

Segurança na Internet

Miriam von Zuben

miriam@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

Agenda

- **Contextualização**
 - Internet no Brasil
 - CERT.br / NIC.br / CGI.br
- **Cenário atual**
 - estatísticas
 - ataques mais frequentes
- **Desafios**
- **Considerações finais**

Internet no Brasil

Evolução da Internet no Brasil



1989	Criação e delegação do código de país (ccTLD) “.br” à FAPESP
1991	Primeira conexão TCP/IP brasileira, realizada entre a FAPESP e o Energy Sciences Network (ESNet) por meio do Fermilab (<i>Fermi National Accelerator Laboratory</i>)
1995	Criação do CGI.br (Portaria Interministerial MC/MCT nº 147, de 31 de maio) com a missão de coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados
1995	Criação do Registro.br
1997	Criação do CERT.br (à época NBSO)
2005	Criação do NIC.br, entidade sem fins lucrativos para executar as diretrizes do CGI.br e prestar serviços para a estabilidade e segurança da Internet no Brasil

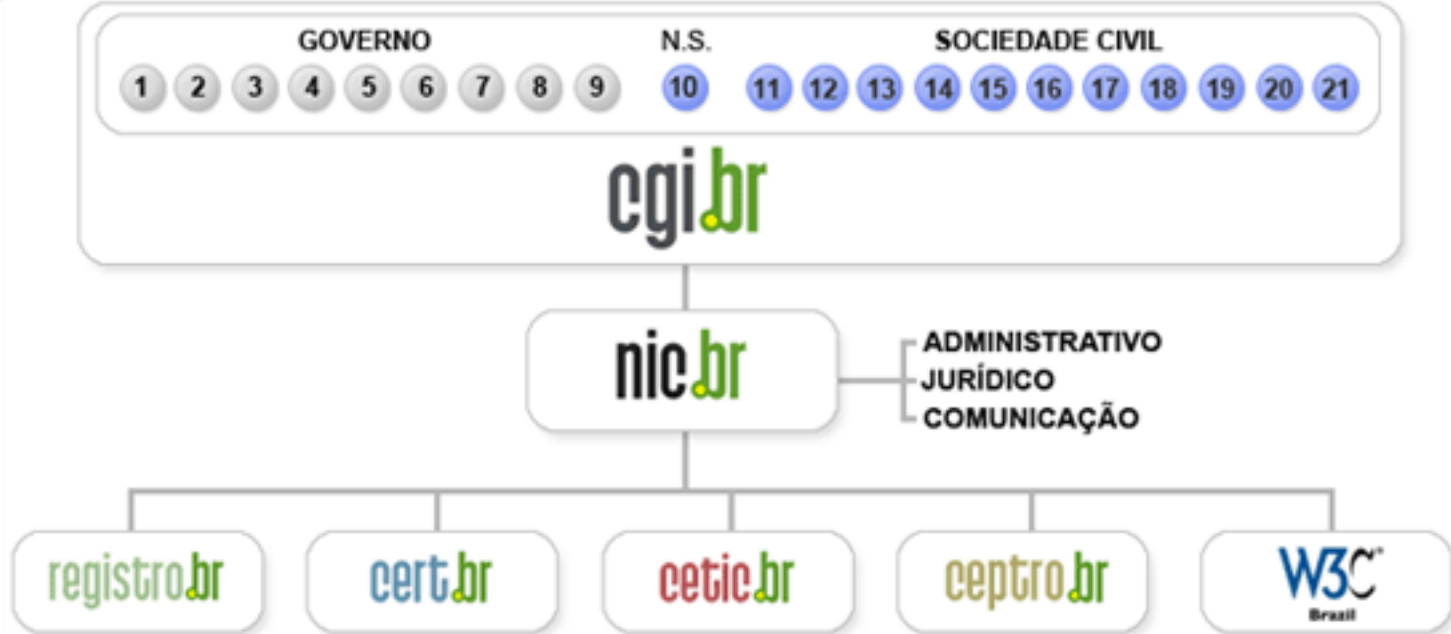
Comitê Gestor da Internet no Brasil – CGI.br

