Nossos problemas

Ameaças

Ameaças à segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas 3 características principais, quais sejam:

- Perda de Confidencialidade: seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo com que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.
- Perda de Integridade: aconteceria quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.
- Perda de Disponibilidade: acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento.

No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como crackers, (hackers não são agentes maliciosos, pois tentam ajudar a encontrar possiveis falhas). Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, auto-estima, vingança e o dinheiro. De acordo com pesquisa elaborada pelo Computer Security Institute ([[1]]), mais de 70% dos ataques partem de usuários legítimos de sistemas de informação (Insiders) -- o que motiva corporações a investir largamente em controles de segurança para seus ambientes corporativos (intranet).

Algumas Classes de Ataques:

Engenharia Social
Vírus de computador
Roubo de senhas
Vazamento de informações
Falhas nos sistemas operacionais

Algumas Ameaças Comuns:

Funcionários (incidentes internos)
Espionagem Industrial
Terrorista
Criminoso Cibernético
Desastres naturais

Os problemas mais comuns, ou seja, a raiz deles são:

Má configuração dos hosts

A má configuração pode ocorrer devido a vários problemas, dentre eles, podemos citar:
. a configuração default do sistema, com isso deixando muito a desejar em segurança, as vezes o usuário nem sabe efetuar a instalação.

. instalação ou habilitação de serviços de forma indiscriminada (na dúvida, sempre desabilite).

Falhas inerentes dos sistemas
Nestes casos, a culpa é colocada sempre nos fabricantes, porquê seus sistemas possuem vulnerabilidades e falhas, quando não deveriam ter. Bem, acontece que os bugs são tão naturais em softwares quanto doenças são em nós. Os bugs, falhas e vulnerabilidades sempre irão existir, então cabe a nós, nos manter atualizados quanto ao lançamento de correções, patches, updates, etc.

Deficiência na resposta dos fabricantes
Este sim, é um problema causado pelo fabricante, quando este deixa de manter um controle de qualidade de seu software, e o pior, não alerta os usuários e nem lança correções para tais problemas. Portanto, antes de adquirir um software, verifique, além de sua funcionalidade, se existe uma área de suporte ativa que cuide das atualizações e tenha preocupação com a segurança do produto.

Pobre educação em segurança
É um dos primeiros problemas que devem ser atacados na implementação de um plano de segurança. De nada adianta termos os melhores profissionais na administração, os melhores produtos, se nossos funcionários não estão cientes da real necessidade de segurança, e como se deve proceder.

Script Kiddies

Eles não procuram por maneira mais fácil possível. Eles fazem isto utilizando um pequeno número de códigos e ferramentas disponíveis na Internet facilmente acessíveis e então eles procuram pela Internet inteira, até que conseguem máquina que seja vulnerável (cedo ou tarde isto certamente acontecerá).
Frequentemente eles deixam para trás as ferramentas sofisticadas. Alguns, não tem a mínima idéia do que estão fazendo. Embora o nível técnico deles possa ser diferente, todos eles usam uma ferramenta fácil para abrir caminho para que posteriormente eles possam explorar estas falhas.
Com o número crescente de usuários da rede, não temos mais uma questão de “se” mas sim de “quando” você será testado ou invadido.
Uma maneira de você se proteger é executar somente os serviços que são necessários. Se você não precisa de um serviço, desligue-o. Se você precisa do serviço, então verifique se você possui a última versão ou se você tem todos os patches/fixes instalados.
Os servidores de DNS são muito usados para construir bases de dados dos sistemas que podem ser testados/escaneados. Limite os sistemas que podem fazer a transferência de zona dos seus servidores de DNS. É altamente recomendado atualizar para a última versão e observe se seus sistemas sofrem ataques de scanning.
O script kiddie é uma ameaça a todos os sistemas, eles não tem nenhum preconceito, escaneiam qualquer sistema, em qualquer lugar do mundo, independente do valor do sistema. Cedo ou tarde seu sistema será testado/escaneado.

