SEG DIR DIG A1 - Texto de apoio

Descrição

Índice

1. Introdução

A popularização e o avanço tecnológico proporcionaram uma nova e extraordinária maneira das pessoas se comunicarem, motivando a democratização da informação e oferecendo novas formas de relações profissionais, de consumo e de serviços.

O comércio eletrônico, as transações bancárias, as notícias jornalísticas ou as informações econômicas, científicas, médicas, culturais etc. são exemplos de uma dinâmica na sociedade moderna que necessita cada vez mais de acesso rápido e eficiente aos meios informáticos. A segurança da informação surge nesse contexto. O desenvolvimento tecnológico avança juntamente com a necessidade de privacidade em sistemas computacionais.

A internet e os sistemas computacionais podem sofrer invasões ou ataques indesejados por pessoas desautorizadas, com programas de computador ou conhecimentos técnicos de acesso aos dados individuais ou corporativos, evidenciando problemas na segurança e caracterizando alguns crimes ou delitos informáticos, como fraudes, violação e invasão de dispositivos informáticos ou instalação de vulnerabilidades sem prévia autorização.

O uso da tecnologia é essencial nos tempos modernos, mas pode gerar conflitos e contratempos, como a possibilidade de envio de um e-mail não autorizado, troca de informações ou invasão e captura de dados de forma não autorizada. A segurança em meios informáticos torna-se necessária em um mundo cada vez mais tecnológico. Abordaremos os diversos riscos envolvidos no uso da internet e seus métodos de prevenção e discutiremos as formas que podem aumentar a segurança de um computador. Os riscos e medidas preventivas para o uso de sistemas computadorizados são temas importantes para o conhecimento do profissional da área de tecnologia da informação, auxiliando na segurança de programas de troca de mensagens, de distribuição e compartilhamento de arquivos. Você perceberá a importância da realização de cópias de segurança, backups, baseadas em uma política de segurança, de controle e de direito de acesso.

2. CÓDIGOS MALICIOSOS – MALWARES

Os códigos maliciosos são conhecidos malwares em sistemas informáticos. Esses códigos são programas que possuem o intuito de executar ações impróprias, danosas, visando prejudicar e interferir no funcionamento dos sistemas computacionais. As atividades maliciosas passam a ter acesso ao sistema computacional, executando ações indesejadas. O acesso a dados armazenados por códigos maliciosos interfere e opõe-se diretamente no conceito de segurança, pois o objetivo é obter informações sigilosas, confidenciais e pessoais, acessar informações financeiras ou praticar vandalismo, prejudicando o funcionamento ou comprometendo os dados armazenados.

Entre as diversas formas de infestação de malwares, as mais comuns formas de contato são por meio de programas em mídias removíveis, como o pendrive, ao acessar sites que contenham anexos arquivos executáveis maliciosos, mensagens infectadas em e-mails, entre outros.

Os malwares podem ser classificados ou divididos entre vírus, spyware, cavalo de Troia, worm, bot, alçapão ou backdoor.

Vírus – O vírus é um código ou parte de um código malicioso que é instalado sem autorização. Ele se propaga pelo sistema computacional, tornando-se parte de arquivos e programas, que podem permanecer ocultos, mas infectando arquivos e executando atividades não autorizadas sem que os usuários do sistema computacional percebam; fazendo autocópias, ou seja, multiplicando-se e infectando outros arquivos ou contatos que possam acontecer, por e-mails, mensagens, transferência de dados, anexos, ou mídias removíveis.

Spyware – O spyware é um programa de computador que monitora informações de um sistema computacional e as fornece a terceiros. Este programa poderá ser utilizado de forma legítima como forma de controle, mas geralmente funciona de maneira não autorizada e maliciosa.
O spyware executa ações no sistema computacional de maneira indesejada, altera configurações, páginas iniciais de web; monitora sites durante a navegação captura informações tecladas ou acessadas, vasculha dados e arquivos, inclusive localização e monitoramento do mouse e teclado durante a visita a uma página web.

Cavalo de Troia – O cavalo de Troia é um programa de computador que executa funções aparentes e maliciosas, esta de forma oculta, sem autorização ou conhecimento do usuário. Geralmente, o cavalo de Troia pode estar associado a programas ou a arquivos anexados, como jogos, fotos, protetores de tela, cartões virtuais etc. Entre as ações maliciosas do malware, pode-se citar a captura e o envio de senhas e dados financeiros para terceiros ou para o invasor, destruição ou alteração de arquivos, instalação de outros malwares. O cavalo de Troia se diferencia do vírus e do worm pois não se propaga instantaneamente e não realiza autocópias. Este malware geralmente possui um único arquivo que poderá ser executado, de forma programada, podendo ficar inativo por algum tempo e executar atividades maliciosas conforme seu objetivo prévio.

