Fundamentos de redes de computadores

Segurança da Informação

CONCEITOS DE PROTEÇÃO DE SEGURANÇA

Para manter o computador minimamente seguro, é necessário:

- *Manter o SO sempre atualizado;*
- *Possuir um bom Antivírus e um bom Antispyware;*
- *Manter o Firewall ativo;*
- *Criar senhas de acesso.*

CONCEITOS DE PROTEÇÃO DE SEGURANÇA

Ameaça

Causa potencial de um incidente indesejado que pode resultar em danos a um sistema ou organização.

Ataque

Tudo aquilo que tenta destruir, expor, alterar, desativar, roubar, obter acesso não autorizado ou fazer uso não autorizado de um ativo.

Ativo

Qualquer coisa que tenha valor para uma pessoa ou organização.

PRINCÍPIOS BÁSICOS DE SEGURAÇA DE REDE

Confidencialidade: é a capacidade de um sistema de não permitir que informações estejam disponíveis ou sejam reveladas a entidades não autorizadas – incluindo usuários, máquinas, sistemas ou processos. Seria algo similar à privacidade, em que pessoas autorizadas podem acessar e visualizar uma informação e pessoas não autorizadas não podem.

PRINCÍPIOS BÁSICOS DE SEGURAÇA DE REDE

Integridade: é a capacidade de garantir que a informação manipulada está correta, fidedigna e que não foi corrompida. Esse princípio geralmente trata da salvaguarda da exatidão e completeza da informação, com o intuito de aferir que a informação não tenha sido alterada sem autorização durante seu percurso, de sua origem ao seu destino, mantendo todas as características originais estabelecidas pelo proprietário da informação.

PRINCÍPIOS BÁSICOS DE SEGURAÇA DE REDE

Disponibilidade: é a propriedade de uma informação estar acessível e utilizável sob demanda por uma entidade autorizada. De certa forma, ela garante que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Se eu recebi uma carta, eu devo ter acesso a sua informação sempre que desejar.

PRINCÍPIOS BÁSICOS DE SEGURAÇA DE REDE

Autenticidade: é a propriedade que trata da garantia de que um usuário é de fato quem alega ser. Em outras palavras, ela garante a identidade de quem está enviando uma determinada informação. Sabe quando você assina um contrato? A sua assinatura é uma forma (frágil) de garantir que você é quem diz ser! O cartório tem a sua assinatura (chamada firma) e ele pode comparar com a assinatura que consta no contrato.

PRINCÍPIOS BÁSICOS DE SEGURAÇA DE REDE

Irretratabilidade ou Irrefutabilidade ou Não-repúdio: trata da capacidade de garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria. No Direito, o não-repúdio implica a intenção de cumprir as obrigações de um contrato. Implica também que uma parte de uma transação não possa negar ter recebido uma transação, nem a outra parte pode negar ter enviado uma transação.

CRIPTOGRAFIA

Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la.

Chaves Criptográficas: trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e decodificar informações.

CRIPTOGRAFIA

CHAVE SIMÉTRICA: Esse é um tipo de chave mais simples, onde o emissor e o receptor fazem uso da mesma chave, isto é, uma única chave é usada na codificação e na decodificação da informação.

CHAVE ASSIMÉTRICA: Também conhecida como "chave pública", a chave assimétrica trabalha com duas chaves: uma denominada privada e outra denominada pública. Neste método, a chave pública é uma informação que fica no servidor na internet para quem precisar dela enquanto a chave privada é um código que somente o proprietário deve conhecer.

CRIPTOGRAFIA

Pelo princípio da **CONFIDENCIALIDADE**, a criptografia é feita com a chave pública para que somente o destinatário possa abrir com a chave privada.

Na **AUTENTICIDADE**, a criptografia é feita pelo remetente com a sua chave privada, em que qualquer destinatário possa usar a chave pública para abrir.

A contratação do par de chaves assimétricas deve ser feita perante a **AUTORIDADE CERTIFICADORA**, a qual emite o par de chaves.

A **AUTORIDADE DE REGISTRO** simplesmente verifica dados do usuário e encaminha para a autoridade certificadora.

CRIPTOGRAFIA

CERTIFICADO DIGITAL

1. Dados do proprietário e da Autoridade Certificadora;
2. Validade;
3. Assinatura do proprietário;
4. Versão e Número de Série;
5. **CHAVE PÚBLICA!**

CRIPTOGRAFIA

ASSINATURA DIGITAL: É uma tecnologia que utiliza a criptografia e vincula o certificado digital ao documento eletrônico que está sendo assinado.

Para assegurar a integridade da mensagem, utiliza-se um algoritmo codificador chamado de HASH.

Assinatura digital com criptografia HASH assegura a INTEGRIDADE E AUTENTICIDADE.

ENVIO: MSG original ---> HASH ---> Chave Privada ---> Enviar!
RECEBIMENTO: Chave Pública ---> HASH ---> Comparação ---> Abre!

CÓDIGOS MALICIOSOS (MALWARES)

São programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador (tanto em software quanto em hardware). Algumas das diversas formas, como os “códigos maliciosos”, podem infectar ou comprometer um computador são:

- *Pela exploração de vulnerabilidades existentes nos programas instalados;*
- *Pela autoexecução de mídias removíveis infectadas, como pendrives;*
- *Pelo acesso a páginas web maliciosas, utilizando navegadores vulneráveis;*
- *Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;*
- *Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas web ou diretamente de outros computadores (através do compartilhamento de recursos).*

CÓDIGOS MALICIOSOS (MALWARES)

1. VÍRUS: é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

CÓDIGOS MALICIOSOS (MALWARES)

1.1. TIPOS DE VÍRUS:

Vírus de script: escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.

