SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Diferentes dimensões da informação

- A informação possui diferentes dimensões:
  - Pode estar na cabeça das pessoas.
  - Pode estar em um meio físico, como em um pedaço de papel ou em uma árvore, rochas, etc.
  - Pode estar em um meio digital, como em um smartphone, em um servidor, na nuvem ou sendo transmitida pelo ar.

- Qual das opções acima é a mais segura?

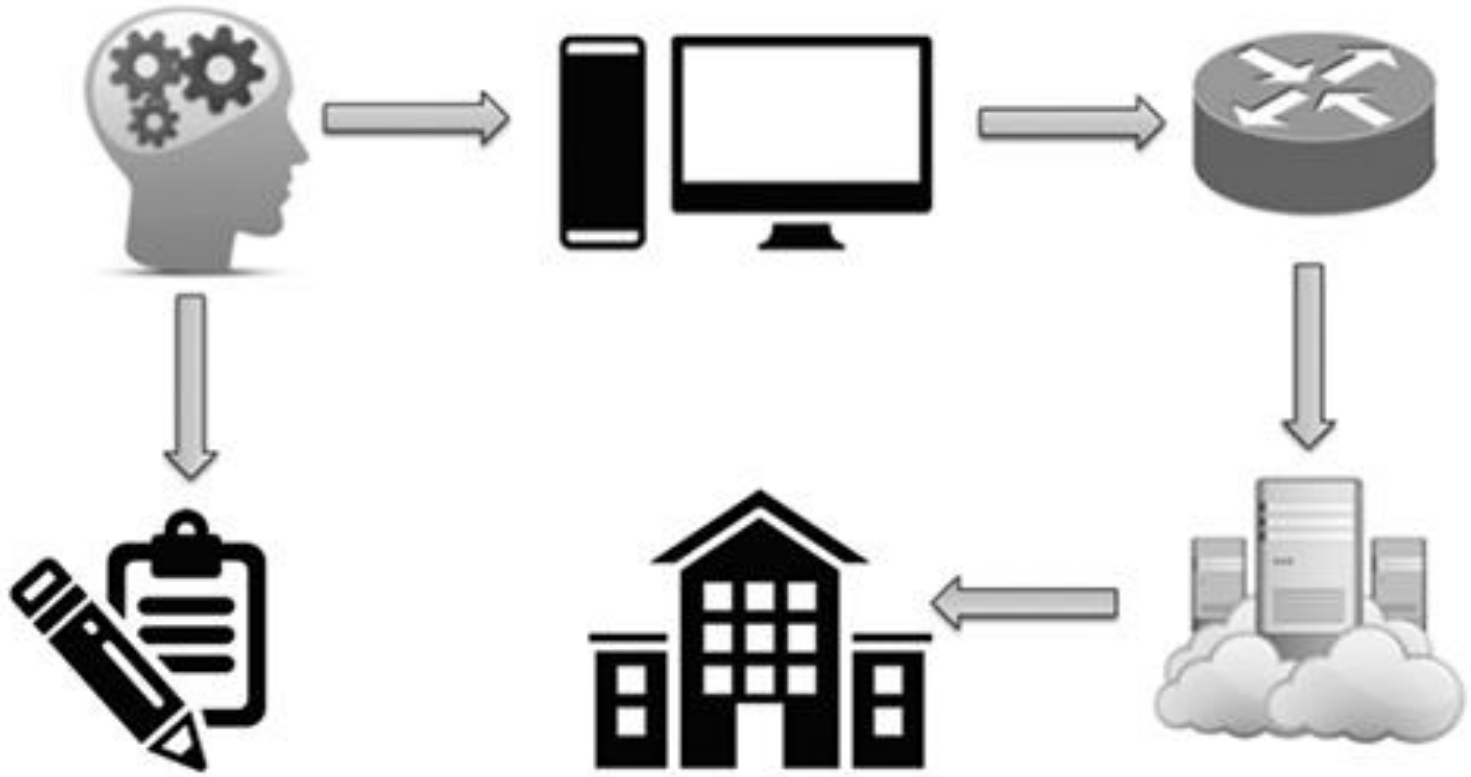
Fluxo de Informações

- Uma das principais estratégias para mapear os elementos a serem protegidos é o entendimento do fluxo de informação. Por onde a informação passa?

- Ela pode surgir na cabeça de um membro da equipe, que faz um rascunho e cria documentos no computador. A partir daí, a informação passa pela rede até chegar ao servidor, que está em um datacenter.

- Qualquer um desses elementos pode ser alvo de um ataque, portanto, deve ser protegido.

Fluxo de Informações



Elementos a serem protegidos

- A partir dessa análise, precisamos imaginar quais são os elementos que necessitam ser protegidos?

- Pensando apenas no computador e no servidor do exemplo podemos identificar que pelo menos os seguintes são pontos possíveis de ataques: sistema operacional, serviços, hardware.

- Outro elemento importante a ser protegido é a rede de comunicação. Vários e diferentes ataques podem ocorrer nessa rede.