Engenharia Social

Existe algum método mais rápido e eficiente de se descobrir uma senha? Que tal simplesmente perguntar? Por mais extraordinário que possa parecer, o método mais simples, mais usado e talvez mais eficiente de se recolher informações é simplesmente chegar e perguntar.

Você também poderia subornar, mas dependendo da situação, isto pode lhe custar muito caro, então porquê não tentar enganar e obter tais informações? De fato, este método é bastante utilizado, e existem hackers que sabem usá-lo com grande destreza, um exemplo é o famoso hacker Kevin Mitnick que era um expert em fazer tais “vigarices”.
Essa tática de ataque é conhecida como “Engenharia Social”. Basicamente, esta é a arte de fazer com que outras pessoas concordem com você e atendam aos seus pedidos ou desejos, mesmo que você não tenha autoridade para tal.

Popularmente, pode-se dizer que engenharia social é simplesmente a arte de se contar uma mentira bastante convincente. Dentro da área de segurança podemos definir engenharia social como a aquisição de informações preciosas ou privilégios de acesso por "alguém de fora", baseado em uma relação de confiança estabelecida, inapropriadamente, com "alguém de dentro". Profissionais utilizam este tipo de aproximação para adquirir informações confidenciais, como organogramas de organizações, números de cartões de crédito e telefone, senhas de acesso, diagrama de rede, etc, com o objetivo de avaliar as vulnerabilidades de uma organização para futuros ataques.

Geralmente este tipo de aproximação envolve muito mais do que simples raciocínio rápido e uma variedade de frases na ponta da língua. Engenharia social pode envolver muito trabalho de aquisição de informação antes de uma real ação de qualquer tipo.
Para de iniciar um ataque, a maior parte do trabalho está na preparação, muito mais que no próprio ataque (leva-se tempo...).

Dizem que o único computador totalmente seguro é aquele desligado da tomada. A arte da engenharia social concentra-se no elo mais fraco da corrente da segurança de computadores: os seres humanos. O simples fato de que se pode facilmente convencer uma pessoa a ligar o computador, torna vulnerável, até mesmo, os computadores desligados.
Na medida em que a parte humana de um sistema de segurança é a mais essencial, não existe computador na face da Terra que não necessite de seres humanos. Isso significa que essa é uma fraqueza universal, independente de plataforma, software, tipo de conexão de rede ou idade do equipamento. Qualquer pessoa com acesso à qualquer parte do sistema, física ou remota, pode ser uma falha de segurança em potencial. Qualquer informação adquirida pode ser utilizada para um outro ataque de engenharia social. Isso significa que qualquer pessoa, mesmo que não seja considerada integrante da política de segurança pode servir como uma porta de entrada (estagiários, faxineiros, etc).

O primeiro método é também o mais óbvio. Um pedido simples e direto, onde se solicita ao indivíduo alvo que se execute uma determinada tarefa. Embora este método seja o menos provável a trazer um resultado positivo, é com certeza o mais simples, onde o indivíduo sabe exatamente o que você quer que ele faça.

O segundo é criar uma situação onde o indivíduo é apenas uma parte dela. Com muito mais fatores que um simples pedido, o indivíduo preocupado estará bem mais predisposto a ser persuadido. Isso não significa que as situações propostas devam ser fictícias. Quanto menos você faltar com a verdade, melhor. Isso requer muito mais trabalho por parte de quem faz o ataque e com certeza envolve um recolhimento de informação e conhecimento prévio do alvo.
Se a situação proposta, real ou imaginária possuir certas características, o indivíduo alvo estará mais propenso a concordar com o seu pedido. Estas características incluem:

. Difusão da responsabilidade. Fazer com que o alvo acredite que ele não é o único responsável por suas ações e pelas informações que ele possa divulgar. Mantenha a responsabilidade longe do alvo.
. Troca de favores. Permitir que o alvo acredite que esta prestando um favor a você e que você é extremamente grato. As pessoas geralmente mostram-se mais dispostas a cooperar quando acreditam que poderão obter alguma vantagem no futuro, como se você ou o chefe ficassem devendo um favor.
. Dever moral. É quando o alvo coopera, pois acha que é a coisa certa a fazer. É seu dever moral. Parte disso é culpa. As pessoas procuram evitar o sentimento de culpa e farão o possível para evitar esse sentimento.