Worm – O worm é um programa de propagação automática entre sistemas computacionais, enviando cópias desse mesmo programa entre os computadores. Ele é diferente do vírus, pois – ao se propagar e infectar novos sistemas computacionais – o worm executa sua cópia nos novos sistemas, buscando vulnerabilidades para esta execução.

Bot – O bot é um programa de computador destinado a propagação automática, similar ao worm, buscando falhas e vulnerabilidades em softwares e configurações. Diferencia-se dele, pois envia informações ao invasor, permitindo que este controle o sistema computacional a distância. Quando vários computadores são invadidos por bots, eles formam uma rede controlada remotamente, chamada de botnet, que controla os computadores infectados a distância.

Alçapão ou Backdoor – O termo alçapão ou backdoor tem origem na associação entre passagens secretas ou passagens para entrada no sistema computacional. São caminhos de acesso ao computador utilizados por invasores experientes, pois o usuário não percebe a falha na segurança. Este malware é uma maneira de retornar ao sistema computacional sem ser notado, ou precisar de novos métodos para invasão; é uma forma de deixar o caminho de acesso sempre disponível para o invasor. A instalação desta ação maliciosa se dá por um cavalo de Troia e determina o controle e acesso remoto dos invasores.

3. VULNERABILIDADE

A vulnerabilidade é uma falha de projeto, no processo, na configuração ou na fase implementada de aplicação e uso de sofwtares ou sistemas computacionais e operacionais. Esta falha é uma ameaça à segurança. Sistemas operacionais ou softwares desatualizados, instalações defeituosas, acesso e autorizações inadequadas, falhas na configuração da rede de acesso, ausência de equipamentos necessários, entre outros exemplos, pode ser considerados falhas e, assim, determinam o conceito de vulnerabilidade que ameaça à segurança do sistema computacional e dos recursos envolvidos.

Vulnerabilidades podem ser encontradas desde o aspecto estrutural, como instalações suscetíveis a perigos físicos (incêndios, depreciação material, vazamentos de líquidos ou material químico), até o aspecto natural, como desastres naturais, aumento de temperatura ou umidade. Outros aspectos sobre as vulnerabilidades seriam os relacionados a falhas tecnológica, de instalação ou de configuração dos softwares, aos acessos indesejados ou desautorizados e à usabilidade, devido a falhas humanas por desconhecimento ou mau uso de sistemas ou de equipamentos, de forma intencional ou não.

Estas falhas ou vulnerabilidades precisam ser revistas e identificadas para sanar todo o risco envolvido. As vulnerabilidades são a porta de entrada dos malwares.

4. ENGENHARIA SOCIAL

Engenharia Social é considerada a habilidade de persuasão, a habilidade de conseguir dados confidenciais por meio do trato social. É considerado um método de invasão, uma forma de ataque à segurança com o uso da persuasão para obter acesso não autorizado a informações ou a sistemas computacionais. Esta habilidade é um risco à segurança da informação, induzindo um usuário a executar tarefas ou fornecer informações sigilosas. Este método de ataque pode ocorrer por diversos meios, como e-mails, ligações telefônicas, sites que induzem fraudes no comércio eletrônico, entre outros.

Para se proteger deste tipo de ataque e diminuir o risco, você não deve fornecer dados importantes, como senhas ou informações financeiras, não deve executar programas recebidos ou clicar em links contidos em e-mails. Informe-se sobre a procedência da mensagem ou das ligações telefônicas, verificando a veracidade das solicitações e dos diálogos estabelecidos. No caso de atividades corporativas, treinamentos de funcionários e alertas sobre essa forma de abordagem que compromete a segurança deverão ser detalhados, como forma de prevenção.

5. CRIPTOGRAFIA

A criptografia é uma técnica de escrever mensagens de maneira cifrada ou por meio de códigos. Essa técnica utiliza uma comunicação codificada, secreta, e auxilia na transferência de dados e informações que não devem ser interceptadas ou acessadas.

Uma informação criptografada autêntica a identidade dos usuários, protege os dados e informações pessoais, auxiliando na integridade das informações acessadas e comunicadas. As informações criptografadas podem identificar o remetente e, desse modo, são caracterizadas como informações privadas, de remetente para destinatário, somente acessadas por estes dois usuários.

A criptografia auxilia na segurança dos dados, considerado um método seguro para transmissão e acesso de informações privadas. Você pode usar a criptografia para proteger arquivos e senhas, proteger uma área específica no seu computador (criada para armazenar informações), criptografar dados financeiros, backups, e-mails ou mensagens.