Elementos a serem protegidos

- De maneira geral, existem três grandes grupos de elementos a serem protegidos:
  - **Pessoas**: possuem informações que podem ser obtidas de várias formas, sejam elas maliciosas ou não. Suborno e engenharia social são exemplos de ataques que exploram as fraquezas ou vulnerabilidades humanas.
  - **Ativos**: há ativos físicos e tecnológicos que devem ser protegidos. Exemplos de ativos físicos são hardwares ou locais físicos. Já exemplos de ativos tecnológicos são sistemas operacionais, aplicativos, sistemas e softwares de uma forma geral.
  - **Informação**: é o principal elemento a ser protegido, e é aquele que trafega de formas diferentes por variados elementos, o que leva às necessidades de proteção também das pessoas e dos ativos físicos e tecnológicos.

ATIVOS

INFORMAÇÃO

PESSOAS

GERAM AS IDEIAS, DETÉM AS INFORMAÇÕES NA CABEÇA, POSSUEM INFORMAÇÕES CONFIDENCIAIS DE UMA EMPRESA

PESSOAS

INFORMAÇÃO

ATIVOS

FÍSICOS (SERVIDORES) E LÓGICOS (REDE, SISTEMAS, BANCO DE DADOS). ARMAZENAM, PROCESSAM OU TRANSMITEM INFORMAÇÕES, E REPRESENTAM PONTOS QUE PODEM SER ATACADOS, PORTANTO PRECISAM SER PROTEGIDOS

PESSOAS

ATIVOS

INFORMAÇÃO

O ATIVO DE MAIOR VALOR, AQUILO QUE PRECISA DE PROTEÇÃO, E PASSA PELAS PESSOAS E ATIVOS FÍSICOS E LÓGICOS.

Elementos a serem protegidos

- A informação que está:
  - Armazenada em computadores;
  - Transmitida através da rede;
  - Impressa ou escrita em papel;
  - Armazenada em fitas ou disco;

- A informação que é:
  - Falada em conversas ao telefone;
  - Enviada por e-mail ou outros tipos de mensagens;
  - Armazenada em Banco de Dados;
  - Mantida em filmes e microfilmes;
  - Apresentada em Projetores;

Elementos a serem protegidos

- Quais vulnerabilidades cada item pode ter? Por que protege-los? Quais possíveis tipos de ataques?
  - **Pessoas**
  - **Ativos**
  - **Informação**

OS ELEMENTOS PRECISAM SER PROTEGIDOS PORQUE:

ATIVOS

INFORMAÇÃO

PESSOAS

POSSUEM INFORMAÇÕES QUE PODEM SER OBTIDAS DE VÁRIAS FORMAS, COMO POR ENGENHARIA SOCIAL OU SUBORNO

OS ELEMENTOS PRECISAM SER PROTEGIDOS PORQUE:

PESSOAS

INFORMAÇÃO

ATIVOS

POSSUEM VULNERABILIDADES QUE PODEM SER EXPLORADAS. HÁ OS ATIVOS FÍSICOS (HARDWARES OU LOCAIS) E OS ATIVOS LÓGICOS OU TECNOLÓGICOS (SISTEMAS OPERACIONAIS, APLICATIVOS, SISTEMAS E SOFTWARES)

OS ELEMENTOS PRECISAM SER PROTEGIDOS PORQUE:

PESSOAS

ATIVOS

INFORMAÇÃO

É O PRINCIPAL ELEMENTO, AQUELE QUE TRAFEGA DE FORMA DIFERENTE POR PESSOAS E ATIVOS.

Elementos a serem protegidos

- Proteger a informação de que?
  - Espionagem Industrial;
  - Fraude;
  - Arrombamento;
  - Gravação de Comunicação;
  - Escuta telefônica;
  - Acesso acidental;
  - Empregado desleal;
  - Crime organizado;
  - Crackers.

Elementos a serem protegidos

- Por que alguém iria querer invadir meu computador?
  - Utilizar seu computador em alguma atividade ilícita, para esconder sua real identidade e localização;
  - Utilizar seu computador para lançar ataques contra outros computadores;
  - Utilizar seu disco rígido como repositório de dados;
  - Meramente destruir informações (vandalismo);
  - Disseminar mensagens alarmantes e falsas;
  - Ler e enviar *e-mails* em seu nome;
  - Propagar vírus de computador;
  - Furtar números de cartões de crédito e senhas bancárias;
  - Furtar dados pessoais (....)

EXERCÍCIOS

1) Em segurança da informação, é preciso proteger diferentes elementos, tais como pessoas, informação e ativos. Considere as seguintes razões:

I. Porque cada um desses elementos podem ter vulnerabilidades.

II. Porque cada um desses elementos podem ser atacados.

III. Porque a informação passa por cada um desses elementos.

Assinale a resposta correta:

a) Apenas I está correta.

b) Apenas I e II estão corretas.

c) Apenas II e III estão corretas.

d) I, II e III estão corretas.

e) Nenhuma das afirmações está correta

EXERCÍCIOS

2) Uma empresa que está passando por um momento de grande crescimento possui um servidor de arquivos no data center com documentos confidenciais sobre salários de todos os empregados.

Considere os seguintes elementos:

I. Serviço de servidor de arquivos.

II. Sistema operacional.

III. Serviço de controle de acesso aos arquivos.

IV. Data center.

Qual dos elementos você considera o mais importante para ser protegido?

a) Apenas I.

b) Apenas II.

c) Apenas III.

d) Apenas IV.

e) I, II, III e IV.

RESOLUÇÃO

1) D

2) E

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera