Introdução à Segurança da Informação

Prof. Dr. Volnys Borges Bernal[2]
Prof. Dr. Adilson Eduardo Guelfi[1]

(1) Faculdade de Informática de PP
FIPP/UNOESTE

(2) Laboratório de Sistemas Integráveis
Escola Politécnica da USP

Agenda

- Ataques à Segurança
- Serviços e Mecanismos de Segurança
- Referências Bibliográficas

Ataques à Segurança

Ataques à Segurança

- **Ataque à Segurança**
  - Qualquer ação que comprometa a segurança da informação pertencente a uma organização

Ataques à Segurança

- **Ataques à segurança são classificados em dois grandes grupos: ataques passivos e ataques ativos**
- **Ataques Passivos**
  - Ataques que deixam de alterar, perturbar ou afetar um sistema, recursos ou um fluxo de comunicação
  - Possuem a natureza de bisbilhotar ou monitorar transmissões
  - O objetivo é obter informações
  - Ataques passivos são muito difíceis de detectar, portanto o principal controle está na prevenção
  - Exemplos: Leitura desautorizada de uma mensagem ou análise de tráfego

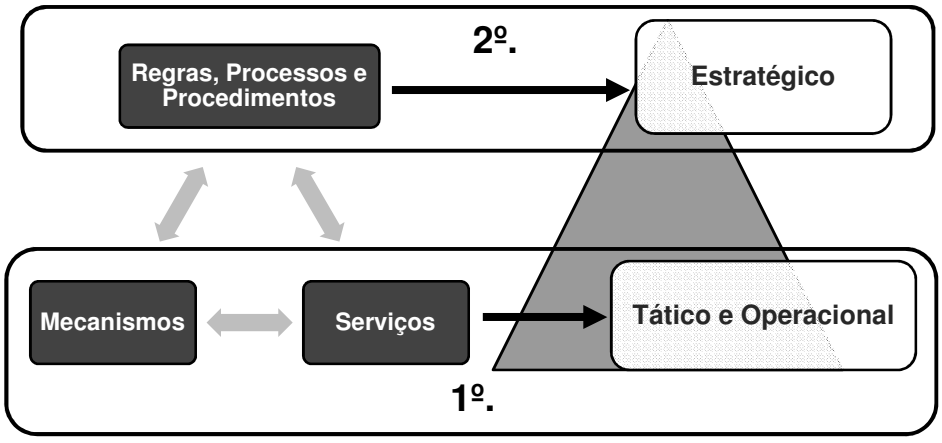
Ataques à Segurança

- **Ataques Ativos**
  - Ataques que modificam ou geram perturbação em um sistema, recursos ou um fluxo de comunicação
    - Exemplos: modificação de mensagens ou arquivos, negação de serviço, disfarce, replay etc.
  - Ataques ativos são mais fáceis de detectar e em geral envolvem mais recursos ou esforços de prevenção
  - Ataques ativos exigem detecção, prevenção e recuperação dos efeitos por eles causados

Serviços e Mecanismos de Segurança

Serviços e Mecanismos de Segurança

- **A segurança da informação está conceitualmente baseada nos seguintes princípios teóricos:**

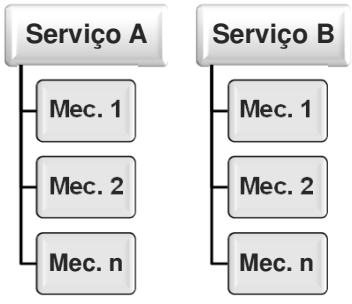


Serviços e Mecanismos de Segurança

- **Serviço de Segurança**
  - Um serviço de processamento ou comunicação que aumenta o controle e a proteção dos recursos dos sistemas e das transferências de informação de uma organização
  - Serviços servem para frustrar ou controlar ataques à segurança
  - Um serviço de segurança é uma funcionalidade relacionada à segurança computacional
  - Serviços utilizam um ou mais mecanismos de segurança

Serviços e Mecanismos de Segurança

- **Mecanismo de Segurança**
  - Qualquer processo, implementação, ação, algoritmo ou meio projetado para detectar, impedir ou permitir recuperar-se de um ataque à segurança
  - Alguns exemplos de mecanismos de segurança são algoritmos de criptografia, assinaturas digitais e protocolos de autenticação



Serviços e Mecanismos de Segurança

- **O conhecimento dos principais serviços de segurança possibilita:**
  - A um projetista, verificar quais são os serviços de segurança necessários a um sistema
  - A um profissional de TI, na escolha de um produto, identificar quais serviços de segurança são relevantes
  - A um auditor, durante a auditoria de um sistema, verificar se um determinado serviço é suportado

Serviços e Mecanismos de Segurança

- **O suporte a um serviço e mecanismo de segurança por um sistema depende dos seguintes fatores:**
  - Se o serviço e o mecanismo de segurança é relevante
  - Qual o nível de segurança que se deseja atingir
  - Custo envolvido
  - Viabilidade tecnológica

Serviços e Mecanismos de Segurança

- **Níveis de segurança**
  - O fornecimento de um serviço de segurança por um ou mais mecanismos define o nível de segurança atingido
  - Exemplo: Transferência sigilosa de arquivos entre filiais autenticadas
    - **Serviços de segurança implementados**:
      - Confidencialidade (sigilo)
      - Autenticação de parceiro
    - **Mecanismos utilizados:**
      - Confidencialidade: criptografia simétrica AES 256 bits
      - Autenticação de parceiro: senha
    - **Nível de segurança:**
      - **Confidencialidade: nível BOM**
      - **Autenticação de parceiro: nível MEDIANO**

Referências Bibliográficas

Referências Bibliográficas

- **Criptografia e Segurança de Redes - Princípios e Práticas (4a. Edição)**
  - Willian Stallings, Pearson. 2008
- **NIST Special Publication 800-33**
  - Computer Security: Underlying Technical Models for Information Technology Security
  - NIST, Dec, 2001
- **IETF - Network Working Group**
  - Request for Comments: 2828 (RFC 2828). Internet Security Glossary.
  - R. Shirey. May 2000 (https://www.ietf.org/rfc/rfc2828.txt)

Referências Bibliográficas

- **Sites Recomendados – Procurar por:**
  - COAST
  - The Cryptography FAQ
  - Tom Dunigan´s Security Page
  - Helgar Lipma´s Cryptology Pointers
  - Computer Security Resource Center (NIST – procurar pelos FIPS Special Publications)
  - SANS Institute