Políticas de Segurança

Introdução

1. Potencial de Ataque
2. Nível de Segurança
3. Análise de Risco
4. Política de Segurança

Motivações para um ataque

- Ataques do interior da organização – representam 70% das ocorrências
  - Intensionais – colaboradores insatisfeitos, ...
  - Acidentais – equipa de limpeza
  - Difíceis de proteger
- Ataques do exterior – representam 30% das ocorrências
  - Concorrência – espionagem industrial, DoS, alteração de conteúdos web (*defacing*), etc
  - Militância – ambientalistas, pacifistas, ...
  - Visibilidade – ataques ao site da NASA ou do FBI
  - Publicidade indesejada – relay de mensagens SPAM

Potencial de ataque (1)

- Classificar de 1 a 5 treze questões:
  1. Acesso físico de público ao interior das instalações?
  2. Acesso de estranhos à organização aos recursos?
  3. Suporte de serviços de comunicação para o público em geral (ex. ISP)?
  4. Além da equipa de gestão, mais alguém tem acesso a previlégios de administração?
  5. Existe partilhas de contas entre utilizadores ou contas genéricas?
  6. A actividade da organização pode ser considerada controversa?
  7. A actividade da organização está relacionada com a àrea financeira?
  8. Existem servidores expostos à Internet?
  9. São usadas redes públicas (Internet, Frame Relay, RDIS) para dados sensíveis?
  10. A actividade da organização é altamente especializada?
  11. A organização teve um crescimento muito rápido?
  12. A organização tem tido muita visibilade nos media?
  13. Os utilizadores são especialistas em informática?

Potencial de ataque (2)

- Pontuação
  - <15 pode dormir descansado (mais ou menos)!
  - >15 e <30 potencial de ser alvo de ataque baixo
  - >30 e <40 potencial de ser alvo de ataque médio
  - >40 e <50 potencial de ser alvo de ataque elevado
  - >50 e <60 potencial de ser alvo de ataque muito elevado
  - >60 você está neste momento a ser atacado!

Nível de Segurança

- Análise de risco
  - Identificar os bens a proteger
  - Identificar as ameaças a esses bens
  - Identificar os custos associados
- Definição de uma política de segurança
  - Objectivos
  - Definição das medidas a implementar
  - Papel dos vários elementos da organização
  - Definição das medidas para impor a política de segurança
  - Relação com legislação em vigor
- Implementação da política de segurança
  - Instalação de mecanismos de segurança
  - Monitorização de segurança
  - Auditorias de segurança

Análise de Risco (1)

- O que é que necessita de protecção?
  - Recursos físicos (computadores, impressoras, ...)
  - Recursos intelectuais (informação)
  - Tempo (tempo de reparação, tempo de indisponibilidade)
- De quem é necessário garantir protecção?
  - Rede local
  - Redes remotas de outros ofícios
  - Redes de clientes ou fornecedores
  - Internet
  - Acesso comutado através de modems ou RDIS

Análise de Risco (2)

- Quem é que pode estar interessado em atacar os recursos informáticos?
  - Colaboradores
  - Concorrência
  - …
- Qual é a probabilidade de uma tentativa ser bem sucedida?
  - Quais os acessos ao exterior existentes?
  - Quais os mecanismos de autenticação existentes?
  - Quais os mecanismos de firewall existentes?
  - Que ganhos pode ter o atacante?

Análise de Risco (3)

- Quais são os custos imediatos de uma intrusão?
  - Custos de reparação
  - Custos de produtividade
  - Implicações na vida humana (ex. Hospital)
- Quais são os custos de recuperar de um ataque?
  - Custos de recuperação de sistemas
  - Custos de recuperação de informação
  - Custos de negação de serviços (DoS)
  - Custos devidos a acessos não autorizados e não detectados a informação

Análise de Risco (4)

- Como garantir a protecção a custos controlados?
  - Que nível de protecção é necessário?
  - Instalar firewall?
  - Contratar perito em segurança?
  - Quais os custos de produtividade dos mecanismos a instalar?
  - Não sobredimensionar as soluções (*overkill*)!
  - O custo de garantir protecção deve ser inferior ao custo de recuperação
- Existe alguma legislação que regulamente as medidas de segurança a adoptar?
  - É obrigatória a instalação de mecanismos de segurança (ex bancos)?
  - É proibido a utilização de algum mecanismo de segurança (ex cifragem)?

Política de Segurança (1)

- Introdução
  - Destinatários
    - Administradores de redes informáticas
    - Gestores (*decision makers*)
    - Utilizadores
  - Compromissos
    - Serviços oferecidos – segurança proporcionada
    - Facilidade de utilização – segurança
    - Custo da segurança – risco de perdas

Política de Segurança (2)

- Plano de Segurança (1)
  - Identificar o que se quer proteger
  - Determinar do que é que (ou quem) se está a proteger
  - Determinar o risco - quão provável é a ameaça
  - Implementar medidas de protecção tendo em conta a relação custo-eficácia
  - Rever e aperfeiçoar o processo quando existem pontos fracos

Política de Segurança (3)

- Plano de Segurança (2)

“O custo da protecção deve ser menor do que o custo do restabelecimento se uma ameaça se concretizar”

Política de Segurança (4)

- O que é?
  - É uma declaração formal das regras pelas quais as pessoas a quem é dado acesso ao **activo tecnológico e à informação** duma organização se devem reger

Política de Segurança (5)

- Porque deve existir?
  - Para informar as pessoas acerca dos requisitos obrigatórios para proteger o activo tecnológico e informação da organização
  - Para especificar os mecanismos pelos quais se podem atingir os requisitos de segurança
  - Para estabelecer uma base a partir da qual se pode configurar, auditar e adquirir sistemas informáticos para atingir os requisitos de segurança

Política de Segurança (6)

- Quem deve ser envolvido na definição da Política de Segurança?
  - Administrador(es) da rede
  - Responsáveis pela gestão da organização
  - Representantes dos utilizadores afectados pela Política de Segurança
  - Conselheiro legal (se apropriado)

Política de Segurança (7)

- Características
  - Deve definir claramente as responsabilidades dos utilizadores, administradores e gestores
  - Deve ser executável com ferramentas de segurança e prever sanções onde a prevenção não é tecnicamente viável
  - Deve ser implementada através dos procedimentos de administração dos sistemas

Política de Segurança (8)

- Componentes
  - Guia de aquisição de material informático
  - Política de privacidade
  - Política de acesso aos recursos
  - Política de responsabilidade
  - Política de autenticação
  - Disponibilidade dos recursos
  - Política de manutenção
  - Procedimentos em caso de transgressão
  - Informação de apoio

Política de Segurança (9)

- Flexibilidade
  - Independência do hardware
  - Independência do software
  - Mecanismos de actualização da Política de Segurança
  - Contemplar excepções
  - Partilha de informação

- Para saber mais:
  - RFC 2196 “Site Security Handbook”