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



Tratamento de Incidentes
<ul style="list-style-type: none"> – Articulação – Apoio à recuperação – Estatísticas

Treinamento e Conscientização
<ul style="list-style-type: none"> – Cursos – Palestras – Documentação – Reuniões

Análise de Tendências
<ul style="list-style-type: none"> – <i>Honeypots</i> Distribuídos – SpamPots



Criado em 1997 para:

- Ser um ponto de contato nacional para notificação de incidentes
- Prover a facilitação e o apoio necessários no processo de resposta a incidentes
- Estabelecer um trabalho colaborativo com outras entidades
- Aumentar a conscientização sobre a necessidade de segurança na Internet
- Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades

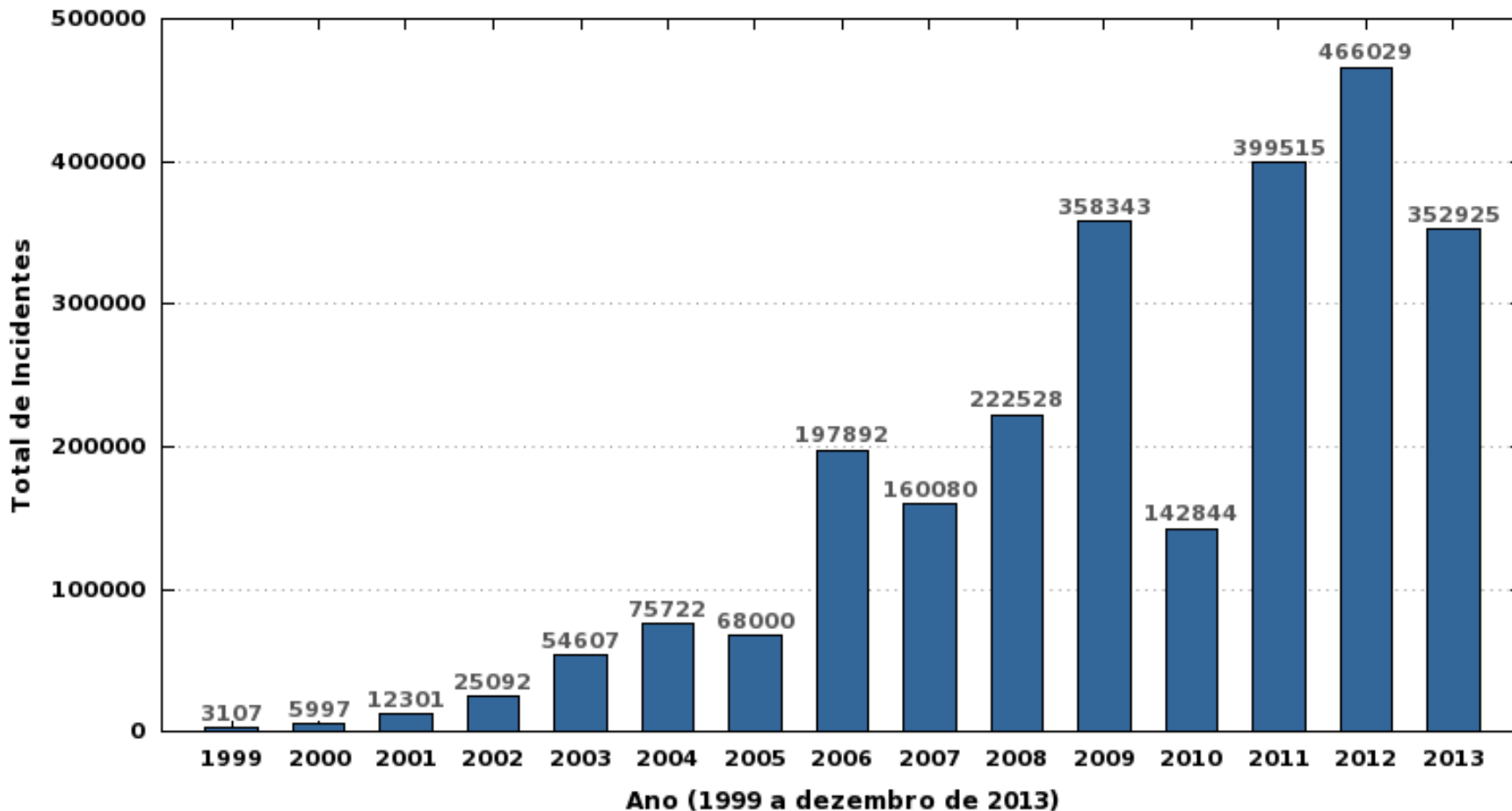
Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil

<http://www.nic.br/grupo/historico-gts.htm> | <http://www.cert.br/sobre/>

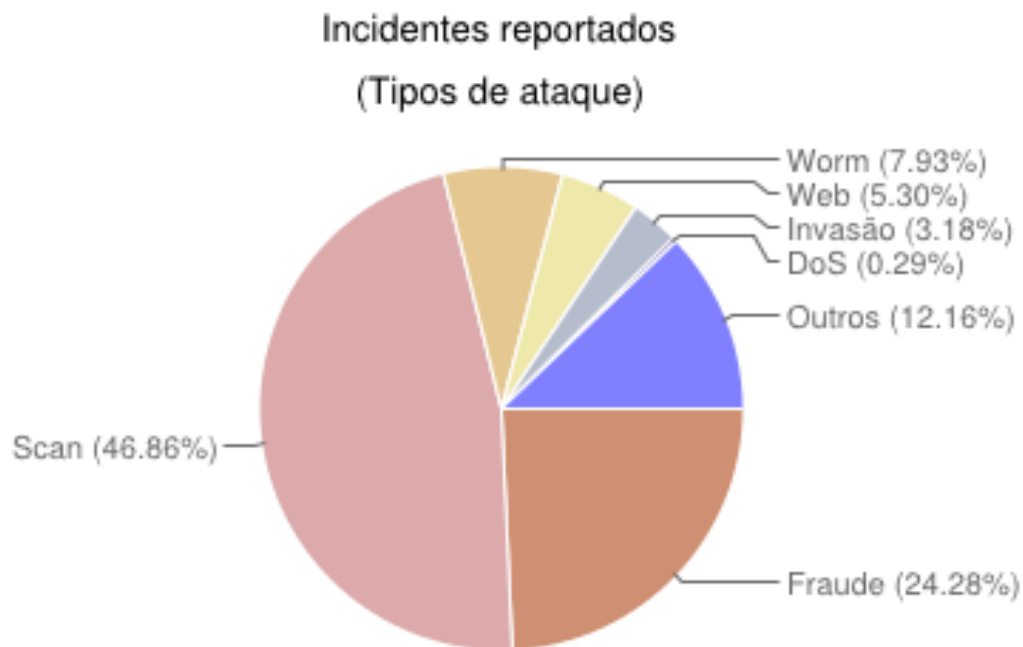
Cenário atual

Incidentes reportados ao CERT.br

Total de Incidentes Reportados ao CERT.br por Ano

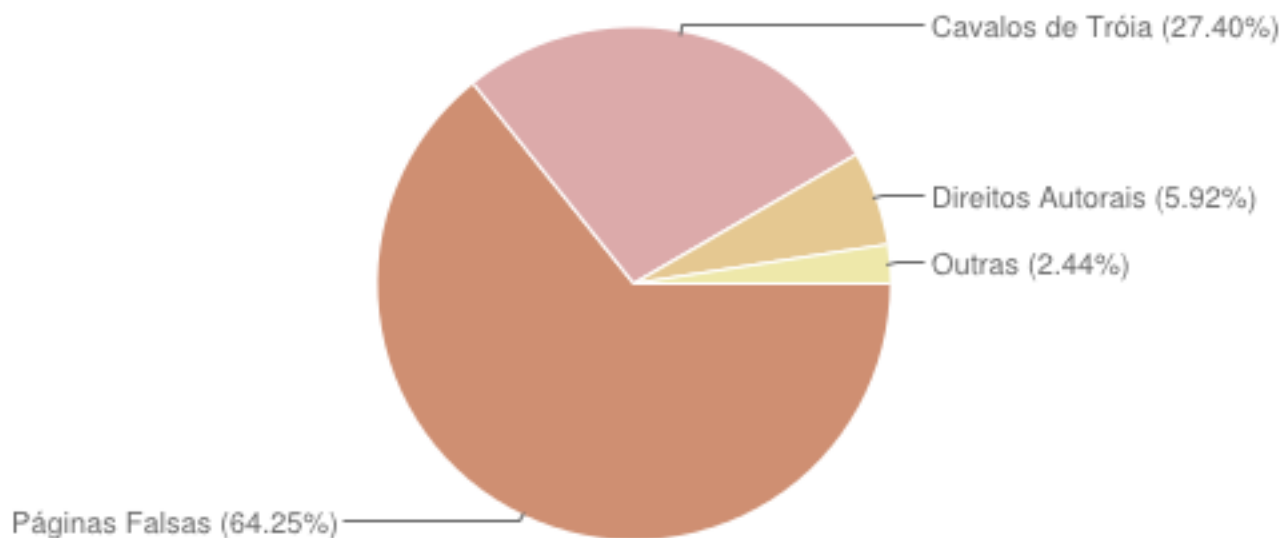


Tipos de ataque – 2013



Tentativas de fraudes – 2013

Tentativas de fraudes reportadas



Ataques a usuários finais

- **Fruto da mudança no enfoque dos atacantes**
 - é mais fácil e “rentável” atacar um usuário
- **Fraudes financeiras**
 - páginas falsas estão voltando a ter números significativos
 - *drive-by downloads* sendo usados intensamente no Brasil
 - casos publicados na mídia incluem:
sites principais da Vivo, da Oi e da Ambev
- **Outras motivações**
 - espionagem, sabotagem
 - nesses casos chamados de APTs (“*Advanced Persistent Threats*”)

Ataques a dispositivos

- **“Modems” e roteadores banda larga (CPEs)**
 - *botnets* usadas para ataques diversos
 - comprometidos via força bruta (telnet)
 - vários modelos com vulnerabilidades
 - comprometimento para alteração do serviço DNS para
 - fraudes financeiras
 - redirecionamento para obter “cliques” de propaganda
 - DDoS
- **Dispositivos com sistema Android**
 - *botnets*, fraudes e outros tipos de *malware*

Ataques a serviços de rede

- **Força bruta contra serviços de rede**
 - SSH, FTP, Telnet, VNC, etc
 - acesso a servidores, roteadores, CPEs, celulares, etc
- **Não tão frequentes, mas com grande impacto por serem contra a infra-estrutura crítica da Internet**
 - ataques contra servidores DNS
 - contra protocolos de roteamento como o BGP
