

Capítulo 2 - Conceitos de Segurança Física e Segurança Lógica

- ✓ 2.1 - Introdução
- ✓ 2.2 - Segurança Física
 - 2.2.1 - Segurança externa e de entrada
 - 2.2.2 - Segurança da sala de equipamentos
 - 2.2.3 - Segurança dos equipamentos
 - 2.2.4 - Redundância lógica
 - 2.2.5 - Segurança no fornecimento de energia
 - 2.2.6 - *No-break*
 - 2.2.7 - Gerador
 - 2.2.8 - Salvaguarda (*backup*)
 - 2.2.9 - Cortador de papel

✓ 2.3 - Segurança Lógica

- 2.3.1 - *Firewalls*
- 2.3.2 - Autenticação e autorização
- 2.3.3 - Detectores de intrusos
- 2.3.4 - Redes virtuais privadas (VPN's)

2.1 - Introdução

- ✓ Segurança física → ambiente
- ✓ Segurança lógica → programas
- ✓ A segurança começa pelo ambiente físico
 - *“Não adianta investir dinheiro em esquemas sofisticados e complexos se não instalarmos uma simples porta para proteger fisicamente os servidores da rede.”*
- ✓ A segurança lógica deve ocorrer após a segurança física, através de softwares e protocolos

2.2 - Segurança Física

- ✓ Abrange todo o ambiente onde os sistemas de informação estão instalados:
 - prédio
 - portas de acesso
 - trancas
 - piso
 - salas
 - computadores
- ✓ Requer ajuda da engenharia civil e elétrica
- ✓ A norma NBR ISO/IEC 17799:2001 divide a área de segurança física da seguinte forma:

✓ Áreas de segurança

- perímetro da segurança física
- controles de entrada física
- segurança em escritórios, salas e instalações de processamento
- trabalhando em áreas de segurança
- isolamento das áreas de expedição e carga

✓ Segurança dos equipamentos

- instalação e proteção de equipamentos
- fornecimento de energia
- segurança do cabeamento
- manutenção de equipamentos
- segurança de equipamentos fora das instalações
- reutilização e alienação segura de equipamentos

✓ Controles gerais

- política de mesa limpa e tela limpa
- remoção de propriedade

2.2.1 - Segurança externa e de entrada

- ✓ Proteção da instalação onde os equipamentos estão localizados, contra:
 - entrada de pessoas não autorizadas
 - catástrofes ambientais
- ✓ O prédio deve ter paredes sólidas e número restrito de entradas e saídas
- ✓ Evitar baixadas onde a água possa se acumular → enchentes
- ✓ Evitar áreas muito abertas → descargas atmosféricas
- ✓ Em qualquer lugar, usar pára-raios
- ✓ Usar muros externos e manter a área limpa → queimadas

- ✓ Controle de acesso físico nas entradas e saídas:
 - travas
 - alarmes
 - grades
 - vigilante humano
 - vigilância eletrônica
 - portas com senha
 - cartão de acesso
 - registros de entrada e saída de pessoas e objetos
- ✓ Funcionários que trabalham na instituição devem ser identificados com crachás com foto
- ✓ Visitantes devem usar crachás diferenciados por setor visitado
- ✓ Todos funcionários devem ser responsáveis pela fiscalização

2.2.2 - Segurança da sala de equipamentos

- ✓ Agrega todo o centro da rede e os serviços que nela operam
- ✓ Entrada somente de pessoal que trabalha na sala
- ✓ Registro de todo o pessoal que entra e sai
- ✓ A sala deve ser trancada ao sair
- ✓ Deve fornecer acesso remoto aos equipamentos
- ✓ O conteúdo da sala não deve ser visível externamente
- ✓ Além do acesso indevido, a sala deve ser protegida contra:
 - vandalismo
 - fogo
 - interferências eletromagnéticas
 - fumaça
 - gases corrosivos
 - poeira

