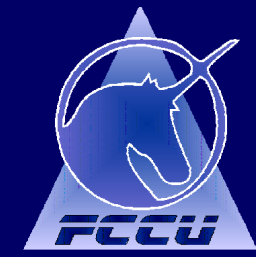


9-11 in cyberspace ?

Threats of e-insecurity in Belgium and the Belgian response

OWASP Conference

September 06th 2007, Brussels

Presentation by ...

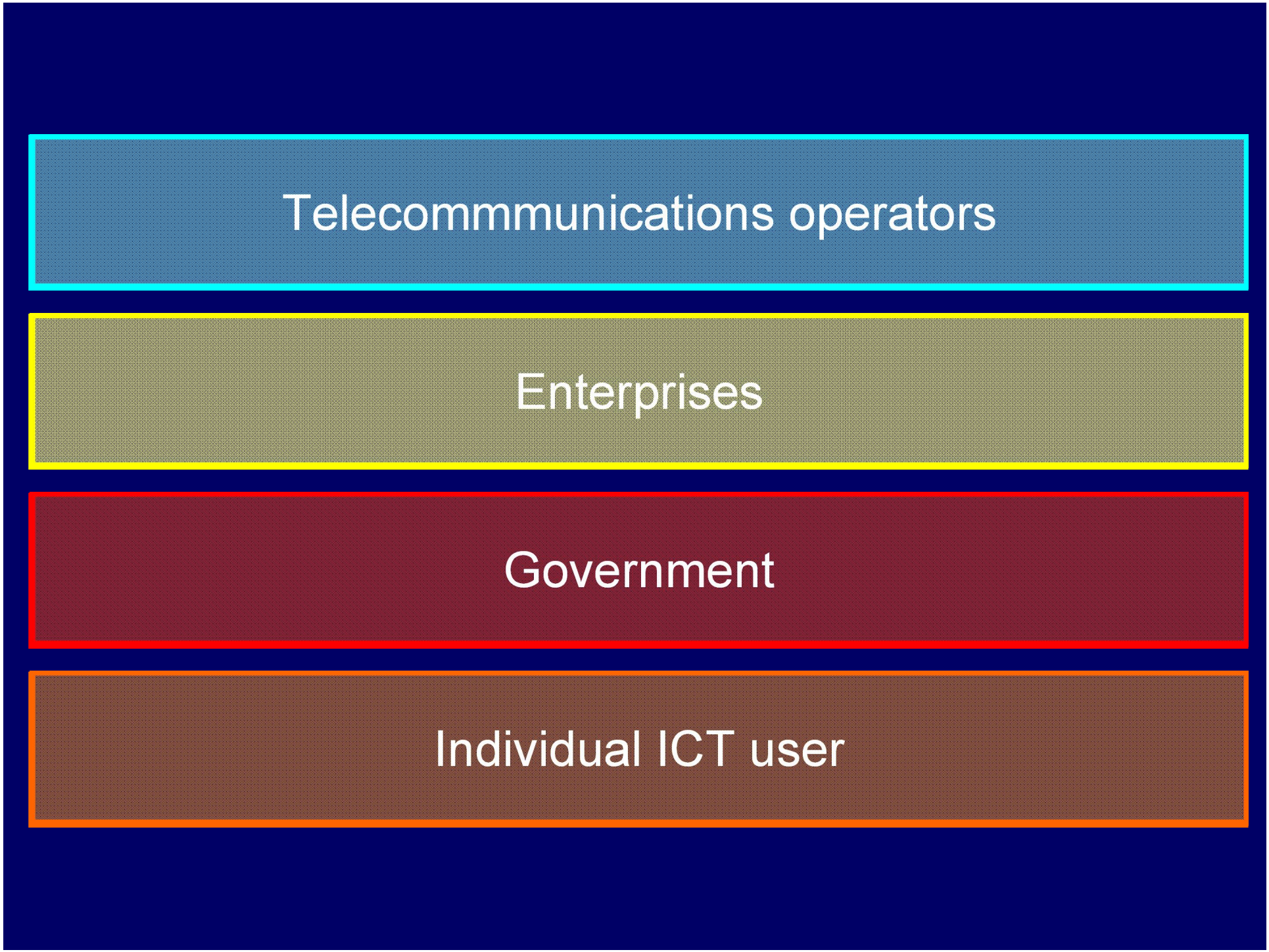
- Luc Beirens
  Head of the Federal Computer Crime Unit

