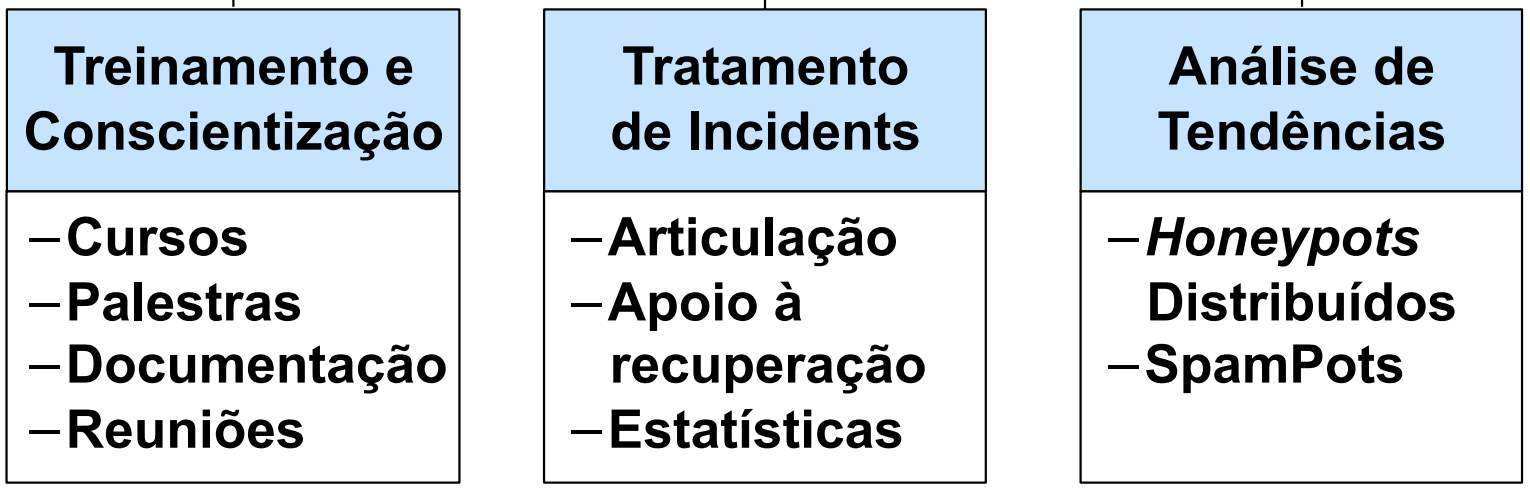
Segurança × Privacidade?

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

CERT.br



SEIPartner CERT Courses

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT®

Criado em 1997 para:

- Ser um ponto de contato nacional para notificação de incidentes de segurança
- Prover a coordenação e o apoio necessários no processo de resposta a incidentes
- Estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones
- Auxiliar novos CSIRTs a estabelecerem suas atividades
- Aumentar a conscientização sobre a necessidade de segurança na Internet

