



Cloud-Lösungen für Kritische Infrastrukturen?

Dietmar W. Adam

CSI Consulting AG, Senior Consultant

10.09.2014



Inhalt

Herbsttagung 2014

- Einleitung
- Begriffe
- Rahmenbedingungen und Anforderungen
- Vorgehen und Beispiele aus der Praxis
- Schlussfolgerungen





Eine Regierung in der Cloud?

Herbsttagung 2014

30.05.2014 11:50

Vorsorge für eine Invasion: Estlands Regierung zieht in die Cloud

Estland arbeitet angeblich daran, Regierungsfunktionen in die Cloud zu verlagern. Das Land möchte unter anderem sicherstellen, dass staatliche Stellen auch bei einer Invasion weiterarbeiten. Einen Nachbarn haben die Esten ganz besonders im Blick.



Quelle: <http://www.heise.de/newsticker/meldung/Vorsorge-fuer-eine-Invasion-Estlands-Regierung-zieht-in-die-Cloud-2211360.html>



Begriffe



Definitionen

Herbsttagung 2014

- Business-kritische Prozesse in einem Unternehmen:
 - Diejenigen Prozesse, die zu einem Misserfolg des Unternehmens oder zur Nichterreicherung wichtiger Ziele führen können.
- Kritische Infrastrukturen (KI)
 - Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind. (NDG, 2014)
 - Infrastrukturen, deren Störung, Ausfall oder Zerstörung gravierende Auswirkungen auf die ganze Gesellschaft, die Wirtschaft und den Staat hat. (BABS, Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2012)

