- Luciano Gonçalves Moreira

Segurança informação

Está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento

Segurança da Informação

Principais características:

- Disponibilidade:
  Garantia de que a informação estará sempre disponível, para uso legítimo.
- Integridade:
  Garantia de que a informação não sofra alteração indesejada.
- Confiabilidade:
  Garantia de que a informação só será acessada por pessoas autorizadas.
- Autenticidade:
  propriedade que garante que a informação é proveniente da fonte anunciada

Segurança da Informação

Principais ameaças:

- Defeitos de hardware
  - Não há como impedir, mas pode ser prevenido.
- Hackers e Crakers
  - Usuários experientes que invadem sistemas.
- Programas desatualizados
  - Sistemas operacionais, antivírus, firewalls, etc.
- Usuários descontentes / leigos
  - Podem causar problemas com ou sem intenção.
- Bugs (defeitos)
  - São falhas que os sistemas podem apresentar.

Segurança da Informação

Principais ameaças:

- Vírus de computador
  - Um vírus é um programa ou código, que se anexa a outro programa ou arquivo para poder se espalhar entre os computadores, infectando-os à medida que se desloca. Ele infecta enquanto se desloca. Os vírus podem danificar seu software, hardware e arquivos.
  - Um verdadeiro vírus não se dissemina sem ação humana. É necessário que alguém envie um arquivo ou envie um email para que ele se alastre.

Segurança da Informação

Worms

Uma subclasse de vírus. Um worm, assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente. Primeiro, ele controla recursos no computador que permitem o transporte de arquivos ou informações. Depois que o worm contamina o sistema, ele se desloca sozinho. O grande perigo dos worms é a sua capacidade de se replicar em grande volume, causando um efeito dominó de alto tráfego de rede que pode tornar mais lentas as redes corporativas e a Internet como um todo. Um worm geralmente se alastra sem a ação do usuário e distribui cópias completas (possivelmente modificadas) de si mesmo através das redes. Um worm pode consumir memória e largura de banda de rede, o que pode travar o seu computador.

Como os worms não precisam viajar através de um programa ou arquivo "hospedeiro", eles também podem se infiltrar no seu sistema e permitir que outra pessoa controle o seu computador remotamente.

Segurança da Informação

Principais ameaças:

- Cavalos de tróia (trojan)

  Criam canais de comunicação para os invasores. Assim como o mitológico cavalo de Tróia parecia ser um presente, mas na verdade escondia soldados gregos em seu interior que tomaram a cidade de Tróia, os cavalo de Tróia da atualidade são programas de computador que parecem ser úteis, mas na verdade comprometem a sua segurança e causam muitos danos. Os cavalos de Tróia se alastram quando as pessoas são seduzidas a abrir o programa por pensar que vem de uma fonte legítima.

  Os cavalos de Tróia também podem ser incluídos em software que você baixa gratuitamente. Nunca baixe software de uma fonte em que você não confia.

Segurança da Informação

Principais ameaças:

- Sniffers

  Que espionam a comunicação em uma rede em busca de senhas e usernames.
- Spyware

  Copiam tudo que é digitado, armazena e envia ao autor.
- Adware

  Fazem anúncios ou propagandas, abrem telas repetidamente.
- Cookies

  Pequenas informações armazenadas pelos sites
- War dialer

Realizam chamadas telefônicas a procura de modem. Phreaking é o termo usado para os truques de violação telefônica. Phreacker

Segurança da Informação

Principais ameaças:

HOAX - Vírus boato. Mensagens que geralmente chegam por e-mail alertando o usuário sobre um vírus mirabolante, altamente destrutivo.

MACRO - Tipo de vírus que infecta as macros (códigos executáveis utilizados em processadores de texto e planilhas de cálculo para automatizar tarefas) de documentos, desabilitando funções como Salvar, Fechar e Sair.

PHISHING, termo oriundo do inglês (fishing) que quer dizer pesca, é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais.

Segurança da Informação

Principais ameaças:

- **Spam**
  Mensagem de e-mail sem autorização. É o termo pelo qual é comumente conhecido o envio, a uma grande quantidade de pessoas de uma vez, de mensagens eletrônicas, geralmente com cunho publicitário, mas não exclusivamente.
  O spam também é conhecido pela sigla inglesa UCE (Unsolicited Commercial
  Email, ou Mensagem Comercial Não-Solicitada).
  O termo derivou para designativo de qualquer comunicação eletrônica indesejada.

Segurança da Informação

Existem hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer a segurança da informação. Alguns exemplos são :

- *Controles físicos*: são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação) que a suporta.
  - *Mecanismos físicos:*
    - Portas / trancas / paredes / blindagem / guardas / etc ..

Segurança da Informação
Mecanismos de segurança

- *Controles lógicos*: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

  - *Mecanismos lógicos:*
    - *Criptografia. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros* .

Segurança da Informação
Mecanismos Lógicos

- *Assinatura digital*. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade.

- *Mecanismos de controle de acesso*. Palavras-chave, sistemas biométricos, cartões inteligentes.

Segurança da Informação

Antivírus

Os **antivírus** são programas de computador concebidos para prevenir, detectar e eliminar vírus de computador. Software antivírus ajuda a proteger seu computador contra vírus específicos e software mal-intencionado, como worms e cavalos de Tróia. O software antivírus deve estar sempre atualizado. Essas atualizações em geral estão disponíveis por meio de uma assinatura junto a um fornecedor de software antivírus.

- Programa residente em memória, protege os sistema contra a entrada de vírus, worms e cavalos de troia.
- Não protegem contra tentativas de invasão

Segurança da Informação

- Anti-Spywares:

  O software anti-spyware ajuda a detectar e remover spyware de seu computador . "Spyware" (também chamado de "adware") normalmente refere-se a software destinado a monitorar as atividades de seu computador . Spyware pode exibir pop-ups de propaganda indesejados, coletar informações pessoais sobre você ou alterar a configuração de seu computador com as especificações do criador do spyware. No pior cenário, o spyware pode permitir que criminosos desativem seu computador e roubem sua identidade.

- Anti-Spam
  - Verificam e selecionam as mensagens de e-mail.

Segurança da Informação

Firewall:

Em português: muro corta-fogo. Pode ser um software ou Hardware. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra. Ajuda a tornar seu computador invisível para invasores online. Também pode ajudar a impedir que software de seu computador acesse a Internet e aceite atualizações e modificações sem sua permissão.

- Informa sobre as tentativas de invasão.
- Trabalha com regras de liberação e bloqueios;
- Não impede a entrada de vírus, worms ou cavalos de troia, mas impede que se comuniquem com o autor.

Segurança da Informação

- IDS (Sistema Detector de Intrusos)

  Hardware e programa que protegem uma rede

  - tem como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum usuário legitimo está fazendo mau uso do mesmo.