Desafios da Segurança na Internet e o Papel do CERT.br

Internet Security Challenges and the Role of CERT.br

Cristine Hoepers

cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

*Computer Emergency Response Team Brazil - **CERT.br***
*Network Information Center Brazil - **NIC.br***
*Brazilian Internet Steering Committee - **CGI.br***

Desafios para Melhorar a Segurança na Internet

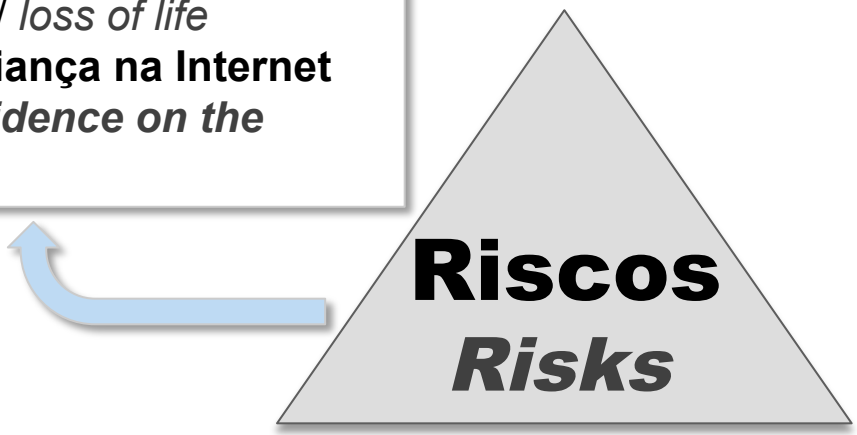
Challenges to Improve Internet Security

Riscos em Sistemas Conectados à Internet

Risks on Internet Connected Systems

- indisponibilidade de serviços
  services unavailability
- furto de dados / *data theft*
- perdas financeiras / *financial losses*
- danos à imagem / *reputation loss*
- risco de morte / *loss of life*
- **perda de confiança na Internet**
  loss of confidence on the internet

Internet



Atacantes/*Attackers*

- criminosos
  criminals
- espionagem industrial
  industrial espionage
- governos de outros países
  foreign governments
- vândalos / *vandals*

Vulnerabilidades/*Vulnerabilities*

- defeitos de *software*
  software bugs
- falhas de configuração
  configuration problems
- uso inadequado
  inadequate use
- fraquezas advindas da complexidade dos sistemas
  systems complexity leading to weaknesses

O que favorece o sucesso dos ataques?

What make the attacks easier?

Uma base muito grande de computadores com *software* desatualizado/vulnerável sendo ativamente abusada por atacantes

Attackers actively abuse a large base of end-user vulnerable computers

- **Especialmente em países em desenvolvimento**

  Specially in developing countries

As pessoas não compreendem o risco de

People don't understan the risks of

- **Colocar seus dados *online***

  publish their data online

- **Compartilhar seu dia-a-dia em público**

  publicly share their daily lives

- **Não entendem que não é possível ter privacidade e ao mesmo tempo compartilhar as informações em fóruns públicos**

  Finally, they don't understand that it is not possible at the same time to have privacy and share information in public foruns

Fatores que Contribuem para este Cenário
Factors that Contribute to this Scenario

Há grande motivação para ter usuários como alvo e não os servidores das organizações:

There are incentives to target end users and not organizations servers:

- **A tecnologia usada é muito complexa e poucos a compreendem**

  The technology is too complex and few understand it

- **É muito difícil entender o que é necessário para se proteger**

  It is very hard to understand what to do for protection

Fatores de comportamento também contribuem:

Behavior is a key factor too:

- **A noção de que a Internet é "virtual" e não "real"**

  The notion that the Internet is "virtual" and not "real"

- **Informações antes restritas ao círculo familiar e/ou de amigos, agora estão *online***

  Information that was restricted to family and friends is now online for everyone to see

  - **twitter, orkut, facebook, foursquare, etc…**

Segurança vs. Privacidade / *Security vs. Privacy*

- **Grande parte das contramedidas são tomadas sem considerar as questões de privacidade**

  Most countermeasures are taken without considering privacy issues

  - **A maioria sequer melhora a segurança**

    Most don't even improve security

  - **São medidas de controle**

    They are control measures

    - **Ex.: "*Unique IDs*", "*RFID passports*", RFID nos carros, banalização da biometria**

