Segurança da Informação

Prof. Jefferson Moreira

Conceitos e Princípios

- **Ativo:** Qualquer tipo de informação, independente do tipo de meio que esteja armazenada, que seja importante para a empresa e seus negócios. Ex: Arquivos com a declaração de receita de uma pessoa.
- **Segurança da Informação** está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

Conceitos e Princípios

- São princípios da SI: **C**onfidencialidade, **I**ntegridade, **D**isponibilidade e **A**utenticidade.

Confidencialidade

- A informação computacional não será aberta sem a devida autorização, ou ainda, garantir que as informações sejam acessíveis apenas àqueles autorizados a terem acesso;
- **Confidencialidade = Sigilo= privacidade.**
- **Quebrando a Confidencialidade da Informação:**
- Ex: alguém obtém acesso não autorizado ao sua conta bancária via Internet Banking e tem acesso não autorizado as suas finanças.

Integridade

- A informação se manterá inalterada ao longo da comunicação.
- **Quebrando a Integridade dos dados:**
- Ex: alguém intercepta um email que você enviou, modifica o texto da mensagem.

Disponibilidade

- A informação estará acessível para os usuários quando solicitada, ou ainda, garantir que os usuários autorizados tenham acesso às informações e ativos associados quando necessário.
- **Quebrando a Disponibilidade de um serviço:**
- Ex: o seu sistema de informação do banco sofre uma grande sobrecarga de dados ou um e por este motivo o terminal de autoatendimento fica fora do ar.

Autenticidade

- Confirma a identidade de um indivíduo, ou ainda, certeza absoluta de que um objeto (em análise) provém das fontes anuaciadas.
- **Quebra da Autenticidade de um indivíduo:**
- Ex: Alguém envia uma mensagem de email se passando por outra pessoa.
- Ex. Um orkut fake.

Outro Princípio: Não-Repúdio

- É a garantia de segurança que impede uma entidade participante numa dada operação de essa participação.
- **Exemplos:** Um vendedor de produtos ou serviços por via eletrônica pode negar que recebeu um pagamento (adiantado) e recusar-se a fornecer o produto ou prestar o serviço. Da mesma forma, um comprador desonesto pode recusar-se a pagar um produto (digital) que lhe foi fornecido, negando a sua recepção.
- A garantia de segurança destinada a combater este tipo de
- fraude chama-se Não-Repúdio = a não negação de uma ação!

Vulnerabilidade, Ameaça e Risco

- **Vulnerabilidade:** Ponto fraco em um sistema de informação. Ex: bugs.
- **Ameaça:** Tudo que pode causar danos a um sistema; Podem surgir dentro da própria organização. Ex: hacker, vírus etc.
- **Risco:** Expor o Sistema Computacional às ameaças. Ex: Não exigir senha para acessar um sistema.

Ameaças

- Vírus 75%
- Divulgação de senhas 57%
- Hackers 44%
- Funcionários insatisfeitos 42%
- Acessos indevidos 40%
- Vazamento de informações 33%
- Erros e acidentes 31%
- Falhas na segurança física 30%
- Acessos remotos indevidos 29%
- Super poderes de acesso 27%
- Uso de notebooks 27%
- Pirataria 25%
- Lixo informático 25%
- Divulgação indevida 22%
- Roubo / Furto 18%
- Fraudes 18%

Mecanismos de Segurança

- Para assegurar que os sistemas implantem as propriedades de Segurança e sejam ditos seguros, existe a necessidade de adoção de **Mecanismos de Segurança**
- Os são os Mecanismos de Segurança responsáveis efetivos pela garantia das propriedades da **política de segurança da informação.**

Política de Segurança da Informação

- A política de segurança relaciona as propriedades e mecanismos de segurança a um domínio, além de definir o escopo e as características de cada serviço que se pretende proteger. Ela determina regras que, quando seguidas corretamente, diminuem os riscos de incidentes de segurança à organização.
- É um conjunto de leis, regras e práticas que regulam como a organização gerencia, protege e distribui suas informações e recursos.

Autenticação

- Autenticação é uma prova de identidade.
- Métodos usados para identificar um usuário:
- Alguma coisa que você sabe . (Ex. senha)
- Alguma coisa que você tem . (Ex. token)
- Alguma coisa que você é . (Ex. impressão digital) - biometria

Senha

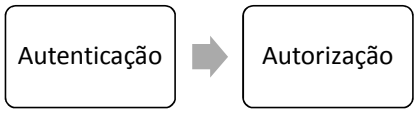
- Uma senha ( ) na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, é utilizada no processo de verificação da identidade do usuário, assegurando que .
- O que não se deve usar na elaboração de uma senha?
- Nomes;
- Sobrenomes;
- Números de documentos;
- Placas de Carro;
- Números de Telefone;
- Data

Controle de Acesso

- Controlar o acesso a um sistema
- Estabelecer a associação entre cada usuário e e privilégios.
- Indicar quem (ou o quê) pode ter acesso a algum objeto.
- **Objeto tangivel:** impressora.
- **Objeto intangivel:** diretório, arquivo ou serviço de rede

Autenticação x Autorização

- Por que a autenticação é uma condição prévia para a autorização?
- Não existe como estabelecer os direitos de uma entidade dentro de um sistema sem antes a sua identidade.