- **Sistemas SIP (VoIP)**
 - força bruta para realização de ligações internacionais e fraudes
 - “Anatomy of SIP Attacks”
<https://www.usenix.org/publications/login/december-2012-volume-37-number-6/anatomy-sip-attacks>

Ataques a servidores Web

- **Muitas vulnerabilidades de *software***
 - ***softwares* de CMS desatualizados**
 - Wordpress, Joomla
 - **uso de pacotes prontos**
 - **falta de atualização dos sistemas operacionais**
 - **muitas falhas de programação:**
 - falta de validação de entrada
 - falta de checagem de erros
 - **exploração automatizada**
 - Ex.: *botnet* Brobot
 - **“Aumente a segurança de websites com Wordpress”**
<http://www.security.unicamp.br/artigos/23-seguranca-site-wordpress.html>

O Foco da Maioria dos Ataques Continuará Sendo

Serviços *Online*

- Grande demanda por *e-services*
- Dados sensíveis estão mais expostos
 - por necessidade, comodidade ou descuido
- Segurança não é prioridade
- Impactos não são compreendidos
- Sistemas críticos são conectados à Internet
 - controle de infra-estruturas críticas
 - caixas automáticos (ATMs)
 - sistemas de imigração e identificação

Clientes/Usuários

- Internet como parte do dia-a-dia
- Usuários não são especialistas
- Grande base
 - de dispositivos vulneráveis
 - com banda disponível
- Mais fáceis de atacar
- Possuem dados de valor
 - dados financeiros
 - endereços de *e-mail* válidos
 - credenciais de acesso
- Dispositivos podem ser usados para outros ataques
 - *botnets*
- BYOD
- Internet das Coisas

➤ Os criminosos estão apenas migrando para onde os negócios estão

Por que são tão fáceis?