      Ex.: Unique IDs, RFID in passports and cars, biometry banalization

- **Como resultado, medidas necessárias são questionadas em nome da privacidade**

  As a result important measures are questioned in name of privacy

- **Não é necessário comprometer a privacidade para ter mais segurança**

  There is no need to compromise privacy to have more security

  - **mas controles e registros de eventos (*logs*) são necessários tanto para garantir tanto confidencialidade quanto disponibilidade**

    but control measures and logs are needed to guarantee confidentiality and availability

O Que Fazer? / *What to do?*

- **Riscos sempre vão existir, em qualquer meio**

  Risks will always exist, in any medium

- **A melhora não virá somente do uso de tecnologias de segurança ou da criação de leis, mas também:**

  Improvement won't come only from the use of security technologies or from the creation of new legislation, but also from:

  - **da compreensão dos problemas**

    understing the problemas

  - **da mudança em como as pessoas usam e desenvolvem a tecnologia**

    changes on how people use and develop technologies

- **Educação e conscientização são fatores chave**

  Education and awareness are key factors

  - **usuários, desenvolvedores e administradores de redes**

    users, developers and network administrators

  - **empresários, terceiro setor, executivo, legislativo e judiciário**

    businessmen, civil society, government as a whole

Situação no Brasil e o Papel do CERT.br

Developments in Brazil and the Role of CERT.br

Evolução do Tratamento de Incidentes no Brasil

Evolution of Incident Handling in Brazil

- **Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]**

  August/1996: CGI.br published the report "Towards the Creation of a Network Security Coordination Center for the Internet in Brasil"[1]

- **Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]**

  June/1997: CGI.br creates CERT.br (at the time called NBSO – NIC BR Security Office), based on the report and as a team with national focus

- **Agosto/1997: a RNP cria seu próprio CSIRT (CAIS)[3], seguida pela rede acadêmica do Rio grande do Sul (CERT-RS)[4]**

  August/1997: RNP creates its CSIRT (CAIS)[3], as well as the Rio Grande do Sul Academic Network (CERT-RS)[4]

[1] http://www.nic.br/grupo/historico-gts.htm
[2] http://www.nic.br/grupo/gts.htm
[3] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/cert-rs.html

Evolução do Tratamento de Incidentes no Brasil (cont.)

Evolution of Incident Handling in Brazil (cont.)

- **1999: outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs**

  1999: other organizations, including universities and Telecommunication Providers, began creating their CSIRTs

- **2003/2004 : grupo de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal**

  2003/2004: a working group was created to define the structure of a CSIRT for the Federal Public Administration

- **2004: o CTIR Gov foi criado, com a Administração Pública Federal como seu público alvo[5]**

