nic.br cgi.br

20 years cert.br

ITU Regional Workshop on
“Strengthening capacities in international Internet governance”
Brasilia, DF **|** August 14 to 16, 2017

The Multistakeholder Nature of Internet Security and the Need for Cooperation

Lucimara Desiderá, MSc, CISSP
lucimara@cert.br

Main Objectives and Agenda

Objective:

Discuss some technical concepts related to **security and resilience** of Internet-connected systems, the **role of CSIRTs**, and the **need for cooperation** to achieve resilience/ security in a multistakeholder ecosystem.

Agenda:

- **Security and the Principles of Internet Governance**
- **Concepts:**
  - Resilience
  - Incident Management
- **The role of CSIRTs**
- **Cooperation**
  - International Forums

WSIS:
Declaration of Principles

Document WSIS-03/GENEVA/DOC/4-E

12 December 2003

[...]

B5) Building confidence and security in the use of ICTs

35. Strengthening the trust framework, **including information security and network security, authentication, privacy and consumer protection**, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

[...]

http://www.itu.int/wsis/docs/geneva/official/dop.html

CGI.br:
Principles for the Governance and Use of the Internet

CGI.br/RES/2009/003/P – PRINCIPLES FOR THE GOVERNANCE AND USE OF THE INTERNET

February 2009

[...]

8. Functionality, security and stability
The **stability, security and overall functionality** of the network must be actively **preserved through the adoption of technical measures that are consistent with international standards and encourage the adoption of best practices**.

[...]

http://www.cgi.br/resolucoes-2009-003-en/

NETmundial:
Internet Governance Principles

NETmundial Multistakeholder Statement

April, 24th 2014, 19:31 BRT

[...]

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a **secure, stable, resilient, reliable and trustworthy network**. **Effectiveness** in addressing risks and threats to security and stability of the Internet **depends on strong cooperation among different stakeholders**.

[...]

http://netmundial.br/netmundial-multistakeholder-statement/

Concepts
Resilience

100% Security is not feasible

- **Resilience:** the ability to recover from / adjust to a disruption (a fail or an incident)
  - **Identify what is critical** and need to be protected
  - **Define policies** (acceptable use policy – AUP, security policy, etc)
  - **Train technical staff**
  - **User awareness**
  - **Implement security measures** (in accordance to policies)
    - e.g. **keeping up to date** with the latest **security patches**
  - Establish an **incident management strategy**
    - a formally established and **properly trained CSIRT**

Concepts
Incident Management

- **Computer Security Incident –** any **adverse event, confirmed or suspected**, in relation to the security of computer systems or computer networks.
- **Incident Management –** ability to provide end-to-end management of events and incidents across and organization
- **Incident Handling –** process **of detecting and responding to** computer security incidents
- **CSIRT –** international acronym for **"Computer Security Incident Response Team**" an organization or team that provides **services** and support, **to a defined constituency**, for **preventing**, **handling** and **responding** to computer security incidents
  - other acronyms : **IRT, CIRC, CIRT, SERT, SIRT, CERT®**

The role of CSIRTs
Main objective: reduce damage / #victims

Reducing the impact of an incident depends on:

- the **agility** to **detect, analyze and respond** to an incident

The role of a CSIRT is:

- respond to incidents
  - reduce the damage/number of victims
  - help to return the environment to the production state
- help to protect the infrastructure and information assets
- prevent incidents and raise awareness
- help to detect security incidents

Key to success: Trustworthiness

- never expose sensitive data or victims

The role of CSIRTs
Main objective: reduce damage / #victims

CSIRT is not an investigation bureau or LEA

- focus on “**what/how**” not on “who”
- when a crime is identified it can help/cooperate
  - e.g. on preserving evidences

IGF Best Practices Forums

- **Establishing and supporting CSIRTs and Fighting Spam**

  2015: http://www.intgovforum.org/cms/best-practice-forums/2015-best-practice-forum-outputs

  2014: http://www.intgovforum.org/cms/best-practice-forums/igf-2014-best-practices-forums

Main Objective is a Healthy Ecosystem

No single group or structure can do security or incident response alone - everyone has a role

- **developers**
  - need to think about security since the early stages of development
- **management**
  - need to consider security as an investment and allocate adequate resources
- **network/system administrators and security professionals**
  - do not emanate "dirty" from their networks
  - **adopt best practice**s
- **users**
  - Understand the risks and take protective measures
- **educators**
  - building professional capacity on Security

Yet security attacks and incidents will occur

Cooperation is paramount - national and international

International Forums
Incident Response and Anti-Abuse

FIRST (Forum of Incident Response and Security Teams)

- Create in **1990**
- 380 members, from 81 countries, from various sectors (industry, academia, government).

