Unidade IV

4 AMEAÇAS E MECANISMOS DE ATAQUE A REDES

Como já indicado, a transmissão da informação requer atenção especial. Durante o tráfego de um ponto a outro, a informação pode ser, por exemplo, interceptada e alterada de maneira fraudulenta. Por esse motivo, as organizações precisam adotar processos que garantam a segurança da informação.

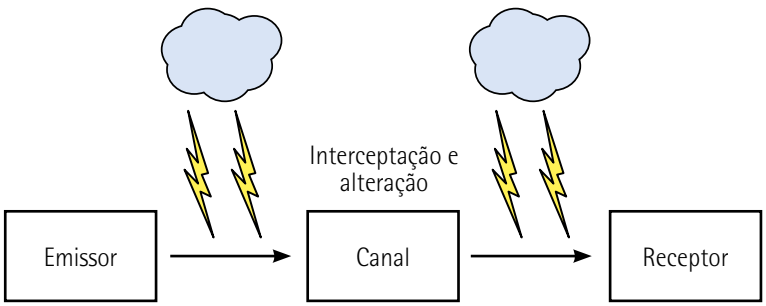

Figura 10 – Processo de adulteração da comunicação

Segundo Beal (2005), devem-se assegurar:

- **A integridade do conteúdo da mensagem**: o que é enviado pelo emissor chega ao receptor de forma completa e exata.
- **A irretratabilidade da comunicação**: o emissor ou o receptor não podem negar que a comunicação da mensagem foi bem-sucedida.
- **A autenticidade do emissor e do receptor**: o emissor e o receptor são realmente quem dizem ser no processo de comunicação.
- **A confidencialidade do conteúdo**: apenas os destinatários têm acesso ao conteúdo da informação.
- **A capacidade de recuperação do conteúdo pelo receptor**: é possível recuperar o conteúdo em sua forma original caso haja problemas na comunicação.

Quando falamos de controle de acesso lógico e de interligação em redes, os problemas de segurança se multiplicam de forma alarmante. Basta um único usuário descuidado para comprometer a segurança de uma rede inteira. No caso de redes conectadas à internet, como os equipamentos físicos se tornam lógicos no ciberespaço, a proteção física não é suficiente para garantir a segurança da informação. Nesse ambiente, multiplicam-se e potencializam-se as ameaças, tanto as externas (p. ex., invasões e ataques de negação de serviço) quanto as internas (p. ex., erros, abusos de privilégios e fraudes).

Com isso, devem-se analisar as novas tecnologias para que medidas de segurança sejam devidamente implementadas. Beal (2005, p. 92) afirma que "os controles lógicos podem ser fundamentais para adequar a organização aos seus requisitos de segurança". A fim de facilitar a implantação e o controle dos mecanismos de proteção lógica, a segmentação dos problemas em áreas pode ser uma solução.

4.1 Formas de ataque

A ausência de segurança em redes amplia os riscos para a informação, uma vez que, no processo de comunicação, é no canal de comunicação que ela fica mais exposta. Hoje em dia, as redes se confundem com o próprio negócio da organização. Assim, implantar um mecanismo de segurança para elas é fundamental.

As ameaças que exploram as vulnerabilidades das redes podem ser internas ou passivas. Nas internas, desencadeia-se um ataque que interage diretamente com o ambiente. Nas passivas, em vez de interagir com o ambiente, o ataque coleta informações sobre o alvo, pela interceptação de comunicações ou por buscas em quaisquer fontes que possam ter informações relevantes.

De acordo com o objetivo dos ataques, é possível classificá-los como de interceptação, de modificação, de interrupção ou de fabricação.

Na interceptação, o atacante se posiciona entre dois dispositivos que estão se comunicando e faz essa comunicação passar por ele. Desse modo, consegue copiar as informações transmitidas.

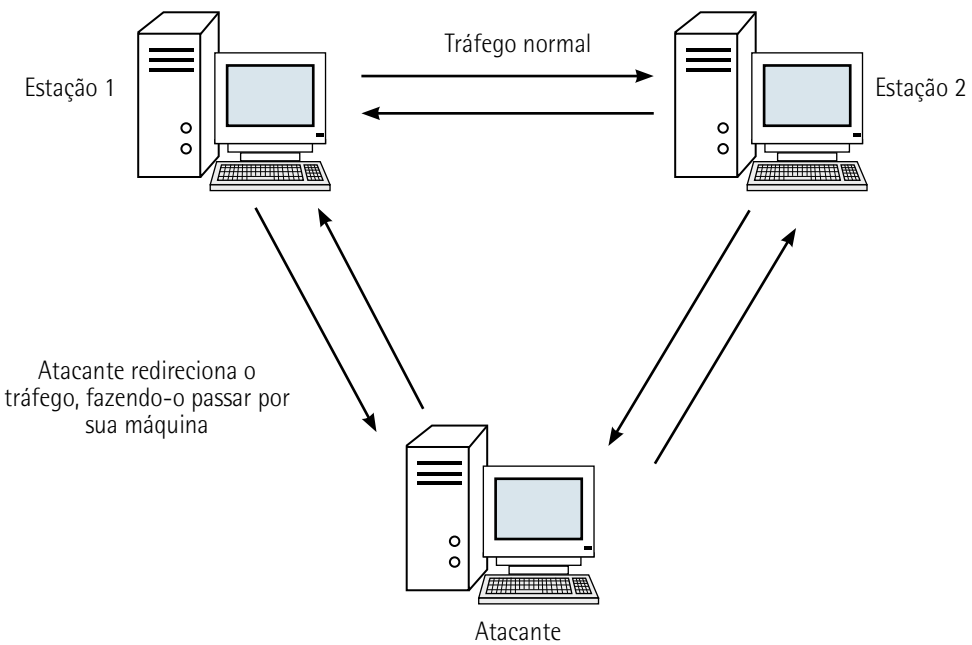

Figura 11 – Ataque de interceptação

Uma das principais formas desse tipo de ataque é o man-in-the-middle, em que o invasor, assumindo a identidade de um usuário válido, simula ser o parceiro de cada parte envolvida na conexão.

O ataque de modificação altera a comunicação entre duas partes, afetando assim a integridade das informações comunicadas naquele canal.

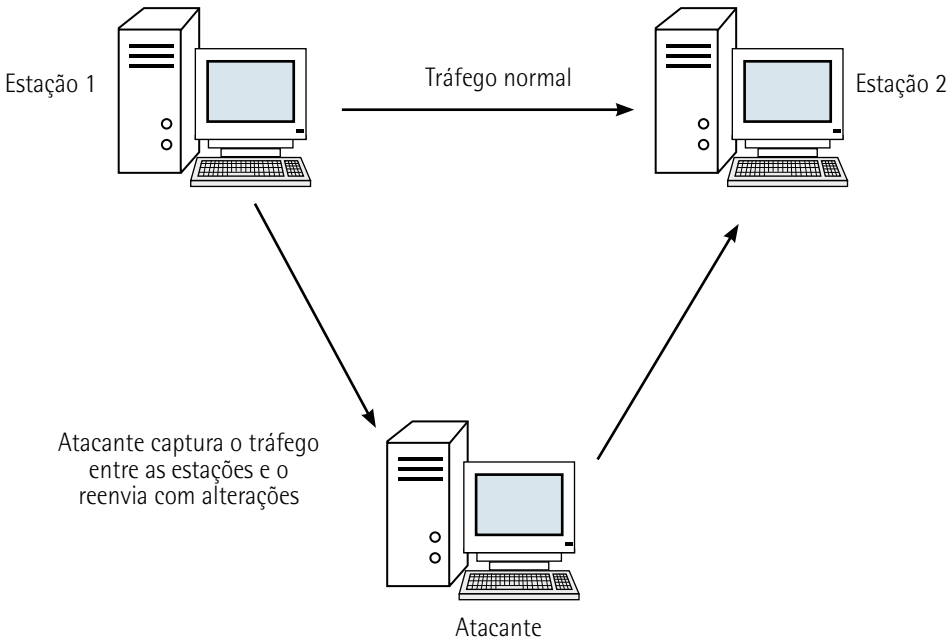

Figura 12 – Ataque de modificação

Como exemplo, pode-se citar o replay, em que parte de uma transmissão da rede é copiada e posteriormente reproduzida, simulando-se um usuário autorizado.

