Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

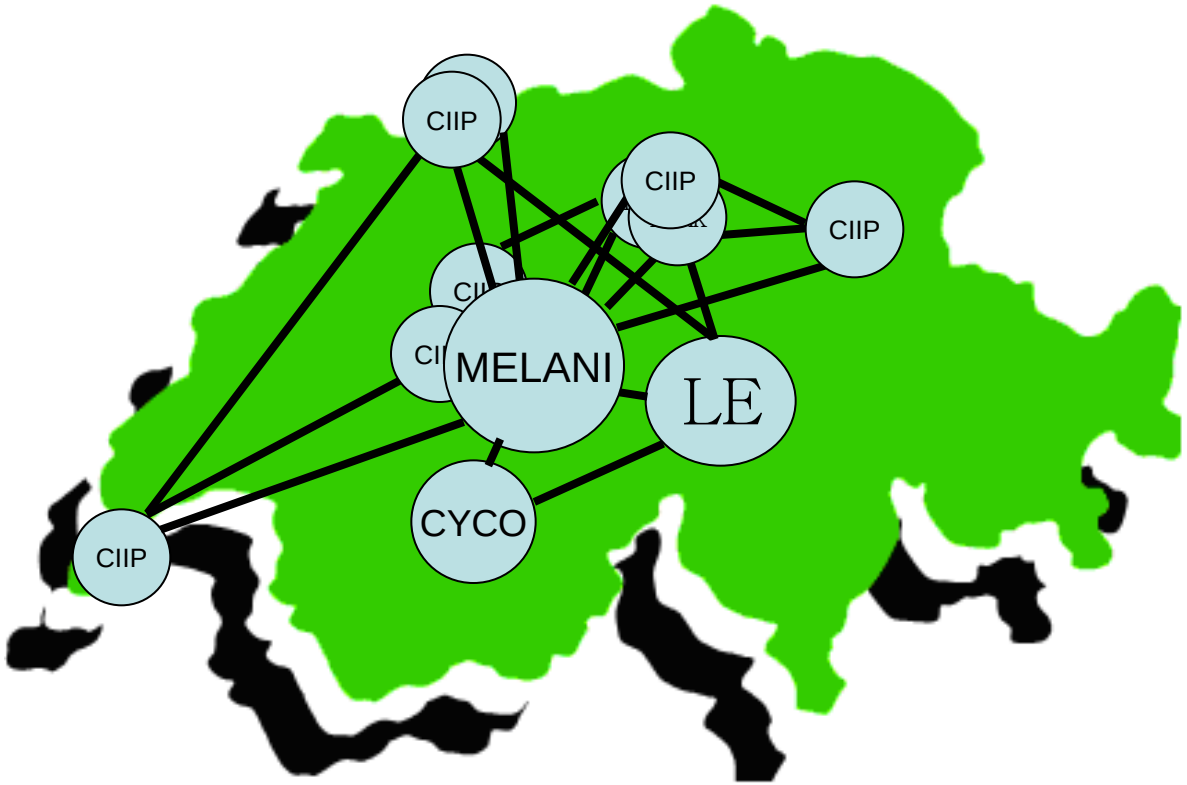
Federal Strategy Unit for Information Technology FSUIT
Federal Intelligence Service

Reporting and Analysis Centre for Information Assurance MELANI

MELANI: Information exchange – a story of success

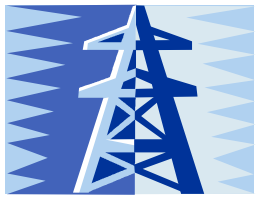
Max Klaus, Deputy Head
Reporting and Analysis Centre for Information Assurance MELANI