Reais Causas dos Problemas

- **Cenário atual é reflexo direto de**
 - aumento da complexidade dos sistemas
 - **softwares com muitas vulnerabilidades**
 - segurança não é parte dos requisitos
 - falta de desenvolvedores capacitados para desenvolver com requisitos de segurança
 - pressão econômica para lançar, mesmo com problemas
- **Administradores de sistemas, redes e profissionais Web**
 - segurança não é parte dos requisitos
 - tem que “correr atrás do prejuízo”
 - ferramentas de segurança não conseguem remediar os problemas
 - ferramentas de ataque “estão a um clique de distância”

Consegue-se Quase Tudo no Mercado Negro

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	\$0.07-\$100
2	2	Bank account credentials	16%	19%	\$10-\$900
3	3	Email accounts	10%	7%	\$1-\$18
4	13	Attack tools	7%	2%	\$5-\$650
5	4	Email addresses	5%	7%	\$1/MB-\$20/MB
6	7	Credit card dumps	5%	5%	\$0.50-\$120
7	6	Full identities	5%	5%	\$0.50-\$20
8	14	Scam hosting	4%	2%	\$10-\$150
9	5	Shell scripts	4%	6%	\$2-\$7
10	9	Cash-out services	3%	4%	\$200-\$500 or 50%-70% of total value

Fonte: Underground Economy Servers—Goods and Services Available for Sale

http://www.symantec.com/es/es/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

Russian Underground – Serviços Disponíveis

- Pay-per-Install (global mix or specific country): \$12–\$550
- Bulletproof-hosting with DDoS protection: \$2000 per month
- Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) \$3000/month
- Programming: web server hacking \$250; browser-in-the-middle \$850; trojans \$1300
- Windows rootkit (for installing malicious drivers): \$292
- Linux rootkit: \$500
- Hacking Facebook or Twitter account: \$130
- Hacking Gmail account: \$162
- Hacking corporate mailbox: \$500

“Proxy service: HTTP, HTTPS, SOCKS4, SOCKS5; prices: 5 days = US\$4; 10 days = US\$8; 30 days = US\$20; 90 days = US\$55”

Offering	Price
Bots (i.e., consistently online 40% of the time)	US\$200 for 2,000 bots
DDoS botnet	US\$700
DDoS botnet update	US\$100 per up

Offering	Price
1-day DDoS service	US\$30-70
1-hour DDoS service	US\$10
1-week DDoS service	US\$150
1-month DDoS service	US\$1,200

“Setup of ZeuS: US\$100, support for botnet: US\$200/month, consulting: US\$30.”

Fonte: Read Russian Underground 101 - Trend Micro
<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>

Desafios

Investir em treinamento e pessoal

- **Há falta de pessoal treinado para lidar com redes e com segurança em IPv4**
 - a falta de pessoal com essas habilidades em IPv6 é ainda mais preocupante
 - o que é IPv6? :-)

<http://ipv6.br>
- **Vencer a cultura de que é melhor investir em tecnologia do que em treinamento e implantação de boas políticas**
- **Ir além do “*compliance*”**
 - Target

Mito de que só quem sabe invadir sabe proteger

- **A realidade:**
 - **proteger é muito mais difícil que atacar**
 - **especialmente contra ataques ainda não conhecidos**
 - **raríssimos os atacantes que sabem como:**
 - **proteger uma rede ou corrigir um problema**
 - **funcionam as ferramentas que utilizam**
 - **maioria absoluta utiliza ferramentas disponíveis na Internet**
 - **um profissional com sólida formação tem mais sucesso em utilizar as ferramentas como auxiliares nos processos de análise de risco e proteção da infra-estrutura que um invasor**
- **Os riscos:**
 - **colocar a segurança nas mãos de quem não está preparado**
 - **ter informações confidenciais comprometidas**
 - **ter *backdoors* e cavalos de tróia instalados em sua infra-estrutura**