Procure seu alvo levando em consideração seu envolvimento, sua experiência e tempo de trabalho junto ao sistema alvo. Alunos, estagiários, secretárias e profissionais iniciantes mostram-se sempre mais dispostos a cooperar. Isto se deve ao fato que estes indivíduos possuem ainda pouco conhecimento e pouca experiência a respeito do sistema alvo e desejam mostrar-se úteis. Eles querem "mostrar serviço".
Quanto menos conflito com o alvo, melhor. É muito mais fácil ganhar a confiança do alvo sendo gentil. Utilizar um tom de voz calmo (se ao telefone) e ser gentil, é um bom começo para que o alvo coopere.

Como um ataque de engenharia social pode revelar muitas informações, como se pode tornar um sistema de computadores mais seguro? A resposta é educação e difusão da informação, explicando aos empregados e pessoas ligadas direta ou indiretamente ao sistema a importância de uma política de segurança, evitando assim o ataque de pessoas que poderão manipulá-los para ganhar acesso a informações privadas. Isto já é um excelente começo para se tornar segura sua rede ou sistema.

Vírus, Worms ou Trojans

Todos os anos, os vírus causam muitos prejuízos ao redor do mundo. A internet é o meio ideal para transmissão. Na década de 80 por exemplo, para conseguirmos transmitir um vírus tínhamos poucos recursos. O mais usado era trasmití-los de máquina em máquina através de disquetes, o que tornava a contaminação bastante lenta. Atualmente as coisas são bem diferentes, através da internet, a contaminação é muito mais rápida e atinge facilmente nível mundial. Além disso, surgiram conceitos novos como vírus de macro, worms e trojans.
Estaremos abordando os vírus e suas variantes no ambiente Windows. Existem vírus nos ambientes Unix, mas a proporção é infinitamente menor. Além disso, os conceitos abordados aqui se aplicam em ambos os casos.

A seguir, um pequeno esclarecimento sobre as diferenças entre os vários invasores que podem vir a nos incomodar:

. VIRUS – São pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e reproduzir (fazer cópias de si), contaminando outros arquivos. Em princípio um vírus poderia contaminar qualquer arquivo. No entanto, só faz sentido contaminar arquivos executáveis, uma vez que estes são carregados e executados na memória. Por exemplo, vamos supor que um vírus contamine o Command.com, um arquivo executável que é carregado pelo computador toda vez que nós ligamos o micro. Desta forma, o programador que fez o vírus sabe que sua "criatura" sempre vai ser carregada na memória. Já se fosse um arquivo de dado como, por exemplo, myfile.txt, nada aconteceria pois o micro em princípio não executa arquivos com extensão TXT.

. TROJANS – São cavalos-de-tróia, assim como na história, enviasse um falso presente para a vítima (geralmente por e-mail), que ingenuamente aceita e o executa. Assim o trojan começa a fazer seu ataque se enviando por e-mail para outras pessoas de sua lista, como se fosse o usuário (esta está sendo uma prática cada vez mais comum também por parte dos vírus). Mas há uma diferença fundamental entre os trojans e os vírus: os primeiros não se reproduzem como os vírus.

. VIRUS DE MACRO – Primeiro vamos esclarecer o que é um Macro: macro é uma VBA – Visual Basic Aplication (linguagem script desenvolvida pela Microsft), que é interpretada pelo M Office (Word, Excel, Access e Power Point), ou seja, podemos fazer pequenos programas que nos ajudem a trabalhar no Office. Como por exemplo, criar um botão na barra de ferramenta do Word que permita abrir diretamente a calculadora do Windows. No entanto, nas mãos erradas, se torna uma arma poderosa capaz de causar muitos prejuizos. Agora é muito fácil entender que um vírus de macro nada mais é que um programa escrito em VBA. No momento em que abrimos um documento do Word contaminado, esta macro é ativada, podendo apagar documentos importantes, por exemplo.

