Unidade 1
Segurança em Sistemas de Informação

Existe uma rede 100% segura?

Riscos não podem ser eliminados !!

- ✓ Riscos podem ser identificados, quantificados e reduzidos, mas não é possível eliminá-los completamente.
- ✓ Não importa quão seguro se faça um sistema, sua segurança "sempre" poderá ser quebrada!

Propósito da Segurança da informação

Assim, o propósito da segurança da informação é garantir a continuidade do negócio da organização, minimizando os danos causados à organização, através da prevenção e redução dos impactos causados por incidentes de segurança.

O que proteger?

Quando se fala em segurança de redes dentro de uma corporação, logo se pensa:

→ Quais itens as organizações devem se preocupar em defender:

- ✓ Documentos
- ✓ Imagem
- ✓ Pessoas
- ✓ Patrimônio

Contra quem?

Terroristas

Espiões Industriais

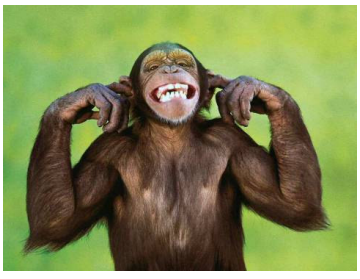
Concorrência Desleal

Ex-funcionários

Contra quem?

Crackers

Phreackers

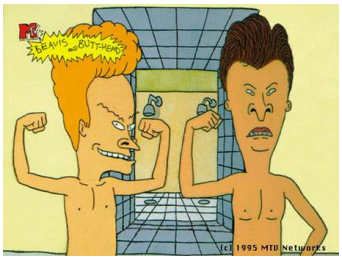


Script Kid

Carders

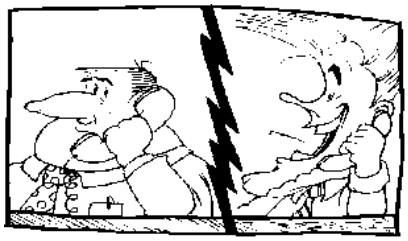
Contra o quê?

Trash Dump



Força Bruta

Sniffer



Engenharia Social

Cavalos de Tróia

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

Contra o quê?

Rootkits

Backdoors

- Adwares
- Spywares
- Dialers
- Keyloggers
- Wardialing
- Wardriving

Norma Básica para Segurança

→ Tudo que não é especificamente negado é permitido

→ Tudo que não é especificamente permitido é negado

Equação Básica da Segurança

Proteção ↑  **Custo** ↑

"Atacai-o onde não estiver preparado. Executai as vossas investidas somente quando não vos esperar."

- Sun Tzu, A Arte da Guerra

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

"Se você conhece a si próprio mas não conhece seu inimigo, você ganhará e perderá muitas batalhas. Se você conhece a si e a seu inimigo você ganhará todas as batalhas. Mas se você não conhece a si nem ao seu inimigo, você perderá todas as batalhas"

- Sun Tzu, A Arte da Guerra

Por que é necessária a segurança da informação

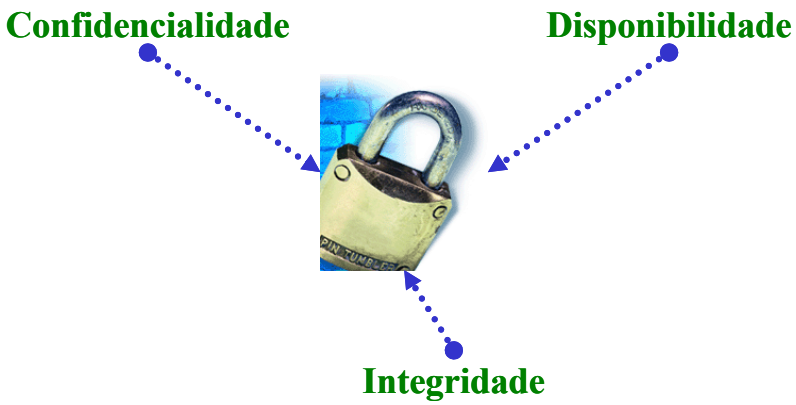
"A dependência nos sistemas de informação e serviços significa que as organizações estão cada vez mais vulneráveis às ameaças de segurança. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída dificulta a implementação de um controle de acesso centralizado realmente eficiente."

(ISO/IEC 17799).

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

Objetivos da Segurança da Informação

A segurança da informação tem como objetivo a preservação de três princípios básicos:



Objetivos da Segurança da Informação

Confidencialidade

- ✓ Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

Integridade

- ✓ Toda a Informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

Disponibilidade

- ✓ Toda a informação gerada ou adquirida por um individuo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

Política de Segurança

- ✓ A política de segurança atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham.
- ✓ Uma política de segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir a política de segurança pode ser considerado um incidente de segurança.
- ✓ Na política de segurança também são definidas as penalidades às quais estão sujeitos aqueles que não cumprirem a política.

