Five years later

Lionel Ferette
Head of CERT
BELNET at-a-glance

• Belgian Research and Education Network

• ISP for all Belgian universities

• But also:
  • Federal Government
  • BNIX: Belgian National Internet eXchange
The BELNET Network
The Past
Five years ago

- Belgium was an empty spot on CERT maps
- Worse, BELNET was one of the very few CERT-less NRENs
- A 2003 user survey showed that security was our customers’ biggest concern
- I got hired at BELNET
The Present
Today

• We’ll be celebrating five years of BELNET CERT early July

• Manpower: 2.5 FTEs
  • Koen Van Impe
  • Christian Van Heurck
  • Lionel Ferette
Services

Security Tools Development
Intrusion Detection
Information Dissemination
Risk Analysis
Business Continuity Planning
Security Consulting
Awareness Building
Product Evaluations
Services

Incident Handling
Alerts & Warnings
Vulnerability Handling
Artefact Handling
Announcements
Technology Watch
Audits / Assessments
Configuration and Maintenance of tools

Security Tools Development
Intrusion Detection
Information Dissemination
Risk Analysis
Business Continuity Planning
Security Consulting
Awareness Building
Product Evaluations
Some Stats

Number of Incidents

- 2004
- 2005
- 2006
- 2007

Number of Incidents - Others
Number of Incidents - BELNET
More Stats

Advisories

Number of Advisories
However

• Belgium still a black spot on the map of Europe
  • NREN and military CSIRTs
  • No National / Governmental CSIRT
    • Competency officially lies with the telecom regulator
  • BELNET CERT used as “last-resort”
Tomorrow
From BELNET CERT to CERT.be

- In November, BELNET was asked to make a proposal for a National CSIRT
- Proposal rounds ended in February
- Still not formally signed, we are waiting for the lawyers to agree on the contract
Project Phases

- Four phases, gradually increasing in manpower and services offering
- Phase 1: this year
- Phase 2: early 2010
- Phase 3: Mid 2012
- Phase 4: Mid 2013
Phase 1

- Basic service: alerts, incident coordination, ...
- Manpower: 5+1 FTEs
- Constituency: Critical Infrastructure, telecom operators, Federal governments and Federal entities
- Authority: mostly based on good will
Phase 2

- Same Services
- Constituency is extended to the greater public
- Manpower: 6+1
- Authority: should shift towards legal authority
Phase 3

- Extension of the services offering, extension of opening hours
- Manpower: 8+1 FTEs
- Constituency unchanged
- Authority hopefully full legal authority
Phase 4

- Full service offering: vulnerability handling, artifact handling, education, consultancy
- Manpower: 10+1 FTEs
- Constituency and authority unchanged
Challenges

• Hiring

• Relation with the telecom regulator

• Addressing the greater public
Thank you!