SSC120 - Sistemas de Informação

Segurança em Sistemas de Informação

Simone S. Souza

ICMC/USP

Segurança em Sistemas de Informação

- Por que os SIs estão tão *vulneráveis* a destruição, erros e uso indevido?
- Qual o valor empresarial da segurança nos SIs?
- Quais são as tecnologias e ferramentas disponíveis proteger a informação?

Desastre 11 de setembro de 2001

- O que aprendemos com o 11 de setembro?

Desastre 11 de setembro de 2001

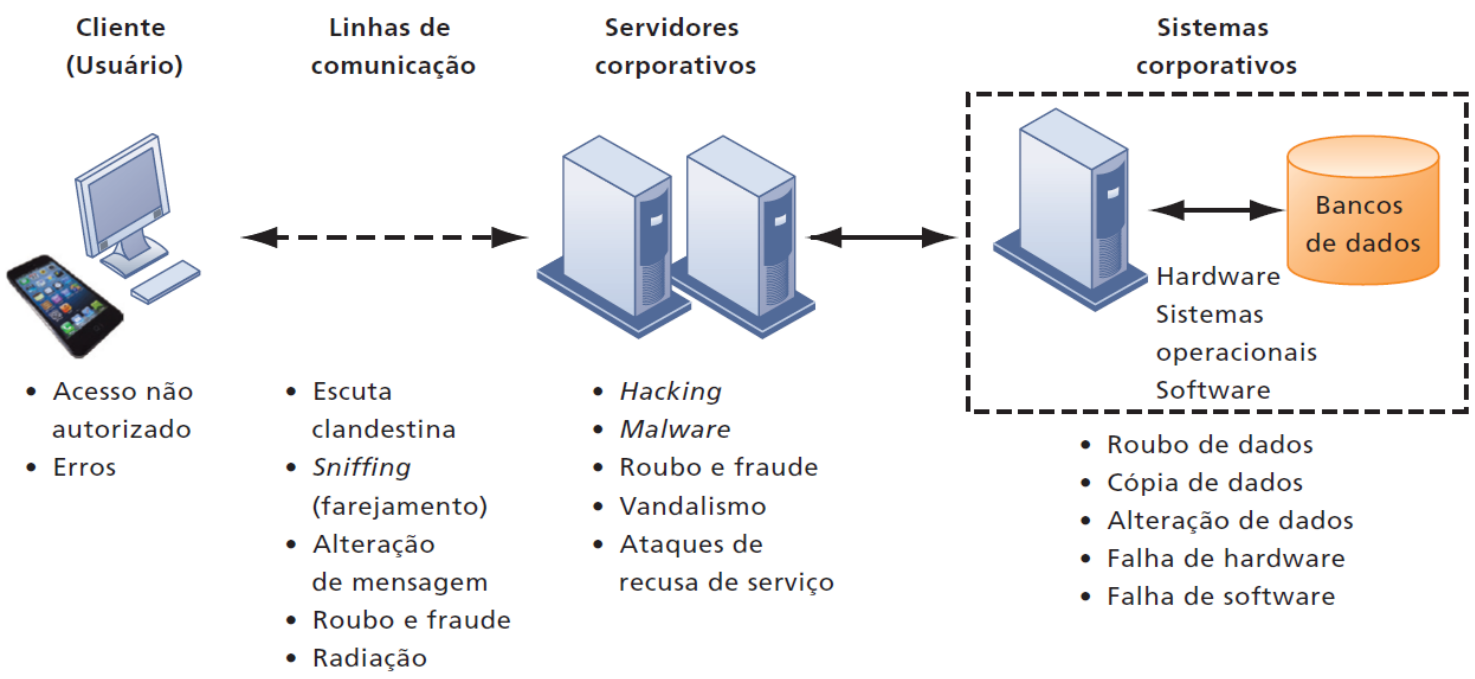
- Nem tudo está sob controle
- Empresas inteiras destruídas
- Gestores de Segurança mantinham backup dos DataCenter.
  - A maioria das empresas mantinha seus backups na Torre ao lado na qual trabalhava.
  - Ou seja, com a destruição das Torres, os backups que continham a vida da empresa, desapareceram.

Desastre 11 de setembro de 2001

- Empresas começaram a agir: E se fosse na minha empresa?
  - Investimento em sistemas de proteção de incêndio, cofre anti chamas
  - Planejamento para backup efetivo e eficiente: fitas backup enviadas para outras filiais, testes de recuperação de dados, contratos com fornecimento de Servidores e DataCenter backup;
  - ...

Vulnerabilidade e uso indevido

- Formato eletrônico X formato manual.
- Desafios contemporâneos:



Vulnerabilidade e uso indevido

- A Internet é culpada pela vulnerabilidade?
- É seguro se conectar a redes sem fio em aeroportos, bibliotecas ou outros locais públicos?
  - Estamos seguros?

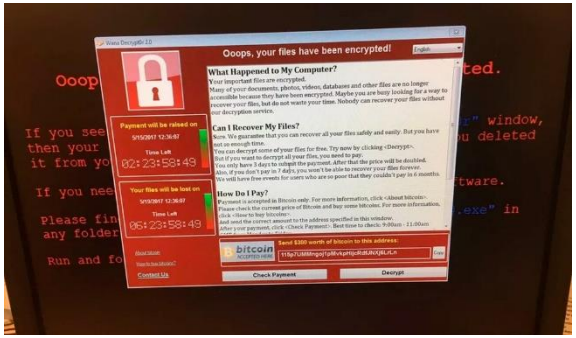
Em 2000, a Amazon.com perdeu 224 mil dólares a cada hora que ficou sem serviço devido ao ataque de um hacker.

