

Segurança da Informação

Introdução

Riscos de Segurança

Vírus

Estratégias de Segurança

Prevenção

Detecção

Recuperação

Introdução

Segurança da Informação (IT Security ou InfoSec) é o termo usado para descrever o processo de proteção de dados do acesso não autorizado, roubo, alteração ou destruição, garantindo a continuidade do acesso a informação sempre que necessário. A Segurança da Informação busca atingir 4 objetivos básicos:

1. **Confidencialidade:** Apenas pessoas autorizadas devem ser capazes de ver os dados;
2. **Integridade:** Apenas pessoas autorizadas devem ser capazes de alterar os dados;
3. **Disponibilidade:** Pessoas autorizadas devem ser capazes de acessar os dados sempre que necessário;
4. **Gerenciabilidade:** Gerentes devem ser capazes de descobrir quem fez o que com os dados.

Riscos de Segurança

Computadores são usados para gerenciamento de processos, transações bancárias, investimentos, compras e comunicação. Apesar da maioria destes processos não serem considerados “secretos”, usualmente não desejamos que outros tenham acesso a nossos dados relacionados.

Os computadores podem ser invadidos pelos chamados Hackers, Crackers ou Attackers. Usualmente eles desejam obter controle do computador para utilizá-lo no ataque a outros sistemas. Tendo controle de outro computador, tem a capacidade de esconder sua verdadeira localização quando lançam ataques contra empresas ou instituições financeiras. Além disso, eles podem ter acesso a todas as suas ações no computador, copiando, alterando ou excluindo dados.

Infelizmente os invasores exploram as várias vulnerabilidades (buracos) dos vários softwares dos computadores. Quando novas vulnerabilidades são descobertas os fabricantes dos softwares lançam atualizações. Estas atualizações devem entretanto ser instaladas pelos usuários dos computadores, dando margem tempo para os invasores agirem.

Os vírus são outro problema grave que expõe a fragilidade dos sistemas. Estes programas são introduzidos na máquina, causando todo tipo de transtorno, desde o uso indevido do sistema para infectar outros sistemas, passando pelo roubo de dados e mesmo destruição de dados.

Vírus

Vírus são programas de computador que podem infectar outros programas de computador modificando-os de forma incluir uma cópia deles mesmos. Esta definição não é unanimidade, pois outros incluem quaisquer programas que tenta esconder funções que podem vir a prejudicar o usuário, como acontece por exemplo com os “Cavalos de Tróia”. Os Vírus serão discutidos em profundidade no próximo capítulo.

Programas “Cavalo de Tróia” (Trojan Horse)

Os programas “Cavalo de Tróia” são programas que executam alguma coisa, não documentada pelo programador, mas que o usuário do computador não aprovaria se soubesse, pois significa um risco ao seu computador. Eles são forma muito comum de enganar os usuários instalando programas que abrem uma “porta” (Back Door Program) no computador, permitindo acesso remoto. Segundo alguns, os Vírus são um caso particular de “Cavalo de Tróia” capaz de transformar outros programas em “Cavalos de Tróia”.

Programas de “Porta dos Fundos” (Back Door Programs) ou de administração Remota (Remote Administration Programs)

Estes programas, por exemplo, BackOrifice, Netbus e Subseven, são utilizados para obter acesso remoto aos recursos do computador. Uma vez instalados, permitem a outra pessoa acessar e controlar seu computador.

Negação de Serviço (DoS, Denial of Service)

O ataque de DoS faz o computador cair ou então ficar tão lento que se torna impossível usá-lo. Em essência uma grande quantidade de computadores começa a fazer requisições de determinado serviço, por exemplo, páginas Web ou remessa de e-mails, que o computador não consegue atender a tempo, comprometendo o desempenho de outros serviços.

Intermediário de DoS

Invasores usualmente utilizam computadores de outras pessoas para lançar ataques DoS. Programas são instalados nestes computadores, usando “Cavalos de Tróia”, e ficam esperando determinado comando ou data para executarem o ataque DoS.

Windows: Código de Script Java, JavaScript e ActiveX

As páginas Web vem se tornando cada vez mais dinâmicas o que obriga a parte do código ser executado dentro do Browser do usuário. O Browser e os programas de e-mail, que também podem receber e-mails em formato HTML com scripts, podem desabilitar este tipo de script. Em especial merecem atenção os scripts em formato ActiveX. Estes scripts rodam nativamente no Windows, ou seja, com pleno acesso a máquina. Os scripts JavaScript, e principalmente Java, são mais protegidos.

