

Security and Confidence in Internet Technology Issues

Cristine Hoepers

[<cristine@cert.br>](mailto:cristine@cert.br)

CERT.br – CERT Brazil

<http://www.cert.br/>

NIC.br – Brazilian Network Information Center

<http://www.nic.br/>

CGI.br – Brazilian Internet Steering Committee

<http://www.cgi.br/>

The [In]Security Scenario

- **The Internet is part of the critical infrastructure of most countries**
 - **government, media, business, education and financial sectors, among others, rely on it**
- **New vulnerabilities every day**
- **Complexity of the infrastructure creates non-obvious vulnerabilities**
- **The technology and the security measures are too complex for the average user**
 - **even with awareness campaigns, some current threats will lure users**
- **Organized crime is also using the Internet as infrastructure and a vehicle for crime**

How is the Community Reacting to the Threats (1/2)

Network administrators/managers focus on

- Patch management
- Firewalls, IDSs, Antivirus, Antispyware, Antiphishing and other reactive technologies' deployment

More and more initiatives involving

- User awareness
- Network monitoring
 - Botnet and Fast Flux networks
- PKI and other crypto technologies' deployment

How is the Community Reacting to the Threats (2/2)

CSIRTs and security professionals are performing incident handling activities, which include:

- determining the impact, scope, and nature of the events**
- understanding the technical cause of the events**
- researching and recommending solutions and workarounds**
- coordinating and supporting the implementation of the response strategies with other parts of the enterprise or constituency**
- disseminating information on current risks, threats, attacks, exploits, and corresponding mitigation strategies through alerts, advisories, Web pages, and other technical publications**
- coordinating and collaborating with external parties such as vendors, ISPs, other security groups and CSIRTs, and law enforcement**

Clearly, the deploy-and-patch cycle is not working and won't work in the future

What is Missing?

- **Real improvement will come only with better software development practices**
 - **even the best protocol design or security measure is worthless if poorly implemented**
- **Better software depends on**
 - **demand from governments and society**
 - **industry applying software security practices through all the development phases**
 - **forming professionals that take security issues into consideration during design, implementation, test and deployment phases**

Next Steps?

- **Short/medium term:**
 - **continue with the current efforts of awareness, training, legal measures, among others**
 - **form CSIRTs and security professionals ready to deal with the threats and cooperate**

- **Long term:**
 - **update university curriculums**
 - **this means changing the mindset of the current teachers and researchers**
 - **demand better software security practices from the industry**
 - **governments and large organization can demand better software**
 - **support the current initiatives of secure software development and design**