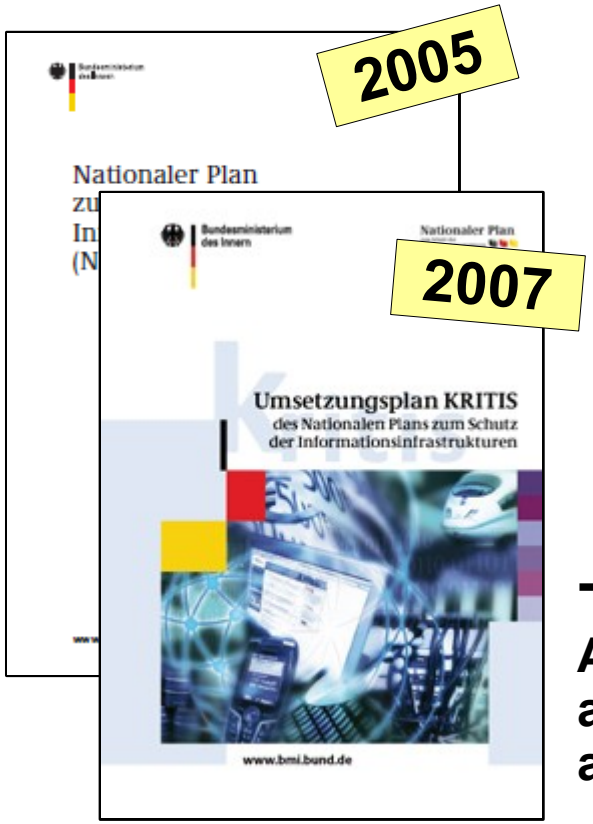
- Etablierte, gut funktionierende, Kommunikationsstruktur im UP KRITIS
- Brancheninterne **S**ingle **P**oint **O**f **C**ontact**s**
  - Bündelung bzw. Verteilung von Informationen, 24/7 Erreichbarkeit

UP KRITIS - Übungen

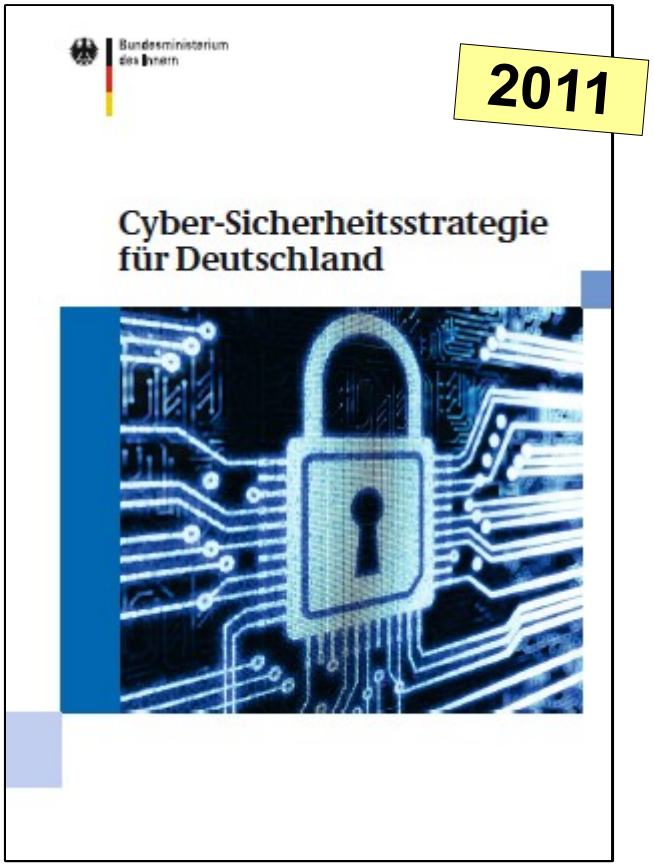
Durchführung von Übungen wesentlicher Bestandteil eines umfassenden Schutzes der Kritischen Infrastrukturen

- **Innerhalb des UP KRITIS** - AG1: „Notfall und Krisenübungen“
  - Konzept: „IT-Notfall und Krisenübungen in kritischen Infrastrukturen“
  - Strategischer Übungsplan, regelmäßige Durchführung in Aufbau/Erhaltungsphase
- **LÜKEX Übungsreihe** (Länder Übergreifende Krisenmanagement-Übung/ EXercise)
  - LÜKEX 2011 mit IT-Krisenszenario für Bund, Länder, Kommunen, **Unternehmen**
  - Projektleitung LÜKEX durch das BBK
- Zukünftig auch auf europäischer Ebene z.B. „Cyber Europe“

Cyber-Sicherheitsstrategie



Anpassung der Maßnahmen aus UP KRITIS & UP BUND an die Gefährdungslage



Veröffentlichung
14.03.2011

Cyber-Sicherheitsstrategie

Wesentliche Ziele der Cyber-Sicherheitsstrategie:

- **Schutz Kritischer Informationsinfrastrukturen**
  - Systematischer Ausbau der Zusammenarbeit im UP KRITIS
  - Prüfung der Einbeziehung weiterer Branchen durch den Cyber-Sicherheitsrat
  - Prüfung rechtlicher Verpflichtungen des UP KRITIS
- Sichere IT-Systeme in Deutschland
  - Mehr Sicherheit auf IT-Systemen der Bürger und von **KMUs**
- Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
- Nationales Cyber-Abwehrzentrum
  - In Betrieb seit dem 01.04.2011
- Nationaler Cyber-Sicherheitsrat

Vielen Dank für Ihre Aufmerksamkeit!