GESTÃO DE SEGURANÇA DA INFORMAÇÃO

AMEAÇAS AOS SISTEMAS DE INFORMAÇÃO

Olá!

Nesta aula você irá estudar sobre ameaças ao sistema de informação.

1. Irá compreender o que são ameaças de segurança.

2. Conhecer os principais tipos de ameaças.

3. Identificar as diferenças entre ameaças passivas e ativas.

Introdução às ameaças de segurança

Os incidentes de segurança da informação vêm aumentando consideravelmente ao longo dos últimos anos motivados não só pela difusão da Internet, que cresceu de alguns milhares de usuários no início da década de 1980 para centenas de milhões de usuários ao redor do globo nos dias de hoje, como também pela democratização da informação. A internet tornou-se um canal on-line para fazer negócios, porém viabilizou também a atuação dos ladrões do mundo digital, seja hackers ou leigos mal-intencionados. Proporcionou também a propagação de códigos maliciosos (vírus, worms, trojans etc.), spam, e outros inúmeros inconvenientes que colocam em risco a segurança de uma corporação.

Outros fatores também contribuíram para impulsionarem o crescimento dos incidentes de segurança, tais como:

O aumento do número de vulnerabilidades nos sistemas existentes, como, por exemplo, as brechas de segurança nos sistemas operacionais utilizados em servidores e estações de trabalho.

O processo de mitigar tais vulnerabilidades com a aplicação de correções do sistema, realizadas muitas vezes de forma manual e individual: de máquina em máquina.

A complexidade e a sofisticação dos ataques, que assumem as formas mais variadas, como, por exemplo: infecção por vírus, acesso não autorizado, ataques denial of service contra redes e sistemas, furto de informação proprietária, invasão de sistemas, fraudes internas e externas, uso não autorizado

de redes sem fio, entre outras.

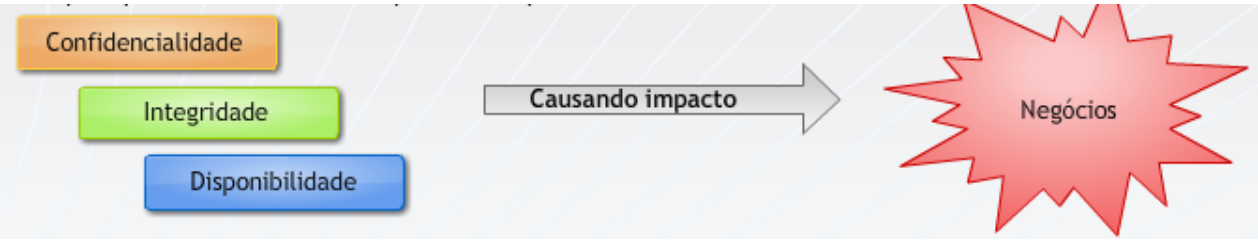
É a conjunção dessas condições que culmina na parada generalizada de sistemas e redes corporativas ao redor do mundo.

Você sabe o que é uma ameaça?

Uma ameaça, segundo a definição da RFC 2828, Internet security glossary, é?

"Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade."

Segundo Marcos Sêmola, as ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de:



Quando classificadas quanto a sua intencionalidade as ameaças podem ser:

Naturais	Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc.
Involuntárias	Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidente, erros, falta de energia, etc.
Voluntárias	Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computadores, incendiários.

Códigos maliciosos (Malware)

Segundo o Wikipédia, o termo malware é proveniente do inglês malicious software; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Vírus de computador, worms, trojan horses (cavalos de troia), backdoors, keyloggers, bots, rootkits e spywares são considerados malware. Também pode ser considerada malware uma aplicação legal que por uma falha de programação (intencional ou não) execute funções que se enquadrem na definição supra citada.

Vírus

O vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

Para se tornar ativo e dar continuidade no processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro .

Normalmente o vírus tem controle total sobre o computador, podendo fazer de tudo, desde mostrar uma mensagem de "feliz aniversário", até alterar ou destruir programas e arquivos do disco.

Como uma máquina pode ser infectada?

É preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

- Abrir arquivos anexados aos e-mails;
- Abrir arquivos do Word, Excel, etc;
- Abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- Instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes,pen drives, CDs, DVDs, etc;
- Ter alguma mídia removível (infectada) conectada ou inserida no computador, quando ele é ligado.

