nic.br cgi.br | cert.br

Rio 2016 Cyber Security Integration Meeting

24 de novembro de 2014
Rio de Janeiro, RJ

Desafios e Lições Aprendidas no Tratamento de Incidentes em Grandes Eventos

Cristine Hoepers
cristine@cert.br

cert.br nic.br cgi.br

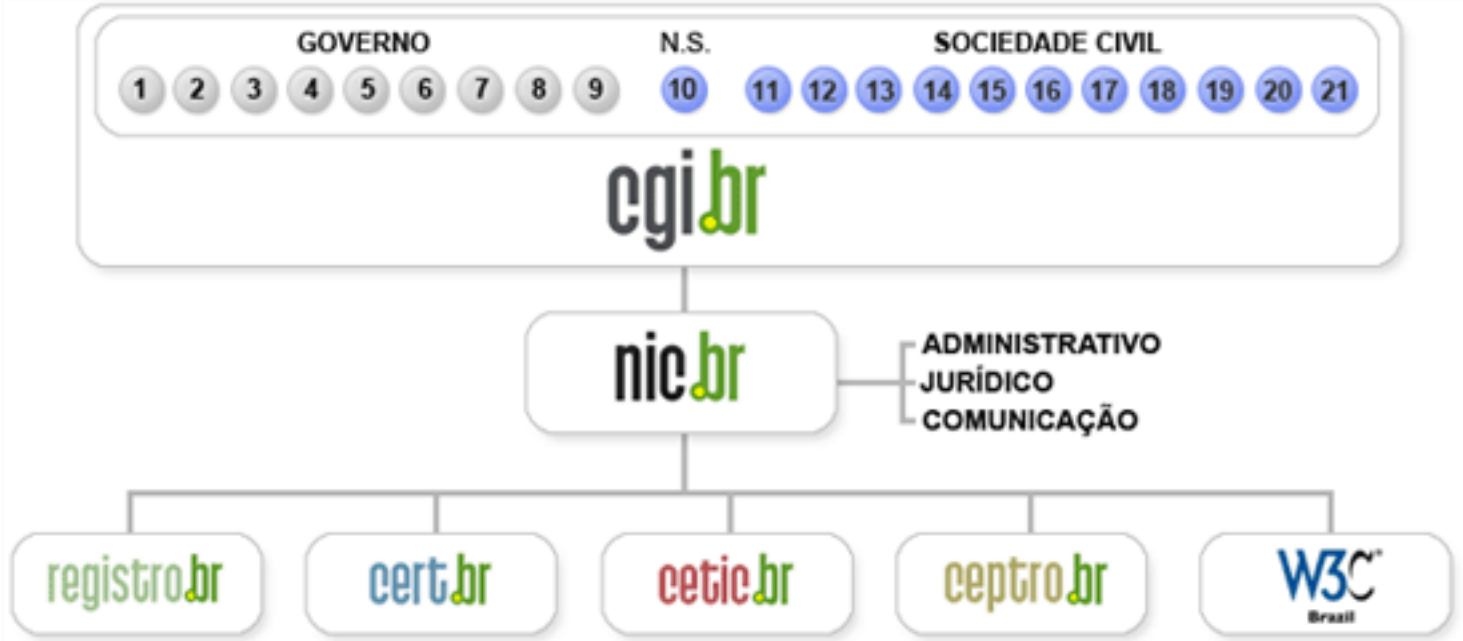
Comitê Gestor da Internet no Brasil – CGI.br