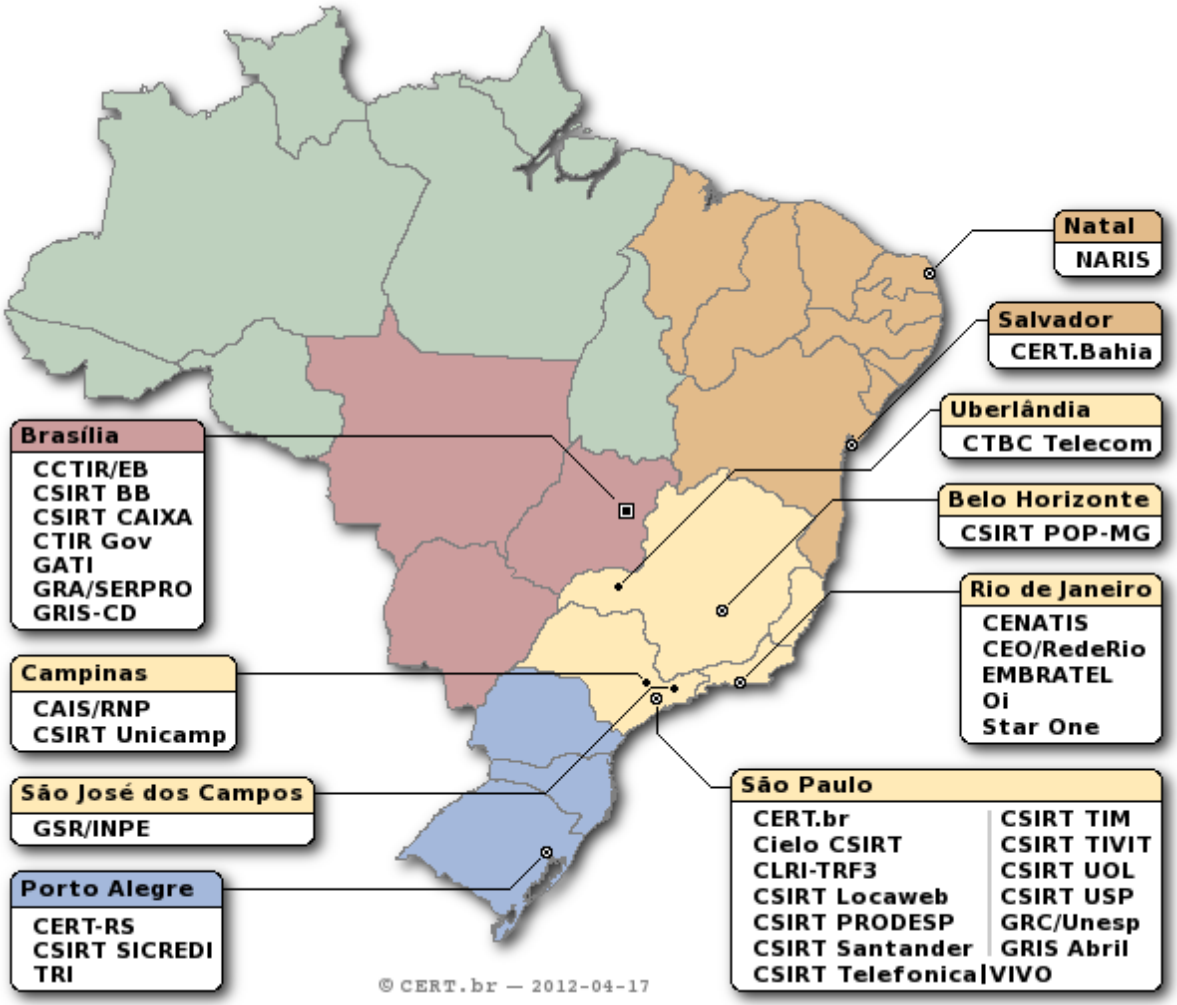
  2004: CTIR Gov was created with the Federal Public Administration as their constituency

[5] http://www.ctir.gov.br

CSIRTs Brasileiros – 35 em Dezembro/2012

Brazilian CSIRTs – 35 as of December/2012

Público Alvo *Constituency*	CSIRTs
Qualquer Rede no País *Any network in Brazil*	CERT.br
Governo Government	CCTIR/EB CLRI-TRF-3, CSIRT Prodesp, CTIR Gov, GATI, GRA/SERPRO, GRIS-CD
Setor Financeiro *Finantial Sector*	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, CSIRT Locaweb, EMBRATEL, CSIRT TIM, CSIRT UOL, StarOne, Oi, CSIRT Telefoncia|VIVO
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CERT-Bahia, CSIRT USP, GRC/UNESP, TRI
Outros / *Others*	CSIRT TIVIT, GRIS Abril



http://www.cert.br/csirts/brasil/ - http://www.cert.br/csirts/brazil/

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
– Articulação – Apoio à recuperação – Estatísticas	– Cursos – Palestras – Documentação – Reuniões	– *Honeypots* Distribuídos – SpamPots

cert.br

Incident Handling	Training and Awareness	Trend Analysis & Net. Monitoring
– Coordination – Facilitation – Support – Statistics	– Courses – Presentations – Documents – Meetings	– Distributed Honeypots – SpamPots

SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

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

Material Gratuito para Educação sobre Riscos e Proteção na Internet

Free Material for Education and Awareness

- Cartilha de Segurança para Internet
- Site Antispam.br
- Vídeos Educacionais
- InternetSegura.br

INTERNET SEGURA.BR

Contatos / *Contacts*

Cristine Hoepers

cristine@cert.br

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do Ponto br**
  http://www.nic.br/
- **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/