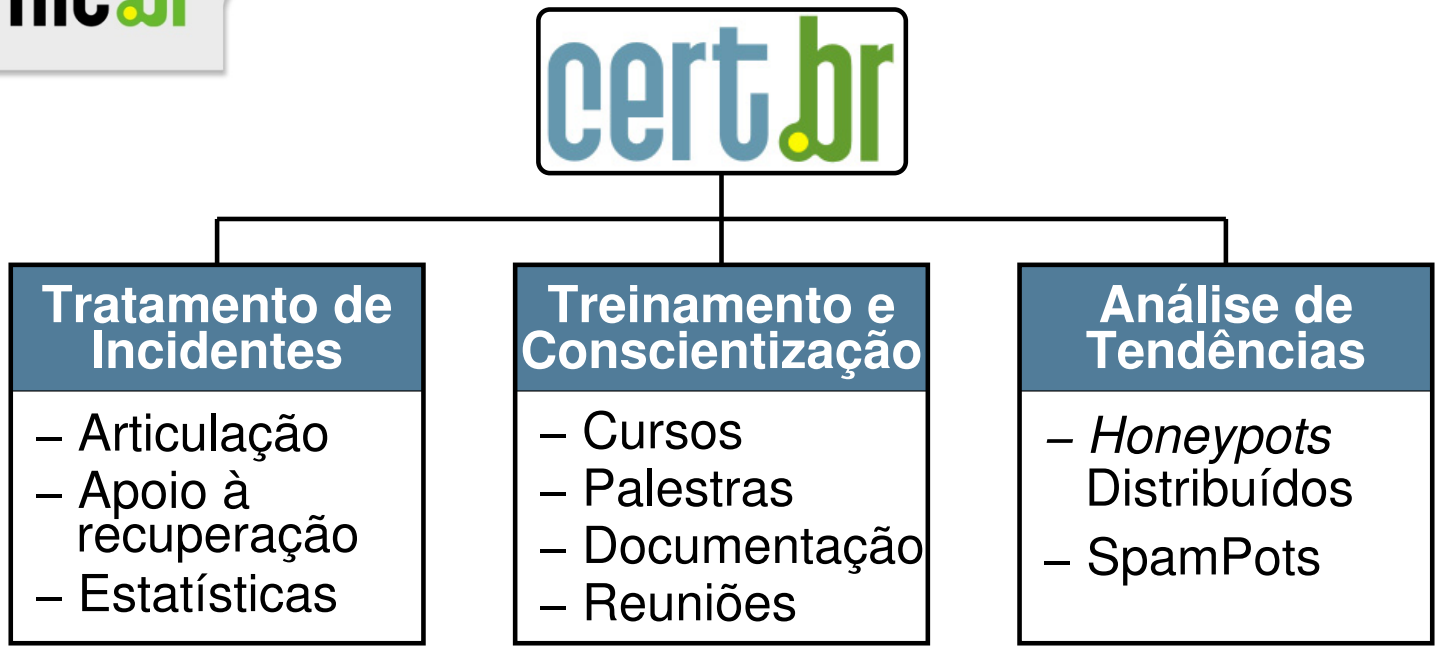
Desafios e Lições Aprendidas no Tratamento de Incidentes em Grandes Eventos

Cristine Hoepers, D.Sc.

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



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**

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/

Slides a seguir foram apresentados originalmente em 2012 – em reflexão sobre como seria o tratamento de incidentes em grandes eventos

Reunião de Trabalho de Coordenação de Segurança Cibernética em Grandes Eventos
SRCC/DPF, setembro de 2012, Brasília, DF
http://www.cert.br/docs/palestras/certbr-srcc-dpf2012.pdf

Diferenças com outros Incidentes

Um único evento que:

- Atrai mais atenção por parte do mundo
  - e dos atacantes
- Os momentos críticos tem data e hora marcados com antecedência
- Os incidentes tem impacto na imagem do país
- A Internet é infraestrutura crítica, entre outros, para:
  - trasmissão dos jogos
  - comunicação dos jornalistas
  - comunicação da própria organização do evento

Pontos Chave para o Sucesso

A rede que estiver provendo conectividade precisa

- **ter um time atuante e experiente**
- **compartilhar informações**

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 das operadoras**
- **e todos os CSIRTs formados no Brasil**

Ações necessitam iniciar já

Ações do NIC.br/CGI.br para Resiliência e Estabilidade das Infraestruturas Críticas de Internet

PTT.br – Pontos de Troca de Tráfego nas grandes áreas metropolitanas

- "uma única saída é o mesmo que nenhuma"

Estabilidade da Infraestrutura de DNS (Registro.br)

- Diversos mirrors no Brasil dos Servidores DNS Raíz
- Mirrors do `.br` hospedados em outros países
- Suporte a DNSSEC no ccTLD `.br`
  - Segundo país no mundo a ter DNSSEC disponível na raíz

Capacitação de profissionais

- IPv6 e gerência de redes (CEPTRO.br)
- Tratamento de incidentes (CERT.br)

Rede iNOC-DBA

- mas as operadoras precisam usá-lo

Análise de tendências e tratamento de incidentes (CERT.br)

O que pode ser feito pelo CERT.br

Ajudar na identificação de

- possíveis ameaças e cenários de ataques
- necessidades de infraestrutura (como redundância de conectividade)

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

O que realmente aconteceu :-)

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

Cooperação entre CERT.br, CTIR Gov e CDCiber

A cooperação já era grande

Ficou fortalecida após os grandes eventos

Houve

- **divisão de tarefas**
- **troca de informações**

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

A Atuação do CERT.br foi a Prevista

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

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 das operadoras
- e todos os CSIRTs formados no Brasil

Ações necessitam iniciar já

Contato

Cristine Hoepers, D.Sc.

cristine@cert.br

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

cgi.br
Comitê Gestor da Internet no Brasil