O ataque de interrupção acontece quando o atacante se posiciona entre as partes em comunicação e consegue que o tráfego gerado pela origem não chegue ao destino.

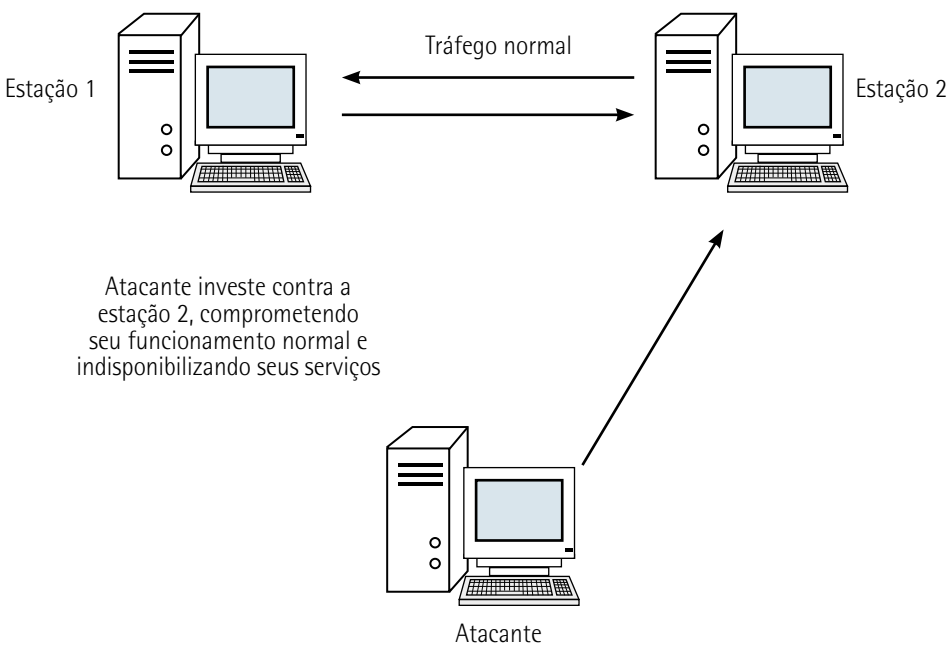

Figura 13 – Ataque de interrupção

Um exemplo desse tipo de ataque é o DoS (denial of service), o envio de requisições em massa para determinado computador, de modo que ele fique sobrecarregado, sem conseguir responder a todas elas, e o serviço pare de funcionar.

No ataque de fabricação, o atacante produz mensagens para um destino passando-se por algum outro componente.

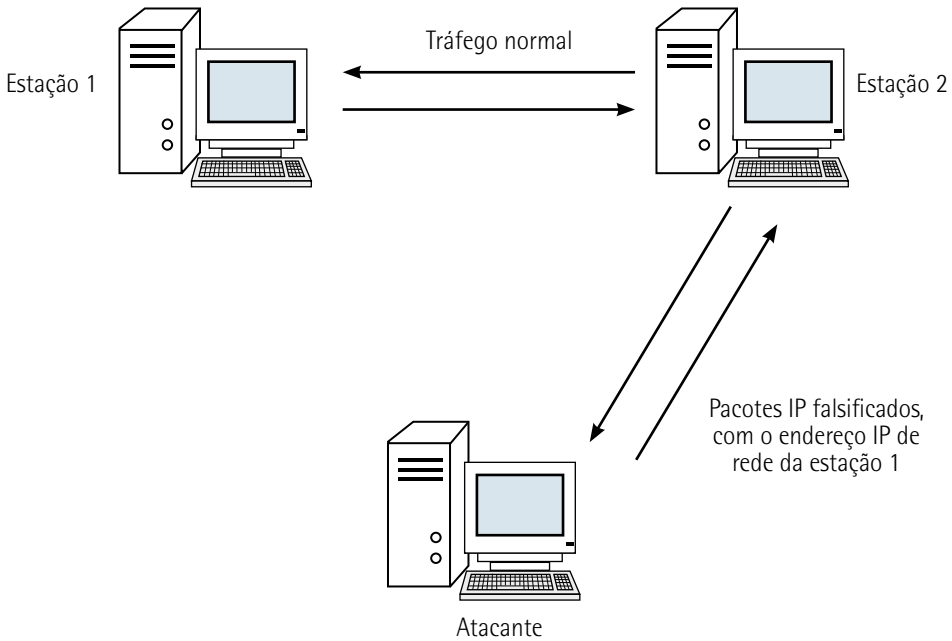

Figura 14 – Ataque de fabricação

Um meio comum de ataque de fabricação é o IP spoofing, a substituição do endereço IP do computador do invasor, fazendo-o passar por um computador confiável da rede e obter privilégios na comunicação.

4.2 Hackers e crackers

Toda organização deve preocupar-se em defender três ativos de informação em especial: seus dados, seus recursos e sua reputação diante dos clientes e do mercado.

A fim de conseguir mais eficácia na utilização dos recursos tecnológicos para a segurança da informação, as vulnerabilidades e as ameaças devem estar bem definidas na mente dos profissionais de TI e de segurança da informação.

Como vimos, vulnerabilidades são falhas no projeto ou na implementação de um software ou sistema operacional, as quais, quando exploradas por um atacante, permitem violar a segurança de um computador.

As ameaças, por sua vez, ao contrário das vulnerabilidades, que podem ser sanadas ou minimizadas, são constantes: estão sempre à espreita, procurando vulnerabilidades para concretizar um ataque. Mas quem é o agente que utiliza as ameaças?

Hackers são pessoas intensamente interessadas nos trabalhos misteriosos e esotéricos de qualquer sistema operacional de computador. Em geral, são programadores e têm conhecimento avançado de sistemas operacionais e linguagens de programação. Podem identificar brechas em sistemas e as razões para a existência delas. Os hackers buscam constantemente mais conhecimento, compartilham livremente o que descobriram e jamais corrompem dados de maneira intencional.

Crackers são pessoas que violam a integridade de um sistema de máquinas remotas com intenção maliciosa. Tendo obtido acesso não autorizado, eles causam vários problemas para o alvo, como a destruição de dados vitais e a negação de serviços a usuários legítimos. Os crackers são facilmente identificados pela motivação de suas ações.

Observação

Vale lembrar que, no mundo real, a delimitação entre hacker e cracker é bem mais complicada do que na teoria.

A invasão praticada por um cracker pode ser de vários tipos. Alguns exemplos:

- O invasor ganha acesso e nada mais (acesso aqui entendido como entrada simples, não autorizada, numa rede que requer, no mínimo, login e senha).
- O invasor ganha acesso e altera, corrompe ou destrói dados.
- O invasor ganha acesso e toma controle de parte do sistema ou do sistema inteiro, podendo negar acesso até a usuários privilegiados.
- O invasor não ganha acesso; em vez disso, forja mensagens para o sistema atacado. Isso costuma ser feito para enviar correio não solicitado ou fazer inundação (spam).
- O invasor não ganha acesso; em vez disso, implementa procedimentos maliciosos, que fazem a rede falhar, reinicializar, travar ou manifestar uma condição inoperável, temporária ou permanentemente.

