



SWITCH

The Swiss Education & Research Network

Critical Information Infrastructure Protection (CIIP)

Christoph Graf

SWITCH

<christoph.graf@switch.ch>

- Protecting critical infrastructure (CI) is a government task -> CIP
- Typical CIs: telecom, energy, finance, transport, water, emergency, government services, etc., (comes in national flavours)
- Critical infrastructure is increasingly operated by non-gov bodies
- This is certainly true for the telecommunication services
- Some sectors operate CIP structures
... but rarely co-ordinated across sectors
- Trend: CIs depend increasingly on telecommunication -> CIIP
- Most governments run public-private-partnership initiatives (PPP) aiming at establishing cross-sectoral CI(I)P structures
- The CSIRT model seems quite attractive for CIIP activities
- Effects: New teams popping up, or new clients for existing teams

National CIIP initiative under the control of the IT strategy unit of the federal government: MELANI

Make or buy?

- The functions “situation centre” and “CERT” were analysed

Decision was taken to partner with existing bodies:

- A section of the federal police for the situation centre (Fedpol, already operating a “Internet crime report” site)
- SWITCH-CERT for the CERT-function (because of its CERT experience)

The whole thing corresponds to about 10 FTE

Dual track strategy

- Open constituency: SMEs, citizens
- Closed constituency: CI operators

Open constituency - the public

- Based on unilateral trust
- Online since end of 2004: <http://www.melani.admin.ch>
- Addressing reasonably security aware, but technically not necessarily interested people (reporting option and information)
- Quite some echo in the press and linked from several e-banking sites

Closed constituency - handpicked CI operators

- Based on multilateral trust
- A reasonable number of CI operators from several sectors joined (represented by named individuals)
- Focus on establishing and fostering the human network within this group
- Information is provided on a voluntary base
- Informant stays in control of the information provided
- Typical CERT services offered to this group (by SWITCH-CERT)
- Option to link into relevant international law enforcement circles (Fedpol)