Papel dos CSIRTs no Cenário Atual de Segurança

Cristine Hoepers

cristine@nic.br

NIC BR Security Office – NBSO

Brazilian Computer Emergency Response Team

Comitê Gestor da Internet no Brasil

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

NBSO – NIC BR Security Office

- Grupo de Resposta a Incidentes para a Internet Brasileira
  - coordena ações
  - desenvolve documentação de apoio
  - mantém estatísticas
  - trabalha na conscientização sobre os problemas de segurança
  - dá apoio à criação de novos CSIRTs
- Mantido pelo Comitê Gestor da Internet no Brasil

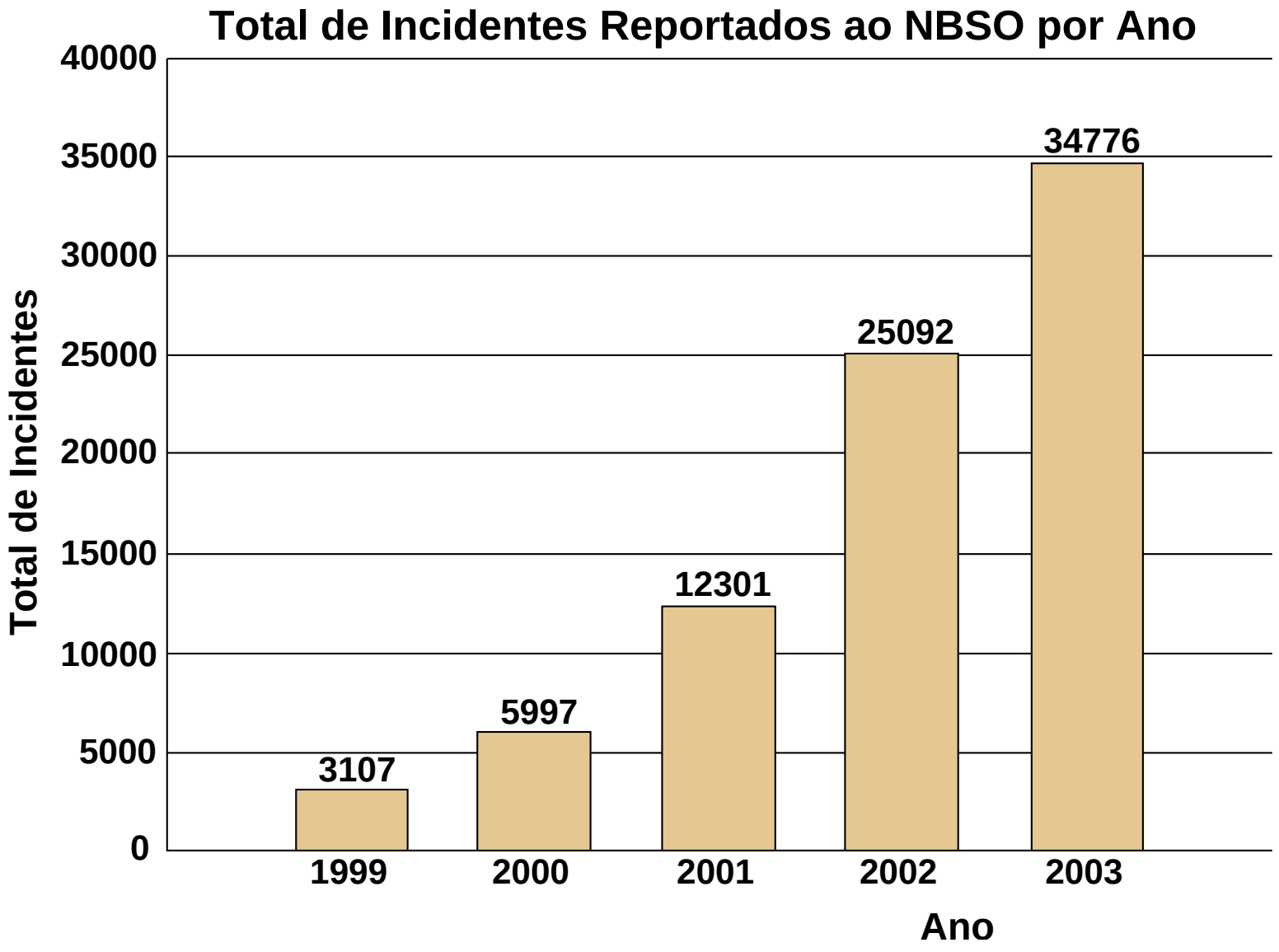
Roteiro

- Cenário Atual
- Papel dos CSIRTs
- Perfil do profissional
- Fatores de sucesso
- Cooperação entre times
- Onde obter treinamento

Cenário Atual

- Complexidade crescente dos sistemas
- Grande número de vulnerabilidades
- Ataques não são barrados pela maioria dos firewalls (e.g.: IIS, DNS, Vírus)
- Facilidade em ocultar os passos de uma invasão
- Aumento dos incidentes de segurança

Cenário Atual (Cont.)