Técnicas modernas tornaram a atividade do cracker mais difícil, mas não impossível. De fato, eles têm hoje acesso a uma grande variedade de informações sobre segurança, muitas das quais estão livremente disponíveis na internet. No entanto, o conhecimento de crackers e de especialistas de segurança é cada vez menos desproporcional.

4.3 Ferramentas de ataque

Para concretizar um ataque, os crackers necessitam utilizar ferramentas que auxiliem na ação contra redes e computadores. A essas ferramentas damos o nome de **dispositivos destrutivos**, programas que permitem incomodar ou destruir dados.

Dispositivos destrutivos são geralmente empregados por usuários imaturos, por funcionários descontentes ou por crianças.

A maioria dos dispositivos destrutivos não representa riscos de segurança, mas aborrecimentos. Entretanto, esses programas podem ocasionalmente ameaçar a capacidade de uma rede funcionar de maneira adequada. Por exemplo, um programa que expõe um roteador ou um servidor de correio a um ataque contínuo de recusa de serviço pode constituir um risco de segurança. Até o fim desse ataque, os usuários legítimos serão incapazes de acessar recursos valiosos da rede. Enquanto o ataque não resulta em acordo de sistema, ele rompe operações do sistema. Por causa disso, cada novo administrador de sistema deveria aprender sobre recusa de serviço e dispositivos destrutivos em geral.

Podemos destacar três dispositivos destrutivos importantes:

- bombas de correio eletrônico e listas de mala direta;
- negação de ferramentas de serviço;
- softwares maliciosos.

4.3.1 Bombas de correio eletrônico e listas de mala direta

As bombas de correio eletrônico raramente culminam em perda de dados ou brecha de segurança, mas são ferramentas que incomodam e atrapalham a disponibilidade da informação.

Uma bomba tradicional de correio eletrônico é simplesmente uma série de mensagens (talvez milhares) enviadas para uma caixa de correio com o objetivo de inundá-la com lixo. A maioria dos usuários de internet recebe uma bomba de correio eletrônico dentro de um ano de conexão on-line. O atacante costuma ser alguém com quem se discordou num fórum de discussão. O tamanho médio de uma bomba de correio eletrônico é de 2 MB. Esse dispositivo pode produzir aumento de encargos de conexão e desperdício de tempo, atacando a disponibilidade das informações.

Pacotes de bomba de correio eletrônico são programas que automatizam o processo. Os administradores de rede devem estar cientes desses pacotes e dos nomes de arquivo associados a eles. Embora esse conhecimento não impeça ataques ao seu sistema, ele pode impedir que seus usuários ataquem outros sistemas e redes.

Esquemas de exclusão, destruição de arquivos e filtros de correio são formas de evitar bombas de correio eletrônico.

Há várias maneiras de implementar um esquema de exclusão. Se alguém começar a bombardeá-lo, você pode, por exemplo, tentar uma abordagem humana e entrar em contato com o postmaster dele. Isso geralmente funciona. O usuário é alertado de que esse comportamento não será tolerado. Alguns provedores são até bastante enérgicos para que a história termine por ali mesmo.

Outra solução é um pouco meticulosa, mas funciona bem e pode ser automatizada. Escreva um script que capture o endereço de correio eletrônico ofensivo. Para cada mensagem recebida, autorresponda com uma recomendação gentil, de dez páginas, sobre como tais ataques violam políticas de uso aceitáveis e, sob certas circunstâncias, violam a lei. Depois que a parte ofensiva receber muitos retornos dessa natureza, o provedor dela enlouquecerá e lhe negará acesso.

Observação

Nem todos os provedores de acesso são responsáveis. Alguns não se importam se os usuários estão bombardeando o correio eletrônico de outros. Se você se encontrar nessa situação, procure a justiça.

Como ataques através de bombas de correio eletrônico podem resultar em queda do serviço, é muito comum que ocorram para impedir o acesso dos usuários as suas mensagens. Caso passe por esse tipo de ataque, entre em contato com as autoridades. Isso é especialmente aplicável quando o atacante varia sua origem, escapando de filtros de correio ou esquemas de exclusão no nível do roteador.

Existem pacotes de bomba de correio eletrônico que automatizam o processo de inscrição em mala direta. Os resultados dessa vinculação podem ser desastrosos. A maioria das listas de mala direta gera pelo menos cinquenta mensagens de correio diárias, algumas das quais incluem anexos binários. Se o atacante o vincular a cem listas, você receberá 5 mil mensagens por dia. Uma forma de sanar o problema é desvincular-se dessas listas. Essa atitude, porém, não é tão simples quanto parece. Uma razão é que novas listas raramente incluem instruções sobre como cancelar a inscrição. Assim, você pode ser forçado a rastrear essas informações na web e, com isso, o tempo de paralisação pode durar várias horas.

A capacidade de cancelar rápida e efetivamente a inscrição em todas as listas também dependerá de seu pacote de correio eletrônico. Se o cliente de correio eletrônico tiver funções poderosas de pesquisa, que permitam varrer assuntos e títulos de remetente, você poderá reunir os endereços de servidor de lista em pouco tempo. Entretanto, se o cliente de correio eletrônico não tiver funções estendidas de pesquisa, você enfrentará uma batalha árdua. Se estiver atualmente nessa situação, inscrito em muitas listas, o recomendado é obter um novo endereço de correio eletrônico e eliminar o antigo.

Outra questão que irrita muitos administradores é o **relay de correio eletrônico**, em que clientes conectados a outros provedores utilizam seu servidor para correio eletrônico. Esse procedimento permite a usuários com endereços IP diferentes utilizar seus serviços de correio eletrônico (em vez de apenas aqueles endereços em sua rede ou em sua sub-rede). Como consequência, spammers e outros bottom-feeders (alimentadores de lixo) sequestram parte de seu sistema e o utilizam para poluir a internet com junk mail. A única forma de contornar essa situação é filtrar por endereço IP, fechando redes indesejáveis.

4.3.2 Negação de ferramentas de serviço

Os ataques de recusa de serviço (DoS) são muito mais perigosos que as bombas de correio eletrônico, em especial para redes corporativas e provedores de acesso. Isso porque esses ataques podem temporariamente incapacitar sua rede inteira ou, pelo menos, os hosts baseados em TCP/IP (transmission control protocol/internet protocol).

O primeiro ataque de DoS de importância foi o Morris worm. Estima-se que cerca de 5 mil máquinas foram tiradas de serviço durante várias horas. Na época (novembro de 1988), foi um desastre para centros acadêmicos de pesquisa, mas teve pouco impacto no restante do mundo. Hoje, um ataque de DoS similar poderia levar à perda de milhões de dólares.

O objetivo de um ataque de DoS é simples: arremessar seu host fora da internet. Exceto quando especialistas de segurança conduzem testes de DoS contra a própria rede (ou outros hosts que consentem nisso), os ataques de DoS são sempre maliciosos. Não há razão legítima para qualquer pessoa incapacitar a própria rede. Ataques de DoS são ilegais sob uma variedade de leis estaduais e federais. Se rastrear alguém promovendo ataques de DoS contra sua rede, alerte as autoridades. Ataques de DoS não são práticas de hackers curiosos; são atos criminosos, feitos com intenções hostis.