Windows: Compartilhamentos de Rede

Os recursos compartilhados do Windows, em especial em máquinas com Windows 95, 98 e ME podem ser explorados pelos invasores como forma de infectar vários computadores em um só ataque. Os vírus do tipo Verme (Worm) são particularmente perigosos neste ambiente, pois podem facilmente infectar todas as máquinas da rede.

Windows: Ocultação de Extensões

O Windows tem a opção "Ocultar extensões de arquivos conhecidos", configurada nas "Opções de Pasta" do Internet Explorer. Esta opção, que por padrão fica habilitada, remove extensões do tipo ".EXE", ".DLL", ".DOC" e outras, dos arquivos mostrados nos programas do Windows. Infelizmente, se o usuário enviar um arquivo "CARTA.TXT.EXE" ele será mostrado como "CARTA.TXT", enganando o usuário, que ao tentar abri-lo estará na verdade executando um programa. O Outlook Express tem a opção "Não permitir que sejam abertos anexos que possam conter vírus" na parte de "Segurança", porém esta opção restringe totalmente o acesso aos anexos.

Spoofing de e-mail

"Spoofing" é a técnica de alterar o IP de origem do pacote TCP/IP enganando assim quem recebe o e-mail, fazendo-o pensar que vem de outra origem. O "Spoofing" é uma tentativa de ocultar a verdadeira origem ou então enganar o usuário, na busca de informações sigilosas, fazendo-o acreditar que determinada pessoa que ele conhece está solicitando informações.

Leitura de Pacotes TCP/IP (Packet Sniffing)

Um Leitor de Pacotes é um programa capaz de capturar e ler pacotes TCP/IP que trafegam pela rede. Grande parte dos protocolos não é segura, ou seja, não criptografam os dados enviados, permitindo assim a sua leitura. A solução para isso é a utilização de protocolos seguros como HTTPS e SSH, ou então criptografar os dados à nível de aplicação, antes de serem entregues ao TCP/IP.

Vírus

Os vírus servem para demonstrar o quanto nossos computadores são vulneráveis. Um vírus adequadamente projetado pode infectar toda a Internet, mostrando o quão sofisticados e interconectados se tornaram os seres humanos.

Tipos de Vírus

Os Vírus vem evoluindo muito nas 2 últimas décadas, mas de forma geral, existem 2 classes de vírus: Vírus de Arquivos e Vírus de Boot ou Sistema.

Os Vírus de Arquivos são aqueles que infectam programas que são de alguma forma executados pelo Sistema Operacional, como, por exemplo, “.EXE”, “.COM”, “.DLL” e mesmo arquivos de script como .VBS. Os Vírus de Arquivos podem ser de Ação Direta ou Residentes. Os de Ação Direta infectam um ou mais arquivos a cada vez que o programa que os contém é executado. Os Vírus Residentes são bem mais perigosos, pois se escondem na memória ao serem executados pela primeira vez e então infectam outros programas quando são executados ou quando determinada condição, por exemplo, uma data, é alcançada.

Os Vírus Residentes podem ainda ser divididos em Vírus de Infecção Rápida e Infecção Lenta. Os de Infecção Rápida infectam não apenas os programas que estão sendo executados, mas também os que estão sendo acessados. Assim, ao executar um programa Anti-Vírus estaremos infectando todos os programas. Os de Infecção Lenta modificam apenas os arquivos no momento em que são criados ou modificados, enganando assim algum programa Anti-Vírus também residente, fazendo-o acreditar que alteração do programa é normal.

Os Vírus de Boot ou Sistema infectam áreas do disco que não são arquivos comuns. Existe o Setor Mestre de Boot (MBR), o Setor de Boot, onde fica o código necessário a carregar o sistema operacional no momento em que o computador é ligado e a Tabela de Alocação de Disco (FAT), que mostra onde ficam armazenados os arquivos no disco. Em qualquer caso, o Vírus é executado antes da que seria normalmente executado.

De forma geral, os Vírus de Boot não são mais problema por várias razões. Os programas hoje são enormes e, usualmente, vem gravados em CD, o que impede a infecção. Antigamente os programas eram gravados e trocados em disquetes o que facilitava a infecção. Além disso, os Sistemas Operacionais modernos protegem o Setor de Boot.