- Belgian Federal Judicial Police
  Direction Economical and financial crime

Topics - overview

- Risks of e-insecurity : an analysis of the situation
  - Who are concerned ?
  - Who is threating us ?
  - Where are the threats
- Possible damage
- Belgian response
  - Governmental initiatives
  - Public Private partnerships
  - Police and justice response

Who is concerned ?


Telecommmunications operators
Enterprises
Government
Individual ICT user

Telecommmunications operators

- Information highway

⇒ Interconnexion of all

⇒ base of the new e-society

⇒ critical infrastructure

- Technology in different layers but the IP-layer in common

⇒ Base for all kinds of applications
=> replaces multiple infrastructures

⇒ strength but also the weakness of the system

- More and more operators – subcontractors

⇒ who is responsible for what ?

⇒ complexity for obtaining evidence

⇒ who will react in case of an incident ?

Enterprises

- Broadband = speed

⇒ Business opportunities

⇒ Replacing people by machines

⇒ New ways of working

⇒ connecting to the Internet

- Security = very often something for ICT
- Underestimation of value of data

Government

- Pushing e-society
- Allowing access to the digital world for all
- Developping e-government initiatives
- Creating legal framework to work in
  - Obligations of operators
  - Protection of privacy
- Responsible for national security and national economical interests

Individual ICT user

- Is customer for all these new e-world applications
- Is very often unaware of security risks
  - Badly protected
  - Behaves very unsecure

⇒ Gets infected with malware

⇒ weakest link in the chain => biggest danger

Who is threating us ?

High way criminals

Individual hacker

- Script kiddies
- Lonesome ICT-specialist in your company

Loosely organised criminals

- Individuals with specializations get in contact with each other over the internet
- Abuse evident security holes

Firmly organized criminals

- We see more and more organization in the criminal activity on the internet
- Financial intent
- Taking over legal businesses (development firms, operators, ...)
- Cooperation with moneylaunderers
- Different specialisations recruting persons – ICT development – handling money

Terrorist / hacktivists

- No financial intent

⇒ Political / social objectives

- Attact and create chaos and disaster

⇒ Destabilize economy and society

- Take time to prepare and ... BANG

Nations warfare troups

- Objectifs : supremacy
- Several nations with cyber troops
- Attacks ?
  - Recently … UK, Germany, US

Where are the main threats ?

Where are the main threats ?

- Malware attacks (viruses, worms, trojans, ...)
  fast spreading day zero infections
  => no immediate cure => lot of victims
  (especially home PC's – 24 / 365 available)

- Abuse of infected computers to create botnets
  (large "armies" of PC's under control of 1 master)
  => used to make massive attacks on
  webservers or network nodes
  => high risk for your critical ICT infrastructure

Why ? Making money !

- Sometimes still for fun (scriptkiddies)
- Spam distribution via Zombie
- Click generation on banner publicity
- Dialer installation on zombie to make premium rate calls
- Spyware installation

- Espionage => banking details / passwords / keylogging

- Ransom bot => encrypts files => money for password

- Capacity for distributed denial of service attacks DDOS => disturb functioning of internet device (server/router)

Is it realistic ?