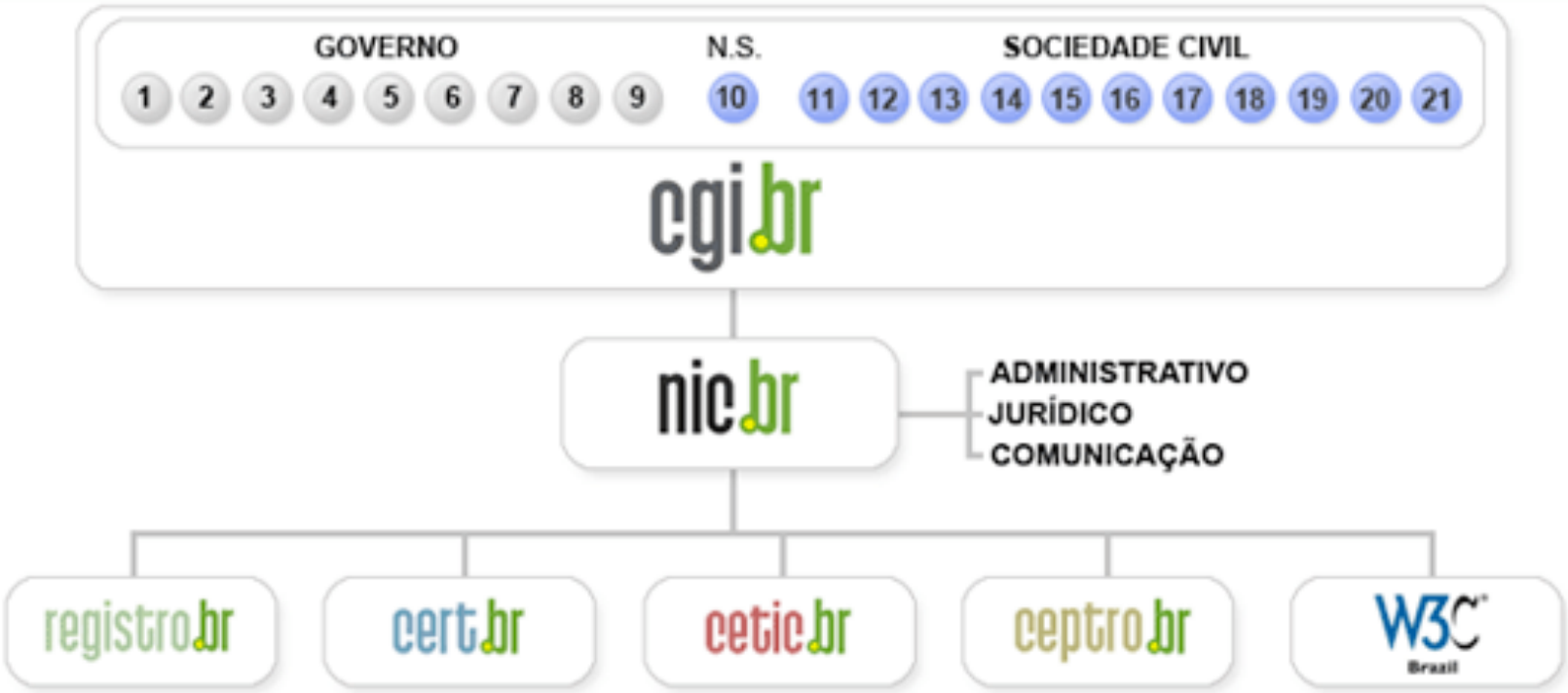
Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre-cg/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Agenda

- Antes de mais nada: qual o cenário de ataques e ameaças na Internet hoje?
- Afinal, o que é privacidade e o que é segurança?
  - São mesmo conceitos que se opõe?
- Desafios

Cenário

Características dos Ataques mais Freqüentes

- Contra usuários finais
  - fraudes, *phishing*, *bots*, *spyware*, etc
  - motivação financeira
  - abuso de *proxies*, na maioria instalados por *bots*
- De força bruta contra serviços de rede
  - Tentam adivinhar senhas de forma sucessiva
  - Serviços mais atacados: SSH, FTP, Telnet, VNC, etc
- Com rápido crescimento nos últimos meses
  - ataques a aplicações Web vulneráveis
- Não tão freqüentes, mas com grande impacto por serem contra a infra-estrutura crítica da Internet
  - ataques contra servidores DNS
  - contra protocolos de roteamento como o BGP

Quem está perpetrando os ataques?

Ameaças:

- Vem do crime organizado
- E continuarão vindo do crime organizado
- Quanto maior o número de informações e serviços online, maior o incentivo para atacar

Usuários são o maior alvo:

- Tem pouco conhecimento da tecnologia
  - A tecnologia é muito complexa
- É muito difícil entender o que é necessário para se proteger
- Eles memo põe sua privacidade em risco ao colocar todas as suas informações online
  - Facebook, twitter, orkut, etc…

Definições de Privacidade e Segurança

Privacidade

Merriam-Webster

http://www.merriam-webster.com/dictionary/privacy

1 a : the quality or state of being apart from company or observation : seclusion b : freedom from unauthorized intrusion <one's right to privacy>

RFC 4949 – Internet Security Glossary, Version 2

http://www.ietf.org/rfc/rfc4949.txt

1. *(I) The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.*
2. *(O) "The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed."*

Segurança

RFC 4949 – Internet Security Glossary, Version 2

http://www.ietf.org/rfc/rfc4949.txt

1a. *(I) A system condition that results from the establishment and maintenance of measures to protect the system.*

