“Security made in Luxembourg”

TF-CSIRT

Hamburg 25-01-2010
Grand-Duchy of Luxembourg

- .lu
- Small European country
  - ~500,000 citizens
    (nearly doubling during working time)
- Main economic sectors:
  - Banking (~200)
  - Steel (HQ of ArcelorMittal)
  - ICT (EMEA HQs of Paypal, Amazon, iTunes, Huawei, Rakuten, etc.)
  - Biotech (Integrated Biobank of Luxembourg)
  - 99% SMEs

www.promoteluxembourg.lu
National strategy

“Plan directeur pour la sécurité des systèmes de l'information et de la communication”

(1) Awareness and prevention
   - CASES

(2) Incident handling
   - CIRCL

(3) Investigation and repression
   - PGD

(4) Legislation and standardisation
   - ILNAS

Strategy defined by the Ministry of the Economy and Foreign Trade
National structures

- **CASES** - [www.cases.lu](http://www.cases.lu) (FR, DE) (national IS portal)
  - Non-experts (general public) oriented
    - Awareness raising (e.g. SNS)
    - Fostering the "culture of security"
    - Communication driven

- **CIRCL** - [www.circl.lu](http://www.circl.lu) (EN)
  - "technical backend" for CASES
    - Technology watch, alerts and warnings
  - Constituency oriented
    - Incident response, handling & mitigation
  - Security professionals oriented
    - Foster national cooperation
    - Provide international coordination
Promote the “culture of security”

Tools used:
- Glossary
- Fact sheets in layman language
- Elaborated dossiers on special issues
- Behaviour rules
- Policy documents
- Certification labels

Communication channels used:
- Internet portal (www.cases.lu)
- Newspapers, Radio
- E-learning platform
- Workshops
- Conferences
- Poster-Teasers
- Large campaigns
- Fairs
CIRCL (Computer Incident Response Centre Luxembourg)

- Government CSIRT for the Grand-Duchy of Luxembourg

Constituency

- Ministries, administrations, municipalities, public organisations...
- Critical infrastructures (banking, ICT...)

Services focused on constituency interests'

- Proactive approach
  - Technology watch
- Reactive approach
  - Incident response/handling
  - Targeted distribution of alerts and warnings
- Quality management
  - Training and “consultancy” for constituency and partners

De facto national responsibility → ISAAC

International involvement

- TF-CSIRT, TI-listed (acc. 2010)
- FIRST (membership 2010)
National coordination: ISAAC
Information Sharing Analysis and Alerting Centre

**Information Sharing**
- incidents & vulns
- relevant information
- various

**Analysis &**
- interpretation
- contextualisation
- research

**Alerting Centre**
- warnings
- good practice

FI-ISAAC
ICT-ISAAC
...

Training
Alerts & Warnings

Incident mgmt
Incident handling
After care

Evaluation
Investigation
Research framework: LEWIS
Luxembourg Early Warning and Information Sharing System

• Build on existing projects/systems
  – Honeylux (capturing and analyzing malware)
  – CSIRT community (exchange of malicious IPs)
  – Online (shadowserver, malwareurl...)
  – New projects (passive DNS, network telescope...)

• To provide early-warning signs
  – Placement of network sensors on strategic intersection points
  – Active and passive intrusion detection
    • Honeynets / sensors
    • Phishing | spam | malware trapbox

• By analysing relevant data
  – Correlation of early-warning signs
  – Partly automated

• Fostering information exchange (input for ISAAC)
  – In a standardised, anonymous format
  – Daily security dashboard to members of the project
  – Dissemination of alerts and warnings
Security made in Letzebuerg
a national model

Children, citizen, SMEs

LuSI

R&D

ISAAC
NIS professionals

LEWIS
Security made in Letzebuerg
intragovernmental cooperation structure

- Ministry of education
- Ministry of the economy
- Ministry of the family
- Local gov. agencies
**Structure:**
- Publicly financed, private agency
- Stakeholders:
  - 3 ministries (MECO, MEN, MF)
  - 2 syndicats (SYVICOL, SIGI)
- Permanent support to CASES & CIRCL
  - Up to 8 FTE
  - Start spring 2010

**Goals:**
- Focus on the “weak”
  - schools, municipalities, youth houses,…
- Develop SME/SMA “markets”
- Foster national cooperation (ISAAC support)
- Enhance R&D (LEWIS operator)
last but not least, some news from the front...
the good, the bad and the ugly

(1) The good: *PGD – NTIC (ICT LE)*
✓ Recent take down of a “Trojan.Bredolab” C&C
✓ You'll get more information soon

(2) The bad: *Root eSolutions*
✓ AS5577 & AS44042
✓ 212.117.160/19
✓ NOT a bullet proof hoster
✓ we have direct contacts

(3) The ugly: *LuxSurf*
✓ domainhosting.lu
✓ we have an eye on them ;)

13