. WORMS – Os worms são programas que aproveitam falhas do sistema para se propagar e se replicar. Ao contrário dos trojans, os worms não contaminam os arquivos. O primeiro worms que se tem notícia foi criado por Robert Morris, em 1988. Este programa aproveita uma falha do finger daemon do Unix e do SendMail. Mais o worms de Morris tinha um bug que o fazia reinfectar máquinas já contaminadas. Isso provocou a queda de vários computadores de várias instituições nos EUA.
Atualmente está cada vez mais difícil classificar um programa malicioso em uma destas categorias, pois os "vírus" modernos estão usando cada vez mais técnicas mistas de contaminação. Não é raro encontrar programas com técnicas de worms para entrar no sistema, alterar as configurações de segurança e infectar seu computador como se fosse um vírus de macro. Esta se tornando cada vez mais comum encontrar vírus que usam arquivos de lote (.BAT) para se infiltrar no sistema.

Vírus que se espalham por e-mail:

Criadores de vírus geralmente usam e-mail para a propagar de suas criações. Na maioria dos casos, é necessário que o usuário ao receber o e-mail execute o arquivo em anexo para que seu computador seja contaminado. O criador do vírus pensa então em uma maneira de fazer com que o usuário clique no anexo. Uma dos métodos mais usados é colocar um texto que desperte a curiosidade do usuário. O texto pode tratar de sexo, de amor, de notícias atuais ou até mesmo de um assunto particular do internauta. Um dos exemplos mais clássicos é o vírus I Love You, que chegava ao e-mail das pessoas usando este mesmo nome. Ao receber a mensagem, muitos pensavam que tinham um(a) admirador(a) secreto(a) e

na expectativa de descobrir quem era, clicavam no anexo e contaminam o computador. Repare que neste caso, o autor explorou um assunto que mexe com qualquer pessoa. Alguns vírus possuem a característica de se espalhar muito facilmente e por isso recebem o nome de worms (vermes). Aqui, a engenharia social também pode ser aplicada. Imagine, por exemplo, que um worm se espalha por e-mail usando como tema cartões virtuais de amizade. O internauta que acreditar na mensagem vai contaminar seu computador e o worm, para se propagar, envia cópias da mesma mensagem para a lista de contatos da vítima e coloca o endereço de e-mail dela como remetente. Quando alguém da lista receber a mensagem, vai pensar que foi um conhecido que enviou aquele e-mail e como o assunto é amizade, pode acreditar que está mesmo recebendo um cartão virtual de seu amigo. A tática de engenharia social para este caso, explora um assunto cabível a qualquer pessoa: a amizade.

E-mails falsos (spam):

