Formas de Proteção contra Ataques a Redes e Serviços

Klaus Steding-Jessen
jessen@nic.br

NIC BR Security Office – NBSO
Brazilian Computer Emergency Response Team
http://www.nbso.nic.br/

Comitê Gestor da Internet no Brasil
http://www.cg.org.br/

Roteiro

- principais ameaças
- formas de proteção
  - políticas de atualização
  - segurança em camadas
  - proteção da rede interna
  - treinamento

Principais Ameaças

Principais Ameaças

- vulnerabilidades freqüentes
- códigos maliciosos explorando essas vulnerabilidades, em curto espaço de tempo
- ferramentas automatizadas de ataque
- vírus
- worms / bots
- atacantes + spammers
- fraudes / scams / phishing / crime organizado

Formas de Proteção

Segurança desde o Princípio

- planejamento do ambiente e da instalação
- política de segurança
- política de uso aceitável
- investir em treinamento
  - administradores de redes
  - desenvolvedores
  - suporte, etc

Política de Atualização e Correção

- possuir uma política de atualização de sistemas e aplicação de patches
  - sistema operacional (servidores e desktops)
  - aplicativos
  - hardware de rede
- não aplicar apenas quando estiver sendo explorado
  - tarde demais
- seguir a política!

Proteção da Rede Interna

grande risco: propagação de códigos maliciosos de dentro para fora (worms e bots)

- compartimentalização da rede
- política de atualização e correção
- política de conexão de equipamentos na rede interna
  - terceirizados
  - notebooks de funcionários, etc

Segurança em Camadas

Não há uma solução única para resolver todos os problemas.

- combinar soluções
- firewall, IDS, sistemas atualizados, antivírus
- múltiplas plataformas
- treinamento, atualização dos profissionais

Equipe de Segurança e Resposta a Incidentes

Deve:

- ser altamente especializada
- ter relação com outras instituições
- ter interação com outras equipes
  - operação
  - redes
  - help desk
  - etc

Educação dos usuários

- usuários podem ser um risco para a organização
- vetores de disseminação de worms/vírus
- alvos de:
  - ataques de engenharia social
  - phishing/scam
  - cavalos de tróia
  - furto de informações

Referências

- Esta palestra
  http://www.nbso.nic.br/docs/palestras/
- NBSO - NIC BR Security Office
  Brazilian Computer Emergency Response Team
  http://www.nbso.nic.br/
- Comitê Gestor da Internet no Brasil
  http://www.cg.org.br/
- Práticas de Segurança para Administradores de Redes Internet
  http://www.nbso.nic.br/docs/seg-adm-redes/
- Cartilha de Segurança para Internet
  http://www.nbso.nic.br/docs/cartilha/