

II Semana de Informática - CEUNSP

Segurança da Informação



João Carlos da Silva Jr

- Especialista em Segurança no Desenvolvimento de Software (Microsoft)
- MBA em Gestão de Negócios e Tecnologia (IPT/USP)
- Bacharel em Análise de Sistemas (PUC-Campinas)
 - Analista de Sistemas – ESPM
 - Consultor – Stefanini IT Solutions
 - Analista de Sistemas – Banco Unibanco S/A
 - Analista de Sistemas – IBM
- Colunista UML do site iMasters (<http://www.imasters.com.br>)

Objetivo

- Apresentar os principais conceitos sobre Segurança da Informação
- Foco não é técnico
- Indicar onde conseguir informações e cursos gratuitamente
- Criar uma rede de relacionamento sobre Segurança da Informação

Evolução

- Anos 70 - Plataforma Tecnológica de mainframe
 - Fronteiras virtuais rígidas entre os ambientes tecnológicos internos e o mundo externo.
- Anos 80 e início dos anos 90 - Migração para cliente/servidor
 - Fronteiras virtuais rígidas entre os ambientes tecnológicos internos e o mundo externo.
- Características da Segurança - Proteção
 - Conceder acesso aos sistemas e aplicações através da identificação combinada de nome do usuário e senha
 - Permitir comunicação eletrônica com parceiros externos apenas por meio de aplicações que foram preparadas previamente

Evolução

- Final dos anos 90 e o início dos anos 2000
 - Aplicações Internet: clientes, funcionários e parceiros de negócio tendo acesso aos sistemas pelos navegadores.
 - Soluções web: portais de usuário, portais de fornecedores, intranets e extranets.
 - Empresa expandida: alteração no tratamento da segurança da informação.
- Características da Segurança - Proteção
 - Os recursos tecnológicos certos devem ser conectados e estar disponíveis para as pessoas certas, no momento certo.
 - Proteção e monitoramento de perímetro são assegurados
 - Confidencialidade e integridade dos dados

TI nos últimos anos

- Ambiente cheio de mudanças
- Motivador: Evolução tecnológica acelerada
 - Redução do tamanho e do custo dos equipamentos e componentes
 - Aumento da capacidade de processamento
 - Aumento da capacidade de armazenamento e transmissão de dados

TI nos últimos anos

- Motivador: Novas necessidades e oportunidades
 - Criatividade é o limite para o uso da tecnologia

TI nos últimos anos

- A popularização da tecnologia
 - Cada vez mais as pessoas convivem em seu dia a dia com as aplicações, equipamentos e informações de tecnologia
 - Semelhança com o ambiente de trabalho

Problema: A crescente complexidade da TI

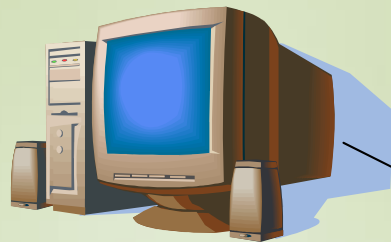
Sistema Operacional	Ano	Linhas de Código
Windows 3.1	1992	3 milhões
Windows 95	1995	15 milhões
Windows 98	1998	18 milhões
Windows 2000	2000	40 milhões

Segurança da Informação – Ontem e Hoje

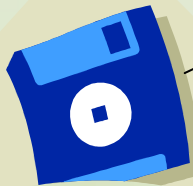
	Ontem	Hoje
Segurança	Internet	Sistemas Financeiros
Inimigo	Hacker	Crime Organizado
Tipo de ataque	Pichação, DoS	Fraude

O que são ativos?

Tudo que possui valor para a organização



**Equipamentos e
Sistemas**



Informações



Processos



Pessoas



Serviços

Princípios da Segurança

- **Confidencialidade**
 - Garantir que apenas a pessoa correta tenha acesso à informação que queremos distribuir
- **Integridade**
 - Garantir que os dados não sofram alterações
- **Disponibilidade**
 - Informação chegar no momento oportuno

Perguntas para pensar

- Quanto importante é para você que as informações sobre os salários dos funcionários de sua empresa não sejam alteradas por acidente ou delito?
- Você sabe quem pode ter acesso a suas informações?
- A informação necessária para a tomada de decisões críticas para o negócio se encontra sempre disponível?