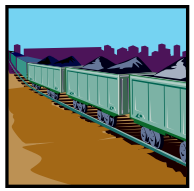
Information Exchange Switzerland



Critical Infrastructures

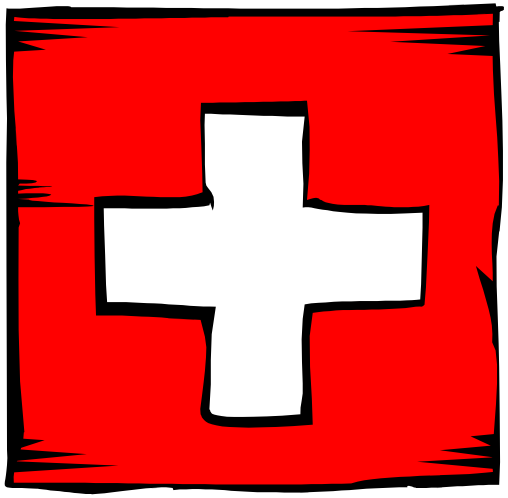
- Definition: Systems **critical** to the **functioning of our society**, such as
  - energy supply
  - telecommunications
  - banking & financial services
  - transportation
  - emergency & rescue services
  - health care
  - government & public administration





- In the **information age** these systems **depend** more and more **on IT infrastructures**.
- Hence, they need to be protected → **CIIP**

Public Private Partnership (PPP)



- Constitutional responsibility: Article 2, § 2 of the Swiss Constitituion „[…] aiming to ensure the public welfare […]“
- Government and the private sector must work together in a partnership → public private partnership (PPP)
- The bigger part of Critical Infrastructures lies in the hands of private enterprises

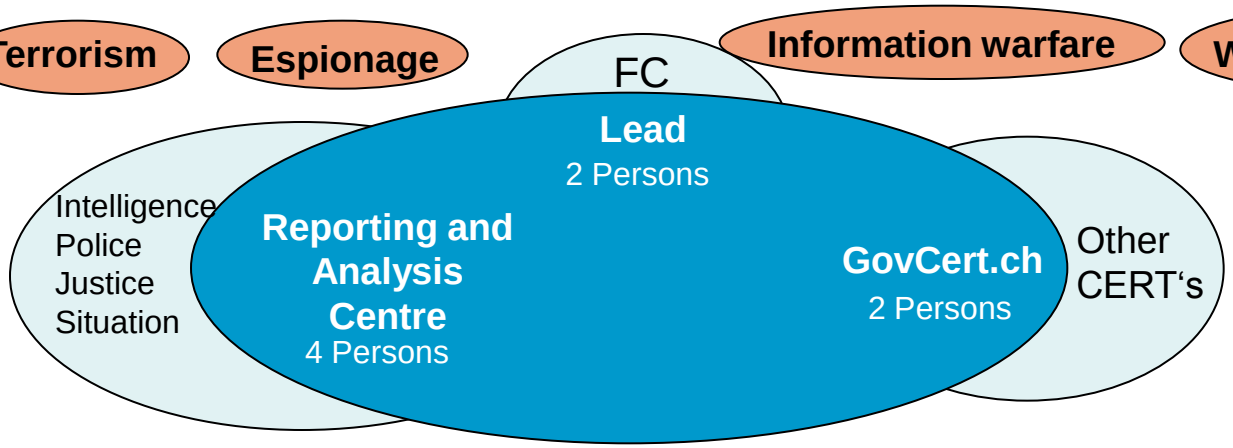
  → Closed Constituency

MELANI at a glance

Threats

Terrorism | **Espionage** | **Information warfare** | **White-collar crime**

Organisation



Services

Exercises
Workshops (SCADA, ISP, phishing, malware)
Incident handling (phishing, espionage)

Products

Analysis (situational report, factsheets, alerts)

Clients

Closed constituency
Finance, telecommunication, energy administration, industry, business

MELANI: Functionalities – Co-operation Partners

- **Intelligence** – **Service for Analysis and Prevention (SAP)** with the Federal Office of Police (**fedpol**)
  - Cybercrime (Cybercrime Co-ordination Unit, CYCO)
  - Federal Criminal Police
  - Well established co-operation with the private sector
- **GovCERT.ch**
  - Technical Experience
  - Access to the world-wide network of CERTs
- **Supervision** – **Federal Strategy Unit for IT (FSUIT)**
  - Active in CIIP since 1997
  - Relations to relevant CIIP organizations abroad

Constituencies

Constituency	Closed		Open
	GovCert.ch	Situation Centre	Situation Centre
Members	Selected Operators of Critical Infrastructures		SMEs Citizen
Number	March 2010: 9 sectors / 83 companies / 213 people		Open
Relationship	Strong Trust Relationship to MELANI		–
Interaction	Regular Meetings, MELANI-Net (Extranet)		Media, WWW, Exhibitions Notification of Incidents