Annual National CSIRTs Meeting (NatCSIRT)

- Organized by the CERT Division of the SEI/CMU since 2006

LAC-CSIRTs

- Latin American and Caribbean CSIRTs Meeting

International Forums
Incident Response and Anti-Abuse

APWG – originally *Anti-Phishing Working Group (since 2003)*

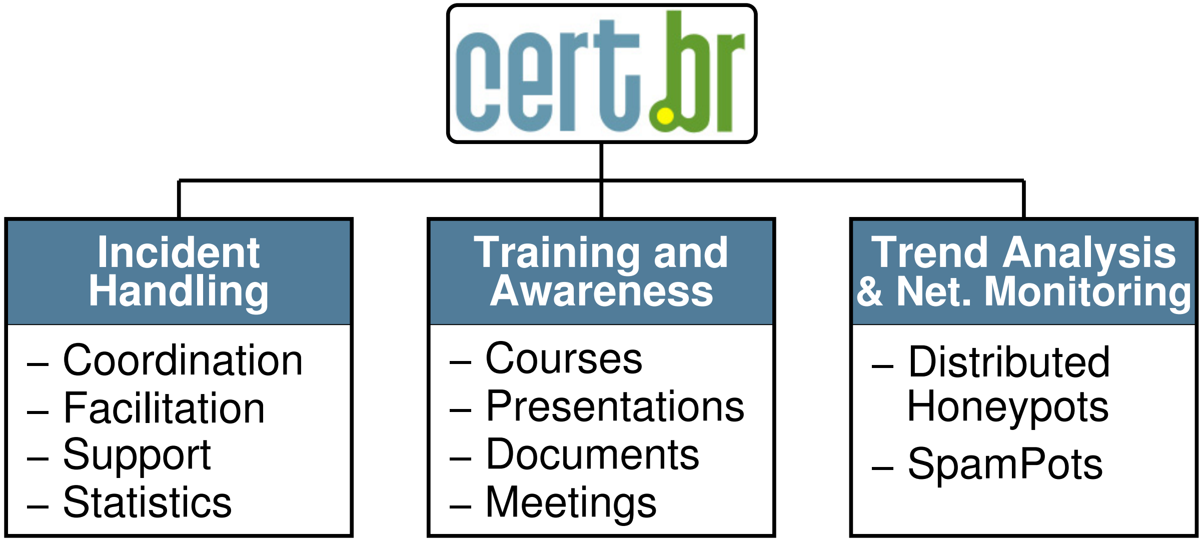
- membership of more than 1800 institutions worldwide from all the sectors. Currently an international coalition against cybercrime

M^{3}AAWG – *Messaging, Mobile, Malware Anti-Abuse Working Group (since 2004*)

- Membership: "*Internet Service Providers (ISPs), telecomm companies, Email Service Providers (ESP), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors and numerous security vendors*"

LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group (Since 2017)

- *Members: General Internet community, Network operators; Maintained by LACNOG, LACNIC and M^{3}AAWG.*



cert.br

Incident Handling
- Coordination
- Facilitation
- Support
- Statistics

Training and Awareness
- Courses
- Presentations
- Documents
- Meetings

Trend Analysis & Net. Monitoring
- Distributed Honeypots
- SpamPots

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon.

The Honeynet PROJECT

- **Incident Handling**
  - **National focal point for reporting security incidents**
  - **Help new CSIRTs to establish their activities**
  - **Establish collaborative relationships with other entities**
- **Training and Awareness**
  - **Training professionals**
  - **Production of best practices and awareness materials for diverse audiences**
- **Network Monitoring and Trend Analysis**
  - **Increase the capacity of incident detection, event correlation and trend analysis**

Since 1997

http://www.cert.br/about/

Thank You!

www.cert.br

lucimara@cert.br

@certbr

August 15th, 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br