Ataques de DoS atingem o núcleo das implementações de IP. Portanto, podem aflorar em qualquer plataforma. Pior ainda: como as implementações de IP não são drasticamente diferentes de plataforma para plataforma, um único ataque de DoS pode trabalhar em vários sistemas operacionais. Além disso, como mostram análises de versões de código de DoS, uma vez que um novo ataque estiver em andamento, ele provavelmente funcionará em quase todas as plataformas, ainda que isso não ocorra num primeiro momento.

Novas versões de ataque de DoS são lançadas aproximadamente a cada duas semanas. Essas versões geralmente são gravadas numa plataforma. Assim que o código é lançado, ele é examinado por comunidades de hackers e crackers. Em poucos dias, alguém lança uma versão modificada (uma mutação), que pode incapacitar uma variedade mais ampla de sistemas operacionais.

Ataques de DoS devem ser levados a sério. Até crackers com mínima perícia em programação podem implementá-los com facilidade. Infelizmente, por não entenderem a recusa de serviço como uma questão crucial, órgãos policiais são, às vezes, reticentes em seguir esses ataques, mesmo quando se sabe quem é o responsável por eles.

4.3.3 Softwares maliciosos

O **vírus** de computador, o mais conhecido dos softwares maliciosos (malwares), é também o dispositivo destrutivo mais perigoso. Não há nenhum mistério quanto à razão disso. Além de poder destruir dados e causar recusa de serviço, alguns vírus (embora em número muito limitado) podem incapacitar completamente uma máquina.

Os vírus representam um risco especial à segurança na internet, porque são mais perigosos quando liberados em ambientes de rede.

Um vírus de computador é um programa que se anexa aos arquivos da máquina-alvo. Esse procedimento é denominado **infecção**. Quando um arquivo é infectado, ele é convertido de arquivo comum a portador. Desse ponto em diante, o arquivo infectado infecta outros arquivos. Por meio desse processo, chamado de **replicação**, os vírus espalham-se numa unidade de disco rígido, alcançando infecção sistêmica. Frequentemente, há pouco aviso antes de a infecção sistêmica se instalar. Assim, quando há algum aviso, já é muito tarde.

O vírus embute uma cópia de si mesmo num programa ou arquivo, o qual, quando executado, também executa o vírus, desencadeando o processo de infecção. Ao assumir o controle de um computador, o vírus pode fazer de tudo, desde mostrar uma mensagem de "Feliz aniversário" até alterar ou destruir programas e arquivos do disco.

Para haver infecção por um vírus de computador, é preciso que, de alguma maneira, um programa previamente infectado seja executado. Isso pode ocorrer de diversas formas. Por exemplo: ao abrir arquivos anexados a um e-mail; ao abrir arquivos guardados em outros computadores, através do compartilhamento de recursos; ao instalar programas de procedência duvidosa ou desconhecida, obtidos pela internet ou armazenados em pendrives, cartões de memória ou mídias magnéticas.

Uma infecção por vírus também pode acontecer sem que o usuário perceba. Alguns vírus procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Outros ficam inativos em certos períodos, entrando em atividade em datas específicas ou quando acionados por seus programadores (redes zumbis).

Um veículo de grande capacidade para propagar um vírus é o e-mail, em que normalmente é recebido como um arquivo anexado a uma mensagem de correio eletrônico. O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, o que fará o vírus ser executado. Quando esse tipo de vírus entra em ação, além de infectar arquivos e programas, ele envia cópias de si mesmo para todos os contatos encontrados nas listas de endereços de e-mail armazenadas no computador. É importante ressaltar que esse tipo de vírus não é capaz de se propagar automaticamente; o usuário precisa executar o arquivo anexado que contém o vírus, ou o programa de e-mail precisa estar configurado para autoexecutar arquivos anexados.

As macros podem ser outro mecanismo de infecção. Uma macro é um conjunto de comandos armazenados em algum aplicativo a fim de automatizar tarefas repetitivas. Um exemplo seria, num editor de textos, uma macro com a sequência de passos necessários para imprimir um documento com orientação retrato e escala de cor em tons de cinza. Um vírus de macro é escrito com o intuito de explorar essa facilidade de automatização e inserido num arquivo normalmente manipulado por algum aplicativo que utiliza macros. Para que o vírus seja executado, o arquivo que o contém precisa ser aberto. A partir daí, o vírus executa uma série de comandos automaticamente e infecta outros arquivos no computador.

Existem aplicativos que têm arquivos-base (modelos), os quais são abertos sempre que o aplicativo é executado. Caso um arquivo-base seja infectado por um vírus de macro, toda vez que o aplicativo for executado, o vírus também o será.

Arquivos nos formatos gerados pelos aplicativos Word, Excel, PowerPoint e Access são os mais suscetíveis a esse tipo de vírus; arquivos nos formatos RTF e PDF, por sua vez, são menos suscetíveis, o que não significa que não possam conter vírus.

Os malwares englobam os vírus, mas existem variações de formato e de atuação desses softwares maliciosos. Veja os quadros a seguir.

Quadro 18 – Tipos de software malicioso

Tipo	Descrição
Vírus	Programa que infecta e se propaga por outros programas, podendo destruí-los. Requer execução.
Trojan (cavalo de Troia)	Programa que, além das funções para as quais foi aparentemente projetado, também executa outras funções, em geral maliciosas e sem o conhecimento do usuário.
Worm	Programa que propaga cópias de si mesmo automaticamente. Não requer execução.
Ad-Aware	Programa que executa ações danosas e atividades maliciosas em um computador.
Backdoor	Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.
Bot	Programa que dispõe de mecanismos que permitem ao invasor controlá-lo remotamente.
Spyware	Programa que monitora as atividades de um sistema e envia as informações coletadas para terceiros.
Rootkit	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso num computador comprometido.
Phishing	Tipo de fraude em que um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social, enviados para o e-mail da vítima.
Smishing	Tipo de fraude em que um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social, enviados para o dispositivo móvel da vítima.
Ransomware	Tipo de código malicioso que torna inacessíveis os dados armazenados num equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso do usuário.

Adaptado de: CGI.br (2012, p. 24-30).

Quadro 19 – Comparativo entre códigos maliciosos

Códigos maliciosos							
	Vírus	Worm	Bot	Trojan	Spyware	Backdoor	Rootkit
Como é obtido							
Pela rede		✓	✓				
Por e-mail	✓	✓	✓	✓	✓		
Por download em sites da internet	✓	✓	✓	✓	✓		
Pelo compartilhamento de arquivos	✓	✓	✓	✓	✓		
Pelo uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Pelas redes sociais	✓	✓	✓	✓	✓		
Por mensagens instantâneas	✓	✓	✓	✓	✓		
Pela ação de um invasor		✓	✓	✓	✓	✓	✓

Pela ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação							
Pela execução de um arquivo infectado	✓						
Pela execução explícita do código malicioso		✓	✓	✓	✓		
Pela execução de outro código malicioso						✓	✓
Pela exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga							
Pela inserção de uma cópia de si mesmo em arquivos	✓						
Pelo envio automático de uma cópia de si mesmo pela rede		✓	✓				
Pelo envio automático de uma cópia de si mesmo por e-mail		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns							
Alterar e/ou remover arquivos	✓			✓			✓
Consumir uma grande quantidade de recursos		✓	✓				
Furtar informações sensíveis			✓	✓	✓		
Instalar outros códigos maliciosos		✓	✓	✓			✓
Possibilitar o retorno do invasor						✓	✓
Enviar spam e phishing			✓				
Desferir ataques na internet		✓	✓				
Procurar manter-se escondido	✓				✓	✓	✓

Adaptado de: CGI.br (2012, p. 31).