Closed Constituency (March 2010)

Critical Infrastructure	# Companies	# People
Chemical industry	**2**	**4**
Energy Suppliers	**9**	**23**
Finance	**37**	**102**
Health Care	**4**	**4**
Industry	**2**	**7**
Telecommunication	**8**	**20**
Transport	**5**	**10**
Insurances	**2**	**2**
Government (Cantonal/Federal)	**14**	**41**
Total	**83**	**213**

Services for the Closed Constituency

➔ **Information Sharing Network „MELANI-Net“**

Öffentliche MELANI-Meldung zur aktuellen IE Schwachstelle (Sichtbar für alle)
Erstellt: 18.01.2010 11:24, Stephan Glaus, Sektor: MELANI, Firma: Lagezentrum (NDB)
Letzte Änderung: 21.01.2010 11:23, Stephan Glaus, Sektor: MELANI, Firma: Lagezentrum (NDB)

Gozi (Sichtbar für Sektor Finanz)
Erstellt: 26.01.2010 16:24, Andreas Greulich, Sektor: MELANI, Firma: GovCERT.ch
Letzte Änderung: 27.01.2010 14:33, Andreas Greulich, Sektor: MELANI, Firma: GovCERT.ch

E-Mail mit Worddokument nutzt Schwachstelle aus (Sichtbar für Firma [redacted] AG)
Erstellt: 07.08.2009 09:51, Stephan Glaus, Sektor: MELANI, Firma: Lagezentrum (NDB)

Services for the Closed Constituency

➔ Detection and Analysis

Datum: 6/1/08 2:45 PM

Von:

An:

Betreff: Abrechnungsvertrag

Grösse: 88 KB

Anlagen: Rechnung.rar (85.9 KB)

Sehr geehrter Kunde, sehr geehrte Kundin!
Ihr Abbuchungsauftrag Nr. 373646627373 wurde erfullt.
Ein Betrag von 9027.00 EURO wurde abgebucht und wird in Ihrem Bankauszug als "Paypalabbuchung " angezeigt.
Sie finden die Details zu der Rechnung im Anhang

