CSIRT – Computer Security Incident Response Team

Definição, Implantação e Importância

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

Cristine Hoepers
cristine@nic.br

COMDEX 2002
São Paulo
21 de agosto de 2002

CSIRTs
Definição, Implantação e Importância

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

Motivação: Problemas no Cenário Atual

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)

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

Problemas no Cenário Atual (cont.)

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

CSIRT

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

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

Serviços Possíveis do CSIRT

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

Autoridade do CSIRT

- Completa
- Parcial
- Indireta
- Sem autoridade

Tipos de CSIRTs

- Empresas
- Países
- Backbones
- Órgãos Governamentais

Implantação de um CSIRT

Plano de Ação

Não existem regras para a formação de um CSIRT. Alguns passos sugeridos:

- Definir uma equipe/coordenador para guiar a implantação
- Envolver todas as partes da instituição
- Obter informações relevantes para a definição dos serviços a serem prestados

Plano de Ação (cont.)

- Definir a visão do CSIRT
  - Identificar a comunidade a ser atendida
  - Definir a missão e os objetivos
  - Definir o nível de autoridade
  - Inserir o CSIRT na estrutura organizacional
  - Identificar os recursos necessários para o grupo

Plano de Ação (cont.)

- Iniciar a implantação do grupo
  - Contratar e treinar o pessoal
  - Definir as políticas e procedimentos do grupo
  - Desenvolver documentos com orientações para notificação de incidentes e contato com o grupo
  - Comprar equipamentos
  - Implantar uma infra-estrutura de rede adequada
- Anunciar o CSIRT para a comunidade

Cuidados com a 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

Fatores de Sucesso do CSIRT

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

Onde obter treinamento

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

Leitura Recomendada

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

Leitura Recomendada (cont.)

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

Sites de Interesse

- Documentação sobre CSIRTs (Português e Inglês)
  http://www.nbso.nic.br/csirts/
- Documentos, RFCs e sites relacionados
  http://www.nbso.nic.br/links.html
- Security Knowledge in Practice
  http://www.cert.org/security-improvement/skip.html