Aula VIII Segurança de sistemas de informação

Eduardo Kinder Almentero

ekalmentero@gmail.com

Sumário da Aula

- Vulnerabilidade de sistemas
  - Por que sistemas são vulneráveis?
  - Vulnerabilidade da Internet
  - Software malicioso
  - Alguns Tipos de ataques
- Definindo políticas de segurança
  - Avaliação de risco
- Tecnologias e ferramentas
  - Proteção de dados
  - Disponibilidade do sistema
  - Qualidade de software

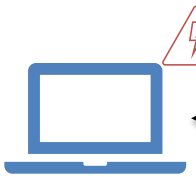
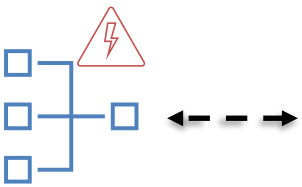
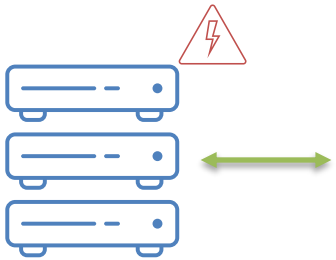
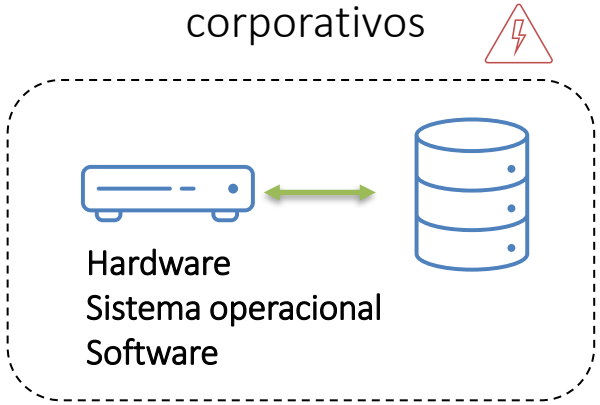
Vulnerabilidade de Sistemas

- Vulnerabilidade
  - É uma **fraqueza no projeto ou implementação do sistema** e pode estar no **hardware** ou **software**.
- Segurança
  - **Políticas**, **procedimentos** e **medidas técnicas** utilizadas para prevenir o **acesso não autorizado**, **modificação**, **roubo** ou **dano físico** a sistemas de informação.
    - **Proteção de ativos organizacionais**
- Controles
  - São **métodos**, **políticas** e **procedimentos** que asseguram a **segurança** dos **ativos organizacionais**, a **qualidade** (**precisão** e **confiabilidade**) de seus **dados** e a **aderência operacional** à **padrões de gestão**.
- As vulnerabilidades são derivadas de fatores **técnicos**, **organizacionais** e **ambientais** associados a **decisões de gestão ruins**.

Por que os sistemas são vulneráveis?

- Dados armazenados de maneira **eletrônica** são **vulneráveis a mais tipos de ameaças** que dados na forma **manual**.
  - Sistemas de informação em diferentes locais podem estar **interligados através de redes** de comunicações.
  - O **potencial** de **acesso não autorizado**, **fraudes** e **abusos** não está limitado a um local apenas – pode ocorrer **a partir de qualquer ponto de acesso** da rede.

Vulnerabilidade de Sistemas

Cliente (Usuário)	Rede de comunicação	Servidores corporativos	Sistemas corporativos
			
- Acesso não autorizado - Erros	- Tapping (grampo) - Sniffing (analisadores) - Alteração de mensagem - Roubo e fraude - Radiação	- Hacking - Malware - Roubo e fraude - Vandalismo - Ataque de negação de serviço	- Roubo de dados - Cópia de dados - Modificação de dados - Falha de hardware - Falha de software

Arquitetura típica de um sistema Web inclui um **cliente Web**, um **servidor** e um sistema de informação corporativo ligado a um banco de dados

Figura adaptada de LAUDON, Kenneth C. et al. **Management information systems: Managing the digital firm**. Pearson Education India, 2007.

Vulnerabilidades da Internet

- **Grandes redes públicas** de computadores, como a **Internet**, são mais vulneráveis que **redes privadas internas**.
  - **Qualquer pessoa** pode acessá-la;
  - **Muitos pontos de acesso**;
  - **Componentes da rede** sob controle de terceiros.
- O **porte da Internet** também **potencializa** o **impacto** se a **segurança** dos ativos organizacionais for **comprometida**.
- Quando a **Internet** se torna **parte** de **uma rede corporativa**, os **sistemas de informação** da organização **estão ainda mais vulneráveis** a ações de terceiros.
  - Qual o caminho a seguir?
    - Não utilizar a Internet?
    - Mais controles?