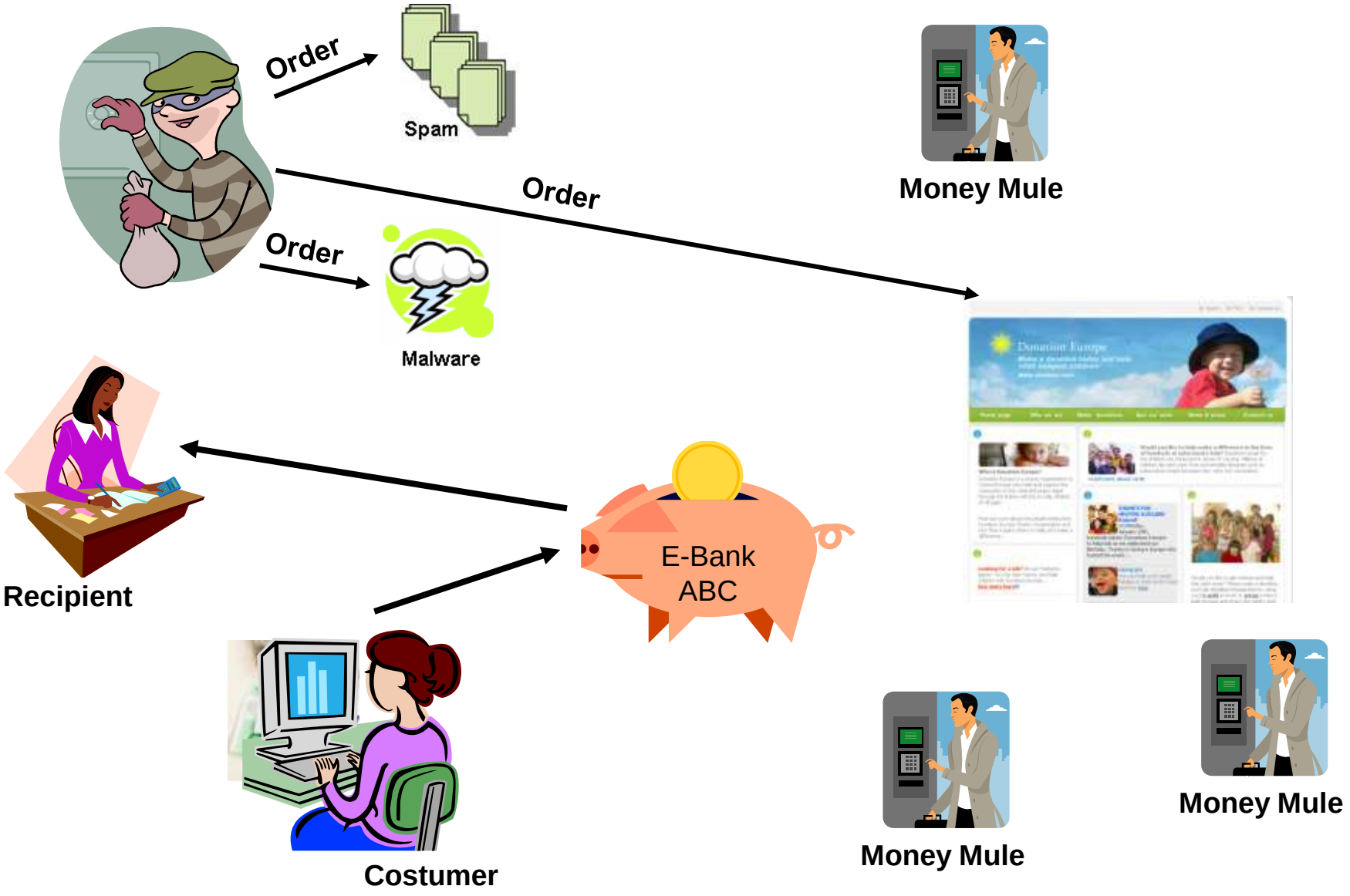
PayPal (Europe) S.224; r.l. & Cie, S.C.A.
22-24 Boulevard Royal
L-2449 Luxembourg

Vertretungsberechtigter: Brent Bellm
Handelsregisternummer: R.C.S. Luxembourg B 118 349

