CERT.be status update

Christian Van Heurck
CERT.be
25 September 2015 - TF-CSIRT 46 Tallin (open)
Agenda

1. CERT.be: *team update*

2. Projects 2015-2016
CERT.be - **PRESENT**

- End 2014 Publication of royal decree
  - Exit Fedict
  - Enter FPS Chancellery of the Prime Minister
- Since 2015: financed by the FPS Chancellery of the Prime Minister
  - Budget 2015 +/- 1.8 million €
- Still operated by Belnet
  - Protocol agreement between Belnet and Chancellery
CERT.be - PRESENT

- Team: 9 FTE
  - 1 Press & Communication
  - 1 Sysadmin+
  - 5 Security Analysts
  - 1 Coordinator
  - 1 Consultant Kris Boulez (1 year ½ FTE)
  - 1 Temporary FTE for BISC and National Campaign
- 3 Open positions
  - 2 Security Analysts
  - 1 Deputy Coordinator
Main goals for 2015:

- 12 FTE
- OPS back on track
- Study “National Detection Network”
- Awareness campaign
- BISC 2015
- BICO
- Cyber Security Coalition
- Strategic contacts & alliances
CERT.be - PRESENT

- Director and Deputy Director of BCC are in place
  - Miguel De Bruycker - Director
  - Phédra Clouner - Deputy Director

- Focus on “as-is” & “to-be”

- Focus on Incident Response & Handling
  - Critical Sectors
  - Including GOV and Academic & Scientific Potential

- Reforms in the background
  - Ministerial Committee for Intelligence and Security
CERT.be - FUTURE

• 16 FTE foreseen for 2015:
  • + Security Analysts
  • + Legal
  • + Admin

• Probably budget of +/- 2,3 Million Euro for 2016

• Protocol for 2016 is being created
CERT.be - Projects

• POC National Detection Network
  • Lessons learned - DONE
  • Stakeholders - DONE
  • Final report - ONGOING
  • Plan for POC - ONGOING

• MISP
  • Public - Private - ONGOING

• Intel MQ
  • Implementation - DONE
  • Documentation - DONE
  • In production - ONGOING
CERT.be - Projects

• Taxonomy
  • Root cause & Impact - ONGOING

• Reporting
  • Now directly to BCC - ONGOING
  • Including Shadowserver type data - ONGOING

• Knowledge Management
  • Define needs - DONE
  • Propose and implement - ONGOING

• BISC 2016
  • Theme and scope - TO BE DEFINED
CERT.be - Projects

• Awareness Campaign
  • 2015 - 1/10/2015 - Passwords
  • 2016 - TO BE DEFINED

• Internal Systems - ONGOING
  • Procedures
  • Documentation
  • Monitoring
  • Staging website(s)
  • ...

• Incident Handling & Response - ONGOING
  • Processes & Procedures
  • Training
  • ...

25/09/2015 - TF-CSIRT Tallin
CERT.be - Projects

• **Strategic Alliances - ONGOING**
  • CSC
  • B-BICO
  • TF-CSIRT
  • FIRST
  • EGC
  • CEP-Platform

• **RT-IR - ONGOING**
  • New setup
  • Implement taxonomy
  • Integration with Intel-MQ
  • ...

25/09/2015 - TF-CSIRT Tallin
CERT.be - Projects

• Secure Exchange & Storage
  • TO BE DEFINED

• Data Classification
  • Also within Belnet
  • TO BE DEFINED

• Upgrade www.safeonweb.be
  • 1/10/2015

• Upgrade www.cert.be
  • TO BE DEFINED
CERT.be - Projects

- CERT.be Certification
  - TO BE DEFINED

- Publications & Blogposts
  - ONGOING

- Recruitment
  - ONGOING