Worm (verme) é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Ao contrário do que ocorre com o vírus, o worm não necessita ser explicitamente executado para se propagar; antes, ele explora vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Em geral, o worm não tem as mesmas consequências de um vírus (infecção de programas e arquivos, destruição de informações etc.). Isso não quer dizer que não represente uma ameaça à segurança de um computador ou que não cause danos.

Worms são 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 mesmos que costumam propagar. Além disso, podem gerar transtornos para os que recebem essas cópias.

Às vezes, um atacante quer garantir uma forma de retornar a um computador comprometido sem precisar recorrer ao método usado na invasão. Na maioria dos casos, a intenção dele é retornar sem ser notado. Aos programas de retorno a um computador comprometido, utilizando serviços criados ou modificados para esse fim, dá-se o nome de **backdoors**.

As formas mais comuns de incluir um backdoor são a adição de um novo serviço ou a substituição de determinado serviço por uma versão alterada, normalmente com recursos que permitem o acesso remoto (através da internet). Outra forma é por meio de pacotes de software, como o Back Office e o NetBus, conhecidos por disponibilizar backdoors nos computadores em que são instalados.

Observação

O Back Office é um programa desenvolvido pela Microsoft que permite o acesso remoto. O NetBus é um sistema de administração remoto.

Alguns fabricantes incluem backdoors em seus produtos (softwares, sistemas operacionais) alegando necessidades administrativas. No entanto, mesmo que os backdoors sejam incluídos por fabricantes conhecidos, eles ainda constituem uma séria ameaça à segurança de um computador. Todos os sistemas operacionais podem ter backdoors inclusos.

Conta a mitologia que o cavalo de Troia foi uma grande estátua usada pelos gregos para obter acesso à cidade de Troia. A estátua foi recheada com soldados, os quais, durante a noite, abriram os portões da cidade, possibilitando a entrada dos gregos e a dominação de Troia. Daí surgiram as expressões **presente de grego** e **cavalo de Troia**.

Para a área de TI, um cavalo de Troia (Trojan horse) é um programa que, além das funções para as quais foi aparentemente projetado, também executa outras funções, em geral maliciosas e sem o conhecimento do usuário. Algumas funções maliciosas que podem ser executadas por um cavalo de Troia:

- alteração ou destruição de arquivos;
- furto de senhas e outras informações sensíveis, como número de cartão de crédito;
- inclusão de backdoors para um atacante ter total controle sobre o computador.

Um cavalo de Troia se distingue de um vírus ou de um worm por não se replicar, por não infectar outros arquivos e por não propagar cópias de si mesmo de forma automática. Costuma ser um único arquivo, que necessita ser explicitamente executado.

Em alguns casos, um cavalo de Troia pode conter um vírus ou um worm. Mesmo nesses casos, porém, é possível distinguir as ações decorrentes da execução do cavalo de Troia propriamente dito daquelas relacionadas ao comportamento de vírus e worms.

O cavalo de Troia, em geral, vem anexado a um e-mail ou está disponível em algum site da internet. Em programas de e-mail configurados para executar automaticamente arquivos anexados às mensagens, o simples fato de ler a mensagem já é suficiente para executar o anexo.

Os exemplos mais comuns de cavalos de Troia são programas recebidos ou acessados por um site que dizem ser jogos ou protetores de tela.

Spyware é um software malicioso que, uma vez instalado no computador, monitora as atividades dos usuários, coletando informações (senhas, logins, números de documentos) e enviando-as para terceiros.

Phishing é um golpe em que o fraudador envia mensagens em nome de instituições oficiais com o objetivo de induzir o acesso a páginas falsas. Para tanto, utilizam-se imagens, textos e links reais para instalar um programa que tenta furtar dados pessoais e financeiros do usuário, ou induzir a vítima a fornecer esses dados.

Boatos (hoaxes) são e-mails com conteúdo alarmante ou falso, que geralmente apontam como autor da mensagem uma instituição, uma empresa importante ou um órgão governamental. Uma leitura minuciosa desse tipo de e-mail permite identificar em seu conteúdo elementos absurdos e, muitas vezes, sem sentido. Entre os diversos boatos típicos que chegam às caixas postais de usuários conectados à internet, é possível citar: correntes ou pirâmides; pessoas ou crianças que estão prestes a morrer de câncer; países oferecendo elevadas quantias em dinheiro e pedindo a confirmação do usuário, ou solicitando algum dinheiro para efetuar a transferência. Histórias como essas são criadas não só para espalhar desinformação na internet, mas também para outros fins maliciosos.

Normalmente, o objetivo do criador de um boato é verificar o quanto ele se propaga pela internet e por quanto tempo permanece se propagando. De modo geral, os boatos não são responsáveis por grandes problemas de segurança, a não ser ocupar espaço na caixa de e-mail dos usuários. Mas podem existir casos com consequências mais sérias. Por exemplo, boatos que procuram induzir usuários de internet a fornecer informações importantes (como números de documentos, de contas-correntes ou de cartões de crédito), ou que indicam uma série de ações a serem realizadas pelos usuários e que, se forem realmente efetivadas, podem resultar em danos mais sérios (como instruções para apagar um arquivo que supostamente contém um vírus, mas que na verdade é parte importante do sistema operacional instalado no computador). Além disso, e-mails de boatos podem conter vírus ou cavalos de Troia anexados.

Vale ressaltar que um boato pode ainda comprometer a credibilidade e a reputação tanto da pessoa ou entidade referenciada como criadora dele quanto daqueles que o repassam.

Os boatos costumam propagar-se pela boa vontade e pela solidariedade de quem os recebe. Muitas vezes, isso ocorre porque aqueles que os recebem confiam no remetente da mensagem, não verificam a procedência dela ou não checam a veracidade de seu conteúdo.

Para evitar a distribuição de boatos, é muito importante conferir a procedência dos e-mails. Mesmo que tenham como remetente alguém conhecido, é preciso certificar-se de que a mensagem não é um boato

Spam é o termo usado para referir-se a e-mails não solicitados, geralmente enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem também é chamado de UCE (unsolicited commercial e-mail).

Os usuários de serviços de correio eletrônico podem ser afetados de diversas formas pelos spams. Alguns exemplos:

- **Não recebimento de e-mails**: boa parte dos provedores de internet limita o tamanho da caixa postal do usuário em seu servidor. Se o número de spams recebidos é muito grande, o usuário corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isso ocorrer, todas as mensagens enviadas a ele, a partir desse momento, serão devolvidas ao remetente, e o usuário não conseguirá mais receber e-mails até liberar espaço na caixa postal.

- **Gasto desnecessário de tempo**: para cada spam recebido, o usuário necessita gastar determinado tempo para lê-lo, identificá-lo e removê-lo.

- **Aumento de custos**: independentemente do tipo de acesso à internet utilizado, quem paga a conta pelo envio do spam é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à internet, cada spam representa alguns segundos a mais de ligação para pagar.

- **Perda de produtividade**: para quem utiliza o e-mail como ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à leitura de e-mails, além de haver a chance de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.

- **Recebimento de conteúdo impróprio**: como a maior parte dos spams são enviados para conjuntos aleatórios de endereços de e-mail, não há como prever se uma mensagem com conteúdo impróprio será recebida. Os casos mais comuns são de spams com conteúdo pornográfico.

