Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Projekt Informationssicherheitsgesetz ISG

Das geplante Informationssicherheitsgesetz

Referat VIS!T 2016

Christophe Perron, Projektkoordinator

Übersicht

1. Wieso ein Gesetz?
2. Inhalt des geplanten Gesetzes
3. Rechtsvergleichende Bemerkungen

Wieso ein Gesetz?

Vorgeschichte

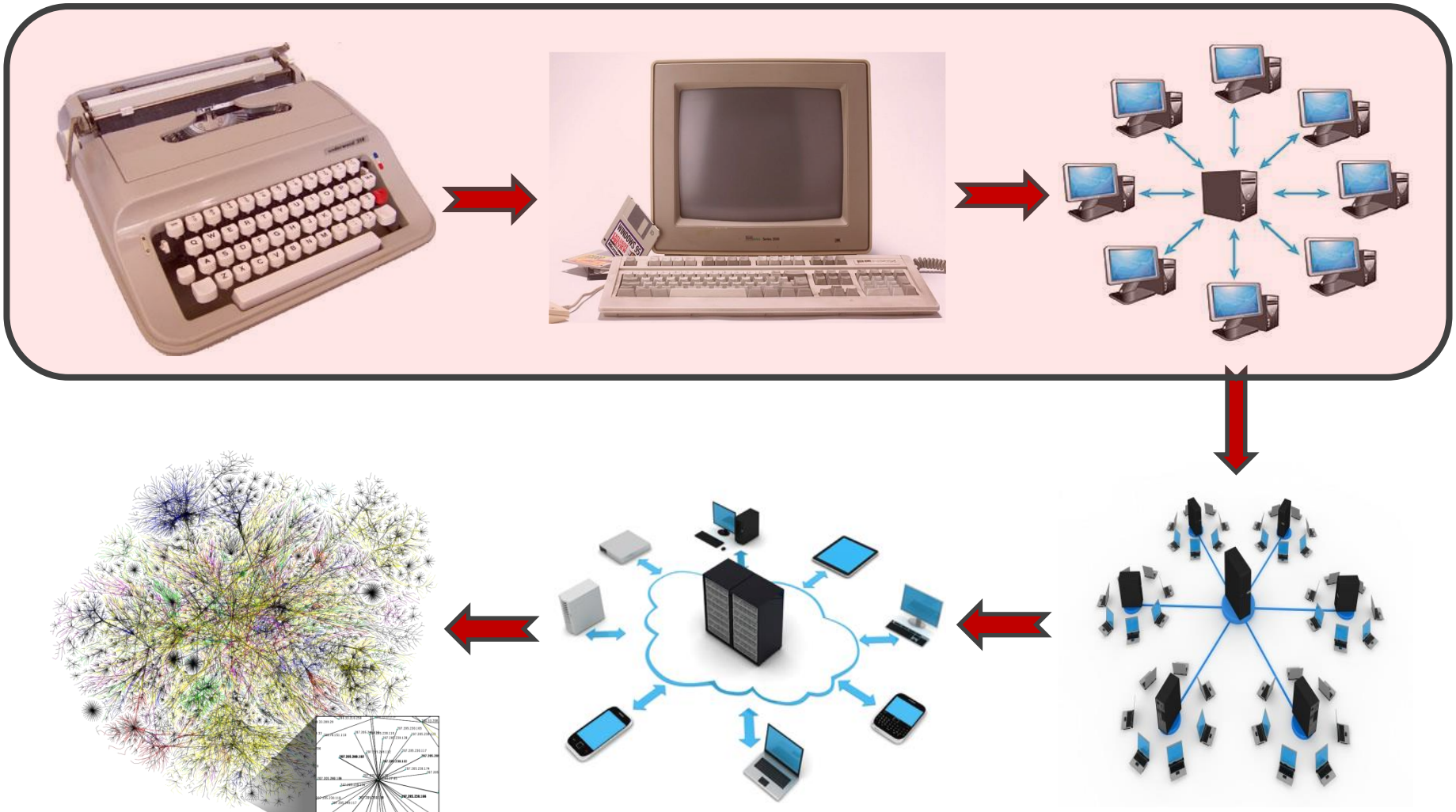
- 2007: Vereinheitlichung Informationsschutz Bund
- 2010: Grundauftrag Informationsschutz
- 2011: Erstreckung auf Informationssicherheit
- 2012-2015: Weitere Aufträge

Wieso ein Gesetz?

