Resposta a Incidentes no Brasil: Situação Atual e o Papel do NBSO

Cristine Hoepers
cristine@nic.br

Klaus Steding-Jessen
jessen@nic.br

NIC BR Security Office – NBSO
Brazilian Computer Emergency Response Team
Comitê Gestor da Internet no Brasil
http://www.nbso.nic.br/

Roteiro

- História do CGI.br e do NBSO
- O cenário nacional e internacional de CSIRTs
- Iniciativas e projetos do NBSO
- Resposta a incidentes
  - notificações, ferramentas, etc
- Referências

Comitê Gestor da Internet no Brasil – CGI.br

- Criado por portaria interministerial MCT/MC 147, de 31 de maio de 1995.
  - recomendar padrões e procedimentos técnicos e operacionais para a Internet no Brasil;
  - coordenar a atribuição de endereços Internet, o registro de nomes de domínios, e a interconexão de *backbones*;
  - coletar, organizar e disseminar informações sobre os serviços Internet.

CGI.br (cont.)

Decreto Nº 4.829, de 3 de setembro de 2003:

- Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
- Composição: 21 membros – MCT, Casa Civil, MC, Defesa, MDIC, MP, Anatel, representantes da comunidade acadêmica e empresarial, entre outros.

---

http://www.cg.org.br/regulamentacao/

Criação do NBSO

Agosto/1996, documento: “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”

- Ponto central de contato;
- Manutenção de estatísticas sobre incidentes na Internet brasileira;
- Neutralidade para coordenar ações entre redes envolvidas em incidentes;
- Representação do Brasil junto a órgãos internacionais de segurança.

Junho/1997: criado o NBSO

http://www.cg.org.br/grupo/historico-gts.htm

Missão do NBSO

CSIRT responsável por receber, analisar e responder a incidentes de segurança em computadores envolvendo redes conectadas à Internet brasileira. Atua:

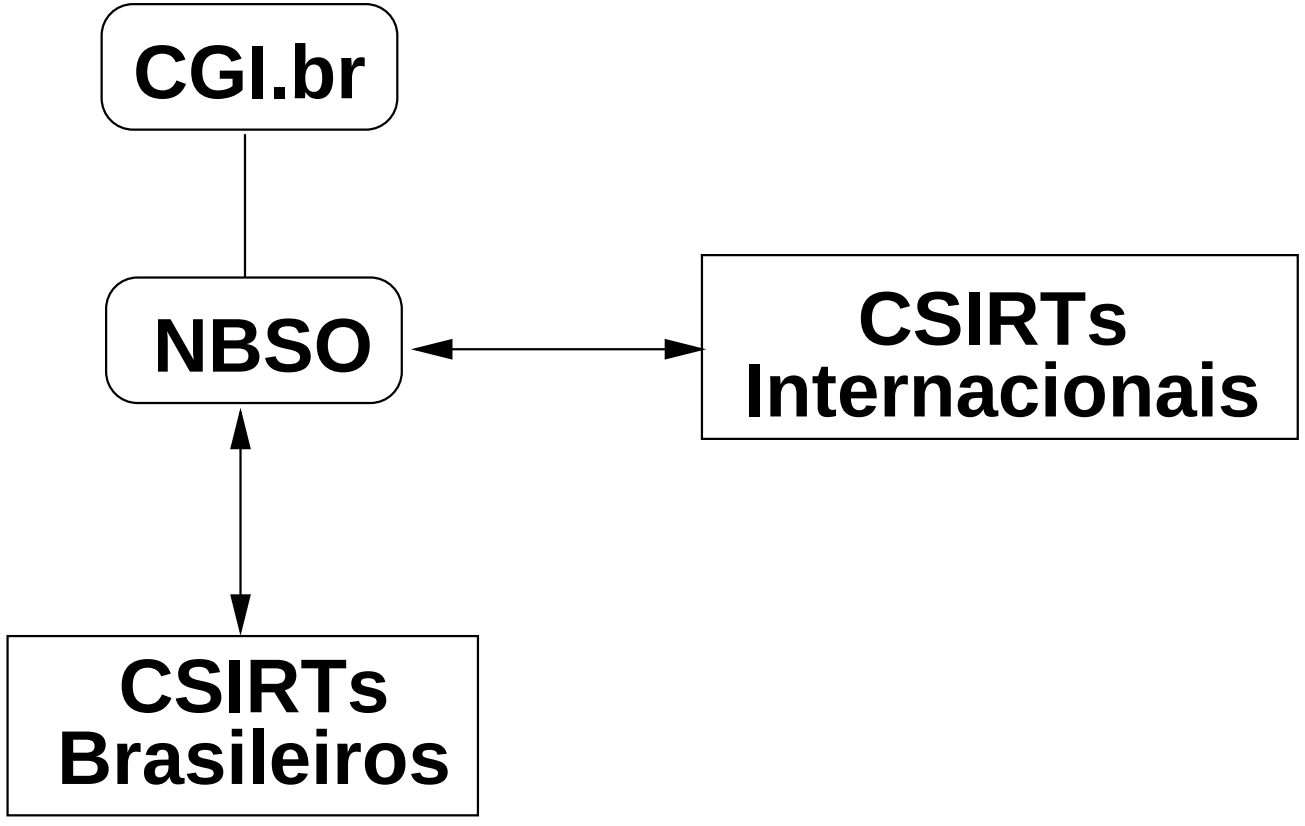
- no trabalho de conscientização sobre os problemas de segurança;
- na correlação entre eventos;
- no auxílio ao estabelecimento de novos CSIRTs no Brasil.
- coordenação de resposta a incidentes

http://www.nbso.nic.br/missao.html

Coordenação de Resposta a Incidentes

- Ponto central de contato para a Internet no Brasil;
- Coordenação de ações entre redes envolvidas em incidentes;
  - prover apoio necessário para recuperação e análise de sistemas comprometidos.
- Estabelecer um trabalho colaborativo com outras entidades, como as polícias, provedores e backbones;

Coordenação de Resposta a Incidentes (cont.)