Este é um dos tipos de ataque de engenharia social mais comuns e é usado principalmente para obter informações financeiras da pessoa, como número de conta-corrente e senha. Neste caso, o aspecto explorado é a confiança.
Boa parte dos criadores desses e-mails são criminosos que desejam roubar o dinheiro presente em contas bancárias. Porém, os sistemas dos bancos são muito bem protegidos e quase que invioláveis! Como é inviável tentar burlar a seguranças dos sistemas bancários, é mais fácil ao criminoso tentar enganar as pessoas para que elas forneçam suas informações bancárias. A tática usada é a seguinte: o criminoso adquire uma lista de e-mails usados para SPAM que contém milhões de endereços, depois vai a um site de um banco muito conhecido, copia o layout da página e o salva em um site provisório, que tem a url semelhante ao site do banco. Por exemplo, imagine que o nome do banco seja 'Banco Dinheiro' e o site seja www.bancodinheiro.com. O criminoso cria um site semelhante: 'www.bancodinhero.com' ou 'www.bancodinheiro.com.br' ou 'www.bancodinheiro.org', enfim. Neste site, ele faz uma cópia idêntica a do banco e disponibiliza campos específicos para o usuário digitar seus dados confidenciais. O passo seguinte é enviar um e-mail à lista adquirida usando um layout semelhante ao do site. Esse e-mail é acompanhado por um link que leva ao site falso. Para fazer com que o internauta clique no link, o texto da mensagem pode, por exemplo, sugerir uma premiação: "Você acaba de ser premiado com 10 mil reais. Clique no link para atualizar seu cadastro e receber o prêmio". Como a instituição bancária escolhida geralmente é muito conhecida, as chances de que o internauta que recebeu o e-mail seja cliente do banco são grandes. Assim, ele pode pensar que de fato foi o banco que enviou aquela mensagem, afinal, o e-mail e o site do link tem o layout da instituição. Como conseqüência, a vítima ingenuamente digita seus dados e dias depois percebe que todo o dinheiro da sua conta sumiu! Repare que em casos assim, o golpista usa a imagem de confiabilidade que o banco tem para enganar as pessoas. Mensagens falsas que dizem que o internauta recebeu um cartão virtual ou ganhou um prêmio de uma empresa grande são comuns. Independente do assunto tratado em e-mails desse tipo, todos tentam convencer o internauta a clicar em um link ou no anexo. A forma utilizada para convencer o usuário a fazer isso é uma tática de engenharia social.

Phishing

Para quem não sabe, o phishing (“pescando”, em inglês) é uma modalidade de fraude na Web em que os crackers criam páginas falsas com o intuito de induzir o internauta a fornecer dados confidenciais - principalmente senhas bancárias e números de cartões de crédito - por meio de e-mails com supostos avisos de bancos, sites de compras ou de instituições como o SERASA e a Receita Federal.

Em 2006, segundo estatísticas do Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), das 197 mil tentativas de ataques registradas pela entidade, 21% tinham como alvo dados pessoais, que inclui o phishing.
Além disso, de acordo com um levantamento da empresa de segurança digital Fortinet, este tipo de fraude foi a mais ativa em fevereiro deste ano, respondendo por quase 19% do total das ofensivas. E, para completar, mais uma notícia desanimadora: um relatório da ISS (Internet Security Systems) avisa que os crackers brasileiros estão desenvolvendo phishings cada vez mais sofisticados, com páginas muito próximas das originais, temas pontuais como campeonatos de futebol e promoções, além de usar o nosso idioma com cada vez mais freqüência.

Portanto, sendo o phishing um dos golpes mais utilizados na Web para quem quer ganhar dinheiro em cima da boa fé

alheia, cabe a pergunta: como se precaver contra este tipo de prática? A resposta não está em softwares revolucionários que consigam detectar as páginas fraudulentas, mesmo porque a maioria dos filtros do gênero deixa muito a desejar. As melhores dicas para não ser "fisgado" estão em informação e olho vivo.

A dica para quem não quer cair no golpe do phishing é saber que a maioria dessas companhias **não** envia e-mails para seus clientes, a não ser que eles solicitem previamente. Em outras palavras, se você receber mensagens do banco X, da operadora Y ou de órgãos públicos, simplesmente apague-as. Para induzir os internautas, cria falsos avisos informando que a vítima tem débitos ou que documentos como CPF e o título de eleitor apresentam irregularidades e podem ser cancelados.

Como você já sabe, o phishing se baseia em páginas falsas para induzir o usuário a fornecer seus dados. Para isso, o criminoso coloca na mensagem links que levarão a vítima a páginas manipuladas, que roubarão as informações confidenciais.

Caso ocorra dúvidas em relação a pendências ou problemas de qualquer natureza envolvendo essas empresas, a dica é: simplesmente abra o navegador, digite o endereço eletrônico da instituição e procure informações diretamente no site da companhia. Não use qualquer link que esteja anexo à mensagem eletrônica.

