GOVCERT.LU

Luxembourg
22/09/2011
@ 34th TF-CSIRT Meeting

Patrick Houtsch
Luxembourg, a global ICT player

OBJECTIVES
Cyber Security Objectives

• Protect the country against major cyber threats

• Provide an attractive, secure and reliable environment for local businesses

• Protect our citizen’s privacy and fundamental rights
The puzzle was not yet complete

THE NEEDS
Needs

• At the basis
  – Constant awareness
  – Strong prevention
  – Efficient reaction

• On top
  – National Cyber Security Strategy
  – Governmental coordination
  – National and international coordination
The missing parts

• Cyber Security Board
  – Maintain and enforce a national cyber security strategy

• Governmental CERT
  – Covers classified and non-classified infrastructures
  – React and coordinate in case of incidents
  – Prevent and detect major incidents
  – Coordination of governmental actors
Know your enemy

THE THREATS
The threats as seen by CTIE

- Until today CTIE acted as de facto GOVCERT
  - Seeing about 10 attacks per day
  - Seeing about 2 targeted attacks per week
  - Some interesting malware analysis has been done

- Major potential threats
  - Espionage
  - Denial Of Service

We needed a dedicated team to handle incidents
The governmental CERT

GOVCERT.LU
GOVCERT.LU - Creation

• An in-depth study on needs & feasibility
• The result of collaboration
  – CTIE
  – HCPN
  – ANS
  – CCG/ANSSI
  – CASES/CIRCL
• Creation on the 15th of July 2011 by Council of Government
• Maximum collaboration through a coordination committee embracing all stakeholders
GOVCERT.LU - Mutualize

• Small country same challenges

• GOVCERT.LU is designed
  – To reuse the existing where possible
  – To offer more that incident handling
GOVCERT.LU - Structure

• Operated by the State Ministry

• All internal personnel has necessary security clearances

• Offices, forensic lab and servers located at CTIE, thus mutualizing high physical security standards

• Staff: 7 full time planned for now
GOVCERT.LU - Constituency

- About 400 contacts
  - All ministries and administrations (12K Users)
  - Critical infrastructure operators
  - Some major players in sensitive sectors
• Incident handling services
• Notification services
• Analysis
• Consultancy
• Expertise
GOVCERT.LU - Deployment

• Phase 1
  – Incident response (coordination)
  – Incident response (on-site)
  – Response to DoS incidents (coordination)
  – Anti-Phishing notification & closure
  – Compromised systems detection (passive)
  – Stolen credentials notification
  – Targeted malware notification
  – General security announcements (non public)

• Phase 2
  – Compromised DNS detection
  – Domain names surveillance
  – Malware analysis
  – Vulnerabilities analysis
  – Vulnerabilities notification
  – Vulnerability management

• Phase 3
  – Compromised systems detection (active scan)
  – Domain names incident intervention
  – Compromised BGP notification and intervention
  – Yearly security watch reports
  – Consulting services (technical recommendations)
  – Expertise services (audit, pentest)
  – Software analysis (non-malware)
GOVCERT.LU – and more

- Secretariat of the Cyber Security Board

- Animation of the « inter-ministerial coordination committee»
  - In closed configuration
  - In open configurations

- Yearly constituency meeting organization
GOVCERT.LU

www.govcert.etat.lu
www.govcert.lu
www.cert.lu (portal)

soc@govcert.etat.lu
info@govcert.etat.lu
A8B2CAC5 954C03F2 BFC720DA 1A33CF46 1DB41DEC

Patrick.Houtsch@govcert.etat.lu
5A618D56 31488912 374BC709 4EE967F5 802FF57A