Cenário Atual (cont.)

- Redes Brasileiras sendo utilizadas como ponto de partida para ataques a outros países
- Falta de administradores experientes
- Poucos CSIRTs estabelecidos
- Sensação de impunidade por parte dos invasores
- Comunicação rápida e eficiente entre invasores (email, Web, conferências, chats)

Cenário Atual (cont.)

- Banalização do “Consultor de Segurança”
  - mito do “hacker ético”
- “ex”-invasores vendendo “proteção”
- “saber” invadir = saber proteger?
  - invasores com baixo nível técnico
  - ferramentas automáticas (e.g. `rootkits`)
  - ataques coordenados em grande escala

Cenário Atual (cont.)

- “Economia” do *underground*
  - máquinas invadidas e CC são moeda de troca
  - *spammers* pagando por máquinas invadidas
- *Script-kiddies* se envolvendo em crimes
  - aliciados pelo crime organizado
  - envolvidos em roubo de cartão de crédito
- *Worms*

Cenário Atual (cont.)

Resumindo:

- muitas fontes de problemas de segurança
- necessidade de filtragem de informações – foco no ambiente da instituição
- necessário desenvolver mecanismos para manter-se atualizado
  - gerenciamento de aplicações de *patches*
  - pessoal para desenvolver o trabalho
- tempo para reação cada vez menor

CSIRT

Computer Security Incident Response Team

Um grupo ou organização que provê serviços e suporte para um público bem definido, para prevenção, tratamento e resposta a incidentes de segurança.

Papel do CSIRT

- Fornececer informações confiáveis
  - reduzir as informações que chegam aos administradores de redes e usuários
- Prover recomendações e estratégias
- Determinar o impacto de incidentes
- Prover meios para recuperação rápida
- Ser o ponto de contato com outros grupos, polícia, mídia, etc

Serviços de um CSIRT

Proativos

- Filtragem e repasse de informações
- Disseminação da cultura de segurança
- Desenvolvimento de documentação
- Treinamentos e orientação a usuários
- Configuração e manutenção dos sistemas
- Desenvolvimento de ferramentas

Serviços de um CSIRT (cont.)

Reativos

- Tratamento de Incidentes
- Coordenação de ações
- Detecção e rastreamento de invasões
- Preservação de evidências
- Análise de artefatos
- Análise de vulnerabilidades

Perfil do Profissional

- Integridade e discrição
- Sem prévio envolvimento com atividades de “hacking”
- Conhecimentos:
  - TCP/IP
  - ambiente de TI da instituição
  - comunicação (oral e escrita)

Fatores de Sucesso

- Perfil e motivação dos profissionais
- Reconhecimento por parte da comunidade a que atende
- Grau de confiança adquirido
- Relacionamento com outros CSIRTs
- Apoio por parte da administração/alta gerência

Cooperação

- Essencial para a operação
  - permite acesso a informações relevantes
  - permite correlação de eventos
  - facilita a resolução de incidentes
- Não existe fórmula mágica, o grupo necessita
  - construir sua reputação
  - ganhar a confiança de outros grupos

Cooperação (cont.)

Como conhecer outros CSIRTs:

- Durante o processo de resposta a incidentes
- Participando de Conferências
- FIRST (Forum of Incident Response and Security Teams)
  - Reúne CSIRTs de todo o mundo
  - Promove e facilita a comunicação

http://www.first.org/

Treinamentos e Certificações

Administração de redes, forense, análise de artefatos:

- SANS Institute

  http://www.sans.org/

- GCIH – GIAC Certified Incident Handling Analyst
  - habilita o analista a tratar incidentes envolvendo código malicioso
  - http://www.giac.org/GCIH.php

Treinamentos e Certificações (cont.)

Específicos sobre implantação e operação de CSIRTs e processo tratamento de incidentes:

- AusCERT

  http://www.auscert.org.au/

- CERT/CC

  http://www.cert.org/training/

  - dois cursos serão licenciados e ministrados pelo NBSO a partir de 2004
  - Informações: <cursos@nic.br>

Treinamentos e Certificações (cont.)

- CERT-Certified Computer Security Incident Handler

  http://www.cert.org/certification/

  - exige quatro cursos do CERT/CC
  - três anos de experiência
- Habilita o analista certificado a:
  - criar ou gerenciar CSIRTs
  - analizar incidentes e identificar estratégias para resposta

Referências

- Material desta apresentação

  http://www.nbso.nic.br/docs/ssi2003/

- Documentação sobre CSIRTs

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

Incident Response – Kenneth R. van Wyk, Richard Forno, ISBN 0-596-00130-4, http://www.oreilly.com/catalog/incidentres/

Referências (cont.)

- Estatísticas do NBSO

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

- Documentação sobre Segurança e Administração de Redes

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

- Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?

  http://www.cert.org/csirts/csirt-staffing.html