Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Mauro Vignati
Analyste MELANI / Cybercrime, Service d'analyse et prévention

But visé par MELANI: protéger les infrastructures vitales

Systèmes vitaux pour le bon fonctionnement de la société:

- approvisionnement en énergie
- télécommunications
- services financiers et assurances
- transports et logistique
- services de secours et de sauvetage
- santé (y c. approvisionnement en eau)
- gouvernement et administrations publiques

A l'ère de l'information**, leur fonctionnement dépend toujours plus des** TIC
→ protection des infrastructures d'information critiques
(critical information infrastructure protection CIIP**)**

Centrale nucléaire de Davis-Besse, Ohio, U.S.A.

Le 25 janvier 2003, le virus Slammer **s'introduit dans le** réseau LAN de la centrale.

Le système de contrôle de la sécurité est mis hors service **pendant cinq heures.**

Panne électrique du Nord-Est américain

13 août 2003

Un **coup de foudre** a-t-il provoqué une surcharge dans une centrale électrique située aux chutes du Niagara?

14 août 2003

21 centrales déconnectées du réseau (→ effet de domino); le **virus Blaster** est apparu le 12 août 2003…

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di Giustizia e Polizia
Ufficio federale di Polizia
Servizio d'analisi e prevenzione

Attaque DDoS contre Worldpay

- **Une attaque DDoS** paralyse presque complètement les transactions financières.
- **Près de 30'000 commerces sont touchés, dans 70 pays.**
- **Certains subissent** pendant 2 ou 3 jours **un** manque à gagner de 50 à 80% de leur chiffre d'affaires**.**
- **Les pertes économiques sont lourdes pour les pays touchés.**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di Giustizia e Polizia
Ufficio federale di Polizia
Servizio d'analisi e prevenzione

Centrale d'enregistrement et d'analyse pour la sécurité de l'information

- **En tant que centre d'analyse et de renseignement de la Confédération préposé à la** protection des infrastructures critiques d'information**, MELANI**
- **propose** à titre subsidiaire **aux** exploitants **concernés:**
  - entreprises d'approvisionnement en énergie
  - banques
  - entreprises de transport
  - etc.,

  des connaissances et des instruments de sources diverses:
  - **Services de renseignements**
  - **autorités de poursuite pénale**
  - **CERT** (computer emergency response team) **nationaux**

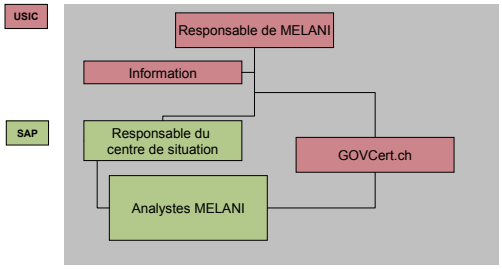
Tâches de MELANI

- Observation et rapports sur la situation**, à des fins de**
  - prévention
  - détection précoce
  - coordination des moyens lors de crises (→ état-major pour la sûreté de l'information SONIA)
- Création et maintien d'un réseau de relations avec les exploitants d'infrastructures vitales **(→ cercle fermé)**
- Soutien **des exploitants d'infrastructures vitales dans la** résolution concrète des incidents
- Travail de prévention au profit des PME et de la population **(→ cercle ouvert, CO)**

Organisation de MELANI: fonctions – partenaires (coopérations)

- Fonction de service des renseignements –
  Service d'analyse et de prévention (SAP)
  à l'Office fédéral de la police (fedpol)
  - tâches relevant du hacktivisme (attaques politiques électroniques), de la criminalité informatique et de la protection de l'Etat)
  - collaboration bien établie avec l'économie, réseau de contacts
- Fonction de CERT
  GOVCert.ch
  - au sein de l'USIC, subordination directe au resp. de MELANI
  - intégration au réseau mondial des CERT (EGC, ...)
- Direction et fonction spécialisée –
  Unité de stratégie informatique de la Confédération (USIC), au Secrétariat général du Département fédéral des finances (SG-DFF)

Modèle organisationnel de MELANI



Groupes de clients 1/2

Groupe de clients	Cercle fermé GovCERT / Centre d'analyse	Cercle ouvert Centre d'analyse
Membres	Exploitants choisis d'infrastructures vitales	PME population
Nombre	~ 90 personnes (fin 2007)	illimité
Confiance	relation de confiance étroite avec MELANI	rapports impersonnels
Instauration de rapports de confiance	MELANI (ateliers, MELANI-Net)	médias, www, présence à des expositions (p. ex. Cybernetguard) PME: associations de branche

Groupes de clients 2/2

Groupe de clients	Cercle fermé GOVCert	Cercle fermé Centre d'analyse	Cercle ouvert Centre d'analyse
Contact	courriel MELANI-Net fax, tél.	courriel MELANI-Net fax, tél. (joignabilité 7/24h)	www.melani.admin.ch

Services destinés au cercle ouvert (CO)

Voir: www.melani.admin.ch/dokumentation

Cercle fermé (CF): nombre de membres (automne 2007)

Infrastructure vitale	Nombre d'entreprises
Télécommunications:	7
Approv. en énergie:	7
Finances:	20
Transports et logistique:	3
Santé:	1
Administration publique:	4
Total:	40 (~ 90 personnes)

MELANI: centre de compétences national