Vulnerabilidade e uso indevido

- Ameaças externas:
  - Software mal intencionado
  - Crimes de informática
- Ameaças internas
  - Funcionários (erros nas entradas dos sistemas)
  - Defeitos nos sistemas

Vulnerabilidade – Ameaça externa

- Matéria Folha São Paulo*: Ataque cibernético atingiu mais de 300 mil computadores no mundo (Maio/2017)
  - Ransomware – computadores infectados com vírus que "sequestra" arquivos. Invasores pedem um resgate ou ameaçam destruir ou compartilhar arquivos
  - Microsoft havia criado proteção mas nem todos usuários haviam atualizado o sistema e o Ransomware se aproveitou desta vulnerabilidade



* http://www1.folha.uol.com.br/mundo/2017/05/1883484-o-que-se-sabe-ate-agora-do-mega-ataque-cibernetico-em-todo-o-mundo.shtml

Ameaça interna: Bugs no sistema

- Bugs sempre estão presentes no software
- Correções sucessivas "deterioram" o software
- Qualidade comprometida

Vulnerabilidade

- INFORMAÇÃO é um ATIVO importante para todas as organizações
- Importante:
  - Armazenar e gerenciar informação.
  - Compartilhar informação.
  - **Proteger** a informação.

Como proteger a informação??

Valor empresarial da segurança e controle

- Sistemas abrigam informações confidenciais
  - Impostos, ativos financeiros, registros médicos e desempenho profissional das pessoas.
- Controle e segurança inadequados podem criar sérios riscos legais.
- As empresas precisam proteger não apenas seus próprios ativos de informação, mas também os de clientes, funcionários e parceiros de negócios.
- Caso não consigam fazê-lo, podem ter de gastar muito em um litígio por exposição ou roubo de dados.

Prova eletrônica e perícia forense computacional

- Ação legal - pedido de produção de provas
  - Obrigação de fornecer acesso às informações que podem ser usadas como prova.

- **Perícia forense computacional -** procedimento científico de coleta, exame, autenticação, preservação e análise de dados mantidos em meios de armazenamento digital
  - Informações possam ser usadas como prova em juízo.
  - Desafios:
    - Recuperar dados sem prejudicar seu valor probatório;
    - Armazenar e administrar dados eletrônicos recuperados;
    - Encontrar informações em um grande volume de dados;
    - Apresentar as informações em juízo.

Como estabelecer uma estrutura para segurança e controle

- **Controles gerais** controlam projeto, segurança e uso de programas de computadores, além da segurança de arquivos de dados.
- **Controles de aplicação** são controles específicos exclusivos a cada aplicação computadorizada, como processamento de pedidos.
- Uma **avaliação de risco** determina o nível de risco para a empresa caso uma atividade ou um processo específico não sejam controlados adequadamente.
- **Política de segurança** é uma declaração que estabelece hierarquia aos riscos de informação e identifica metas de segurança aceitáveis, assim como os mecanismos para atingi-las.

Como estabelecer uma estrutura para segurança e controle

Tabela 8.5

Avaliação do risco no processamento de pedidos on-line.

Exposição	Probabilidade de ocorrência (%)	Faixa de prejuízo/média (US$)	Prejuízo anual esperado (US$)
Falta de energia	30%	5.000–200.000 (102.500)	30.750
Apropriação indébita	5%	1.000–50.000 (25.500)	1.275
Erro de usuário	98%	200–40.000 (20.100)	19.698

Plano de recuperação de desastres e plano de continuidade dos negócios

- O **plano de recuperação de desastres** inclui estratégias para restaurar os serviços de computação e comunicação após eles terem sofrido uma interrupção.
- O **plano de continuidade dos negócios** concentra-se em como a empresa pode restaurar suas operações após um desastre.
- Como a administração sabe que os controles e a segurança de seus sistemas de informação são eficientes?
- Uma **auditoria de sistemas de informação** avalia o sistema geral de segurança da empresa e identifica todos os controles que governam sistemas individuais de informação.

Tecnologias e ferramentas para garantir a segurança em SI

- **Gestão de identidade**
  - Autenticação
  - Autenticação biométrica
- **Firewall**
- **Sistemas de detecção de intrusão**
- **Software antivírus**
- **Criptografia**
- **Certificados digitais**

Garantia de Qualidade do Software

- Como melhorar a qualidade e a confiabilidade dos sistemas?
  - Métricas de qualidade
  - Teste de software

Controles Gerais – Norma de Segurança

- NBR ISO/IEC 17799 – norma de segurança (2001)
  - Cobre os mais diversos tópicos da área de segurança, possuindo um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações de uma empresa.
  - A obtenção da certificação pode ser um processo demorado e muito trabalhoso.
- A certificação é uma forma clara de mostrar a sociedade que a empresa dá a segurança de suas informações e de seus clientes a importância que merecem.

Controles Gerais – Norma de Segurança

- Definir:
  - **O que** proteger?
  - Contra **o que/quem** proteger?
  - **Como** reagir?
  - **Quem** faz o quê?

Conclusões

- A administração deve ser responsável pelo desenvolvimento de uma estrutura de controle e dos padrões de qualidade desejados.
- Não existem sistemas 100% seguros.
  - Importante planejar e realizar ações preventivas.

Conclusões

- Principais ameaças: vírus, invasões, funcionários insatisfeitos e senhas.
- Aumento do uso da Internet como meio de fraudes e vazamento de informação.
- Necessidade de conscientizar os executivos, motivar os usuários e capacitar a equipe técnica.
- Necessidade de realizar análise de riscos e revisar periodicamente a política de segurança.