(Cartilha de Segurança para Internet – 2006. CERT.br)

Política de Segurança

"A política de segurança trata dos aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos e os negócios, além da legislação local. É com base nessa política de segurança que as diversas normas e os vários procedimentos devem ser criados."

(NAKAMURA, 2007)

"Equipamentos só funcionam se tivermos uma política para cuidar das pessoas que lidam com eles."

(ICC/INATEL)

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

Política de Segurança

- ✓ É, portanto, a declaração de um conjunto de regras às quais toda e qualquer pessoa com acesso aos recursos tecnológicos e/ou de informações de uma empresa ou entidade deve se submeter."
- ✓ Define uma estratégia sobre:
  - A importância da segurança da informação para esta organização?
  - Requisitos de Proteção
  - O que proteger?
  - Análise de riscos
  - Privilégios de usuários
  - Auditoria
  - Medidas a serem tomadas na ocorrência de incidentes

Política de Segurança

Importante !!!

O desenvolvimento de uma política de segurança deve ser uma atividade interdepartamental.

As áreas afetadas devem participar do processo envolvendo-se e comprometendo-se com as metas propostas além de:

- ✓ Entender o que é necessário;
- ✓ Saber pelo que são responsáveis;
- ✓ Conhecer o que é possível com o processo.

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

Política de Segurança

Implementar uma política de segurança em uma empresa ou organização implica em implementar controles de segurança do tipo:

- ✓ Físicos;
- ✓ Lógicos;
- ✓ Organizacionais;
- ✓ Pessoais;
- ✓ Operacionais;
- ✓ De desenvolvimento de aplicações;
- ✓ Das estações de trabalho;
- ✓ Dos servidores;
- ✓ De proteção na transmissão de dados.

Política de Segurança

Controles físicos:

- ✓ Restrição de acesso indevido de pessoas a áreas críticas da empresa;
- ✓ Uso de equipamentos ou sistemas por funcionários mal treinados;

Controles lógicos:

- ✓ Prevenção e fortalecimento de proteção seletiva de recursos;
- ✓ Problemas/prevenção causados por vírus, e acesso de invasores;
- ✓ Fornecer/retirar autorização de acesso;
- ✓ Fornecer relatórios informando que recursos estão protegidos e que usuários tem acesso a esses recursos;

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

Política de Segurança

Controles organizacionais:

- ✓ Responsabilizar cada usuário por lista de deveres;
- ✓ Especificar em cada lista o que, quando, e como deve ser feito;
- ✓ Esclarecer as conseqüências do não cumprimento da lista.

Controles pessoais:

- ✓ Criação de motivação/treinamento sobre segurança;
- ✓ Bloqueio dos arquivos pessoais do empregado quando da sua demissão;
- ✓ Inclusão de tópicos de segurança no manual dos empregados;
- ✓ Cobrar aspectos de segurança na avaliação do funcionário.

Política de Segurança

Controles operacionais:

- ✓ Acompanhar e registrar cada problema, sua causa e sua solução;
- ✓ Planejar estruturas de arquivos e de diretórios;
- ✓ Prever/fornecer proteção de energia ao parque computacional e de conectividade (servidores, switches, roteadores, etc.);
- ✓ Garantir a confidencialidade e a integridade dos dados avaliando o aspecto custo-benefício da rede.

Inatel
Instituto Nacional de Telecomunicações
Segurança em Sistemas de Informação – Unid. 1

Política de Segurança

Controle de desenvolvimento de aplicações:

- ➢ No caso das empresas não-desenvolvedoras de aplicações:
  - ✓ Adquirir software necessário e documentação necessária.
- ➢ No caso de empresas desenvolvedoras de aplicações:
  - ✓ Verificar a existência/eliminar bugs em softwares;
  - ✓ Dar apoio de software em outros locais da organização;
  - ✓ Manter/atualizar documentação.

Política de Segurança

Controle dos servidores:

- ✓ Prover proteção diversa (incêndios, umidade, temperatura, acessos);
- ✓ Mantê-lo em ambiente fechado.

Controle das estações de trabalho:

- ✓ Proteger os computadores contra roubo de placas e acessos ao interior do gabinete (uso de travas);
- ✓ Controlar instalação de programas de captura de senha;
- ✓ Controlar acesso às estações.

Política de Segurança

Controle na transmissão dos dados:

- ✓ Uso de criptografia/certificação digital;
- ✓ Uso de fibras ópticas ou cabos pneumáticos que emitem alarmes quando despressurizados por "grampos";
- ✓ Uso de filtros/proxies/firewall nas fronteiras da rede, e entre redes.

Política de Segurança

Resumindo:

O objetivo da segurança de sistemas de informação é prover um nível adequado de segurança que proteja os recursos da organização contra interrupções; proteger a informação armazenada nos computadores da organização contra modificações e divulgação não autorizada; estabelecer as condições para que a organização se recupere rapidamente de uma interrupção; e é zelar para que os usuários da organização não sejam demasiadamente afetados pelas medidas de segurança."

Lista de Exercícios 01