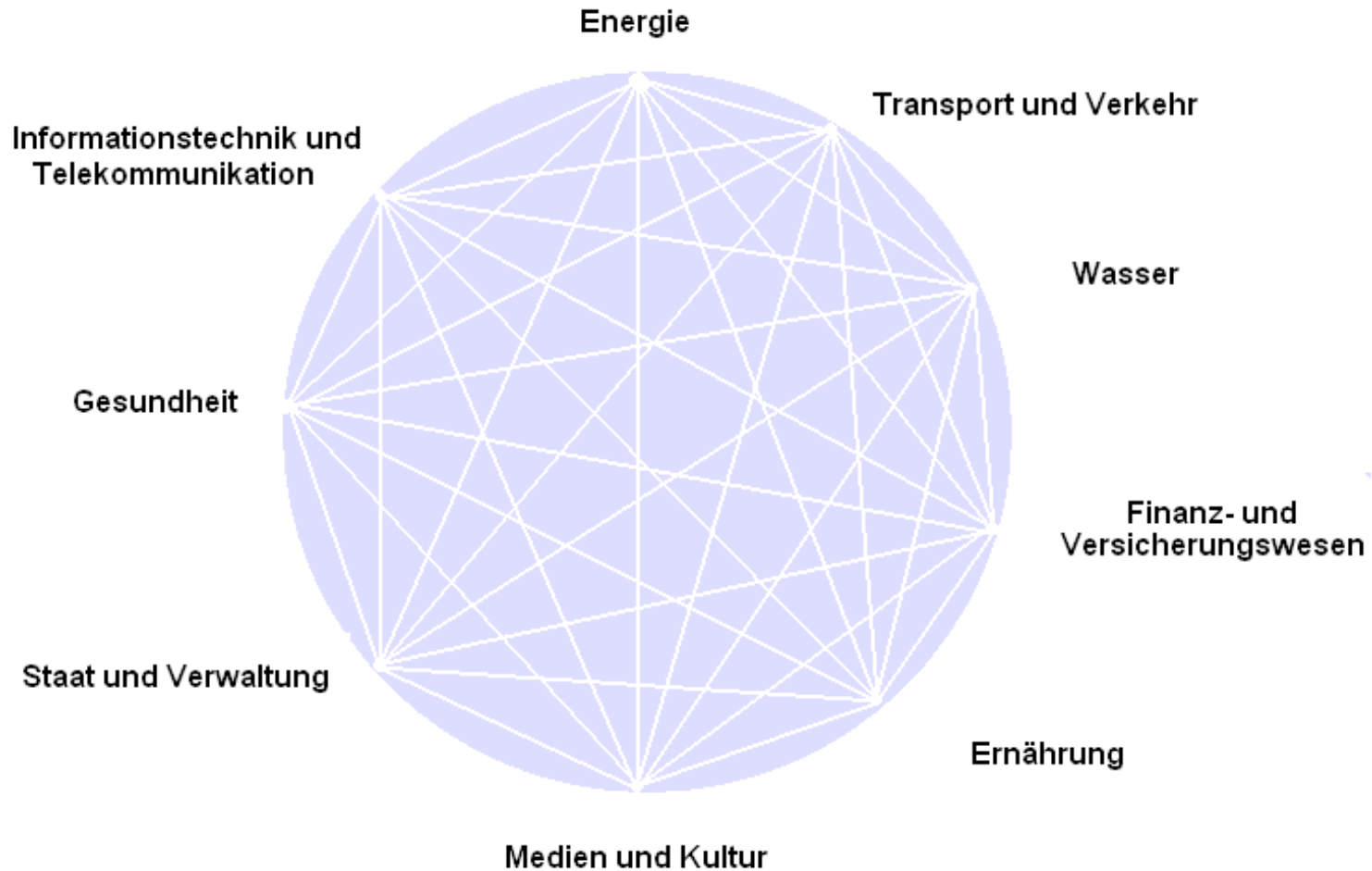
Quelle: BABS,

<http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/nationaleskistrategie.parsysrelated1.54058.downloadList.15281.DownloadFile.tmp/natstratski2012d.pdf>



Kritische Infrastrukturen: Sektoren

Herbsttagung 2014



Quelle: BSI/BBK (DE), http://www.kritis.bund.de/SharedDocs/Bilder/Kritis/DE/Interdependenzen.bmp?__blob=poster&v=2



Rahmenbedingungen & Anforderungen

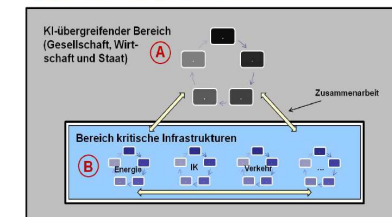


Bundesratsbeschlüsse

Herbsttagung 2014

- Nationale Strategie
 - Der Bundesrat hat eine nationale Strategie zum Schutz Kritischer Infrastrukturen verabschiedet (BRB, 27.06.2012)
 - Für die Umsetzung wurde das Bundesamt für Bevölkerungsschutz beauftragt
- Betreiber der IKT-Infrastruktur
 - Kriterien an die Betreiber von besonders kritischen und zentralen Infrastrukturen der Bundesverwaltung (BRB, 05.02.2014):
 - Handelt unter Schweizer Recht
 - Mehrheit in Schweizer Eigentum
 - Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erzeugt

Handlungsfelder der nationalen SKI-Strategie





Gesetzliche Vorgaben

Herbsttagung 2014

- **Nachrichtendienstgesetz des Bundes**
 - Art. 6 «Erkennen und Verhindern ... von Angriffen auf ... kritische Infrastrukturen.»
- **Energiegesetz des Bundes**
 - Art. 8 «Zu einer sicheren Energieversorgung gehört auch der Schutz der kritischen Infrastrukturen ...»
- **Bundesgesetz über die Informationssicherheit**
 - Einheitliche Grundlagen für die Steuerung und Organisation der Informationssicherheit im Bund
 - Behördenübergreifende Organisation der Informationssicherheit
- **Kantonale Bevölkerungsschutzgesetze**
 - Das BSM stellt «die notwendigen technischen Kommunikationsflüsse sicher». (Kt. BE)
 - Die Kantonspolizei « ... betreibt die Einsatzzentrale ...». (Kt. ZH)



Cloud-spezifische, gesetzliche Vorgaben

Herbsttagung 2014

- Es gibt keine relevanten Cloud-spezifischen, gesetzliche Vorgaben
- SATW – White Paper «Cloud Computing»
 - Das Datenschutzrecht erlaubt die Weitergabe von Personendaten zur Bearbeitung im Auftrag an Dritte. Der Auftraggeber bleibt für den Datenschutz verantwortlich.
 - Wenn im Empfängerland ein dem schweizerischen gleichwertiger gesetzlicher Datenschutz (EU, EWR) besteht, gelten grundsätzlich keine höheren Anforderungen.