Vírus de macro: tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).

CÓDIGOS MALICIOSOS (MALWARES)

2. WORM: é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido `a grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

CÓDIGOS MALICIOSOS (MALWARES)

3. BOT: é um programa que dispõe de mecanismos de comunicações com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

4. BOTNET: é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

CÓDIGOS MALICIOSOS (MALWARES)

5. SPYWARE: é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

5.1. Tipos Específicos de Spyware:

KEYLOGGER: capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

CÓDIGOS MALICIOSOS (MALWARES)

5.1. Tipos Específicos de Spyware:

SCREENLOGGER: similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking

CÓDIGOS MALICIOSOS (MALWARES)

5.1. Tipos Específicos de Spyware:

ADWARE: projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito

CÓDIGOS MALICIOSOS (MALWARES)

6. BACKDOOR: é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços
criados ou modificados para este fim.

7. CAVALO DE TROIA, TROJAN OU TROJAN-HORSE: é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

CÓDIGOS MALICIOSOS (MALWARES)

8. ROOTKIT: é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

9. RANSOMWARE: é um tipo de malware que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, geralmente usando a moeda virtual bitcoin, que torna quase impossível rastrear o criminoso que pode vir a receber o valor. Este tipo de "vírus sequestrador" age codificando os dados do sistema operacional de forma com que o usuário não tenha mais acesso.

CÓDIGOS MALICIOSOS (MALWARES)

10. HIJACKER: Esse Malware tornará o navegador descontrolado e que durante a navegação apresentará várias páginas indesejadas, abrir pop-ups, exibir propagandas, alterar o site de busca padrão do navegador, entre ouras ações.

Todas essas ações são tomadas pelo malware para efetivar o furto das informações, pois quando um site trava, fecha sozinho, pede novamente as mesmas informações, o usuário perde tempo e o atacante consegue desempenhar melhor seu ataque.

Outra característica do Hijacker é que esse programa malicioso é utilizado em ações que redirecionam a navegação do usuário a outras páginas indesejadas, que foram escolhidas pelo programador da praga virtual

GOLPES NA INTERNET

1. PHISHING: é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

2. PHARMING: é um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa.

GOLPES NA INTERNET

3. UM BOATO, OU HOAX: é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

ATAQUES NA INTERNET

1. INTERCEPTAÇÃO DE TRÁFEGO OU SNIFFING: é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers.

2. FORÇA BRUTA OU BRUTE FORCE: consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

ATAQUES NA INTERNET

3. DESFIGURAÇÃO DE PÁGINA, DEFACEMENT OU PICHAÇÃO: é uma técnica que consiste em alterar o conteúdo da página Web de um site.

4. NEGAÇÃO DE SERVIÇO, OU DOS (DENIAL OF SERVICE): é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

5. NEGAÇÃO DE SERVIÇO DISTRIBUÍDO, OU DDOS (DISTRIBUTED DENIAL OF SERVICE): Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque.

SPAM

É o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial E-mail).

Spams estão diretamente associados a ataques à segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos.

BACKUP

É um serviço que garante que você pode sempre recuperar informações de forma confiável e tempestiva.

TIPOS BACKUPS

1. BACKUP COMPLETO: Também chamado de Total, Normal ou Full, trata-se do backup que faz uma **cópia de todos os dados** de uma unidade.

É um procedimento com **tempo de execução maior** e **requer mais espaço de armazenamento**, visto que todos os arquivos serão copiados.

BACKUP

TIPOS BACKUPS

2. BACKUP INCREMENTAL: Trata-se de uma cópia de todos os dados que foram criados ou modificados desde o último *backup* completo ou incremental anterior.

A principal vantagem é que será copiada **uma quantidade menor de dados** do que no caso de um backup completo.

A **recuperação de dados é mais lenta e complexa**, visto que o último backup completo deve ser recuperado e, em seguida, os dados incrementais de cada dia até o momento da falha.

A **restauração do backup é mais trabalhosa.**

BACKUP

TIPOS BACKUPS

3. BACKUP DIFERENCIAL: TAMBÉM CONHECIDO COMO BACKUP INCREMENTAL CUMULATIVO: trata-se de uma cópia de todos os dados que foram criados ou modificados desde o último backup completo ou incremental anterior, mas não removerá o atributo de arquivamento.

Ele **armazena mais dados do que o Backup Increme**ntal. Isso **exige mais espaço e mais tempo de backup** que os backups incrementais.

A grande vantagem é que – para restaurar – nós precisamos apenas do backup completo e do último backup diferencial – pode-se descartar o primeiro backup diferencial.

O Backup Diferencial é **mais rápido de restaurar**, mas é **mais lento para criar**.

FERRAMENTAS DE PROTEÇÃO

FERRAMENTAS ANTIMALWARE: são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

FIREWALL PESSOAL: É um tipo específico de firewall que é utilizado para proteger um computador contra acessos não autorizados vindos da Internet.
Os programas antimalware, apesar da grande quantidade de funcionalidades, não são capazes de impedir que um atacante tente explorar, via rede, alguma vulnerabilidade existente em seu computador e nem de evitar o acesso não autorizado, caso haja algum backdoor nele instalado. Devido a isto, além da instalação do antimalware, é necessário que você utilize um firewall pessoal.