Preparations for the EU presidency in Latvia

19.09.2014, TF-CSIRT in Rome

Baiba Kaskina - CERT.LV

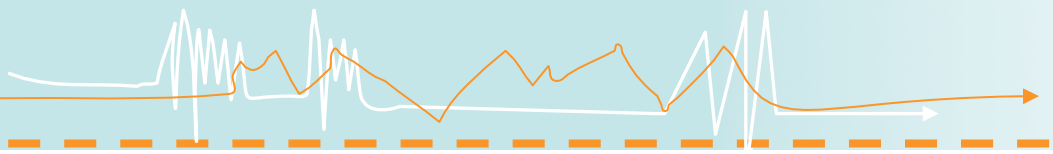
Outline

- Why prepare?
- Penetration tests & critical resources
- ISPs and measures
- Other activities

Why prepare?

EU presidency – January / June 2014

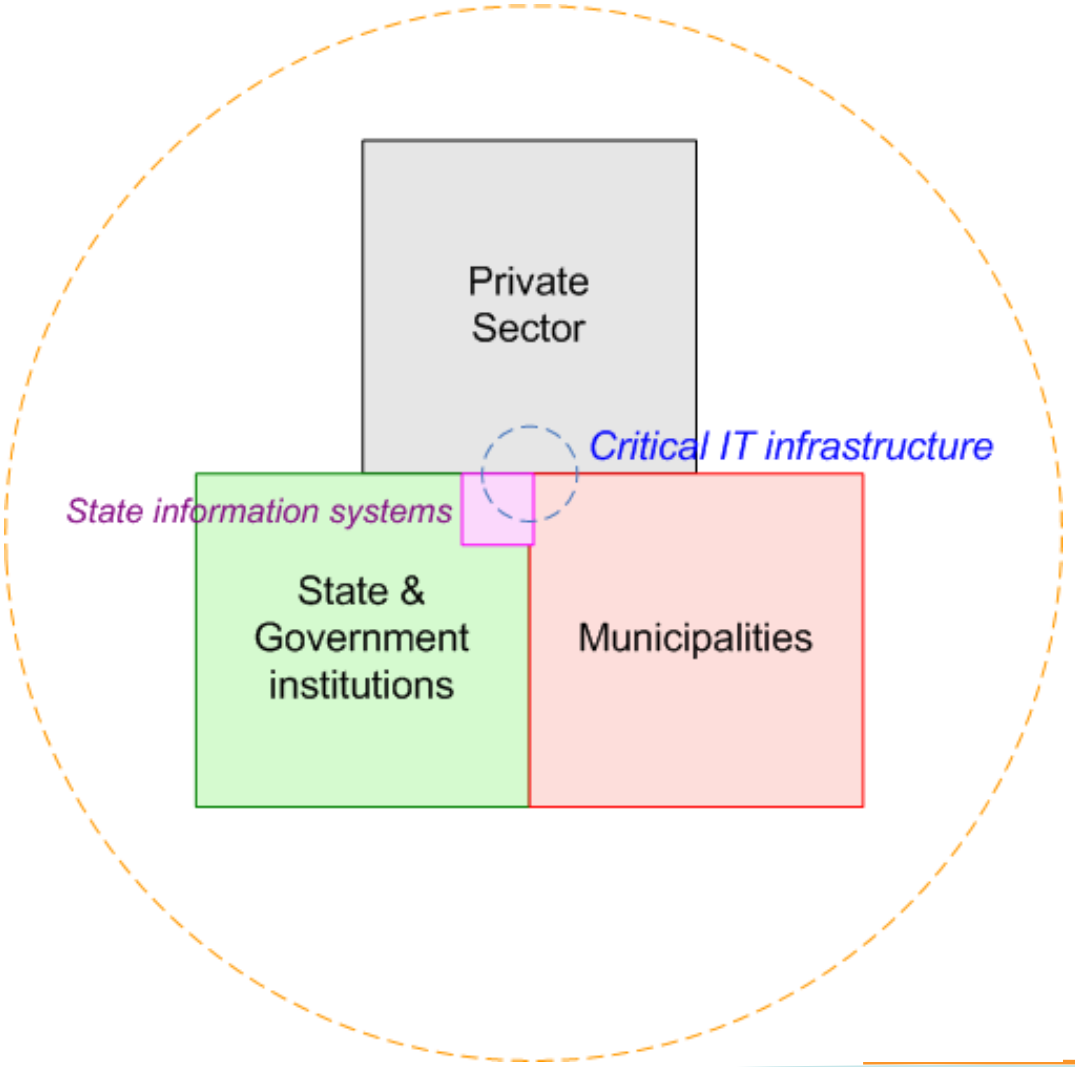
- Experience from others – Lithuania
- Geo-political situation
- It’s cheaper if you plan in advance



CERT.LV

Penetration tests & critical resources

CERT.LV constituency



Which are the critical resources for the presidency??