Verme (Worm)

Um Verme é um programa, ou conjunto de programas, capaz de espalhar cópias de si mesmo para outros computadores, usualmente através de conexões de rede. Existem os Vermes de Computador e os de Rede. Os Vermes de Computador estão completos em determinado computador e fazem cópias completas de si para outro computador. Os Vermes de Rede consistem de vários pedaços, um em cada computador, que fazem uso da rede para se comunicarem e executar determinada tarefa.

Stealth (Furtivo)

Um Vírus Furtivo (Stealth) é capaz de esconder as modificações feitas por ele em arquivos ou na área de sistema, usualmente monitorando as funções da API do Sistema Operacional utilizadas para ler e gravar no disco, falsificando resultados. Entretanto, para que isso seja possível, o Vírus deve estar residente em memória no momento em que, por exemplo, o Anti-Vírus esteja sendo executado.

Polimórfico ou Blindado

Um Vírus Polimórfico é capaz de produzir uma cópia modificada de si mesmo. Isto é necessário porque os programas Anti-Vírus usam as seqüências de instruções do Vírus como um padrão a ser detectado dentro dos programas, para saber se estes estão infectados ou não. Se o padrão for modificado, o Vírus passa a não ser detectado. Um Vírus Polimórfico pode mudar seu padrão, por exemplo, criptografando o seu código usando uma chave aleatória ou alterando a seqüência do próprio código, incluindo instruções extras.

Vírus via e-mail

Atualmente a forma mais comum de espalhar um Vírus é através de e-mail. Usualmente os usuários estão alertas quanto a programas que são descarregados da Internet, mas nem sempre prestam atenção nos anexos de e-mails, muito em função do aumento da quantidade de e-mails e de Spams misturados a e-mails.

Vírus de Macros do MS-OFFICE

O Pacote de Aplicações MS-OFFICE da Microsoft traz embutida a linguagem de programação Visual Basic, chamada de VBA, Visual Basic for Applications. O VBA é uma linguagem de programação completa com acesso nativo a máquina, podendo, por exemplo, alterar arquivos e enviar e-mails. Além disso o MS-OFFICE, por padrão, habilita a opção "Auto Execute", ou seja, ao abrir

um arquivo do Word ou Excel que contenha uma Macro em VBA, ela será executada.

O Vírus Melissa surgido em março de 1999 era enviado via e-mail em um documento “.DOC” para uma lista de discussão. Ao ser executado na máquina do usuário que recebia o e-mail, mandava mais 50 e-mails. Com isso se tornou um dos vírus que se espalhou mais rápido na Internet. Hoje o MS-OFFICE traz a opção “Proteção de Vírus de Macro” nas suas Opções para impedir que uma Macro seja executada automaticamente.

“Logro do Vírus” (Virus Hoax)

Com a explosão da Internet se tornam cada vez mais comuns os “Logros de Vírus” na forma de e-mails. Um exemplo é um e-mail que diz que se for recebido um e-mail com determinado texto no Assunto, o disco será apagado ou algo pior.

Estratégias de Segurança

Conceitualmente existem 3 estratégias para implantar um processo de segurança da informação que busque alcançar os objetivos da Segurança da Informação:

1. **Prevenção:** Esta estratégia representa a necessidade de instalar o software e/ou hardware apropriado a tomar as devidas precauções de modo a evitar o ataque antes que ele ocorra;
2. **Deteção:** Esta estratégia representa a necessidade de manter seu sistema atualizado sobre os tipos de ataques possíveis de modo a identificar quando seu computador foi danificado ou está correndo risco de ser;
3. **Recuperação:** Esta estratégia representa a necessidade de criar um plano de ação que permita reverter, se possível, o dano causado ao seu computador e/ou aos dados.

Prevenção

Controle de Acesso

Os sistemas operacionais de última geração como Linux e Windows possibilitam definir controle de acesso dos usuários do sistema, o que permite gerenciar que terá acesso a que dados. Neste aspecto, os sistemas operacionais baseados em UNIX tem uma longa tradição, com um modelo robusto e largamente testado. Os sistemas operacionais Windows usados em estações de trabalho, como o Windows 95, 98 e ME tinham sérias limitações. O lançamento do Windows XP melhorou a situação, mas sua capacidade plena apenas é alcançada em um ambiente com um servidor de rede Windows.