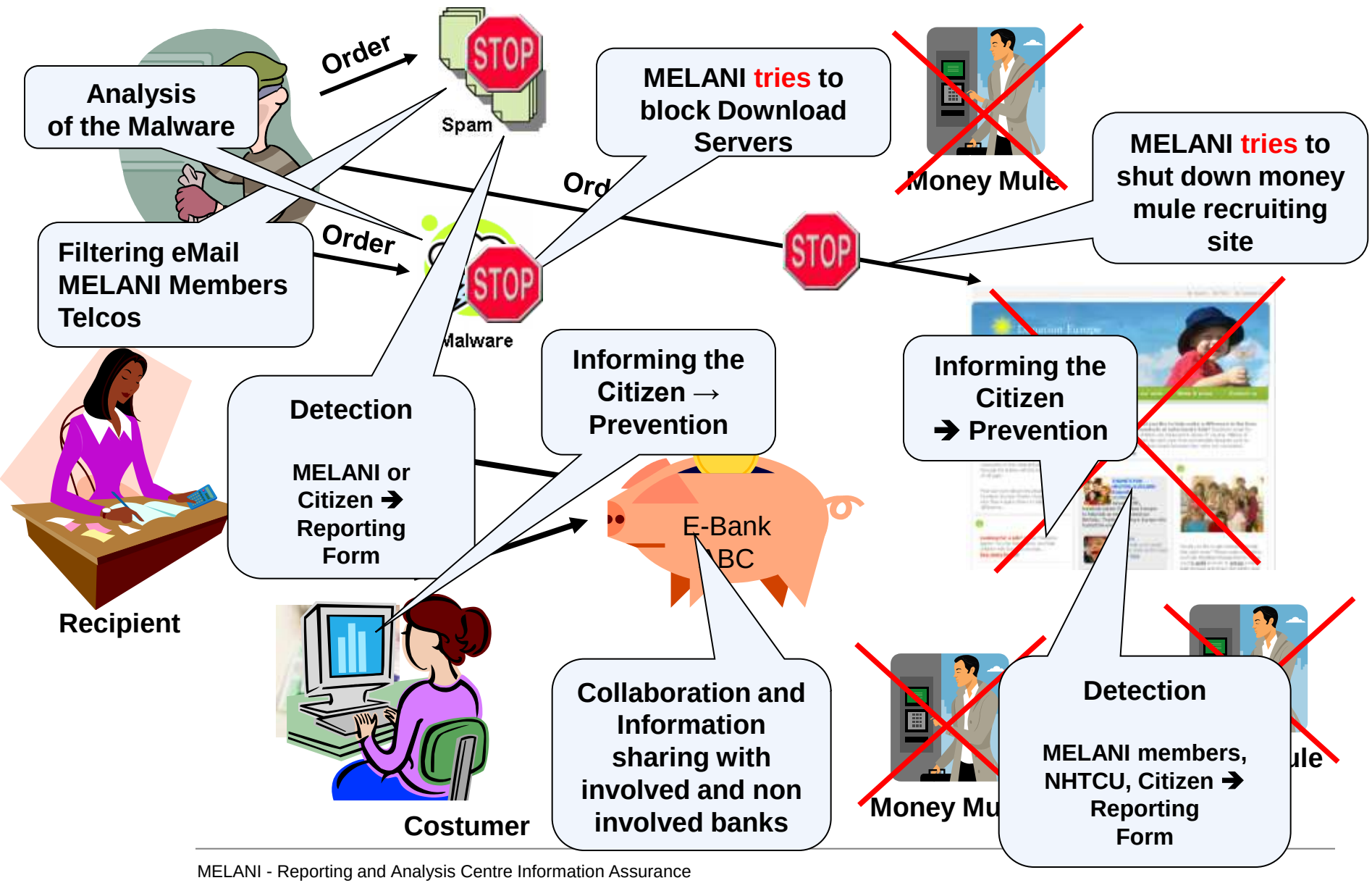
Anhang öffnen Rechnung.rar

Antworten | Allen antworten | Weiterleiten | Löschen | Zu

Example: E-Banking-Attack Information Exchange / Sensors



Example: E-Banking-Attack / Information Exchange - Sensors

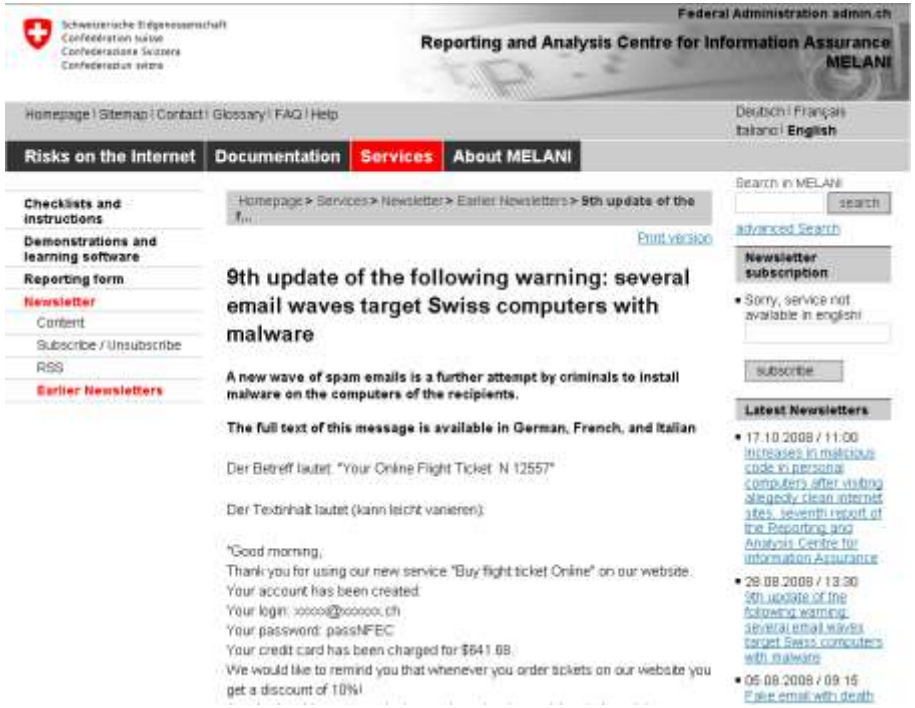


Services for the Open Constituency

Announcement of warnings, and information („tips“) in „**appropriate form**“ (language D, F, I, technical details)