Auditoria

- **Auditoria: É a avaliação do comportamento dos** sistemas analisando seus registros (logs), atividades e serviços.
- **Auditoria é em um exame cuidadoso, sistemático e** independente das atividades desenvolvidas em determinada empresa ou setor, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.

Criptografia

- Problema?
- Nas arquitetura de computador a informação passa o diversos pontos intermediários antes de atingir seu destino.
- A informação pode ser descoberta! (quebra da confidencialidade)
- **Criptografia: ciência de comunicar-se secretamente.**

Criptografia

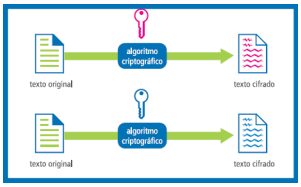
- A mensagem criptografada é codificada (embaralhada) e somente o destinatário sabe como descriptografar (desembaralhar).
- **Tipos de Criptografia:**
- Criptografia Simétrica - também conhecida como criptografia de chave privada.
- • Criptografia Assimétrica - criptografia de chave pública

Criptografia

- O termo "chave " vem do fato de que o número secreto que você escolhe funciona da mesma maneira que uma chave convencional.
- Na criptografia, para proteger o conteúdo dos seus arquivos, você instala uma **fechadura (algoritmo de criptografia**) na sua porta (o computador). Para operar a fechadura (encriptar os dados), você insere a **chave (o número secreto**) e a executa (em vez de girar essa chave, você opera o programa dando um clique duplo, clicando em OK ou pressionando Enter).

Criptografia

- Na criptografia simétrica, a **mesma chave** é utilizada para cifrar e decifrar dados (daí a palavra simetria). A chave é compartilhada.

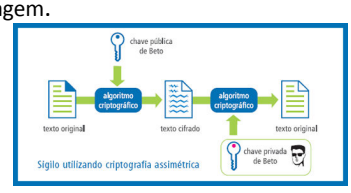


Criptografia

- Na criptografia assimetrica cada usuário possui duas chaves:
- **Uma chave privada.**
- **Uma chave pública.**
- A chave privada deve ser particular e protegida dos demais usuários. A chave pública pode ser mantida pública para os demais.

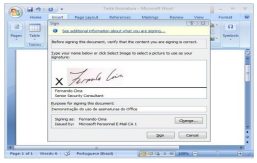
Criptografia

- Se **João** deseja enviar uma mensagem para **Beto** , ele cifra a mensagem com a chave pública de **Beto.**
- Ninguém pode decifrar a mensagem, pois somente **Beto** possui a chave privada que permite decifrar a mensagem.



Certificado Digital

- Uma terceira parte confiável (Autoridade Certificadora - AC) assina um certificado atestando que uma determinada chave pública pertence a tal usuário evitar a utilização ou publicação falsa de chaves públicas.



Antivírus

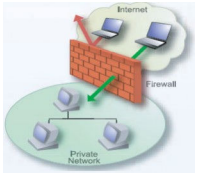
- Os antivírus são programas de computador concebidos para prevenir, detectar e eliminar **vírus de computadores**.
- Vale salientar que os antivírus são programas que procuram por outros programas (os vírus) e/ou os barram, por isso, nenhum antivírus é totalmente seguro o tempo todo, e existe a necessidade de sua **atualização**.

Firewall

- Firewall é um dispositivo de uma rede de computadores que tem como objetivos:
- regular o tráfego de dados entre uma rede local e a rede externa não confiável, por meio da introdução de filtros para pacotes ou aplicações;
- e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados dentro de uma rede local.

Firewall

- Os firewall funciona como uma espécie de filtro onde todas as mensagens não autorizadas, sites indevidos, etc são automaticamente barrados.



PROGRAMAS MALICIOSOS (MALWARE)

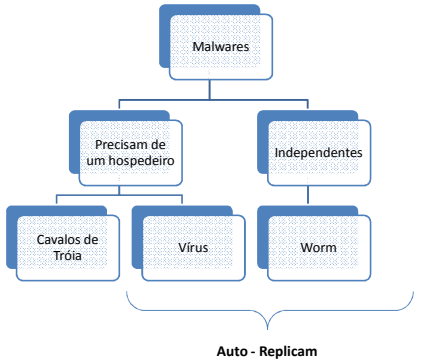
Programas Maliciosos (Malware)

- Códigos Malicioso ou malwares é um termo genérico que abrange todos os tipos de programas que especificamente desenvolvidos para executar ações que possam pôr em risco os ativos de dados.