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;**

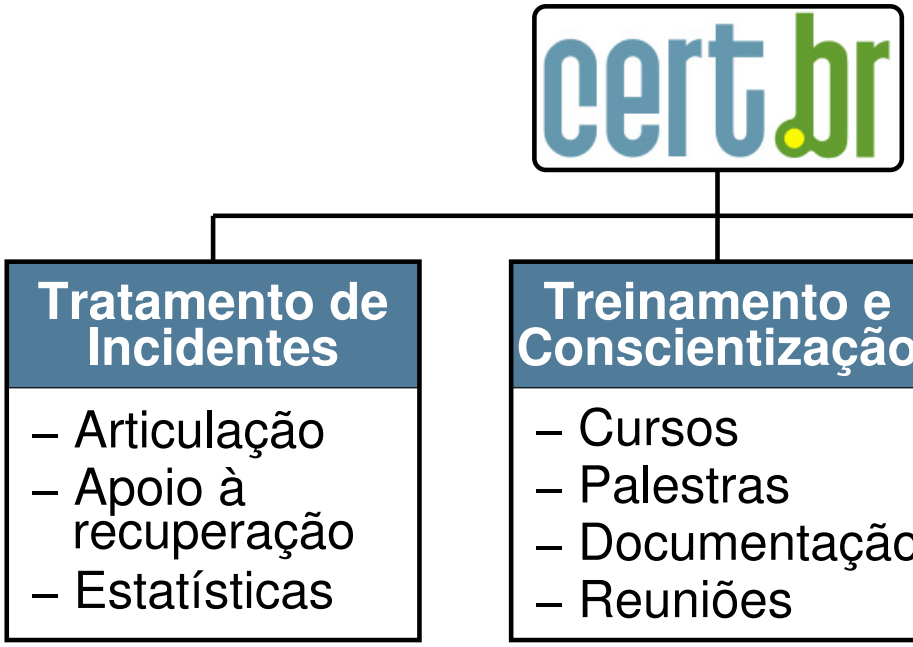
http://www.cgi.br/sobre/

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



SEI Partner
Carnegie Mellon

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**
- **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**

Copa 2014:
Características dos Ataques

"*Hacktivismo*" e manifestações

Ataques contra alvos difusos

- **qualquer rede "`gov.br`", universidades, partidos e patrocinadores**
  - **vazamentos de informações**
  - ***defacements***
  - **DDoS via amplificação (Chargen, DNS, SNMP)**
    - reportados picos de 4Gbps
- **outros não relacionados nem com Brasil nem com a Copa**
  - **como o site "`elections.ny.gov`"**
- **fotos vazando senhas de wi-fi de arenas**
- ***phishings* de *sites* da FIFA, CBF e mídia**

Mídia deu muita atenção nas semanas pré evento

- **foi o período mais intenso de ataques**

A Atuação do CERT.br

Ajudar na identificação de

- possíveis ameaças e cenários de ataques
- necessidades de infraestrutura

Monitoramento extra de incidentes e fontes de dados sobre ataques

- notificações de incidentes
- *feeds* de dados (Honeypots Distribruídos do CERT.br, Team Cymru, Arbor Atlas, ShadowServer, Operações Anti-Botnet)
- fontes públicas de informação (Twitter, IRC, *defacements*)

Facilitação e suporte no tratamento de incidentes

- via a rede de contatos já estabelecida

Adicionalmente

- Treinamento de tratamento de incidentes para o pessoal do Exército, Marinha e Aeronáutica que atuou nos Destacamentos de Defesa Cibernética
- Rede iNOC-DBA mantida pelo NIC.br

Cooperação:
CERT.br, CTIR Gov e CDCiber

A cooperação já era grande

Ficou fortalecida após os grandes eventos

Houve

- **Troca de informações**
- **Divisão de tarefas**
  - **CDCiber: atuação presencial nos CCDAs e CICCRs; coleta de inteligência nas redes sociais.**
  - **CTIR Gov: foco nos ataques às redes do Governo; monitoração de defacements.**
  - **CERT.br: facilitar a comunicação e coordenação com outros atores, principalmente CSIRTs (nacionais e internacionais); monitoração de canais de IRC e Twitter; monitoração dos feeds de dados por qualquer atividade maliciosa saindo das redes mapeadas pelo CDCiber e pelo CTIR Gov.**

Maiores Desafios

FIFA, patrocinadores e algumas operadoras não foram abertos para troca de informações

- ou não havia ponto de contato
- ou a postura era “nos mandem dados”
  - sem compartilhar ameaças, ataques vistos, riscos ou outros dados que pudessem auxiliar o processo de coordenação entre todos

Carga de trabalho maior que o já planejado

- mudanças de planejamento na última hora
- solicitações de relatórios de última hora
- plantões
- pessoal extra para monitoração de fontes públicas

Reflexões para 2016

Cooperação

- nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança ou a resposta a incidentes
- pessoal preparado em todas as redes e áreas
- cooperação direta entre os diversos atores

Os times serão os mesmos de sempre, mas é necessário ter mais troca de informações e cooperação entre

- os grupos organizadores
- o pessoal técnico de todas as operadoras e provedores de serviços Internet
- e todos os CSIRTs formados no Brasil

Ações necessitam iniciar já

Obrigada

www.cert.br

cristine@cert.br

@certbr

24 de novembro de 2014

nic.br cgi.br

www.nic.br | www.cgi.br