CSIRTs Brasileiros

Empresas de Telecomunicações

- Brasil Telecom
- EMBRATEL
- Star One
- Telefônica
- Telemar

CSIRTs Brasileiros (cont.)

Bancos

- ABNAMRO/REAL
- Banco do Brasil
- Bradesco
- Caixa Econômica Federal
- Citibank
- Itaú
- Santander/Banespa

CSIRTs Brasileiros (cont.)

Redes Acadêmicas

- CAIS/RNP
- CERT-RS
- CSIRT Unicamp
- CSIRT USP
- INPE
- RedeRio
- UNESP

CSIRTs Brasileiros (cont.)

Redes do Governo

- CTR/DPF
- GRA/SERPRO

CSIRTs Brasileiros (cont.)

Projeto iNOC-DBA BR

- 120 telefones IP distribuídos pelo CGI.br
  - 100 maiores AS (*Autonomous Systems*) do Brasil
  - 20 CSIRTs (nomeados pelo NBSO)

Lista de CSIRTs no Brasil

- `http://www.nbso.nic.br/contato-br.html`

Iniciativas e Projetos do NBSO

Documentos em Português

Produção de Documentos

- Cartilha de Segurança para Internet
- Práticas de Segurança para Administradores de Redes

Tradução de Documentos do CERT/CC

- Advisories
- Documentos sobre CSIRTs

---

http://www.nbso.nic.br/docs/

Formação e Capacitação de CSIRTs

Enfoque no aumento da capacidade nacional de resposta a incidentes de segurança

- Carnegie Mellon Software Engineering Institute Transition Partner
- Cursos do CERT Coordination Center:
  - *Fundamentals of Incident Handling*
  - *Advanced Incident Handling for Technical Staff*

---

http://www.nbso.nic.br/cursos/

Notificações

- Consultas regulares em bases mundiais de abuso
- Identificação de IPs brasileiros
- Envio de notificações para os responsáveis das redes
- Alguns exemplos:
  - ASN Alert Project
  - The Open Relay DataBase (ORDB.org)
  - Smurf Amplifier Registry (SAR)

Notificações de SPAM

Controle e Acompanhamento de Notificações de Spam

- Recebidos via SpamCop
- Notificações e estatísticas
- Perfil do spam no Brasil: tipo mais comum e origem
- Ajudar redes brasileiras a direcionar esforços
- **Não** usar para blacklist

Estatísticas de Incidentes

- Anunciadas trimestralmente
  - apenas os incidentes reportados ao NBSO
  - divididos por categoria (varredura, fraudes, etc)
- Determinação de novas tendências de ataques

Consórcio Brasileiro de Honeypots

- Honeypots são mantidos pelas instituições consorciadas
- Objetivo de aumentar, no espaço Internet brasileiro, a capacidade de:
  - detecção de incidentes
  - correlação de eventos
  - determinação de tendências de ataques
- Utilização dos dados por grupos de resposta a incidentes

Consórcio Brasileiro de Honeypots (cont)

Uso dos dados pelo NBSO:

- Identificação de ataques conhecidos
  - detecção de servidores comprometidos realizando varreduras
- Detecção de worms/vírus:
  - mostram um número enorme de máquinas vulneráveis, facilmente exploráveis
- Comparação com incidentes reportados voluntariamente

Resposta a Incidentes

Resposta a Incidentes

Recebimento de notificações de incidentes:

- Quase totalidade por email
  - forma mais usada pela comunidade de CSIRTs
- Origem variada
  - administradores de redes, usuários, outros CSIRTs

Resposta a Incidentes (cont.)

- Natureza das notificações:
  - varreduras, tentativas de comprometimento, violação de direitos autorais
- Ações tomadas
  - checagem dos contatos
  - notificações de outros sites
  - acompanhamento e estatísticas

Resposta a Incidentes (cont.)

Outras atividades relacionadas:

- Apoio a recuperação de incidentes
- Correlação de eventos de segurança observados com outras fontes
- Dúvidas sobre segurança: usuários, administradores e mídia

Algumas Ferramentas Utilizadas

Ferramentas padrão, eficientes e de código fonte disponível.

- `OpenBSD / FreeBSD / GNU/Linux`
- `pf`
- `jwhois`
- `procmail / formail`
- `bogofilter / clamAV`
- `gpg / PGP`
- `gcc / Perl`

Ferramentas de Apoio

Ferramentas de uso geral em segurança

- `chkrootkit`
- `nmap`
- `nessus`
- `snort`
- `md5 / SHA1`

---

http://www.nbso.nic.br/tools/

Referências

- NBSO - NIC BR Security Office

  http://www.nbso.nic.br/

- Comitê Gestor da Internet no Brasil

  http://www.cg.org.br/

- Estatísticas de Notificações de Spam Reportadas ao NBSO

  http://www.nbso.nic.br/stats/spam/

- Estatísticas dos Incidentes Reportados ao NBSO

  http://www.nbso.nic.br/stats/incidentes/

Referências (cont)

- Consórcio Brasileiro de Honeypots

  http://www.honeypots-alliance.org.br/