Practical Recommendations for Incident Notifications

Lucimara Desiderá
lucimara@cert.br
CGI.br and NIC.br Structure

GOVERNMENT (Appointed)
1. Ministry of Science and Technology (Coordination)
2. Ministry of Communications
3. Presidential Cabinet
4. Ministry of Defense
5. Ministry of Development, Industry and Foreign Trade
6. Ministry of Planning, Budget and Management
7. National Telecommunications Agency
8. National Council of Scientific and Technological Development
10. Internet Expert

I. E.
11. Internet Service Providers
12. Telecommunication Infrastructure Providers
13. Hardware and Software Industries
14. General Business Sector Users
15. Non-governmental Entity
16. Non-governmental Entity
17. Non-governmental Entity
18. Non-governmental Entity
19. Academia
20. Academia
21. Academia

CIVIL SOCIETY (Elected)

Executive Branch

Administrative Support
Legal Counsel
Public Relations

Domain Registration
IP Assignment

cert.br
Studies and Surveys
About ICT use

etic.br
Internet Engineering
and New Projects

ceptro.br

W3C
Brazilian Office

registro.br
CERT.br Activities

- Incident Handling
  - Coordination
  - Facilitation
  - Support
  - Statistics

- Training and Awareness
  - Courses
  - Presentations
  - Documents
  - Meetings

- Network Monitoring
  - Distributed Honeypots
  - SpamPots

http://www.cert.br/about/
Incident notifications: the challenge
The challenge:

- Why should I notify?
- To whom?
- What information to include?
- How to find the right contacts?
- How to report?

REPORTING

- Who has sent this message?
- Why am I receiving this?
- What is the issue?
- Where are the evidences?
  - Logs saved as jpeg?!
  - No timestamps!
- What is expected from us?
How to make things better?
How to make things better?

GOAL
- make the notifications more understandable and easier to write;
- turn the incident handling process more effective.

A public document (Creative Commons) covering:
- Why to report incidents
- How to select the right contacts
  - Understanding the incident
- Where to look and how to search for contacts
  - WHOIS search samples
- How to write, format and send a notification
  - DO’s and DON’Ts
  - Set of templates
Some highlights
Recommendations for Incident Notifications

- Notifying Security Incidents
- What to notify
- Whom to notify
- Searching contacts
  - WHOIS
  - CSIRTs
  - Creating and maintaining your own database
  - Top-Level Domains (TLDs)
- Notification methods and format
- What to include in a notification
- Appendix A – WHOIS Query Examples
- Appendix B – Notification Templates
What to notify

• Some common incidents
  – Network scan, brute force, vulnerability exploitation attempt
  – Defacement
  – Rogue DNS
  – Malicious artifacts
  – Phishing
    • Regular / geolocation
    • Pharming
  – Denial of service attacks
    • Botnet attack
    • Amplification by service abuse
  – Sensitive data breaches
  – Malicious domains
Whom to notify

• Selecting the right contacts is key:
  • To avoid delays, discarded notification, inefficiency
  • Depends mainly on the characteristics of the incident
    • Not alerting the perpetrator

• Where to find contacts:
  – WHOIS databases => Appendix A – WHOIS Query Examples
  – CSIRTs contact lists
  – Your own database (creating and maintaining)
  – IANA root zone database (all TLDs and new gTLDs)
What to include

DO’s and DON’Ts:

• Text format (avoid data in .jpg, .gif, .xls, .pdf, etc.)
  – Makes it difficult to read and automate
• Avoid long lines (easy reading)
• Timestamps:
  – Time zone matters
  – Synchronization is essential (use NTP)
• Sanitize data (e.g. PII)
• Use cryptography when sending sensitive information
  – PGP is the de facto standard among CSIRTs
• Avoid legal jargon, accusations and retaliation
  – Better try the cooperation approach
What to include

General recipe:

• Salutation

• Short introduction about who’s writing and to whom the message is intended for

• Problem description including:
  – Concise explanation
  – Evidences (logs with time stamps and time zone information)
  – Additional information for clarification (when necessary)

• Expected actions

• Polite closure / thanks in advance

• Short signature
Templates

• Appendix B – Notification Templates
  – Preamble
    • template purpose
    • options that apply
    • how to use
  – Template with tags for tailoring / customizing
    • Portuguese and English
    • Spanish coming soon? ;-)

• Release date: first half of June
Thank You

www.cert.br

© lucimara@cert.br

May 20, 2015

nic.br /cgi.br

www.nic.br  |  www.cgi.br