Segurança de Redes sem Fio (Wireless)

- Redes sem fio **são mais vulneráveis**, pois as **bandas de frequência de rádio são fáceis de escanear**.
  - As redes sem fios mais comuns, Wi-Fi e Bluetooh, são **suscetíveis a interceptação de seus pacotes**.
  - Os hackers usam ferramentas para **detectar redes desprotegidas**, **monitorar** o **tráfego** da rede e, em alguns casos, **obter acesso à Internet** ou a **redes corporativas**.

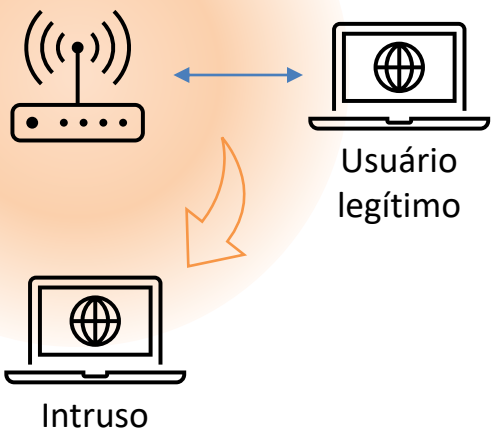


Figura adaptada de LAUDON, Kenneth C. et al. **Management information systems: Managing the digital firm**. Pearson Education India, 2007.

Software Malicioso

- Software malicioso, também chamado de ***malware***, inclui uma série de ameaças, tais como: **vírus**, ***worms***, ***spywares***, ***keylogger*** e **cavalos de Tróia**.
  - ***Vírus***
    - programa nocivo que se **anexa a outros programas, ou ao sistema de arquivos para ser executado**, geralmente, sem o consentimento do usuário;
    - esses programas podem possuir comportamentos benignos, mas, usualmente, **causam problemas destruindo outros programas, apagando dados, obstruindo a memória do computador, reformatando HD e modificando o comportamentos de outros softwares**.
  - ***Worms*** – programas que se **replicam e se espalham** para outros computadores e, normalmente, **causam danos a rede.**
  - ***Spyware*** – programas (em alguns casos legítimos) que **coletam informações sobre o dispositivo** infectado e as envia para Internet.
  - ***Keylogger*** – programa que **grava tudo que é digitado pelo usuário** no dispositivo infectado.
  - Cavalo de Tróia – programa que **aparenta ser benigno**, mas possui **funções escondidas** (vírus, worm etc), na maioria das vezes **danosas ao dispositivo infectado**.

Alguns Tipos de Ataques

- Spoofing e Sniffing
  - Spoofing pode envolver o redirecionamento de um link da Web para um endereço diferente do pretendido, com o site mascarando-se como o destino pretendido.
  - O phising é uma forma de spoofing onde são criados sites ou enviados e-mails falsos, similares ao de grandes empresas, para coletar dados pessoais.
  - Sniffing está relacionado ao monitoramento das informações que trafegam por uma rede
    - Pode ser usado de maneira legítima, para identificar eventuais gargalos na rede.
    - Quando utilizados para propósitos criminosos podem causar um grande dano.
- Negação de serviço (*denial-of-service - DoS*)
  - Os hackers sobrecarregam um servidor de rede ou servidor da Web com muitas (mesmo!) comunicações falsas ou solicitações de serviços para travar a rede.
  - A rede recebe tantas consultas que não consegue acompanhá-las e, portanto, fica indisponível para atender a solicitações legítimas.
- Roubo de identidade
  - Um impostor obtém informações pessoais importantes, como números de cartão de crédito, para se passar por outra pessoa.

Ameaças Internas: Funcionários

- Temos a **tendência** de pensar que as **ameaças à segurança** de uma empresa têm **origem fora da organização**.
- Os **funcionários** possuem **acesso a informações privilegiadas** e na **falta de procedimentos de segurança interna efetivos**, eles muitas vezes são capazes de **percorrer os sistemas** de uma organização **sem deixar rastros**.
- Estudos descobriram que a **falta de conhecimento do usuário** é a **maior causa de violações de segurança de rede** nas organizações.
- Pessoas que buscam **acesso não autorizado** ao sistema às vezes **enganam os funcionários** fingindo ser membros legítimos do empresa que necessitam de informações, para que estes **revelem suas senhas .**
  - Essa prática é chamada de **engenharia social**.

Vulnerabilidade de Software

- Os **erros de software** representam uma **ameaça constante** aos **sistemas de informação**, causando **perdas incalculáveis de produtividade**.
- A **complexidade** e o **tamanho crescentes** dos software, juntamente com as demandas por **entrega mais rápida**, contribuíram para um **aumento nas falhas** ou **vulnerabilidades** de software.
- Um grande problema com o software é a **presença de *bugs* ocultos** ou **defeitos no código**.
  - **Não é possível assegurar que um software não possui defeitos**.
  - Quanto mais se investe na qualidade, menor o número de defeitos, porém, o custo de desenvolvimento é maior.
- Falhas no software **não atrapalham apenas o desempenho**, mas também podem **criar vulnerabilidades de segurança**, abrindo **brechas no sistema para intrusos**.