1b. *(I) A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss.*

2. *(I) Measures taken to protect a system.*

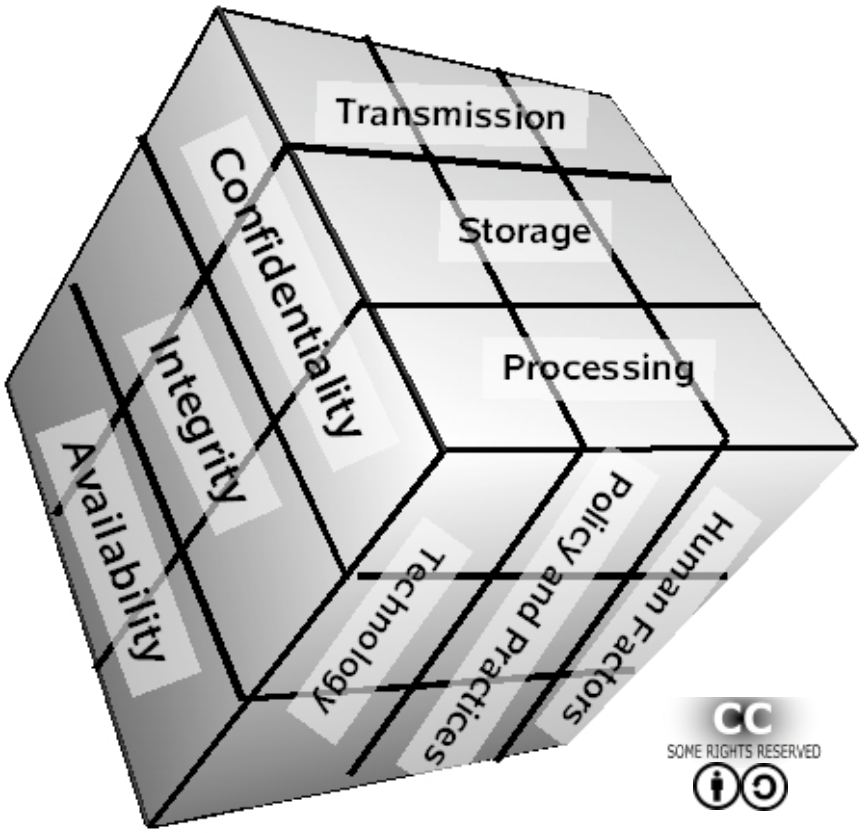
Segurança da Informação

RFC 4949

http://www.ietf.org/rfc/rfc4949.txt

(N) ***Measures that implement and assure security services in information systems, including in computer systems and in communication systems.***

Information Security Rubik's Cube



http://en.wikipedia.org/wiki/File:Mccumber.jpg

Desafios

O Cenário favorece o sucesso dos ataques

- **Muitas vulnerabilidades de Software**
- **Uma base muito grande de computadores com software desatualizado sendo ativamente abusada por criminosos**
  - **Especialmente em países em desenvolvimento**
  - **Usuários tem dados furtados e pagam a conta do uso da Internet por criminosos**
- **As pessoas não compreendem o risco de**
  - **Colocar seus dados online**
  - **Compartilhar seu dia-a-dia**
  - **Não entendem que não é possível ter privacidade e compartilhar as informações em fóruns públicos.**

De onde vem o debate "*Security vs. Privacy*"?

- **Grande parte das contramedidas são tomadas sem considerar as questões de privacidade**
  - **A maioria sequer funciona ou melhora a segurança**
  - **Ex.: "*Unique IDs*", "*RFID passports*",**
- **Como resultado, medidas válidas e necessárias são questionadas em nome da privacidade**
  - **Mesmo que não afetem a privacidade**
- **Não é necessário comprometer a privacidade para ter mais segurança**
- **Muitas das quebras de privacidade não tem nada a ver com segurança**

Resumindo: O desconhecimento do problema e das soluções gera um embate que não deveria existir.

O Que Fazer?

- **Educação é chave**
  - **Mas não só de usuários**
- **Se não mudarmos**
  - **O modo como desenvolvimento de *software* é ensinado nas Univerdades de computação e engenharia**
  - **E o modo como as empresas desevolvem *software***

Não acho que estaremos melhor em 20 anos

A melhora não virá do uso de tecnologias, mas sim da compreensão dos problemas e da mudança em como as pessoas usam a tecnologia.