Aula 01: Introdução à Segurança da Informação

Prof. Daniel Caetano

Objetivo: introduzir o conceito de Segurança da Informação, indicar as metodologias existentes e em que consiste uma Política de Segurança da Informação.

Bibliografia: FERREIRA, 2003; FERREIRA E ARAÚJO, 2006.

INTRODUÇÃO

Conceitos Chave:

- Problemas:
  - * Como proteger a empresa de um ataque de um cracker?
  - * Como transmitir dados com segurança?
  - * Como evitar infecção por vírus?
- Milhares de sistemas são atacados por ano
  - * Bem protegidos => ataque fracassa
  - * Medianamente protegidos => ataque de sucesso, atacante identificado
  - * Mal protegidos => ataque tem completo sucesso, atacante livre

Com o avanço das tecnologias de informação e transmissão de dados, maior tem sido a preocupação com a proteção dados de uma empresa, sejam eles digitais ou não.

Esta preocupação não é sem motivo: todos os anos são milhares de ataques à informação das mais diversas empresas, mas, graças às estratégias e técnicas da segurança da informação, a maior parte deles não obtém êxito.

A fonte de ataques mais citada pela imprensa são os famosos *malware* (vírus, worms e trojans, softwares maliciosos elaboratos por crackers para causar danos a um equipamento ou para dar-lhes o controle de um equipamento). Como proteger uma empresa deste tipo de ataque? Como permitir uma operação segura dos sistemas de informação sem prejudicar demasiadamente sua facilidade de operação?

A resposta para estas perguntas é bem menos complexa do que parece, e as alternativas serão analisadas neste curso.

1. SEGURANÇA DA INFORMAÇÃO

Conceitos Chave:

- Informação na Empresa
    * Ativo
    * Deve ser protegida
- Razões para proteção
    * Garantir continuidade dos negócios
    * Maximizar retorno de investimentos/oportunidades
    * Minimizar transtornos
- Necessidade
    * Informação está em constante risco
    * Originalmente: segurança física
    * Atualmente: segurança física e lógica
- Objetivos:
    * Confidencialidade
    * Integridade
    * Disponibilidade
- Praticidade x Segurança
    * P = 1/S
- Custos
    * Segurança aumenta custos, mas é necessária
    * Como determinar os critérios de segurança?
        - Que informação proteger?
        - Contra o quê/quem?
        - Quais as ameaças?
        - Relação importância/nível de proteção
        - Recursos Disponíveis (financeiros e pessoais)
        - Expectativas dos clientes
        - Consequências das falhas de segurança
- Política de Segurança!

O conceito de "segurança da informação" dentro de uma empresa é relativamente intuitivo: refere-se à proteção das informações daquela empresa. Embora o conceito de informação seja também intuitivo, a razão pela qual ela deve ser protegida nem sempre é clara. O conceito fundamental aqui é: informação é um ativo e, portanto, deve ser protegida.

As razões principais para se garantir a segurança da informação são:

- **Garantir continuidade dos negócios**, já que muitas informações são necessárias para que os negócios ocorram.
- **Maximizar retorno de investimentos/oportunidades**, já que, nas informações, é possível identificar aspectos em que um negócio pode ser melhorado.
- **Minimizar transtornos**, uma vez que algumas informações sigilosas não devem ser divulgadas em público.

Mas... existe sentido em tão grande preocupação com a segurança da informação? Sim, já que **a informação está em constante risco**. E a segurança da informação vem se tornando mais complexa ao longo do tempo. Se **no início** havia apenas a necessidade de **segurança física**, pois os documentos eram todos na forma de papéis, **já há algum tempo** as informações estão todas em computadores, usualmente interligados em redes, cuja **proteção** é bem mais complexa e **envolve aspectos físicos e lógicos**.

O objetivo de toda a segurança da informação é a garantia de:

a) **Confidencialidade**: apenas pessoas autorizadas possuem acesso às informações
b) **Integridade**: as informações são mantidas corretas e completas
c) **Disponibilidade**: as informações estão disponíveis sempre que necessário

Valendo lembrar que, em termos de segurança da informação, vale a regra:

Praticidade = 1/Segurança

Ou seja: quanto mais "prático" é o acesso a uma informação, menos protegida ela estará, e vice versa.

Entretanto, qualquer tipo de **segurança causa custos adicionais**. A segurança da informação não é diferente. Para que seja possível **garantir os objetivos** da segurança da informação de uma maneira fundamentada e **não incorrer em custos adicionais excessivos**, é preciso **responder a algumas questões**.

a) Que informações devem ser protegidas?
b) Contra o quê/quem?
c) Quais são as ameaças?
d) Qual a importância de cada recurso e o nível de proteção desejado?
e) Quais os recursos (financeiros e pessoal) disponíveis?
f) Quais as expectativas dos clientes quanto à segurança?
g) Quais as consequências se houver vazamento de informações?

Vamos discutir as respostas dessas questões ao longo do curso, suas respostas sendo a chave para um planejamento de segurança formando o que se chama de Política de Segurança da Informação de uma empresa.

2. BIBLIOGRAFIA

FERREIRA, F. N. F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003.

FERREIRA, F. N. F; ARAÚJO, M. T. **Política de Segurança da Informação: Guia Prático de Elaboração e Implementação**. Rio de Janeiro: Ciência Moderna, 2006.