Para empresas e provedores, os problemas também são inúmeros, e muitas vezes o custo adicional causado pelo spam é transferido para a conta a ser paga pelos usuários. Alguns problemas enfrentados pelos provedores e empresas:

- **Impacto na banda**: o volume de tráfego gerado por spams obriga empresas e provedores a aumentar a capacidade de seus links de conexão com a internet. Como o custo dos links é alto, isso diminui os lucros do provedor e pode se refletir em aumento do custo para o usuário.

- **Má utilização dos servidores**: os servidores de e-mail dedicam boa parte de seu tempo de processamento para tratar das mensagens não solicitadas. Além disso, o espaço em disco ocupado por essas mensagens é considerável.

- **Perda de clientes**: os provedores muitas vezes perdem clientes que se sentem afetados pelos spams que recebem ou pelo fato de terem seus e-mails filtrados por causa de outros clientes que enviam spam.

- **Aumento de custos**: para lidar com todas as dificuldades causadas por spams, os provedores necessitam contratar mais técnicos especializados e acrescentar sistemas de filtragem de spam, que implicam a compra de novos equipamentos. Como consequência, os custos do provedor aumentam.

Existem basicamente dois tipos de software para barrar spams: aqueles que são instalados nos servidores e filtram os e-mails antes que cheguem ao usuário, e aqueles que são instalados nos computadores dos usuários e filtram os e-mails com base nas regras individuais de cada usuário.

Pode-se combater o spam da seguinte forma:

- Considere utilizar um software de filtragem de e-mails.
- Verifique com o provedor ou com o administrador da rede se é utilizado algum software de filtragem no servidor de e-mails.
- Evite responder a um spam ou enviar um e-mail solicitando a remoção da lista.

Saiba mais

Em sua essência, os spams não representam ameaça à segurança da informação. Para mais informações, consulte o capítulo 5 da *Cartilha de Segurança para Internet*:

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.BR). *Cartilha de segurança para internet*. São Paulo, 2012. p. 33-37. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 5 jul. 2018.

4.4 Detecção e proteção

Antivírus são programas que procuram detectar e anular (ou remover) vírus de um computador. Quanto às funcionalidades de um bom antivírus, podem ser destacadas:

- a identificação e a eliminação da maior quantidade possível de vírus;
- a análise de arquivos obtidos pela internet;
- a verificação contínua de discos rígidos, pendrives e CDs, de forma transparente ao usuário;
- a procura por vírus e cavalos de Troia em arquivos anexados a e-mails.

Uma dica útil é criar, sempre que possível, um pendrive ou CD de verificação (disco de boot), que possa ser usado caso um vírus desative o antivírus instalado no computador.

Alguns antivírus, além das funcionalidades mencionadas, permitem verificar e-mails enviados, podendo detectar e barrar a propagação de vírus e worms.

O bom uso de um antivírus envolve estes procedimentos:

- Mantenha-o sempre atualizado, a fim de que possa detectar as ameaças mais recentes.
- Configure-o para verificar automaticamente arquivos anexados a e-mails e obtidos pela internet.
- Configure-o para verificar automaticamente mídias removíveis (CDs, pendrives etc.).
- Configure-o para verificar todo e qualquer formato de arquivo (qualquer tipo de extensão de arquivo).
- Se possível, crie um pendrive ou CD de verificação e utilize-o esporadicamente, ou quando seu computador estiver apresentando um comportamento anormal (mais lento, gravando ou lendo o disco rígido fora de hora etc.).
- Confirme a procedência de versões gratuitas de antivírus e certifique-se de que o fabricante é confiável.

Algumas medidas de prevenção contra a infecção por vírus:

- Instale e mantenha atualizado um bom programa antivírus.
- Desabilite no seu programa de e-mail a autoexecução de arquivos anexados às mensagens.
- Não execute ou abra arquivos recebidos por e-mail, mesmo que venham de pessoas conhecidas. Se isso for inevitável, certifique-se de que o arquivo foi verificado pelo programa antivírus.
- Não abra arquivos ou execute programas de procedência duvidosa ou desconhecida. Caso você conheça a procedência deles e queira abri-los ou executá-los, certifique-se de que foram verificados pelo programa antivírus.
- Procure utilizar, no caso de arquivos de dados, formatos menos suscetíveis à propagação de vírus, como RTF e PDF. Evite, no caso de arquivos comprimidos, o formato executável. Use o próprio formato compactado – por exemplo, ZIP ou GZ.

A presença de um cavalo de Troia num equipamento ou numa rede também pode ser detectada com a utilização de um bom programa antivírus (desde que seja atualizado regularmente). Vale lembrar, porém, que nem sempre o antivírus será capaz de detectar ou remover os programas deixados por cavalos de Troia, em especial se esses programas forem mais recentes que a versão do antivírus.

As principais medidas preventivas contra a instalação de cavalos de Troia são semelhantes às empregadas contra a infecção por vírus. Também é possível usar um firewall pessoal nas estações de trabalho, a fim de tentar bloquear o recebimento de cavalos de Troia.

Um antivírus não consegue impedir que um atacante tente explorar vulnerabilidades, nem evitar o acesso não autorizado a um backdoor instalado num computador.

Vulnerabilidades em softwares podem representar um risco à segurança da informação. Nesse caso, recomenda-se o acesso a sites que mantêm listas atualizadas de vulnerabilidades em softwares e sistemas operacionais. Alguns desses sites são <http://www.cert.org/> e <http://cve.mitre.org/>. Fabricantes também costumam manter páginas na internet com considerações a respeito de possíveis vulnerabilidades em seus softwares.

A melhor forma de evitar que o sistema operacional e os softwares instalados num computador tenham vulnerabilidades é mantê-los sempre atualizados. Muitas vezes, diante da descoberta de alguma vulnerabilidade, os fabricantes disponibilizam não uma nova versão do software, mas uma correção específica (patch). É extremamente importante que você, além de manter o sistema operacional e os softwares atualizados, instale os patches sempre que forem disponibilizados.

Observação

Em certos casos, os patches são chamados de hotfixes ou service packs.

Detectar a presença de worms num computador não é uma tarefa fácil. Muitas vezes, eles realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento. Alguns antivírus até permitem detectar a presença de worms e impedir que eles se propaguem, mas isso nem sempre é possível. Portanto, para se proteger dessa ameaça, além de utilizar um bom antivírus, é importante que o sistema operacional e os softwares instalados em seu computador não tenham vulnerabilidades, pois é por meio delas que o worm se propaga.

Outra medida preventiva é instalar nos computadores um firewall pessoal. Se bem configurado, ele pode evitar que um worm explore vulnerabilidades num serviço disponível nos computadores. Em alguns casos, mesmo que o worm já esteja instalado no computador, o firewall pode evitar que ele explore vulnerabilidades em outros computadores.

Embora os programas antivírus não sejam capazes de descobrir backdoors num computador, as medidas preventivas contra a infecção por vírus são válidas para evitar algumas formas de instalação de backdoors. A ideia é que não sejam executados programas de procedência duvidosa ou desconhecida, recebidos por e-mail ou obtidos na internet. A execução desses programas pode resultar na instalação de um backdoor.

Caso seja necessário usar algum programa de administração remota, certifique-se de que ele esteja bem configurado, a fim de evitar que seja utilizado como backdoor. O emprego de um firewall pessoal é outra medida preventiva. Apesar de não eliminar os backdoors, se bem configurado, ele pode ser útil para amenizar o problema, barrando a conexão entre invasores e backdoors. Também é importante visitar constantemente sites de fabricantes e verificar a existência de novas versões ou patches para o sistema operacional ou software instalado em seu computador.