Besondere Anforderungen für KI

Herbsttagung 2014

- Hohe Verfügbarkeit gefordert (Häufig via Redundanz realisiert)
- Niedrige Latenzzeiten im Bereich der Infrastruktur-Steuerung (Bsp. Stromnetz)
- Hochsicherheitsbereiche in der (IT-) Architektur
- Spezialgesetzgebung für KI-Sektoren
 - Sektor Energie: Kernenergiegesetz
 - Sektor Finanz- und Versicherungswesen: Geheimnisschutzvorschriften Finanzwesen
 - Sektor Gesundheit: Geheimnisschutzvorschriften Medizinalwesen
 - Etc.



Vorgehen & Praxisbeispiele



Vorgehen

Herbsttagung 2014

Konservatives Vorgehen: Nur Prozesse (bzw. Daten und Werkzeuge) auslagern, die unkritisch sind oder für die eine Rückfallebene besteht.

1. Vorgaben und Rahmenbedingungen analysieren
2. Bewertung der Geschäftsprozesse und Daten, und Triage nach Kritikalität gemäss:
 - a) Verfügbarkeit
 - b) Integrität
 - c) Vertraulichkeit

➡ Cloud-fähige Prozesse (Bzw. Daten und Werkzeuge)
3. Analyse des Cloud-Marktes in CH
4. Projektstudie - Mit Anforderungen & Lösungsansatz



Beispiel I

«Archive as a Service»?

Herbsttagung 2014

- Rechtskonforme und betriebsrelevante Daten- und Dokumentenarchivierung
- # Anforderungen On-Premise-Lösung: 115
- # Anforderungen SaaS-Lösung: +31
- Integration der SaaS-Lösung:
Vergleich zur On-Premise-Lösung
➔ On-Premise-Lösung gewählt



On-Premise

- + Integration diverser Schnittstellen
- + Höhere Wirtschaftlichkeit
- Skalierung aufwendiger

SaaS

- + Service-Bereitstellung, Skalierung
- Geringe Zahl an Anbietern in CH
- Integration Quellsysteme: komplex



Beispiel II

«File-Sharing mit externen Partnern»

Herbsttagung 2014

- File-Sharing und Projektarchiv zur Nutzung mit externen Partnern
- Ergänzung zur internen (Sharepoint-) Lösung
- Sichere Alternative zu ggf. unverschlüsseltem Dateiaustausch per Email
- Rechtsbasis: EU/Schweiz
➔ SaaS-Lösung gewählt

SaaS

- + Firmensitz, Daten und Recht: CH
- + Günstig, sicher und flexibel
- Separate Rechteverwaltung

On-Premise

- + Back-Up-Prozess bestehend
- Aufwand: Implementierung/Betrieb
- IAM für externe Partner



Beispiel III

«Ersatz Intranet - Interne Kollaboration»

Herbsttagung 2014

- Vereinfachen und Beschleunigen der internen Zusammenarbeit
- Ersatz für das wenig genutzte Intranet
- Analyse Geschäftsprozesse (Daten und Werkzeuge)
- «Keine Kundendaten in der Cloud» (Prinzip)
 - ➔ Kritische Prozesse und Kundendaten: On-Premise
 - ➔ Kollaborations-Werkzeug: SaaS



SaaS

- + Günstig und einfach skalierbar
- + Flexible Vertragsdauer
- Funktionalität weniger erhöht

On-Premise

- + Funktionalität stärker erhöht
- Lizenzen erheblich teurer
- Aufwand: Implementierung/Betrieb



Die Zukunft - Hybride ICT-Lösungen für Kritische Infrastrukturen

Herbsttagung 2014

Weniger kritische Prozesse



Private Cloud (SaaS)



Public Cloud (SaaS)

Hochkritische Prozesse



Klassische IT (On Premise)



Private Cloud (On Premise)



Schlussfolgerungen



Cloud-Lösungen für Kritische Infrastrukturen?

Herbsttagung 2014

- Das Bewusstsein für KI ist entwickelt – der Begriff ist gerade in der Gesetzgebung angekommen
- Für KI existieren Strategien auf der Basis von Eigen-Verantwortung (Wirtschaft, Staat), Einheitlicher Vorgaben und Koordinationsaufgaben (Staat)
- Cloud-Lösungen haben Zukunft – auch für Kritische Infrastrukturen (vorerst vor allem für nicht-kritische Prozesse)
- Gründliche Analyse der Rahmenbedingungen und ein umfassendes Anforderungsmanagement ist erforderlich

CSICONSULTING 

INFORMATION AND COMMUNICATION