As ameaças estão sempre por perto?

- Ameaça é qualquer ação ou acontecimento que possa agir sobre um ativo.
- Toda ação ou acontecimento é através de uma vulnerabilidade, gerando um determinado impacto.

Exemplos de Ameaças

- Naturais: raios, incêndios;
- De Negócio: fraudes, erros, sucessão de pessoas;
- Tecnológicas: mudanças, "bugs", invasões;
- Sociais: greves, depredação, vingança;
- Culturais: impunidade;

Estamos preparados?

- Substituição de executivos
- Falha de Hardware e/ou Software
- Falha na Rede
- Invasão da Rede
- SPAM
- Falha Humana
- Espionagem

Mercado x Segurança da Informação

- Os riscos começaram a se materializar mais perto da empresa
- Os impactos começaram a ser consideráveis
- As pessoas começaram a medir e avaliar os impactos

Mercado x Segurança da Informação

- Só 40% das empresas podem garantir que detectariam um ataque.
- 40% das empresas não investigam os incidentes de segurança.
- Menos de 50% das empresas tem um programa de treinamento sobre segurança da informação.

Pesquisa da Ernest&Young de 2002

Os problemas estão longe?

- Dados confidenciais de quase cinco milhões de assinantes da Telefônica valem R\$ 20,00 em camelôs (24/09/2001)
- Hackers brasileiros fazem ataques em massa à sites financeiros (13/11/2002)

Caso: Fevereiro 2003

- Indústria do setor químico de pequeno porte (45 funcionários)
- Fato: Fórmula recém desenvolvida e ainda não lançada oficialmente no mercado aparece negociada em um de seus principais clientes.
- Perda: US\$ 270K/mês (receita) + gastos pesquisas + imagem.
- Dados:
 - 1 ano de investigação sobre o assunto: \$ honorários + \$ despesas
 - 4 pessoas desligadas e 1 preso
 - Impossibilidade de comprovar a posse e o controle da fórmula, ausência total de controles
 - Impossibilidade de recuperar as perdas e parar as vendas do produto
- Conclusões:
 - Após a implantação dos controles sobre PABX, central de fax e e-mail consegue-se identificar um dos envolvidos.
 - Toda a negociação era feito por e-mail, telefone da própria empresa.

O que são medidas de segurança?

- São ações orientadas para a eliminação de vulnerabilidades, com o objetivo de evitar que uma ameaça se torne realidade.
- Ações podem ser:
 - Preventivas: Busca evitar o surgimento de novos pontos fracos e ameaças.
 - Perceptivas: Busca revelar atos que possam pôr em risco as informações.
 - Corretivas: Buscar corrigir os problemas de segurança à medida que eles ocorrem.

O que é segurança?

- Segurança é uma atividade cujo propósito é:
 - Proteger os ativos contra acessos não autorizados
 - Evitar alterações indevidas que possam pôr em risco sua integridade
 - Garantir a disponibilidade da informação

Como se manter atualizado?

- <http://www.technetbrasil.com.br>
- <http://www.infoguerra.com.br>
- <http://www.cartilha.cert.br>
- <http://www.modulo.com.br>
- <http://www.nextg.com.br>
- Revista: Security Review
- Academia Latino Americana de Segurança da Informação (Microsoft)

KIT

- Artigos
 - Técnicas defensivas contra injeção de comandos
 - Orientações para senhas seguras
 - Como rastrear tentativas de invasão no PC
 - O que é TCP/IP?
 - Aspectos de segurança em redes Wi-Fi
 - Como proteger as informações nas empresas
 - Mitos de segurança: Ataques e defesas
 - Como se tornar um hacker
- CheckList
- Glossário

Obrigado

Dúvidas?

Contato

João Carlos da Silva Junior
joao@atenacriacao.com.br

Telefones

11 5085-4660

11 3731-4217

Visite:

<http://www.atenacriacao.com.br>