O objetivo do Controle de Acesso é definir usuários ou grupos de usuários que tem acesso a determinados recursos do sistema. Daí a quase inexistência de vírus no sistema operacional Linux, pois o usuário quase sempre trabalha sem privilégios plenos.

Firewall

Firewalls (Paredes Corta-Fogo) são sistemas que protegem computadores em rede de invasões hostis que possam comprometer os princípios de Segurança da Informação. Firewalls podem ser equipamentos ou programas que são executados em computadores seguros. **Qualquer computador que seja responsável por um computador conectado a uma rede pública, deve ter certeza de ter um Firewall instalado e configurado**

Em essência, o Firewall monitora todo o tráfego entre a rede interna e a rede externa para ver se ele obedece determinado critério. Ele pode ser usado para manter um Histórico, ou Log, das conexões, autorizadas e não autorizadas, avisando quando ocorrer uma tentativa de invasão. Os Firewalls podem ser classificados em 4 tipos:

Firewall de Filtragem de Pacotes

Trabalham na camada de Internet do modelo de camadas TCP/IP, sendo usualmente parte de um Roteador. O Roteador é um dispositivo que recebe pacotes de uma rede e encaminha para outra. A Filtragem de Pacotes compara o endereço/porta de origem e o endereço/porta de destino com critérios pré-estabelecidos, permitindo ou não a passagem do pacote. A vantagem deste tipo de Firewall é a simplicidade e o pequeno impacto no desempenho da rede.

Firewall de Nível de Circuito

Trabalham na camada de Transporte do modelo de camadas TCP/IP, monitorando as sessões abertas pelos diversos protocolos segundo critérios pré-estabelecidos. São simples e baratos, mas não monitoram Pacotes.

Firewall Gateway de Aplicações

Também chamados de Proxy, são similares ao tipo anterior, mas específicos para um determinado protocolo (Ex: Proxy de HTTP, Proxy de FTP). Pacotes de entrada ou de saída não conseguem alcançar seu destino sem que haja um Proxy configurado para aquele protocolo. Podem ser usados para gerar Logs das atividades dos usuários, inclusive a nível de conteúdo, mas tem grande impacto no desempenho da rede e não são transparentes, sendo necessário uma configuração manual dos softwares clientes.

Firewall de Estado Multicamada

Este Firewall combina as funções dos 3 anteriores, sendo normalmente caro e complexo. Eles filtram pacotes na camada de Internet, determinam se as sessões são válidas e verificam o conteúdo dos pacotes na camada de aplicação.

Exemplos de programas Anti-Vírus são o **Zone Alarm**, **Norton Security** e **602 LAN Suite**, gratuito até 5 usuários.

Criptografia

Criptografia é a técnica de embaralhar dados através de um algoritmo específico e uma chave (seqüência de caracteres), evitando assim que outras pessoas tenham acesso a informação.

"Existem 2 tipos de criptografia no mundo: a criptografia que impede sua irmão menor de ler os seus arquivos e a criptografia que impede o governo de ler os seus arquivos"

Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C.

Usualmente a criptografia trabalha com 2 tipos de chaves: simétricas e assimétricas. A chave é chamada de simétrica quando é utilizada tanto para compactar quanto para descompactar os dados, devendo ser informada, de alguma forma segura, a quem recebe os dados para que este possa ter acesso a eles.

A chave é chamada de assimétrica quando utiliza 2 chaves distintas, chamadas de chave pública e chave privada. Com base em técnicas matemáticas avançadas foi criado um algoritmo que permite criptografar dados usando a chave pública, que fica de posse de qualquer um que queira enviar os dados, e descriptografar usando uma chave privada, que apenas a pessoa que recebe os dados tem. A criptografia assimétrica é utilizada, por exemplo, no protocolo HTTPS que permite ter acesso seguro a páginas HTML. Ao iniciar a comunicação com um site HTTPS o Browser e o site trocam entre si as chaves públicas.