Vírus x Worm x Trojan Horse

- Vírus (Fred Cohen – 1983)
  - Código que reside em outro arquivo (hospedeiro) e pode infectar outros arquivos
- Worm (PARC - 1982)
  - Código "auto-remoto-replicável"
- Trojan Horse
  - "Presente de grego"

Vírus x Worm x Trojan Horse



Outros Malwares

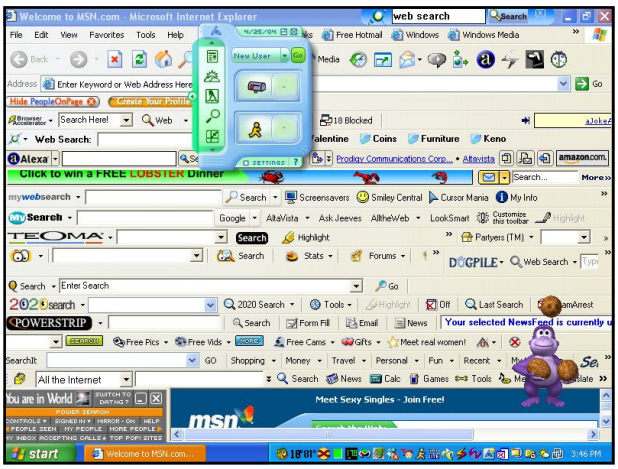
- Backdoors
  - Programas que abrem acesso remoto a um usuário não-autorizado
- Rootkits
  - Conjunto de software com medidas para (ganhar e) manter acesso a um host
  - Tipicamente uma combinação de trojan, backdoor e mais...

Outros Malwares

- Bots (de botnet)
  - Software que executa tarefas automatizadas, sob controle de um operador
  - Frequentemente controlados via IRC (Internet Relay Chat)
  - Comuns *spammers*

Outros Malwares

- Spyware
  - Interceptação da interação do usuário com o computador
  - Monitoramento e interferência (redirecionamento de páginas, instalação de programas...)
- Adware
  - Programa que exibe propagandas
  - Muitas vezes faz uso de spyware



Outros Malwares

- Keylogger
  - Intercepta e registra a interação do usuário com o teclado do computador
- Click-logger
  - Semelhante ao keylogger, mas para *mouse clicks*
- Dialer
  - Discador de 0900

Impacto do Vírus "I Love You"

OUTRAS FRAUDES

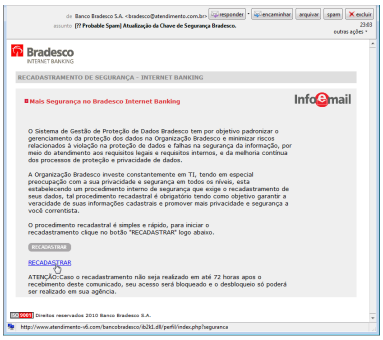
Spam

- Spam: Refere-se ao envio de email não autorizados.
- Tipos de spam:
  - Corrente (chain letters);
  - Boatos (hoax);
  - Propagandas;
  - Cyber-bulling;
  - Pornografia;
  - Fraudes.

Phishing

- Phishing é um tipo de fraude eletrônica projetada para roubar informações particulares.
- Eu um ataque Phishing (conhecido tambem como PhishingScam), uma pessoa mal intecionada envia uma mensagem eletrônica geralmente por email ou recados em redes sociais com objetivo de roubar dados.

Phishing



Phishing

Pharming

- Em informática **Pharming** é o termo atribuído ao ataque baseado na técnica *DNS cache poisoning* **(envenenamento de cache DNS)** que, consiste em corromper o DNS **(Sistema de Nomes de Domínio ou Domain Name System)** em uma rede de computadores, fazendo com que a URL **(Uniform Resource Locator ou Localizador Uniforme de Recursos)** de um site passe a apontar para um servidor diferente do original.
- Ao digitar a URL **(endereço)** do site que deseja acessar, um banco por exemplo, o servidor DNS converte o endereço em um número IP, correspondente ao do servidor do banco. Se o servidor DNS estiver vulnerável a um ataque de *Pharming*, o endereço poderá apontar para uma página falsa hospedada em outro servidor com outro endereço IP, que esteja sob controle de um golpista.

Engenharia Social

- A engenharia social é baseada na utilização da força de persuasão e na exploração da ingenuidade dos utilizadores, fazendo-se passar para uma pessoa da casa, um técnico, um administrador, etc para roubar informações.

A engenharia social pode assumir várias formas:

- ❖Por telefone;
- ❖Por correio eletrônico,
- ❖Por correio escrito;
- ❖Por serviço de mensagens instantâneas,

Formas de Proteção

- Programa Antivírus;
- Programas antispyware;
- Programas IDS;
- Firewall;
- Programas Anti-Spam.