Como se pega Virus de Computador

Fontes de ameaças

Uma pessoa, um grupo de pessoas, ou mesmo alguns fenômenos não relacionados à atividade humana pode servir como uma ameaça à segurança da informação. A partir daí, todas as fontes de ameaça quebram em três grupos:

O fator humano.
Este grupo de ameaças diz respeito às ações de pessoas com acesso autorizado ou não autorizado à informação. Ameaças neste grupo pode ser dividido em:

Externas, incluindo criminosos virtuais, hackers, fraudes internet, parceiros sem princípios, e as estruturas criminosas.
Interna, incluindo ações de funcionários da empresa e usuários de PCs domésticos. Ações tomadas por esse grupo podem ser deliberadas ou acidentais.

O fator tecnológico.
Este grupo de ameaças está relacionado com problemas técnicos - equipamento usado se tornando obsoletos e de baixa qualidade de software e hardware para processamento de informação. Isso tudo leva a falha do equipamento e muitas vezes a perda de dados.

O fator de desastres naturais
Este grupo de ameaças inclui qualquer número de eventos provocada pela natureza e outros eventos independentes da atividade humana.

Como as ameaças se propagam

Como a tecnologia de computador e ferramentas modernas de comunicação se desenvolvem, os hackers têm mais oportunidades para espalhar ameaças. Vamos dar uma olhada neles:

Internet
A Internet é única, uma vez que é propriedade de ninguém e não tem fronteiras geográficas. Em muitos aspectos, isso promoveu o desenvolvimento de recursos web incontáveis e o intercâmbio de informações. Hoje, qualquer pessoa pode acessar dados na Internet ou criar sua própria página web.
No entanto, estas características muito da web em todo o mundo dão aos hackers a capacidade de cometer crimes na Internet, tornando-os difíceis de detectar e punir.

Drives flash USB – Pendrives – Hd´s externos.
Drives flash USB são amplamente utilizados para armazenar e transmitir informações. Quando você usa um disco USB que tem programas maliciosos instalados nele, você pode danificar os dados armazenados no seu computador e espalhar o vírus para outras unidades do seu computador ou outros computadores na rede.

Tipos de ameaças

worms
Esta categoria de programa malicioso em grande parte explora as vulnerabilidades do sistema operacional para se espalhar. A classe foi nomeado de acordo com a forma como os vermes rastejam de computador para computador, usando redes e e-mail. Esta característica dá aos worms uma velocidade bastante elevada na rede espalhando-se, sem controle.

vírus
Programa que infecta outros programas, agregando seu próprio código a eles para ganhar o controle dos arquivos infectados quando eles são abertos. Esta definição simples explica a principal ação de um vírus - infecção.

Trojans
Programas que executam ações não autorizadas em computadores, como excluir informações em unidades, fazendo com que o sistema pare de funcionar, roubar informações confidenciais, etc Esta classe de programa malicioso não é um vírus no sentido tradicional da palavra (o que significa que ele não infecta outros computadores ou dados). Trojans não podem invadir computadores por conta própria e são disseminados por hackers, que os disfarçam como software comum. O dano que deles incorre pode exceder o feito por ataques de vírus tradicionais por várias vezes, pois eles "**podem limpar suas contas bancarias, por exemplo**".

spyware
Software que coleta informações sobre um determinado usuário ou organização sem o seu conhecimento. Você nunca vai poder imaginar que você tenha spyware instalado em seu computador.

riskware
Aplicações potencialmente perigosas que incluem softwares que não tenham características maliciosas, mas poderiam fazer parte do ambiente de desenvolvimento para programas maliciosos ou poderiam ser usados por hackers como componentes auxiliares para criar e instalar programas maliciosos.

rootkits
Utilitários usados para disfarçar a atividade dos mal-intencionados. Eles servem de máscara para programas maliciosos e, para impedir programas anti-vírus de detectá-los. Os rootkits modificam o sistema operacional no computador e alteram suas funções básicas para esconder sua própria existência e ações que o hacker executa no computador infectado.

Afonso Abilio Nunes Blaz
Informática / Reitoria
31-33301507 - 1509
UNIVERSIDADE
DO ESTADO DE MINAS GERAIS
UEMG