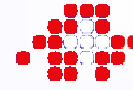


Informatikstrategieorgan Bund
Eidgenössisches Finanzdepartement EFD



Information Assurance

Das Modell Schweiz

Dr. Ruedi Rytz, Informatikstrategieorgan Bund ISB
Friedheimweg 14, 3003 Bern

Tel: +41-(0)31-323-4507 Fax: +41-(0)31-322-4566 E-Mail: ruedi.rytz@isb.admin.ch

Informationssicherung (Information Assurance)



Definition: Informationssicherung umfasst die **Gesamtheit von** aufeinander abgestimmten **Massnahmen**, wie

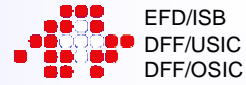
- Arbeitsabläufe
- Organisationsanweisungen
- Schulung und Ausbildung
- Informationssicherheit (Information Security)
- ...

so dass die zur Erfüllung **einer Aufgabe** erforderliche **Qualität der Information**, z.B.

- Korrektheit
- rechtzeitige Verfügbarkeit
- ...

erreicht werden kann.

Vier-Säulenmodell



Sensibilisierung: InfoSurance



Frühwarnung: MELANI



Schadensbegrenzung in der Krise: SONIA, WL



Bekämpfung der Krisenursache: MELANI und Partner

Frühwarnung: Problematik



klassisch

IT-Welt

Detektion

- **klare Messgrößen und Grenzwerte;** häufig automatisierbar (z.B. Radioaktivität)

- **Bestimmung von Grenzwerten** ist prinzipiell **unmöglich** (z.B. Analyse von Viren)

Ursprung

- meist **naheliegend** (z.B. KKW)

- nur **schwer feststellbar** (z.B. DDoS-Attacken)

Massnahmen

- können im **Voraus festgelegt** werden (z.B. Schutzräume)

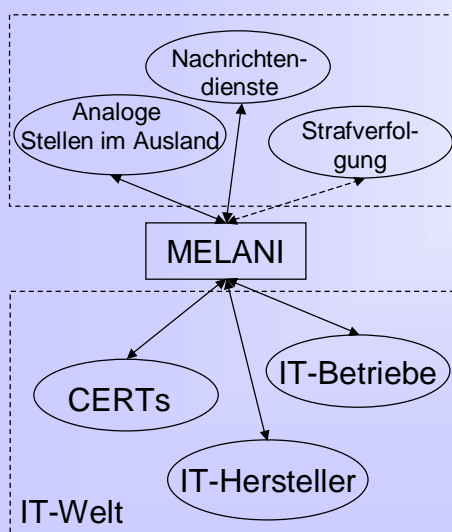
- Müssen **situativ entschieden** werden (z.B. Aufgebot von SONIA)

Frühwarnung: Was kann man in der IT-Welt tun?



- **Frühwarnungen** oder **Alarmierungen** (im klassischen Sinn) sind offenbar **nicht zweckmässig**.
- Die Melde- und Analysestelle Informationssicherung (**MELANI**): Das **Schnee- und Lawinenforschungsinstitut in der IT-Welt**.
- Was es braucht, ist die **fortwährende Beobachtung** und **Darstellung der Lage** zur
 - Beratung der Entscheidungsträger
 - Früherkennung
 - Aufbietung des Sonderstabs Information Assurance (SONIA)
 - Führung in der Krise (Lagezentrum SONIA).

MELANI: Lagezentrum



MELANI: Melde- und Analysestelle Informationssicherung

CERT: Computer Emergency Response Team

Ausl. St.: Ausländische Partner, wie z.B. National Infrastructure Protection Center NIPC (USA) oder das NISCC (GB)

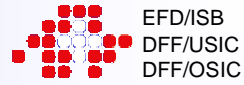
NDienste: Dienst Analyse und Prävention (Bundesamt für Polizei)

Strafverf.: Nur auf ausdrücklichen Wunsch der Opfer. Wird aber meist empfohlen.

Aufgaben:

- Nachrichtenbeschaffung und Analyse
- Lagedarstellung
- Prävention, Früherkennung, Aufgebot von SONIA
- **Koordination bei der IT-Problemlösung**

Vier-Säulenmodell: Zusammenfassung



- Vier Säulen: **Sensibilisierung, Früherkennung, Bekämpfung der Auswirkungen** und **Bekämpfung der Ursachen**.
- Probleme/Krisen werden **gesamtheitlich** unter Beteiligung von allen Partnern (z.B. Wirtschaft, WL, Polizei, Armee) **angegangen**.
- **Analyse** und **Koordination** geschieht "**weit weg**"; die Umsetzung der **Massnahmen** so **nahe wie möglich** bei den betroffenen Stellen.
- **Milizelemente wo sinnvoll (SONIA, WL)** aber eine **professionelle Organisation (MELANI)** wo nötig.
- **Effizientes** und (im Vergleich zum Ausland) **kostengünstiges** Modell.
- Das **Fehlen von MELANI ist das grösste Problem**, das rasch gelöst werden muss.