- ✓ Se possível, uso de salas-cofre



2.2.3 - Segurança dos equipamentos

- ✓ Evitar o acesso físico aos equipamentos
 - acesso ao interior da máquina (*hardware*)
 - acesso utilizando dispositivos de entrada e saída (console)
- ✓ Proteger o setup do BIOS
- ✓ Tornar inativos botões de *setup* e liga/desliga no gabinete
 - colocar senha no BIOS
 - inicialização apenas pelo disco rígido



2.2.4 - Redundância

- ✓ São comuns falhas de *hardware*, causadas por acidentes ou fadiga de componentes mecânicos e eletrônicos
- ✓ “Todo sistema computacional um dia vai falhar” pelos motivos acima
- ✓ **MTBF**: *Mean Time Between Failures*
- ✓ **MTTR**: *Mean Time To Repair*
- ✓ O mecanismo mais importante para tolerar falhas é a redundância
 - redundância de servidores
 - redundância de fonte de alimentação
 - redundância de discos (RAID)
 - redundância de equipamentos
 - redundância de ventilação
 - redundância de interfaces de rede

2.2.5 – Segurança no fornecimento de energia

- ✓ Geralmente o fornecimento de energia é de responsabilidade da concessionária, e pode apresentar:
 - variação de tensão
 - interrupção do fornecimento
- ✓ Para garantir a disponibilidade da informação é preciso garantir o fornecimento constante de energia e que ela esteja dentro da tensão recomendada
 - filtro de linha
 - estabilizador de tensão
 - *no-break*
 - solução mista
 - gerador



2.2.6 - Salvaguarda (*backup*)

- ✓ O processo de backup envolve segurança física e lógica
 - física: armazenamento das mídias
 - lógica: software de backup
- ✓ Backup é o último recurso no caso de perda de informações:
 - garantia de que ele não vá falhar
 - garantir de que ele esteja disponível e acessível quando necessário
- ✓ Hardware mais utilizado para backup são as fitas
 - baixo custo
 - alta capacidade

- ✓ A mídia de *backup* pode ser a única forma de restaurar a informação:
 - proteger contra roubo
 - proteger contra catástrofes naturais
 - há cofres especiais para armazenamento de mídias
- ✓ Prática simples e eficiente é o armazenamento externo ou *off-site*
 - quanto maior a distância, melhor
 - armazenadas em cofre e/ou criptografadas



2.2.7 - Picotador de papel

- ✓ Muita informação ainda reside no papel:
 - folhas de pagamento
 - contra-cheques
 - extratos
 - etc
- ✓ Esse material deve ser descartado de tal forma que não caia em mãos erradas e/ou que sua reconstrução seja inviável
- ✓ Existem diversos tipos de picotadores de papel:
 - cortam o papel em tiras
 - cortam o papel em diagonal
 - picam o papel



2.3 - Segurança lógica

- ✓ Compreende os mecanismos de proteção baseados em *software*
 - senhas
 - listas de controle de acesso
 - criptografia
 - *firewall*
 - sistemas de detecção de intrusão
 - redes virtuais privadas

2.3.1 - *Firewalls*

- ✓ Referência às portas corta-fogo responsáveis por evitar que um incêndio em uma parte do prédio se espalhe facilmente pelo prédio inteiro
- ✓ Na Informática: previne que os perigos da Internet (ou de qualquer rede não confiável) se espalhem para dentro de sua rede interna
- ✓ Um *firewall* deve sempre ser instalado em um ponto de entrada/saída de sua rede interna
- ✓ Este ponto de entrada/saída deve ser único
- ✓ O *firewall* é capaz de controlar todos os acessos de e para a sua rede

✓ Objetivos específicos de um *firewall*:

- restringe a entrada a um ponto cuidadosamente controlado
- previne que atacantes cheguem perto de suas defesas mais internas
- restringe a saída a um ponto cuidadosamente controlado

✓ O *firewall* pode estar em:

- computadores
- roteadores
- configuração de redes
- *software* específico

2.3.2 - Autenticação e autorização

- ✓ **Autenticação** consiste no processo de estabelecer a identidade de um indivíduo
 - identificação e prova desta identificação
- ✓ A prova consiste em três categorias:
 - algo que você sabe
 - algo que você tem
 - algo que você é
- ✓ Algo que você sabe:
 - mais simples de se implementar
 - menor nível de segurança
 - e.g.: senha
 - não requer *hardware* especial