- Already criminal cases in several countries
- Botnets detected
  - 2.000 => 100.000 zombie computers online
  - Infect / protect / stay ahead of Anti-Virus
  - generated huge datatraffic upto 20 Gbps
  - Big webservers went down
  - Their ISP (and their customers) went down
  - Communication networks went down

Important cases

- UK 2004 : gambling website down
  (+ hoster + ISP)
- NL 2005 : 2 botnets : millions of zombies
- BE 2005 : DDOS on chatnetwork of Media firms
- BE 2005 : DDOS on Firm (social conflict)
- US 2006 : Blue security firm stops activity
  after days of DDOS attacks
- SE 2006 : Website Gov and Police down
  due to DDOS after police raid on P2P
- EE 2007 : Widespread DDOS attack on Estonia
  after incidents on moving soldier statue

And the victims ?

- Who ?
  - Transactional websites
  - Communication networks
  - ISPs and all other clients
- Reaction
  - No reaction on blackmail
  - ISPs try to solve it themselves
  - Nearly no complaints made – even if asked …
- Result ? The hackers go on developing botnets

Combined threat

- What if abused by terrorists ?
  ... simultaniously with a real world attack?

- How will you handle the crisis ?
  Your telephone system is not working !

Risks

- Economical disaster
  - Large scale : critical infrastructure
  - Small scale : enterprise
- Individual data
- Loss of trust in e-society

What actions are needed ?

Threats on critical ICT infrastructure

First of all : strategy

- Every initiative for e-security is good

- Working according a strategy is better

⇒ Role of the government

⇒ Creation of BeNIS end 2005

⇒ Belgian Network Information Security

  ⇒ Several public security agencies / 2 subgroups

  ⇒ CIIP / Classified information

  ⇒ Public sector will be invited for projects

  ⇒ White paper for new government

Telecommmunications operators

- CERT ?
- Rapid exchange of information
- Have to make there infrastructure robust

Enterprises

- Evaluate business activity and value of data connected to the internet
- Backup systems if e-society under attack
- E-Security = businessrisk => management responsibility
- Report incidents to CERT ? to police ?

Individual ICT user

- Training / attitude
- Awareness : pcfoobie
- Security applications
- Protection by operators

Public private partnership ?

- Permanent concertation platform for Enterprise Security (since 2001)
  - Started with several groups – holdup / terrorism
  - ICT crime =>inform / handle incident / make report
- Belcliv – Belgian Club information security

E-Police organisation and tasks

<table>
<tr><td colspan="5">National Police</td></tr>
<tr><td rowspan="2">Federal Police
National Level
35 persons</td><td colspan="4">1 Federal Computer Crime Unit - 24 / 7 (inter)national contact</td></tr>
<tr><td>Policy
Training
Equipment</td><td>Internet investigations
Proactive projects
eCops Hotline
Internet fraud</td><td>Intelligence
e-payment
Information analysis</td><td>Operations & Telecom
Forensic ICT analysis
ICT Crime combating</td></tr>
<tr><td rowspan="2">Federal Police
Regional Level
120 persons</td><td colspan="4">22 Regional Computer Crime Units (1 – 3 Judicial districts)</td></tr>
<tr><td colspan="2">Assistance for housesearches, forensic analysis of ICT, taking statements, internet investigations</td><td colspan="2">Investigations of ICT crime case (assisted by FCCU)</td></tr>
<tr><td rowspan="2">Local Level
Fed Police
Local Police</td><td colspan="4">First line police</td></tr>
<tr><td colspan="4">“Freezing” the situation until the arrival of CCU or FCCU
Selecting and safeguarding of digital evidence</td></tr>
</table>

FCCU efforts e-security

- R&D on malware and botnets
- Member of BeNIS
- Member of Botnet WG MS - Interpol
- Member of Shadowserver group
- Member of Malware Alliance (DB)

Conclusion

- Society very heavily depends on availability and functioning of ICT
- ICT Infrastructure is vulnerable
- The tools to attack exist and are being tested

- Now we can wait for a 9-11 cyber attack …

  or act to prevent, protect, reduce damage

Contact information

Federal Judicial Police
Direction for Economical and Financial crime
Federal Computer Crime Unit
Notelaarstraat 211 - 1000 Brussels – Belgium

Tel office : +32 2 743 74 74
Fax : +32 2 743 74 19

E-mail : luc.beirens@fccu.be