Recuperação adequada de incidentes

- **A redução do impacto é consequência da:**
 - agilidade de resposta
 - redução no número de vítimas
- **O sucesso depende da confiabilidade**
- **O papel do CSIRT:**
 - auxiliar a proteção da infra-estrutura e das informações
 - prevenir incidentes e conscientizar sobre os problemas
- **O CSIRT não é um investigador**
- **Tratamento de incidentes não é perícia**
- **A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime**
 - seguir as políticas
 - preservar as evidências
 - responder incidentes – retornar o ambiente ao estado de produção

São necessários novos métodos de detecção

- **Foco atual do mercado é:**
 - no que entra em uma rede, ou
 - no que é conhecidamente malicioso
 - **“*Intrusion Detection*”**
 - IDS / IPS, *firewall*, antivírus
- **Foco precisa ser:**
 - no que sai, ou
 - no tráfego interno:
 - **“*Extrusion Detection*”**
 - *Flows, Honeypots, Passive DNS*
 - Notificações de incidentes
 - *Feeds* de dados (Team Cymru, ShadowServer, outros CSIRTs)

Desafios para a Identificação da Origem de Ataques

- Os ataques partem de vítimas na maioria dos casos
- Investigação sem contexto pode levar a graves consequências
 - e.g. Coreia do Sul x China
 - a rede usava como IPs não roteáveis (no NAT) um bloco de IPs alocado para a China – peritos viram o IP de onde veio o *malware* e anunciaram que o ataque vinha da China

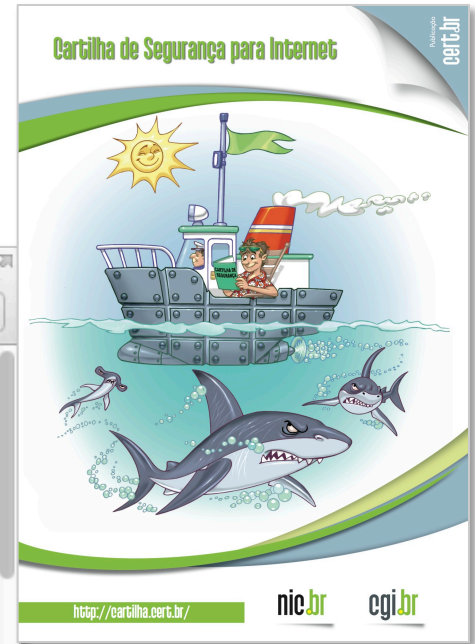
Só haverá reais melhorias quando

- **Processo de desenvolvimento de *software* incluir**
 - levantamento de requisitos de segurança
 - testes que incluam casos de abuso (e não só casos de uso)
- **Desenvolvimento seguro de *software* se tornar parte da formação de projetistas e programadores**
 - desde a primeira disciplina de programação e permeado em todas as disciplinas
- **Provedores de acesso e serviço, operadoras e administradores de redes em geral forem mais pró-ativos**
- **Sistemas e ferramentas forem menos complexos de usar**
- **Investimentos em conscientização de usuários**

Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no site (HTML5)
 Dica do dia no site, via *Twitter* e RSS

<http://cartilha.cert.br/>



Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- *Internet Banking*
- Computadores
- Códigos Maliciosos



Acompanhados de *Slides* de uso livre para:

- ministrar palestras e treinamentos
- complementar conteúdos de aulas

Outros Materiais para Usuários Finais

Portal Internet Segura

- Reúne todas as iniciativas conhecidas de educação de usuários no Brasil

<http://www.internetsegura.br/>



**INTERNET
SEGURA.BR**

Site e vídeos do Antispam.br

<http://www.antispam.br/>



Perguntas?