Mängel

- Bestehende rechtliche Bestimmungen breit gestreut, inkohärent und sehr lückenhaft
- Geltungsbereich bestehender Massnahmen
- Organisation und Zuständigkeiten
- Wirksamkeit und Wirtschaftlichkeit

Wieso ein Gesetz?



Inhalt

Regelungsziele

- Schaffung eines einheitlichen, integralen formell-gesetzlichen Rahmens für die Informationssicherheit des Bundes
- Schaffung eines minimalen «Bundesstandards»
- Anpassung an Anforderungen der Informationsgesellschaft und Behebung von Lücken des geltenden Rechts
- Fokus auf kritischste Informationen und Systeme
- Erhöhung der Effizienz

Inhalt

Aufbau

1. Kapitel: Allgemeine Bestimmungen
2. Kapitel: Allgemeine Massnahmen
3. Kapitel: Personensicherheitsprüfungen
4. Kapitel: Betriebssicherheitsverfahren
5. Kapitel: Kritische Infrastrukturen
6. Kapitel: Organisation und Vollzug

Inhalt

Allgemeine Massnahmen der Informationssicherheit

- ISMS (Sicherheitsmanagement, inkl. Risikomanagement)
- Klassifizierung von Informationen (Vertraulichkeit)
- Sicherheit beim Einsatz von Informatikmitteln
- Personelle Massnahmen
- Physische Sicherheit
- Identity and Access Management

Inhalt

Besondere Massnahmen der Informationssicherheit

- Personensicherheitsprüfungen
  - Klassifizierte Informationen
  - Informatiksysteme mit hohem Schutz
  - Sicherheitszonen
- Betriebssicherheitsverfahren
  - Bisheriges «Geheimschutzverfahren»
  - Wahrung Informationssicherheit bei Vergabe von sicherheitsempfindlichen Aufträgen an Dritte
  - Umgang mit sicherheitsrelevanten IKT-Beschaffungen?

Inhalt

Kritische Infrastrukturen

- Auftrag Melde- und Analysestelle Informationssicherung:
  - Unterstützung beim Risikomanagement
  - GovCERT
  - Bearbeitung und Austausch von Personendaten
  - Sicherer Informationsaustausch national und international
- Keine Verpflichtungen im ISG (Meldepflichten und Mindestandards)

Inhalt

Organisation

- Informationssicherheitsbeauftragte (inkl. Stellvertreter)
- Konferenz der Informationssicherheitsbeauftragten
- Fachstelle des Bundes für Informationssicherheit

Vollzug

- Jede Behörde erlässt ihr Ausführungsrecht, aber die Ausführungsbestimmungen des Bundesrats gelten subsidiär
- Standardmassnahmen des Bundesrats

Inhalt

Stand

- Behandlung Botschaft durch Bundesrat Ende Oktober 2016
- Koordination mit anderen relevanten Geschäften
- Offene Frage betreffend Sicherheitsorganisation (Fachstelle des Bundes für Informationssicherheit)

Rechtsvergleichende Bemerkungen

- Informationssicherheitsgesetz CH:
  - Bundesbehörden, indirekt für Kantone, Wirtschaft und Private
  - Keine zentralen Pflichten für kritische Infrastrukturen (freiwillig) oder Anbieter digitaler Dienste

- NIS-Richtlinie EU:
  - Betreiber wesentlicher Dienste (kritische Infrastrukturen)
  - Anbieter digitaler Dienste
  - Keine Pflichten für öffentliche Verwaltungen
  - Meldepflichten, Mindeststandards, zentrale Sicherheitsbehörde

Rechtsvergleichende Bemerkungen

- IT-Sicherheitsgesetz DE:
  - Betreiber kritische Infrastrukturen
  - Anbieter bestimmter digitaler Dienste
  - Öffentliche Verwaltungen (?)
  - ➢ Sicherheitsüberprüfungsgesetz (SÜG)

- Informationssicherheitsgesetz AT (InfoSiG):
  - Schutz klassifizierter Informationen (international)
  - Sicherheitsbescheinigungen für Unternehmen
  - ➢ Sicherheitspolizeigesetz (SPG)
  - ➢ Geplantes Cybersicherheitsgesetz (Umsetzung EU-NIS-Richtlinie)

Rechtsvergleichende Bemerkungen

Begriffe

- Informationssicherheit
- Informationssicherung
- IT-Sicherheit
- IKT-Sicherheit
- Computersicherheit
- Cybersicherheit
- Cyber-Defense
- Sicherheit der Informationstechnik
- Sécurité des systèmes d’information

Fragen?