14th Annual Technical Meeting for CSIRTs with National Responsibility
Edinburgh, UK | June 22, 2019
New National Initiatives

Dr. Cristine Hoepers
General Manager, CERT.br/NIC.br
cristine@cert.br

TLP as per first.org/tlp/
CGI.br:
A multi-stakeholder organization that coordinates all Internet related activities in Brazil.

**Government Representatives:**
1. Ministry of Science and Technology (Coordination)
2. Presidential Cabinet
3. Ministry of Communications
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

**Civil Society Representatives:**
10. Internet Expert
11. General Business Sector Users
12. Internet Service Providers
13. Telecommunication Infrastructure Providers
14. Hardware and Software Industries
15 a 18. Non-governmental Entity
19 a 21. Academia
NIC.br is a not-for-profit organization that implements all services and decisions of CGI.br.

The General Assembly consists of 7 members elected by the General Assembly.

The Administrative Council is composed of:
- Chief Executive Officer
- Administrative and Financial Director
- IT and Services Director
- Director of Special Projects and Development
- Consulting Director for CGI.br activities

The Executive Board includes:
- Administration
- Legal
- Communication
- Advisories: CGI.br and President

The organizational chart includes:
- registro.br: Domain Registration IP Assignment
- cert.br: Security and Incident Response
- cetic.br: Studies and Surveys About ICT use
- ceptro.br: Internet Engineering and New Projects
- ceweb.br: Web Technologies
- ix.br: Traffic Exchange
- W3C Brasil: Web Standards
CERT.br: Structure and Services

Service Areas:

Incident Handling
- National focal point for reporting security incidents
- Collect and disseminate information about threats and attack trends
- Increase the country’s security awareness and incident handling capacity
- Develop collaborative relationships with other entities
- Help new CSIRTs to establish their activities

Incident Management Training

Best Practices and Awareness Materials
- Network and system administrators
- End users
- Kids and parents

Created in 1997:
August/1996: report with a proposed model is published by CGI.br
June/1997: CGI.br creates CERT.br (at that time called NBSO – NIC BR Security Office)
Brazilian ISPs Ecosystem

Cetic.br National ISPs Survey
- Total ISPs (estimated): 6618
- Respondents: 2177
- 75% have 1000 clients or less

https://www.cetic.br/pesquisa/provedores/

IX.br SP
One of the biggest in the world
- #1 in participants (1467)
- #3 in traffic – both average (3.5T) and peak (5.1T)

https://www.pch.net/ixp/dir

≈700 ASes use MikroTik as core router

http://www.lacnic.net/en/web/lacnic/estadisticas-asignacion
We need a healthier ecosystem:
National Initiative – A More Secure Internet Program

Current Goal:
- Reduce the number of systems that can be abused for DDoS attacks

Incentive to adopt best practices:
- Hardening
- Routing Security
- Anti-spoofing (BCP 38)
- Close open services

Joint initiative involving several organizations
- ISOC and ISPs, Hosting and Telco Associations

https://bcf.nic.br/i+seg
A More Secure Internet Program:
Early Results – Antispoofing (BCP 38) Implementation

- Higher adoption than in other countries
- Noted by CAIDA Spoof Project

Matthew Luckie mjl@caida.org
Mon May 13 23:01:57 -03 2019

- Previous message (by thread): [GTER] Governança de Internet - SSIG 2019 - Ao vivo
- Next message (by thread): [GTER] BCP38 deployment in Brazil
- Messages sorted by: [date] [thread] [subject] [author]

Hi,

I am wondering if you can help me understand why it is that Brazil, as a country, seems to be active in deploying BCP38. When I look at the monthly reports that CAIDA's Spoof Project sends to GTER, there are often 5-6 networks that have deployed BCP38 in the past month. This is more than in other countries / regions.

https://eng.registro.br/pipermail/gter/2019-May/076685.html
A More Secure Internet Program:
Early Results – Reducing Open Services

Focusing more on the top 5:
- The top 1 (SNMP) reduced from 500K IPs to 100K
  - most in the big Telcos
- Ubiquity devices became abused recently
  - mostly on small ISPs

Common denominator in most of them:
- They are low cost CPEs (home routers)
- with bad factory defaults and do not allow changes most of the time

https://www.cert.br/stats/amplificadores/
Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Work developed by the LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group

Joint Publication of

- M³AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
- LACNOG - Latin American and Caribbean Network Operators Group
- Editor: Lucimara, LAC-AAWG Chair / CERT.br

Currently available in:
- English and Japanese

New translations to be released soon:
- Portuguese, Spanish, French, German and Korean

www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP
Awareness Materials Developments: InternetSegura.br Portal

Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!

- para Crianças
- para Adolescentes
- para Pais e Educadores
- para 60+
- para Técnicos
- para Interesse Geral
Portfolio under Creative Commons License Training Teachers to Use it in Class
A final note: National CSIRTs Cooperation
Kids Material – Now in Finish!

– Presented by CERT.br at the 2017 lightning round
– NCSC-FI reached us for permission to translate
  – released in finish at the 2019 Safer Internet Day

https://internetsegura.br/criancas/
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvallisesti-netissa-oppaat-lapsille-ja-vanhemmille
Thenk ye!
Thank You!

www.cert.br

@ cristine@cert.br   © @certbr

June 22, 2019