Mesmo utilizando protocolos não seguros, ou seja, não criptografados, como SMTP, o usuário pode optar por criptografar os dados antes de enviar, por exemplo, um e-mail. Softwares, como o PGP (Pretty Good Privacy), foram desenvolvidos para isso, permitindo ao usuário utilizar o esquema de chave pública/privada. O PGP é uma técnica híbrida simétrica e assimétrica, utiliza as melhores aptidões de cada uma. Os dados a serem criptografados são inicialmente compactados e então criptografados através de um algoritmo de chave simétrica extremamente rápido, sendo a chave gerada aleatoriamente e em tempo real. Isto é feito porque os algoritmos assimétricos são muito lentos. Depois a chave simétrica é ela mesma criptografada com a chave pública e enviada juntamente com os dados criptografados. Assim alia-se o desempenho dos algoritmos de chave simétrica com a segurança dos algoritmos de chave pública.

Os Certificados de Segurança, muitas vezes visíveis no Internet Explorer são chaves públicas associados com informações de quem emitiu estas chaves,

assinados por uma empresa idônea (Ex: Verisign), fazendo com que o usuário possa confiar na sua origem.

Varredura de Portas TCP/UDP

Uma das formas mais usuais de invasão em máquinas são falhas de segurança em programas que respondem ao protocolo TCP/IP. Programas, como o **NMap**, fazem uma varredura nas portas TCP/IP de uma máquina buscando falhas de segurança.

Detecção

Anti-Vírus

Os programas Anti-Vírus se tornaram cada vez mais populares a partir da década de 90, sendo hoje indispensáveis para proteção do usuário. As principais funções que se encontra em um programa de vírus são:

- Varredura do computador no momento do Boot;
- Varredura dos arquivos sendo lidos/gravados;
- Varredura seletiva de arquivos selecionados pelo usuário;
- Atualização automática ou manual do arquivo de dados de vírus;
- Varredura de e-mails enviados ou recebidos;

Exemplos de programas Anti-Vírus são o **AVG**, **Norton Anti-Vírus** e **PC-Cylin**, sendo que o AVG, ainda, é gratuito para uso não comercial. Tão importante quanto instalar o Anti-Vírus e o configurar corretamente é atualizar o arquivo de informações de vírus, utilizado pelo programa para detectar os padrões dos vírus.

Ao ser descoberto um novo vírus, os fabricantes de programas Anti-Vírus desenvolvem uma “vacina”, e quanto mais rápido for este desenvolvimento, maior é a confiança do mercado na empresa e no software. Os milhares de vírus já conhecidos podem ser pesquisados nos sites:

Trend Micro, fabricante do PC-Cylin
www.trendmicro.com/vinfo, em Virus Encyclopedia

Grisoft, fabricante do AVG
www.grisoft.com/virus/encyclopaedia

Recuperação

Backup/Restore

O objetivo das técnicas de Segurança da Informação é garantir a integridade das informações, mas quando isso não é alcançado é necessário recorrer a Recuperação de Dados. Em essência recuperação de dados considera que são feitas cópias constantes das informações, que serão resgatadas quando ocorrer alguma perda.

O termo "Backup" se refere a gravação de cópias de informações e o termo "Restore" se refere a restauração da informação. Servidores de Bases de Dados, por exemplo, sempre possuem rotinas de Backup e Restore que podem ser programadas para fazerem o Backup automaticamente. Em essência estes programas fazem uma "fotografia" dos dados em determinado momento, guardando-os em outro lugar compactados.

Quando se trata de Servidores de Arquivos ou mesmo de Estações de Trabalho, cabe ao administrador da rede ou ao usuário da máquina definir quais arquivos devem ser copiados, o que deve ser feito com muito cuidado. Atualmente existem vários programas de Backup, como, por exemplo, o **Cobian Backup**, que rodam na retaguarda, como aplicativos ou mesmo serviços do Sistema Operacional, e que permitem programar o Backup.

Em especial, merece atenção a grande diferença entre a capacidade de armazenamento dos discos rígidos magnéticos e das mídias de Backup. A tabela abaixo mostra a capacidade atual de armazenamento de várias mídias, que em todos os casos é bem menor que os Discos Rígidos atualmente no mercado, com cerca de 80 GB de capacidade. Assim fica claro que não é possível fazer o Backup em mídia removível/não magnética de todo o conteúdo do Disco Rígido.

Mídia	Capacidade	Capacidade / HD
Disco Rígido (HD)	80 GB	1
Disco Flexível (FD)	1,44 MB	56888
CD	640 MB	125
DVD	4 GB	20
Unidade de Fita DAT	4 GB a 16 GB	20 a 5
ZIP Drive	250 MB	320