Grande parte dos problemas de segurança envolvendo e-mails relaciona-se ao conteúdo das mensagens, o qual normalmente abusa de técnicas de engenharia social ou de características de

determinados programas de e-mail, que permitem abrir arquivos ou executar programas anexados às mensagens automaticamente.

Algumas dicas de configuração para melhorar a segurança do programa de e-mail:

- Desligue as operações que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens.
- Desligue as operações de execução de JavaScript e de programas Java.
- Desligue, se possível, o modo de visualização de e-mails no formato HTML.

Observação

Java é uma linguagem orientada a objetos.

Essas configurações podem evitar que seu programa de e-mail propague automaticamente vírus e cavalos de Troia. Há, porém, programas de e-mail que não implementam essas funções.

Algumas medidas preventivas que minimizam os problemas ligados a e-mails:

- Mantenha seu programa de e-mail sempre atualizado.
- Evite abrir arquivos ou executar programas anexados a e-mails sem antes verificá-los com um antivírus.
- Desconfie sempre de arquivos anexados às mensagens, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado e o arquivo anexo ser, por exemplo, um vírus ou um cavalo de Troia.
- Faça o download de programas diretamente do site do fabricante.
- Desconfie de e-mails pedindo urgência na instalação de aplicativos ou correções de determinados defeitos de um software que você utiliza. Caso receba esse tipo de mensagem, entre em contato com os distribuidores do software para certificar-se sobre a veracidade dela.

Utilizar um browser também tem seus riscos. Entre eles, podem-se citar:

- a execução de JavaScript ou de programas Java hostis;
- a execução de programas ou controles ActiveX hostis;

- a obtenção e a execução de programas hostis em sites não confiáveis;
- a realização de transações comerciais ou bancárias via web, sem qualquer mecanismo de segurança.

Observação

Browsers são os programas que permitem navegar na internet. Entre os mais conhecidos, estão o Mozilla Firefox, o Google Chrome e o Internet Explorer.

Normalmente, os browsers contêm módulos específicos para processar programas Java. Embora esses módulos forneçam mecanismos de segurança, eles podem conter falhas de implementação e, nesse caso, permitir que um programa Java hostil cause alguma violação de segurança num computador.

O JavaScript é bem mais usado em páginas web do que os programas Java e, de modo geral, constitui uma versão enxuta do Java. Um JavaScript hostil pode igualmente violar a segurança de um computador.

Antes de receber um programa ActiveX, o browser verifica a procedência dele através de um esquema de certificados digitais. Se você optar por aceitar o certificado, o programa é executado em seu computador, podendo fazer de tudo, desde enviar um arquivo qualquer pela internet até instalar programas (talvez com fins maliciosos).

Muitos sites, quando acessados, utilizam cookies para guardar informações – as preferências do usuário, por exemplo. Essas informações costumam ser compartilhadas entre diversas entidades na internet e podem afetar a privacidade do usuário.

Em geral, as transações, sejam elas comerciais ou bancárias, envolvem informações sensíveis, como senha e número de cartão de crédito. Assim, ao realizar uma transação via web, é muito importante certificar-se da procedência do site, se ele realmente pertence à instituição a que diz pertencer e se fornece mecanismos de segurança para evitar que alguém conectado à internet obtenha informações sensíveis durante a operação.

Algumas medidas preventivas para o uso de browsers:

- Mantenha seu browser sempre atualizado.
- Desative a execução de programas Java na configuração do browser. Se for absolutamente necessário o Java estar ativado para que as páginas de um site sejam visualizadas, basta ativá-lo antes de entrar no site e desativá-lo ao sair.
- Desative a execução de JavaScripts antes de entrar numa página desconhecida e ative-a ao sair. Caso opte por desativar a execução de JavaScripts na configuração do browser, é provável que muitas páginas web não possam ser visualizadas.

- Permita que programas ActiveX sejam executados em seu computador apenas quando vierem de sites conhecidos e confiáveis.

- Mantenha um maior controle sobre o uso de cookies.

- Certifique-se da procedência dos sites e da utilização de conexões seguras ao realizar transações via web.

Ataques que utilizam softwares maliciosos do tipo ransomware estão se tornando cada vez mais comuns. A intenção, nesse caso, não é furtar informações, e sim sequestrá-las, criptografando-as e adicionando senhas a elas, a fim de pedir um resgate pela senha de acesso. Esse formato de ataque pode ter como alvo desde grandes empresas até usuários domésticos e se propagar como um vírus ou através de falhas já conhecidas em softwares de mercado.

A ação mais conhecida desse ataque aconteceu em 2017. O código malicioso denominado WannaCry afetou governos, órgãos públicos e hospitais ao redor mundo. Para isso, explorou uma falha de segurança conhecida e anteriormente resolvida pela Microsoft em seus sistemas operacionais. O ataque, iniciado na Espanha, logo se espalhou pelo mundo

Saiba mais

Para ver um mapa da infecção do WannaCry, consulte:

FLORENZANO, C. Mapa mostra em tempo real regiões afetadas por mega-ataque de ransomware. *CBSI*, 12 maio 2017. Disponível em: <https://www.cbsi.net.br/2017/05/mapa-mostra-em-tempo-real-regioes-afetadas-por-mega-ataque-ransomware.html>. Acesso em: 5 jul. 2018.

No caso específico do WannaCry, duas atitudes poderiam ter evitado o ataque: manter os computadores e servidores da rede sempre atualizados e ter cópias de segurança (backups) para emergências como essa.

Backups são importantes não só para se recuperar de eventuais falhas, mas também das consequências de uma infecção por vírus ou de uma invasão. As cópias de segurança podem ser simples, como o armazenamento de arquivos em CDs, ou complexas, como o espelhamento de um disco rígido inteiro em outro disco de um computador/servidor ou em uma fita magnética.

Em relação à frequência com que são feitos, os backups podem ser:

- **Incrementais**: realizados de hora em hora, copiando-se apenas os arquivos na rede que foram alterados na última hora.

- **Diários**: consolidando todos os backups incrementais do dia.

- **Semanais**: consolidando todos os backups diários da semana.

- **Mensais**: consolidando todos os backups semanais do mês numa única mídia.

No caso de redes, é necessário fazer backup de todos os arquivos contidos no segmento de rede. Para informações pessoais, o processo depende da periodicidade com que o usuário cria ou modifica arquivos. Cada usuário deve estabelecer sua própria política para a realização de cópias de segurança.

Os cuidados com cópias de segurança dependem das necessidades do usuário. O usuário deve responder a algumas perguntas antes de adotar um ou mais cuidados:

- Que informação é realmente importante armazenar nas cópias de segurança?

- Quais seriam as consequências (ou os prejuízos) se as cópias de segurança fossem destruídas ou danificadas?

- O que aconteceria se as cópias de segurança fossem furtadas?

Baseado na resposta para as perguntas anteriores, o usuário deve atribuir maior ou menor importância a cada um dos cuidados abordados a seguir.

- **Escolha dos dados**: cópias de segurança devem conter apenas arquivos confiáveis do usuário, ou seja, que não tenham vírus nem sejam cavalos de Troia. Arquivos do sistema operacional e que façam parte da instalação de softwares de um computador não devem integrar as cópias de segurança. Eles podem ter sido modificados ou substituídos por versões maliciosas, as quais, quando restauradas, trazem uma série de problemas de segurança para o computador. O sistema operacional e os softwares de um computador podem ser reinstalados de mídias confiáveis, fornecidas pelos fabricantes.

