CSIRT – Computer Security Incident Response Team

Definição, Implantação e Importância Estratégica

NIC BR Security Office
nbso@nic.br
http://www.nic.br/nbso.html

Cristine Hoepers
cristine@nic.br
Klaus Steding-Jessen
jessen@nic.br

SecurityWeek Brasil 2002
São Paulo
25 de março de 2002

Notas:

Notas:

CSIRTs
Definição, Implantação e Importância

- Motivação: Problemas no Cenário Atual
- CSIRT
  - Definição e Papel
  - Tipos e Serviços
  - CSIRTs Existentes
- Implantação de um CSIRT
  - Plano de Ação
  - Fatores de Sucesso

Notas:

Motivação: Problemas no Cenário Atual

Notas:

Problemas no 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
- Comunicação rápida e eficiente entre invasores (email, WEB, conferências, chats, etc)

Notas:

Problemas no Cenário Atual (cont.)

- Banalização do "Consultor de Segurança"
- "ex"-invasores vendendo "proteção"
- "saber" invadir = saber proteger?
  - Invasores com pouco nível de conhecimento
  - Ferramentas automáticas (e.g. rootkits)
  - ataques coordenados em grande escala

Notas:

Problemas no Cenário Atual (cont.)

- Falta de administradores experientes
- Dificuldade em acompanhar as atualizações
- Raros CSIRTs estabelecidos
- Falta de Legislação

Notas:

CSIRT

Notas:

CSIRT – Computer Security and 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.

- Ponto central de contato
- Provê informações para o seu público
- Troca informações com outros CSIRTs

Notas:

Papel do CSIRT

- Coordenar ações
- Determinar o impacto
- Prover recuperação rápida
- Preservar evidências
- Prover recomendações e estratégias
- Ser o ponto de contato com outros grupos, polícia, mídia, etc

Notas:

Serviços Possíveis do CSIRT

- Tratamento de Incidentes
- Detecção e Rastreamento de Invasões
- Análise de Artefatos/Vulnerabilidades
- Definição de Políticas
- Auditoria
- Análise de Riscos

Notas:

Autoridade do CSIRT

- Completa
- Parcial
- Indireta
- Sem autoridade

Notas:

CSIRTs Existentes

- Empresas
- Países
- Backbones
- Órgãos Governamentais

Notas:

CSIRTs em Empresas

- VISA: VISA-CIRT
- Bank of America: BACIRT
- Boeing: BCERT
- Bank of Montreal: BMO ISIRT
- Cisco Systems: Cisco PSIRT
- Citigroup: Citigroup CIRT
- Compaq: Compaq SSRT

Notas:

CSIRTs em Países

- Brasil: NBSO
- Austrália: AusCERT
- EUA: CERT/CC
- Alemanha: DFN-CERT

Notas:

CSIRTs em Backbones

- British Telecommunications: BTCERTCC
- TeleDanmark: CSIRT.DK
- Rede TCHE: CERT-RS
- Embratel: Grupo de Segurança da Embratel
- Unicamp: Grupo de Segurança da Unicamp
- RNP: CAIS

Notas:

CSIRTs em Órgãos Governamentais

- US Department of Energy: CIAC
- NASA: NASIRC
- US Dept. of Navy: NAVCIRT
- French government offices and services: CERTA

Notas:

Implantação de um CSIRT

Notas:

Plano de Ação

- Definir uma equipe/coordenador
- Envolver todas as partes da instituição
- Definir os serviços a serem prestados
- Definir o nível de autoridade
- Inserir o CSIRT na estrutura organizacional

Notas:

Contratação de Pessoal

- Pré-requisitos essenciais
  - Retidão de Caráter
  - Não ter prévio envolvimento com atividades de "hacking"
  - Conhecimento:
    * TCP/IP
    * Ambiente de TI da instituição

Notas:

Fatores de Sucesso do CSIRT

- Credibilidade
- Confiança
- Localização dentro da Instituição
- Capacidade Técnica
- Capacidade de Cooperação com outros grupos

Notas:

Onde obter treinamento

- AusCERT
  http://www.auscert.org.au/Information/auscert_info.html
- CERT/CC
  http://www.cert.org/csirts/
- SANS Institute
  http://www.sans.org

Notas:

Leitura Recomendada

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

Notas:

Leitura Recomendada (cont.)

- Secrets & Lies – Digital Security in a Networked World, Bruce Schneier, ISBN 0-471-25311-1, http://www.counterpane.com/sandl.html

Notas:

Sites de Interesse

- CSIRT FAQ
  http://www.cert.org/csirts/csirt_faq.html
- Forming an Incident Response Team
  http://www.auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html
- Security Knowledge in Practice
  http://www.cert.org/security-improvement/skip.html
- Documentos, RFCs e sites relacionados
  http://www.nic.br/links.html

Notas: