Defesa de sistemas de informação

Víctor Orozco, Dr. Ana Trindade Winck

Centro de Tecnologia
Universidade Federal de Santa Maria

20 de Janeiro de 2013

Objetivos da aula

- Descrever mecanismos generalizados de defesa de sistemas
- Apresentar uma definição conceptual de controles de segurança
- Apresentar uma classificação de controles de segurança

Roteiro

Defesa de sistemas de informação

Defesa

Preciso defender?

Preciso defender?

Depende

Defesa

- Ativos 1-10
- Importância+impacto

Defesa

- Fotos da família - 2
- Filmes - 1
- Jogos (NFS nivel 10) - 1
- Coleção musicas (250gb) - 5

Defesa

- Dissertação de mestrado - 7
- Artigos en andamento - 9
- Documentação para renovação de visto de estudante - 10
- Arquivos de personalização do meu sistema operacional - 9

Defesa

Vale muito a pena

Defesa

Defesa

- Timeout de atividade
- Password BIOS
- Password sistema operacional
- Criptografia de HD em dados importantes
- Monitoramento remoto (Prey)
- Firewall
- Backup on-site semanal
- Backup na nuvem de documentos en andamento
- Atualizações semanais
- Boletim de segurança do Gentoo Linux
- Keyring de senhas

Defesa

Investimento: $ 100 (HD externo)

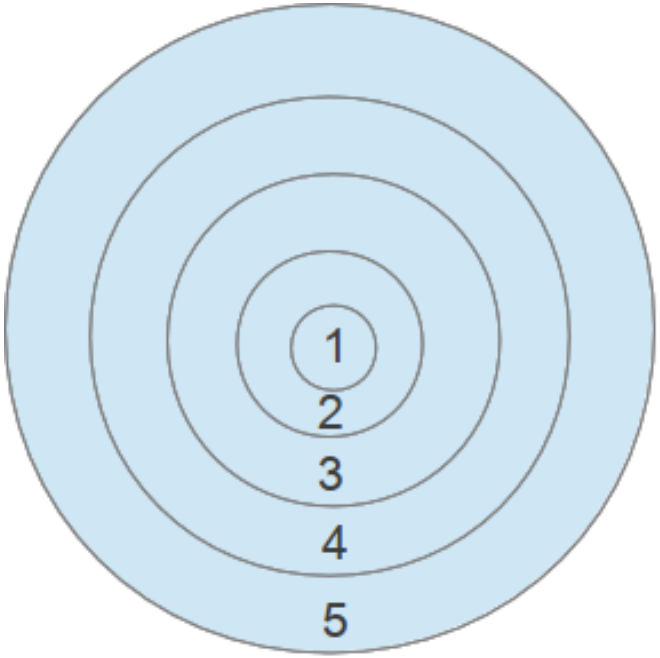
Defesa (experiencias)

- Um pendrive com um vírus 0day estragou meu Windows um dia antes da entrega duma tarefa
- Foi roubado um pendrive com todos os endereços de email da minha faculdade
- Uma versão desatualizada do Joomla deu controle para hackers Islamicos - não é piada

Defesa em profundidade

- Estrategia muito conhecida e comum
- Formular uma defesa de várias camadas que nos permitirá ainda montar um sucesso se uma ou mais de nossas medidas defensivas apresentam falhas

Defesa em profundidade



1- Dados
2- Aplicativos
3- Host
4- Rede interna
5- Rede externa

Defesa em profundidade

- Ela não é uma bala magica
- Não vamos ser capazes de manter todos os atacantes fora por um período indefinido de tempo
- Colocar suficientes medidas defensivas entre nossos ativos é os atacantes
- Comprar tempo suficiente para tomar medidas mais efetivas para impedir o ataque.

Controles de segurança

- Medidas para ajudar a garantir que um determinado tipo de ameaça é contabilizada (neutralizada, prevenida)
- Físicos
- Lógicos
- Administrativos

Fisicos

- Controles do lugar onde nossos sistemas e/ou a nossa informação foi guardada.
- Acesso ?
- Manter o meio físico ?

Fisicos

- Controles do lugar onde nossos sistemas e/ou a nossa informação foi guardada.
- Acesso: Cercas, portões, fechaduras.
- Manter o meio físico: sistemas de ar condicionado, sistemas de extinção de incêndio e geradores de energia.

Fisicos

- Se não formos capazes de proteger fisicamente os nossos sistemas e dados, quaisquer outros controles são irrelevantes.
- Se um atacante tem acesso físico pode acontecer:
  - Melhor caso: Destruir a nossa informação
  - Pior caso: Roubar a nossa informação e fazer com ela o que quiser

Logicos

- Também chamados de controles técnicos, protegem o ambiente que trafega e armazena os nossos dados
- Acesso ?
- Detecção ?

Logicos

- Também chamados de controles técnicos, protegem o ambiente que trafega e armazena os nossos dados.
- Acesso: Passwords, criptografia, firewalls
- Detecção: Antivírus, antispyware, sistemas de detecção de intrusão

Logicos

- Se nossos controles lógicos são implementadas adequadamente e são sucesso, um atacante ou usuário não autorizado não pode acessar nossas aplicações e dados sem subverter os controles que temos no lugar.
- Melhor caso: O acesso foi vulnerado mas foi detectado a tempo
- Pior caso: As medidas falharam e o atacante tem liberdade

Administrativos

- Definem as regras do comportamento esperado dos nossos usuários e o meio ambiente
- Papel ?
- Monitoramento ?

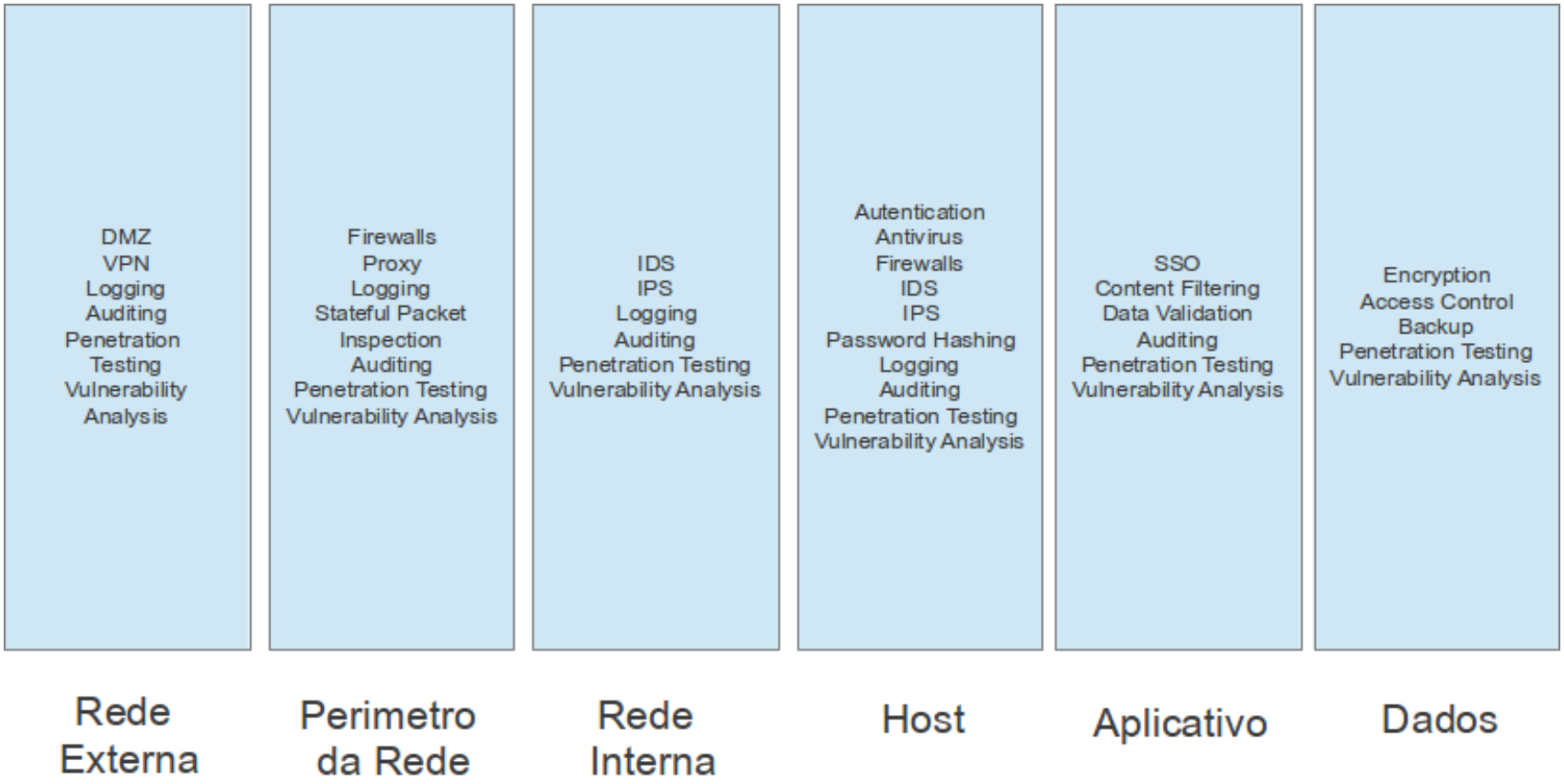
Administrativos

- Definem as regras do comportamento esperado dos nossos usuários e o meio ambiente
- Papel: Regras, leis, políticas, procedimentos, diretrizes
- Monitoramento: Capacidade de forçar as regras

Administrativos

- Se não temos a autoridade ou a capacidade de garantir que nossos controles estão sendo cumpridos, eles criam uma falsa sensação de segurança.
- Uso de telefone e celular, acesso à Web, e-mail, uso conversas de mensagens instantâneas, o software instalado, e outras áreas potenciais de abuso.

Defesa em profundidade



Tarefa

- Objetivo: Conhecer esforços de segurança dentro e fora do Brasil
- Uma instituição de governo ou acadêmica focada na área de segurança de sistemas de informação
  - Orçamento 2012
  - Resultados (comentários)

Tarefa

- Analisar três pesquisas ou ferramentas novas 2011-2013 na área de segurança
  - Problema que ela tenta resolver (ataques)
  - Objetivo da ferramenta/pesquisa (como ela tenta resolver)
  - Pontos de controle que ela estabelece
- Artigos acadêmicos, blogs sérios segurança
- Referencias
- Relatório 3 paginas limite
  - Físicos
  - Lógicos
  - Administrativos

Referencias I


Andress, J. (2011).
The basics of information security understanding the fundamentals of InfoSec in theory and practice.
Syngress, Waltham, MA.