✓ Algo que você tem

- um nível a mais de segurança
- usuário deve possuir algo para se autenticar
- e.g.: cartão magnético, *token* USB
- um invasor pode se fazer passar por um usuário legítimo caso esteja de posse do item necessário
- requer *hardware* especial

✓ Algo que você é

- mais segura
- trata-se de características específicas do indivíduo
- e.g.: impressão digital, leitura de íris, reconhecimento de voz
- uso de dispositivos biométricos: custo elevado

- ✓ Possibilidade de se combinar métodos de autenticação distintos
- ✓ **Autorização** estabelece o que o usuário pode fazer após a autenticação: ACL's e permissões
- ✓ Aplica-se a qualquer acesso a qualquer recurso:
 - arquivo
 - dispositivo
 - rede
 - chamada de sistema de programação
- ✓ Criação de perfil: contém todas as permissões para cada recurso que um usuário poderá utilizar

2.3.3 - Detectores de intruso

- ✓ **IDS** - (*Intrusion Detection Systems*): responsáveis por analisar o comportamento de uma rede ou sistema em busca de tentativas de invasão
- ✓ **HIDS** - (*Host IDS*): monitora um *host* específico
- ✓ **NIDS** - (*Network IDS*): monitora uma segmento de rede
- ✓ Um IDS utiliza dois métodos distintos:
 - detecção por assinaturas
 - detecção por comportamento
- ✓ Detecção por assinaturas:
 - semelhante às assinaturas de antivírus
 - associam um ataque a um determinado conjunto de pacotes ou chamadas de sistema
 - não só detecta o ataque como também o identifica
 - exige atualizações frequentes do fabricante

✓ Detecção por comportamento:

- observa o comportamento da rede em um período normal, e o compara com o comportamento atual da rede
- diferença significativa entre os comportamentos, o IDS assume que um ataque está em andamento
- utiliza métodos estatísticos ou inteligência artificial
- detecta ataques desconhecidos
- não sabe informar qual ataque está em andamento

✓ Falsos positivos e falsos negativos

- amadurecimento da tecnologia
- diferença entre os ambientes

2.3.4 - Redes virtuais privadas

- ✓ **VPN** – (*Virtual Private Networks*): forma barata de interligar duas redes privadas (Intranet) através da Internet
 - ligação entre dois *firewalls* ou entre dois servidores de VPN para interligar duas redes inteiras
 - ligação entre uma estação na Internet e serviços localizados dentro da rede interna (Intranet)
- ✓ VPN emprega criptografia em cada pacote trafegado
 - a criptografia deve ser rápida o suficiente para não comprometer o desempenho entre as redes
 - a criptografia deve ser segura o suficiente para impedir ataques

✓ Vantagens:

- substituição de linhas dedicadas a custo baixo
- uso de infra-estrutura já existente

✓ Desvantagens:

- dados sensíveis trafegando em rede pública
- sensível aos congestionamentos e interrupções que ocorrem na Internet

2.4 - Atividades

1. Imagine três situações reais onde se aplicam a autenticação e a autorização. Procure identificar que categorias de autenticação foram utilizadas e qual foi a autorização concebida. Existem níveis diferentes de autorização? Anote as situações e discuta com os colegas e o professor.
2. Elabore, com o máximo de detalhes, um projeto de segurança física para um prédio que contém todos os servidores importantes e os equipamentos centrais da rede de uma universidade. A seguir, alguns aspectos importantes a considerar. Utilize a Internet para obter mais informações sobre os equipamentos usados.
 - a. sala de servidores
 - b. sala de equipamentos de rede (pode ser a mesma dos servidores)
 - c. contenção de catástrofes (enchentes, incêndios, raios)
 - d. proteção das informações (*backup*)
 - e. controle de acesso
 - f. garantia de fornecimento de energia
 - g. redundância