- **Mídia utilizada**: no caso de redes, devido ao grande volume de dados, o procedimento de backup deve estar documentado e a escolha da mídia deve representar a verdadeira necessidade da empresa. Para o caso de backups pessoais, a escolha da mídia depende da importância das informações e da vida útil que a cópia deve ter. O uso de pendrives para armazenar um pequeno volume de dados que está sendo modificado constantemente é perfeitamente viável. No entanto, um grande volume de dados, de maior importância e que precisa durar longos períodos, deve ser armazenado em mídias mais confiáveis, como CDs, discos externos e discos espelhados.

- **Local de armazenamento**: quando nos referimos a backups de organizações, é necessário que o local de armazenamento das mídias seja uma sala-cofre ou um cofre à prova de fogo. Backups particulares devem ser guardados num local condicionado (longe de muito frio ou de muito calor) e restrito, de modo que apenas pessoas autorizadas tenham acesso a ele (segurança física).

- **Cópia em outro local**: cópias de segurança devem ser guardadas em locais diferentes – por exemplo, em uma filial ou em outro escritório. Também existem empresas especializadas em manter áreas de armazenamento com cópias de segurança de seus clientes. Nesse caso, é muito importante considerar a segurança física de suas cópias.

O uso de criptografia para informações sigilosas armazenadas em cópias de segurança também é recomendado.

O furto de dados pessoais de um colaborador pode ser a porta de entrada para um ataque à organização ou ao próprio colaborador. Por isso, evite fornecer dados pessoais (p. ex., nome, e-mail, endereço e número de documentos) e informações sensíveis (p. ex., senha e número de cartão de crédito) para terceiros, a menos que esteja realizando uma transação – comercial ou financeira – e tenha certeza da idoneidade da instituição.

Essas informações geralmente são armazenadas em servidores das instituições que mantêm os sites. Com isso, corre-se o risco de elas serem repassadas sem autorização para outras instituições, ou de um atacante comprometer esse servidor e ter acesso a todas as informações. Ataques de engenharia social são mais comuns do que se imagina. Ao ter acesso a dados pessoais da vítima, um atacante poderia, por exemplo, utilizar o e-mail dela numa lista de distribuição de spams ou se fazer passar por ela na internet (através do uso de senhas furtadas).

Deve-se dar total atenção aos dados pessoais armazenados no disco rígido das estações de trabalho. Informações sensíveis ou pessoais que não devem ser vistas por terceiros (números de cartões de crédito, declarações de imposto de renda, senhas etc.) precisam ser armazenadas em algum formato criptografado.

Esses cuidados são especialmente relevantes no caso de notebooks, mais visados e, portanto, mais suscetíveis a furto.

Se for necessário levar o computador a uma assistência técnica e as informações não estiverem criptografadas, dados pessoais poderão ser lidos por algum técnico mal-intencionado. Para proteger esses dados, uma opção são os programas que, além de criptografar e-mails, também criptografam arquivos. Pode-se recorrer, por exemplo, a um programa que implemente criptografia de chave pública e chave privada. O arquivo sensível seria criptografado com a chave pública e decodificado com a chave privada, sempre que fosse necessário. A chave privada seria mantida em um CD ou em outro disco rígido (uma gaveta removível), o qual não acompanharia o computador se fosse necessário enviá-lo, por exemplo, para a assistência técnica.

Lembrete

Vale recordar que a segurança desse método de criptografia depende do sigilo da chave privada.

É essencial ser especialmente cauteloso ao trocar ou vender um computador. Apenas apagar ou formatar um disco rígido não é suficiente para evitar que informações antes armazenadas sejam recuperadas. É importante sobrescrever todos os dados do disco rígido. Um exemplo seria gravar o caractere 0 (zero), ou algum caractere escolhido aleatoriamente, em todos os espaços de armazenamento do disco, repetindo essa operação algumas vezes. Existem softwares gratuitos e comerciais que permitem sobrescrever dados de um disco rígido e que podem ser executados em diversos sistemas operacionais.

Quanto às senhas de acesso, podem-se mencionar estas recomendações:

- Elabore uma senha que contenha pelo menos oito caracteres, com letras, números e símbolos.
- Jamais utilize como senha nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas relacionadas a você ou palavras dicionarizadas.
- Use uma senha diferente para cada serviço.
- Altere a senha com frequência.

A primeira atitude para o desempenho eficaz da gestão de incidentes e o correto controle dos registros de eventos (logs) é verificar os logs do firewall pessoal e dos IDSs (intrusion detection systems) instalados no computador. Antes de notificar um incidente, confirme que não se trata de um falso positivo.

Os firewalls, dependendo de como foram configurados, podem gerar logs quando alguém tenta acessar um computador e esse acesso é barrado pelo firewall. Sempre que um firewall gera um log informando que determinado acesso foi barrado, isso pode significar uma tentativa de ataque, mas também pode ser um falso positivo. Já os sistemas de detecção de intrusão podem gerar logs tanto para casos de tentativa de ataque quanto para casos em que um ataque obteve sucesso. Apenas uma análise detalhada pode dizer se uma atividade detectada por um IDS foi um ataque bem-sucedido. Assim como os firewalls, os sistemas de detecção de intrusão também podem gerar falsos positivos.

O termo **falso positivo** é utilizado para designar uma situação em que um firewall ou um IDS classifica uma atividade como ataque quando na verdade não é. Um exemplo clássico disso é o caso de usuários que se conectam a servidores de IRC (internet relay chat) e que têm um firewall pessoal. Atualmente, boa parte dos servidores de IRC conta com uma política de uso que define que o usuário, para se conectar a determinados servidores, não deve ter em sua máquina pessoal nenhum software que atue como proxy. Para verificar se o usuário tem algum software desse tipo, quando recebem uma solicitação de conexão por parte do cliente, os servidores enviam para a máquina dele algumas conexões que checam a existência de tais programas. Se o usuário tiver um firewall, é quase certo que essas conexões serão apontadas como um ataque.

Outro caso comum de falso positivo ocorre quando o firewall não está devidamente configurado e indica como ataques respostas a solicitações feitas pelo próprio usuário.

Os logs relativos a ataques recebidos pela rede, em geral, trazem as seguintes informações: data e horário em que ocorreu determinada atividade, endereço IP de origem da atividade e portas envolvidas. Dependendo do grau de refinamento da ferramenta que gerou o log, ele também pode conter informações como time zone do horário do log, protocolo utilizado – TCP, UDP (user datagram protocol), ICMP (internet control message protocol) etc. – e dados completos que foram enviados para o computador ou rede.

Resumo

Nesta unidade, tratamos das principais vulnerabilidades e ameaças a que uma rede pode estar exposta. Começamos pelas formas de ataque existentes: ataque de interceptação, de modificação, de interrupção e de fabricação.

Vimos depois a diferença entre crackers e hackers. Estes, embora dominem as práticas de invasão, não as utilizam para o mal, e sim para auxiliar na defesa de sistemas e redes. Os crackers, por sua vez, são aqueles que usam seu conhecimento para violar a integridade de um sistema de máquinas remotas com intenção maliciosa.

Discutimos, a seguir, as ferramentas de ataque, que incluem bombas de correio eletrônico e listas de mala direta, negação de ferramentas de serviço e softwares maliciosos. Entre os últimos, destacam-se os vírus, os cavalos de Troia, os worms, os spywares e os backdoors.

Por fim, abordamos métodos de detecção de ameaças e de proteção contra elas. Consideramos recursos como antivírus, firewall pessoal e backup, além de procedimentos que aumentam a segurança no uso de browsers e de programas de correio eletrônico.