Definindo Políticas de Segurança

- **Antes** da organização **comprometer recursos** para controles de **segurança** e sistemas de informação, ela deve saber **quais ativos requerem proteção** e **até que ponto esses ativos são vulneráveis**.
- Uma **avaliação de risco** determina o **nível de risco** para a empresa se **uma atividade ou processo específico** não for **devidamente controlado.**
  - Ex.:
    - Uma avaliação de risco poderia mostrar que a probabilidade de uma falha de energia ocorrer em um período de um ano é de 30 por cento.
    - A perda de transações de pedido enquanto a energia está desligada pode variar de $ 5.000 a $ 200.000 (em média $ 102.500) para cada ocorrência.
- De posse da avaliação de risco, é possível se **concentrar nos pontos de controle com maior vulnerabilidade e potencial de perda**.
  - Ex.: diminuir o risco de falha de energia.

Definindo Políticas de Segurança

- Uma **política de segurança** consiste em declarações que **classificam os riscos** das informações, identificando **objetivos de segurança aceitáveis** e **identificando** os **mecanismos** para **atingir esses objetivos**.
- A **política de segurança** orienta outras políticas que determinam o **uso aceitável dos recursos de informação** da empresa e **quais membros** da empresa **têm acesso aos seus ativos de informação.**
  - O uso de equipamentos e recursos, como notebooks, dispositivos wireless e Internet.
  - É comum, por exemplo, as organizações limitarem o acesso a determinados sites da Internet, e certos tipos de tráfego, de dentro de sua rede privativa.
- A política de segurança também inclui elementos para **gerenciamento de identidade**.

Tecnologias e Ferramentas para Proteção de Dados

- Há uma gama de **ferramentas** que podem ser utilizadas pelas organizações para **proteger** suas **informações**.
  - Prevenindo **acesso não autorizado a dados e sistemas**, **assegurando a disponibilidade de sistemas** e a **qualidade de software**.
- **Gestão e autenticação de identidade**
  - Capacidade de saber que uma pessoa é quem ele ou ela afirma ser;
  - É comum o uso de senha, mas também existem outros recursos como uso de **tokens**, **smard cards**, **biometria** e **autenticação de dois fatores**.
  - **Diferentes indivíduos ou papéis** na organização possuirão **níveis de acesso distinto aos sistemas e informações**.

Tecnologias e Ferramentas: Proteção de Dados

- *Firewalls*
  - Impedir que usuários não autorizados acessem redes privadas;
  - É uma combinação de hardware e software.
- Antivírus e *antispyware*
  - Impede, detecta e remove malware.
- Soluções integradas
  - Combina uma série de ferramentas, como *firewalls*, VPNs, sistemas de detecção de intrusos, antispam etc.
- Criptografia de chaves públicas
  - Criptografia é o processo de transformar texto ou dados simples em conteúdo cifrado, que não pode ser entendido por ninguém além do remetente e do destinatário pretendido;
  - Uma forma de criptografia que usa duas chaves: uma compartilhada (ou pública) e uma totalmente privada;
  - As chaves são matematicamente relacionadas para que o dado criptografado com uma chave só possam ser transformado novamente no original usando a outra chave.

Tecnologias e Ferramentas: Disponibilidade do Sistema

- À medida que as empresas **dependem** cada vez mais de **redes digitais** para **obter receitas** e **operações**, eles precisam tomar **medidas adicionais** para garantir que seus **sistemas** e **aplicativos** estejam **sempre disponíveis**
- **Sistemas tolerantes a faltas**
  - Estes sistemas possuem **hardware**, **software**, e **fonte de alimentação redundantes**, criando um ambiente que possibilita o **serviço contínuo e ininterrupto.**
- **Computação de alta disponibilidade**
  - Ajuda as empresas a se **recuperarem rapidamente** de uma **falha do sistema**.

Tecnologias e Ferramentas: Qualidade de Software

- A **qualidade** e **confiabilidade** do sistema pode ser **melhorada** através da aplicação de **métricas de software** e **testes de software** rigorosos
  - O uso de métricas permite mensurar a performance do software e identificar problemas assim que estes ocorrem.
- **Testes antecipados**, **regulares** e **intensivos** irão **contribuir significativamente** para a **melhoria** da **qualidade** dos sistemas.
  - Quantidade menor de erros.
- **Uso de padrões de qualidade de software**
  - Há uma seria de padrões estabelecidos por entidades renomadas a cerca das atividades do processo de software;
  - Modelos de maturidade: CMMI e MPS.BR.

FIM

Eduardo Kinder Almentero

ekalmentero@gmail.com