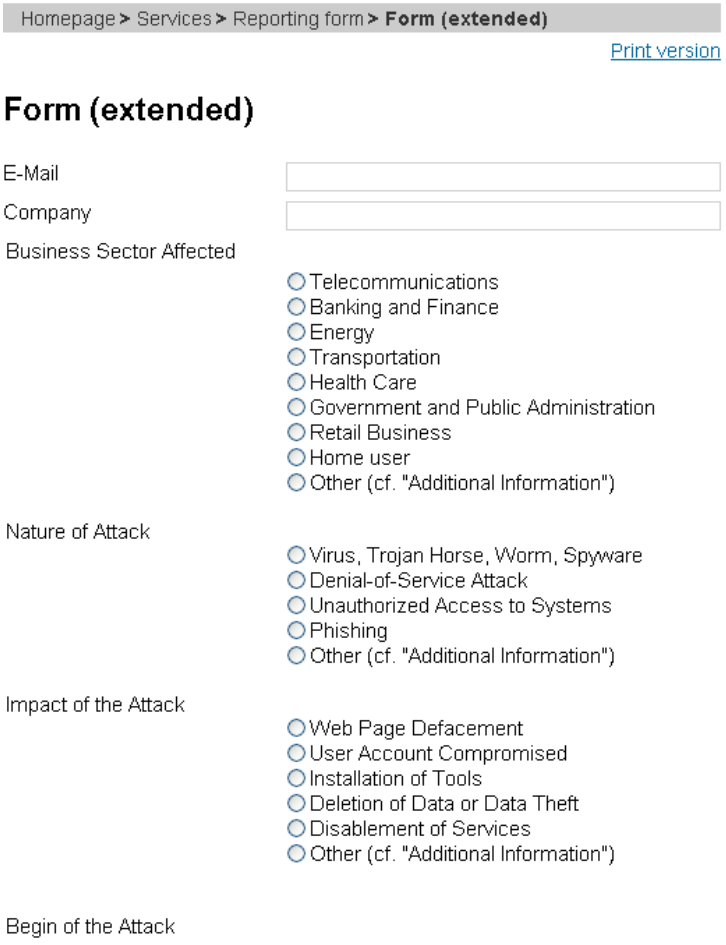
Publication of material for **incident prevention**

(e.g. best practices e.g. for e-banking, operating systems, …)



Services for the Open Constituency

Possibility to **report** incidents and attacks



Homepage > Services > Reporting form > **Form (extended)**

Print version

Form (extended)

E-Mail

Company

Business Sector Affected

- Telecommunications
- Banking and Finance
- Energy
- Transportation
- Health Care
- Government and Public Administration
- Retail Business
- Home user
- Other (cf. "Additional Information")

Nature of Attack

- Virus, Trojan Horse, Worm, Spyware
- Denial-of-Service Attack
- Unauthorized Access to Systems
- Phishing
- Other (cf. "Additional Information")

Impact of the Attack

- Web Page Defacement
- User Account Compromised
- Installation of Tools
- Deletion of Data or Data Theft
- Disablement of Services
- Other (cf. "Additional Information")

Begin of the Attack

Summary

- Law enforcement, intelligence services, CERTs **& the private sector** working together in a partnership is key.
- MELANI‘s **Public Private Partnership is a story of success**.
- A **trust relationship between MELANI** (e.g. Federal and Local Authorities) **and the private sector** boosts the efficiency in sharing information and responding to incidents.
- **Trust is built-up by collaboration** (even on less relevant cases) **and adhering to rules of conduct** (which are partially made explicit in a non-disclosure agreement).

Last but not least

Don‘t think about it…

http://www.perthlaw.biz/Bird%20Week%202006/nike.jpg

Questions?

Swiss Reporting and Analysis Centre for Information Assurance MELANI

http://www.melani.admin.ch

Max Klaus, Deputy Head
max.klaus@isb.admin.ch
+41 31 323 45 07