- Only government?
- Private sector too? Media???
- CII?
- VIP webpages?

Critical resources for the presidency

- ~250 web resources identified by CERT.LV
- Other lists/opinions – still in process

Penetration tests

- Started in January 2014
- WEB pentest and basic Network scan for vulnerable services
- So far ~80 resources tested (from 250)
  - 80% with critical vulnerabilities
  - 70% with medium risk vulnerabilities

XSS

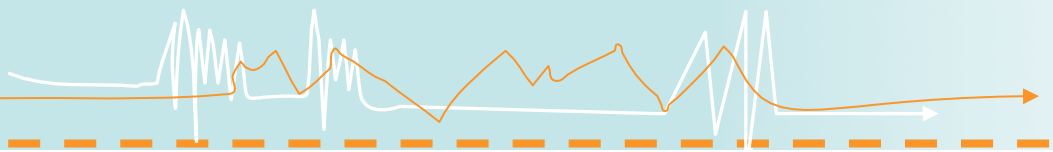
Ietekme:	Augsta
Risks:	Vidējs
Tips:	Ieviešana
Apraksts:	Uzbrucējs var panākt tīmekļa vietnes funkcionalitātes apiešanu, izpildot JavaScript, VBScript, ActiveX, HTML vai Flash patvalīgu kodu. Uzbrucējs var izmantot šo ievainojamību, lai nesankcionēti iegūtu vietnes lietotāju datus (session cookie, pārņemt lietotāja kontu, izmantot lietotāja identitāti. Pie noteiktiem nosacījumiem ir iespējama lietotāja iekārtas nonākšana pilnā uzbrucēja kontrolē.
Rekomendācijas:	Veikt ievades parametru pārbaudi, ievērojot labās prakses vadlīnijas. Veikt tīmekļa vietnes pirmkoda auditu, pārliecināties par ievades parametru drošu apstrādi.
Identificētais resurss:	/docSearch.do [searchtype parametri] /listView.do [type parametri] /newsGroupSave.do [editstate, email, first_name, last_name, regId parametri] Piemēram: GET: GET /newsGroupSave.do? form_name=archiveForm&sessionId=&editstate=new&regId=00ff3"><script>alert('cert.lv')<%2fscript>7768897f98a&first_name=sdfas&last_name=%27f%27%27&email=%27%27%27123%25 HTTP/1.1 Host: [redacted] User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Penetration tests – results and follow-up

- No warning, a sub-test – who notices (we have the mandate)
- All reports sent
  - Some report back when things are fixed
  - From some we never hear back
  - Repeated tests seldom (no time)
  - Popular feedback – «our system is old, no contact with the developer, no possibility to fix anything»...
  - Issues with outsourcing and hosting services
  - Issues with specifying security requirements in public procurement documents (technical specifications) - usually only functionality is described and security not even mentioned

Not everything is bad...

- Some new projects – very high quality
- CERT.LV involved in the public procurement specification regarding IT security of the project
- Some IT specialists are creative and responsible and fix issues themselves or find a solution



CERT.LV

ISPs and measures

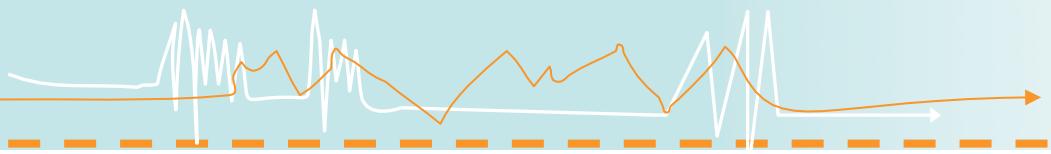
What can an ISP do?

- Most feared – DoS/DDoS
- ISPs – the key element
  - IPS/IDS against application layer DDoS
  - Internet based DDoS mitigation (scrubbing center services)
  - Connection to Tier-1 operator + predefined plans for attack mitigation coordinated with upstream ISP
- Situation
  - Understanding
  - Expenses
  - Government support?

Other activities

Preparations – other activities

- Seminar for State institutions representatives and ISPs (October)
  - How to prepare?
  - What to do when the attack happens?
- Gathering experience from other countries (input from CERT community would be appreciated)
- IT security exercise for heads of the ministries (December)



CERT.LV

Thank you!

http://www.cert.lv/

cert@cert.lv

baiba.kaskina@cert.lv