Clique aqui e conheça alguns tipos de vírus:

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/04GSI_aula04_doc01.pdf

Worms

Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Geralmente o worm não tem como consequência mesmos danos gerados por um vírus, mas são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar.

Cavalos de Tróia

Conta a mitologia grega que o "Cavalo de Tróia" foi uma grande estátua, utilizada como instrumento de guerra pelos gregos, para obter acesso a cidade de Tróia, A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia. Daí surgiram os termos "Presente de Grego" e "Cavalo de Tróia". Fonte: cartilha de código malicioso.pdf

São programas que parecem úteis mas tem código destrutivo embutido. Além de executar funções para as quais foi projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Normalmente é um programa, normalmente recebido como um “presente” (Por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia:

- instalação keyloggers ou screenloggers;
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador;
- alteração ou destruição de arquivos.

Adware (Advertising software)

É um tipo de software especificamente projetado para apresentar propagandas, seja através de um browser, seja através de algum outro programa instalado em um computador. Em muitos casos, os adwares têm sido incorporados a softwares e serviços, constituindo uma forma legítima de patrocínio ou de retorno financeiro para aqueles que desenvolvem software livre ou prestam serviços gratuitos.

Spyware

Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Existem adwares que também são considerados um tipo de spyware, pois são projetados para monitorar os hábitos do usuário durante a navegação na Internet, direcionando as propagandas que serão apresentadas.

Os spywares, assim como os adwares, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Listamos abaixo algumas funcionalidades implementadas em spywares e podem ter relação com o uso legítimo ou malicioso:

- Monitoramento de URLs acessadas enquanto o usuário navega na Internet;
- Alteração da página inicial apresentada no browser do usuário;
- Varredura dos arquivos armazenados no disco rígido do computador;
- Monitoramento e captura de informações inseridas em outros programas, como processadores de texto;
- Instalação de outros programas spyware;
- Monitoramento de teclas digitadas pelo usuário ou regiões da tela próximas ao clique do mouse
- Captura de senhas bancárias e números de cartões de crédito;
- Captura de outras senhas usadas em sites de comércio eletrônico.

É importante ressaltar que estes programas, na maioria das vezes, comprometem a privacidade do usuário e a segurança do computador do usuário, dependendo das ações realizadas pelo spyware no computador e de quais informações são monitoradas e enviadas para terceiros.

Backdoors

Nome dado a programas que permitem o retorno de um invasor a um computador comprometido utilizando serviços criados ou modificados para este fim sem precisar recorrer aos métodos utilizados na invasão. Na maioria dos casos, é intenção do atacante poder retornar ao computador comprometido sem ser notado.

A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet). O backdoor pode ser incluído por um vírus, através de um cavalo de tróia ou pela a instalação de pacotes de software.

Keyloggers

Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. As informações capturadas podem ser desde o texto de um e-mail, até informações mais sensíveis, como senhas bancárias e números de cartões de crédito. Sua ativação está condicionada a uma ação prévia do usuário e normalmente contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de e-mails). A contaminação por Keylogger, geralmente vem acompanhada de uma infecção por outros tipos de vírus, em geral, os Trojans.

Screenloggers

Formas mais avançadas de keyloggers que além de serem capazes de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, também são capazes de armazenar a região que circunda a posição onde o mouse é clicado.

Rootkits

Conjunto de programas que fornecem mecanismos para esconder e assegurar a presença de um invasor. O nome rootkit não indica que o conjunto de ferramentas que o compõem são usadas para obter acesso privilegiado (root ou Administrator) em um computador, mas sim para mantê-lo. Significa que o invasor, após instalar o rootkit, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Um rootkit pode fornecer programas com as mais diversas funcionalidades:

- programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os rootkits), tais como arquivos, diretórios, processos, conexões de rede, etc;
- backdoors, para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos rootkits);
- programas para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
- programas para remoção de evidências em arquivos de logs;
- programas para mapear potenciais vulnerabilidades em outros computadores;

Bots e Botnets

Segundo a wikipédia, uma botnet é uma coleção de agentes de software ou bots que executam autonomamente e automaticamente. O termo é geralmente associado com o uso de software malicioso, mas também pode se referir a uma rede de computadores utilizando software de computação distribuída.

Clique aqui e saiba mais através de reportagens e de um detalhamento de como eles funcionam

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/04GSI_aula04_doc02.pdf

Potenciais atacantes:

Existem controvérsias sobre o conceito e a nomenclatura dos possíveis atacantes. Para saber mais leia o artigo "Como funciona a cabeça de um hacker".

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/347a_de_um_hacker_aula04.pdf

1.Hackers - Pessoa com amplo conhecimento de programação e noções de rede e internet. Não desenvolvem vulnerabilidade, apenas copiam vulnerabilidades publicadas em sites especializados;

2.White-hats - Exploram os problemas de segurança para divulgá-los abertamente;

3. Crackers - Pessoas que invadem sistemas em rede ou computadores apenas por desafio;

4.Black-hats - Usam suas descobertas e habilidades em benefício próprio, extorsão, fraudes, etc.

5.Pheakres - Pessoa que Interferem com o curso normal das centrais telefônicas, realizam chamadas sem ser detectados ou realizam chamadas sem tarifação;

6.Wannabes - Ou script-kiddies são aqueles que acham que sabem, dizem para todos que sabem, se anunciam, divulgam abertamente suas façanhas e usam 99% dos casos de scripts conhecidos;

7.Defacers - São organizados em grupo, usam seus conhecimentos para invadir servidores que possuam páginas web e modificá-las.

Ameaças passivas x ativas:

Nós vimos que as ameaças podem ser classificadas quanto a sua intencionalidade (natural, involuntárias e voluntárias) e podem ser classificadas quanto a sua origem:

Ela pode ser interna, pois nem sempre o principal “inimigo” está fora da nossa empresa, como um hacker ou um cracker, mas sim dentro dela, como um funcionário mal intencionado ou muito insatisfeito, que geralmente possui livre acesso aos recursos disponíveis e que podem comprometer a integridade e a privacidade de informações estratégicas da empresa.

Segundo Stallings, na literatura os termos ameaças e ataque normalmente são usados para designar mais ou menos a mesma coisa

Ameaça

Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.

Ataque

Um ataque à segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada de burlar os serviços de segurança e violar a política de segurança de um sistema.

Podemos classificar os ataques como:

Passivo

Envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso . Os ataques ativos envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso e podem ser subdivididos em quatro categorias: disfarce, modificação de mensagem, repetição e negação de serviço.

Ativo

Possuem a natureza de bisbilhotar ou monitora transmissões. O objetivo dos ataques passivos é obter informações que estão sendo transmitidas.

Saiba mais

Clique e veja como esses ataques ocorrem

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/04GSI_aula04_doc03.pdf

Como proteger um computador contra as ameaças?

Nós vimos que algumas das ameaças estudadas são capazes de se propagar automaticamente, através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador. Porém todas as ameaças exploram as vulnerabilidades encontradas. Segundo a cartilha de Segurança para

internet do CERT.br (Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil),uma das formas de proteger um computador é:

Manter o sistema operacional e os softwares instalados em seu computador sempre atualizados e com todas as correções de segurança (patches) disponíveis aplicadas, para evitar que possuam vulnerabilidades.

Também é recomendado a utilização de antivírus, mantendo-o sempre atualizado, pois em muitos casos permite detectar e até mesmo evitar a propagação de um bot. Porém o antivírus só será capaz de detectar bots conhecidos.

Ao final de nosso estudo podemos concluir que:

A tendência é que as ameaças ou ataques à segurança continuem a crescer não apenas em ocorrência, mas também em velocidade, complexidade e alcance, tornando o processo de prevenção e de mitigação de incidentes cada vez mais difícil e sofisticado. Novas formas de infecção podem surgir. Portanto, é importante manter-se informado através de jornais, revistas e de sites sobre segurança e de fabricantes de antivírus.

Saiba mais

Leia a Cartilha de Segurança para Internet Parte VIII: Códigos Maliciosos (Malware)

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/cartilhacodigo_maliciosos_aula04.pdf

Para saber mais sobre os tópicos estudados nesta aula, pesquise na internet sites, vídeos e artigos relacionados ao conteúdo visto. Se ainda tiver alguma dúvida, fale com seu professor online utilizando os recursos disponíveis no ambiente de aprendizagem.

O que vem na próxima aula

Na próxima aula, aprenderemos o seguinte tema: Ataques à segurança

•Assunto 1: O planejamento de um ataque

•Assunto 2: Principais tipos de ataques.

CONCLUSÃO

Nesta aula, você:

- Compreendeu o conceito de ameaça.

- Estudou os principais tipos de ameaças.
- Compreendeu a diferença entre ameaças ativas e passivas.