Segurança dos sistemas de informação

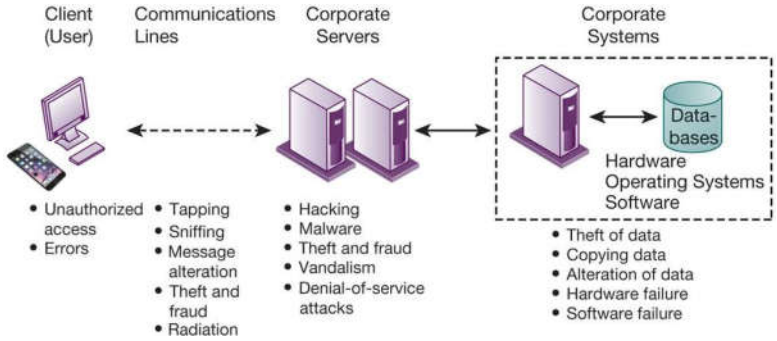
Por que os sistemas são vulneráveis

- **Segurança**
  - Políticas, procedimentos e medidas técnicas utilizadas para evitar acesso não autorizado, alteração, roubo ou dano físico aos sistemas de informação
- **Controles**
  - Métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização; precisão e confiabilidade de seus registros contábeis; e aderência operacional aos padrões de gestão.

- Acessibilidade das redes
- Problemas de hardware (avarias, erros de configuração, danos por uso indevido ou crime)
- Problemas de software (erros de programação, erros de instalação, alterações não autorizadas)
- Catástrofes
- Uso de redes/computadores fora do controle da empresa
- Perda e roubo de dispositivos portáteis

Prof. Dr. Tiago Araújo

Desafios e Vulnerabilidades de Segurança Contemporânea



Vulnerabilidades da Internet

- Rede aberta a qualquer pessoa
- O tamanho da Internet significa que os abusos podem ter amplo impacto
- O uso de endereços fixos na Internet com modems a cabo / DSL cria alvos fixos para hackers
- VOIP não criptografado
- E-mail, P2P, IM
- Intercepção
- Anexos com software malicioso
- Transmissão de segredos comerciais

Desafios da segurança sem fio

- **Faixas de radiofrequência fáceis de escanear**
- **SSIDs (identificadores do conjunto de serviços)**
  - Identificar pontos de acesso, transmitidos várias vezes, podem ser identificados por programas sniffer
- **Condução de guerra**
  - Os espiões passam pelos edifícios e tentam detectar o SSID e obter acesso à rede e aos recursos
  - Uma vez que o ponto de acesso é violado, o intruso pode ganhar acesso a unidades e arquivos em rede
- **Pontos de acesso indevidos**

Software malicioso: Vírus, Worms, cavalos de Tróia e Spyware

- Malware (software malicioso)
- Vírus
- Worms (minhocas)
- Worms e vírus espalhados por:
  - Downloads e dirigidos- por download
  - E-mail, anexos de IM
- Malwares de dispositivos móveis
- Malwares de redes sociais
- Cavalo de Tróia
- Ataques de injeção SQL
- Ransomware
- Spyware
  - Registradores chave
  - Outros tipos
    - Reiniciar a página inicial do navegador
    - Pedidos de busca redirecionada
    - Lentidão no desempenho do computador, ocupação da memória

Hackers e crimes informáticos

- Hackers vs. crackers
- As atividades incluem:
  - Intrusão do sistema
  - Guerra cibernética
  - Cibervandalismo
    - Ruptura intencional, desfiguração, destruição de website ou sistema de informação corporativa
- **Falsificar e sniffing (farejar)**
  - Danos ao sistema
  - Fraude por clique
  - Ciberterrorismo
- Ataques de negação de serviço (DoS)
- Ataques de negação de serviço distribuídos (DDoS)
- Botnets
- Roubo de identidade
  - Phishing
  - Evil twins
  - Pharming
- Spam
- Crimes cibernéticos
  - Computador pode ser alvo de crime
  - O computador pode ser um instrumento do crime

Ameaças Internas: Funcionários

- As ameaças à segurança muitas vezes se originam dentro de uma organização
- Conhecimento Interno
- Procedimentos de segurança descuidados
  - Falta de conhecimento do usuário
- Engenharia social
- Tanto os usuários finais quanto os especialistas em sistemas de informação são fontes de risco

Vulnerabilidades de Software

- **O software comercial contém falhas que criam vulnerabilidades de segurança**
  - Bugs (defeitos no código do programa)
  - Zero defeitos não pode ser alcançado
  - As falhas podem abrir redes para intrusos
- **Vulnerabilidades de dia zero**
- **Patches**
  - Pequenas peças de software para reparar falhas
  - Gerenciamento de patches

Qual é o valor comercial da segurança e do controle?

- Falhas nos sistemas de computador podem levar a uma perda significativa ou total da função comercial
- As empresas estão agora mais vulneráveis do que nunca
  - Dados pessoais e financeiros confidenciais
  - Segredos comerciais, novos produtos, estratégias
- Uma quebra de segurança pode cortar o valor de mercado de uma empresa quase imediatamente
- A segurança e os controles inadequados também trazem problemas de responsabilidade

Política de Segurança

- **Classifica os riscos da informação, identifica objetivos de segurança e mecanismos para atingir esses objetivos**
- **Conduz outras políticas**
- **Avaliação de risco**
- **Política de uso aceitável (AUP)**
  - Define os usos aceitáveis dos recursos de informação e equipamentos de informática da empresa
- **Gestão da identidade**
  - Identificação de usuários válidos
  - Controle de acesso

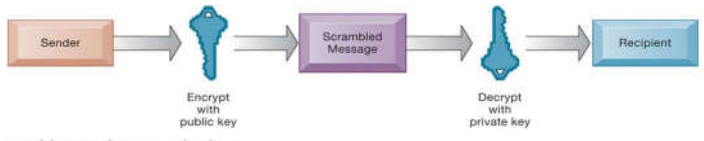
Ferramentas e Tecnologias para Salvaguarda dos Sistemas de Informação

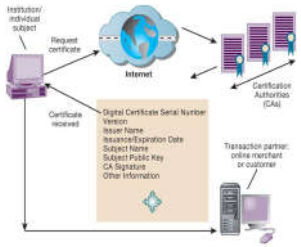
- **Software de gerenciamento de identidade**
  - Automatiza o controle de todos os usuários e privilégios
  - Autentica os usuários, protegendo identidades, controlando o acesso
- **Autenticação**
  - Sistemas de senhas
  - Tokens
  - Cartões inteligentes
  - Autenticação biométrica
  - Autenticação de dois fatores
- **Firewall**
  - Combinação de hardware e software que impede usuários não autorizados de acessar redes privadas
  - Filtragem de pacotes
  - Inspeção estatal
  - Tradução de endereços de rede (NAT)
  - Filtragem por procuração de aplicação

Ferramentas e Tecnologias para Salvaguarda dos Sistemas de Informação (3 de 3)

- **Sistema de detecção de intrusão**
  - Monitora pontos de risco em redes corporativas para detectar e dissuadir intrusos
- **Antivírus e software antispyware**
  - Verifica computadores quanto à presença de malware e pode muitas vezes também o eliminar
  - Requer atualização contínua
- **Sistemas de gestão unificada de ameaças (UTM)**

Criptografia de chave pública & Certificado Digital





Garantindo a disponibilidade do sistema

- **O processamento de transações on-line requer 100% de disponibilidade**
- **Sistemas de computador tolerantes a falhas**
  - Contêm componentes redundantes de hardware, software e fornecimento de energia que criam um ambiente que fornece serviço contínuo e ininterrupto
- **Inspeção profunda de pacotes**
- **Terceirização de segurança**
  - Fornecedores de serviços de segurança gerenciados (MSSPs)