Miriam von Zuben
miriam@cert.br

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



cert.br

Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

egi.br

Comitê Gestor da
Internet no Brasil

3º Fórum Brasileiro de CSIRTs

[Início](#) | [Programação](#) | [Inscrições](#)

English

Keynote

Programação

Envio de trabalhos

Inscrições

Local

Hotéis

Informações de Interesse

Eventos anteriores
 2º Fórum
 1º Fórum

↳ Inscrições Abertas

Estão **abertas as inscrições** para o 3º Fórum Brasileiro de CSIRTs, que será realizado nos dias 15 e 16 de setembro de 2014, no **Hotel Blue Tree Premium Morumbi**, em São Paulo/SP.

O evento é gratuito, para inscrever-se basta preencher o formulário disponível em:

- <http://www.cert.br/forum2014/inscricao/>

As inscrições online serão encerradas às 18:00h UTC-3, do dia 10 de setembro de 2014.

Após esta data e horário, as inscrições poderão ser feitas somente presencialmente no dia do evento.

↳ Destaques em 2014

Veja a Programação Completa

2013 e 2014 foram anos marcados por diversos eventos que impactaram o dia-a-dia de tratamento de incidentes:

- Eventos como a Copa do Mundo 2014 e a Copa das Confederações
- Incidentes envolvendo Infraestruturas Críticas, Internet das Coisas, APTs e vazamentos de dados pessoais
- Novas Leis, como o Marco Civil da Internet

A grade de palestras reflete essa complexidade e abre mais espaço para a troca de ideias, o esclarecimento de dúvidas e o fortalecimento da cooperação entre os CSIRTs no Brasil.

Keynote

Programação

Envio de trabalhos

Inscrições

Local

Hotéis

Informações de Interesse

Eventos anteriores
 2º Fórum
 1º Fórum

Programação do 3º Fórum Brasileiro de CSIRTs

Horário	Atividade - 15/09/2014
09:30-10:30	Welcome Coffee e Registro no Evento Aproveite este tempo para rever os colegas e restabelecer contatos
10:30-10:40	Abertura do Evento
10:40-11:35	Ameaças e Desafios Um Ano Depois [Detalhes] Klaus Steding-Jessen , Gerente Técnico, CERT.br/NIC.br
11:35-12:30	Estratégias para criação e fortalecimento da cultura de Segurança nas Instituições de Ensino e Pesquisa [Detalhes] Rafael Gomes , CERT.Bahia / UFBA
12:30-14:15	Intervalo para Almoço
14:15-16:30	Painel e debates: Impactos do Marco Civil da Internet no dia-a-dia dos profissionais de tratamento de incidentes e segurança da informação [Detalhes] Danilo Doneda , Coordenador-Geral de Estudos e Monitoramento de Mercado da Secretaria Nacional do Consumidor do Ministério da Justiça Carlos Affonso P. de Souza , Diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio) Jorilson Rodrigues , Perito Criminal Federal DPF/MJ, e Coordenador de Segurança do e-Ping Diego Canabarro , Assessoria Técnica do CGI.br
16:30-19:30	Happy Hour Junte-se a nós neste momento descontraído, faça novos contatos, coloque a conversa em dia com antigos colegas e troque ideias com os palestrantes
Horário	Atividade - 16/09/2014
09:30-11:00	Keynote Uma história recente das Ameaças Avançadas Persistentes [Detalhes] Prof. Dr. Adriano Cansian , Laboratório de Segurança ACMEI, Unesp
11:00-11:30	Coffee Break
11:30-12:30	Estruturação de um CSIRT para o Contexto de Smart Grid na Cemig [Detalhes] José Lopes de Oliveira Jr. , Companhia Energética de Minas Gerais - Cemig
12:30-14:15	Intervalo para Almoço
14:15-16:30	Painel e debates: Desafios e Lições Aprendidas no Tratamento de Incidentes em Grandes Eventos [Detalhes] Cel. José Ricardo Souza Camelo , CDCiber Antônio Magno , Coordenador, CTIR Gov, DSIC/GSI/PR Cristine Hoepers , Gerente Geral, CERT.br/NIC.br
16:30-16:40	Encerramento do Evento
16:40-17:30	Coffee Break de Encerramento

Detalhes das Apresentações