Ataques de Negação de Serviço (DoS e DDoS)

O DoS tem sido usado por profissionais de segurança como ferramenta para avaliar a capacidade de sua rede. Por outro lado, do mundo todo têm trazido muitos problemas a pequenos e até grandes sites.
O poder de sobrecarga desses ataques aumenta quando eles vêm de várias máquinas para um alvo, ou seja, o envio de pacotes parte de vários pontos. Trata-se do Distributed DoS – DDoS.

Como funciona o DDoS

A idéia é instalar programas para ataque DoS em diferentes hosts. Esses zumbis começam a enviar o máximo de pacotes para o alvo. Mas antes de existirem ferramentas que automatizassem esse ataque, era necessário usar um gatilho manual para disparar o ataque. Usando o telnet ou SSH, o hacker dispararia o comando na máquina vítima. Para isso, ele poderia usar, por exemplo, o ping do UNIX nos hosts.

Características do DDoS

Vulnerabilidades do TCP/IP são a chave para o desenvolvimento de novos programas, cada vez mais poderosos nesses ataques. Uma delas, é o Stream Attack, descoberta por Tim Yardley. Esta categoria de ataque funciona da seguinte forma: na conexão pacotes são enviados com os indicadores (flags) ACK e SYN ligados ou apenas o ACK ligado. Devido a estes flags não fazerem parte de uma primeira etapa da conexão, a máquina alvo ficará confusa e levará algum tempo para processar tais dados. Imagine então o Stream Attack partindo de vários hosts (modo distribuído), isto ocasionaria uma sobrecarga utilizando-se um menor número de hosts (zumbis) que o DDoS "padrão".

Tipos de ataques de DoS

Consumo de largura de banda – Neste tipo de ataque, existem pelo menos duas possibilidades:
. O atacante possui uma largura de banda maior que a da vítima, o que facilita a inundação.
. O atacante agrega outros computadores para que juntos, disparem o ataque, amplificando seu efeito e consumindo a largura de banda da vítima.
Resumindo, derrubar a comunicação da vítima.

Consumo dos recursos – A idéia aqui é esgotar os recursos do sistema, tais como memória, cpu, quotas de disco, etc, o que pode ocasionar travamento dos processos, entupimento de discos, indisponibilização de recursos.

Ataques a Servidores de Nomes de Domínios (DNS) e a Roteadores – No caso do ataque baseado em roteamento, o atacante manipula a tabela de roteamento com a finalidade de negar serviço a quem consultá-la, explorando falhas dos protocolos de roteamento, como o Protocolo de Informações de Roteamento (RIP) e o Protocolo de Gateway de Fronteira (BGP). Com isso, o atacante pode direcionar todo o tráfego para a máquina dele, ou mesmo para uma rede que não existe, o que chamamos de buraco negro. Assim como nos ataques baseados em roteamento, o ataque a DNS permite direcionar o tráfego. Porém, esses ataques, em sua maioria, consistem em armazenar endereços falsos no cache do servidor da vítima.

Exemplos de ataques DoS

SMURF – O ataque Smurf é um dos mais temidos. Envolvendo vítima, atacante e uma rede auxiliar. É um **ataque** simples baseado em IP spoofing e Broadcast. Um único pacote (conhecido como ICMP Echo Request) é enviado como um direcionador de broadcast para uma subrede na Internet. Todos os computadores naquela subrede responderá para esse direcionador broadcast. Neste caso o IP source deste direcionador broadcast certamente será trocado (técnica spoofing) pelo endereço IP da vitima escolhida pelo atacante. Dessa maneira quando os computadores receberem o broadcast direcionado, responderão com ICMP Echo Replay para o endereço IP (spoofed) contido naquele broadcast. Dependendo do numero de computadores da subrede, dezenas, centenas ou ate milhares de pacotes ICMP Echo Replay serão enviados para o endereço IP da vitima fazendo com que a conexão seja bloqueada ou simplesmente tornando a conexão lenta demais para uso. Essa técnica pode ser aplicada em conjunto com vários outros atacantes para que o efeito seja ainda maior e duradouro. Para a vitima não ha muito o que fazer a não ser contatar o responsável pela subrede que esta servindo de amplificador de Smurf (Smurf Amplifier).

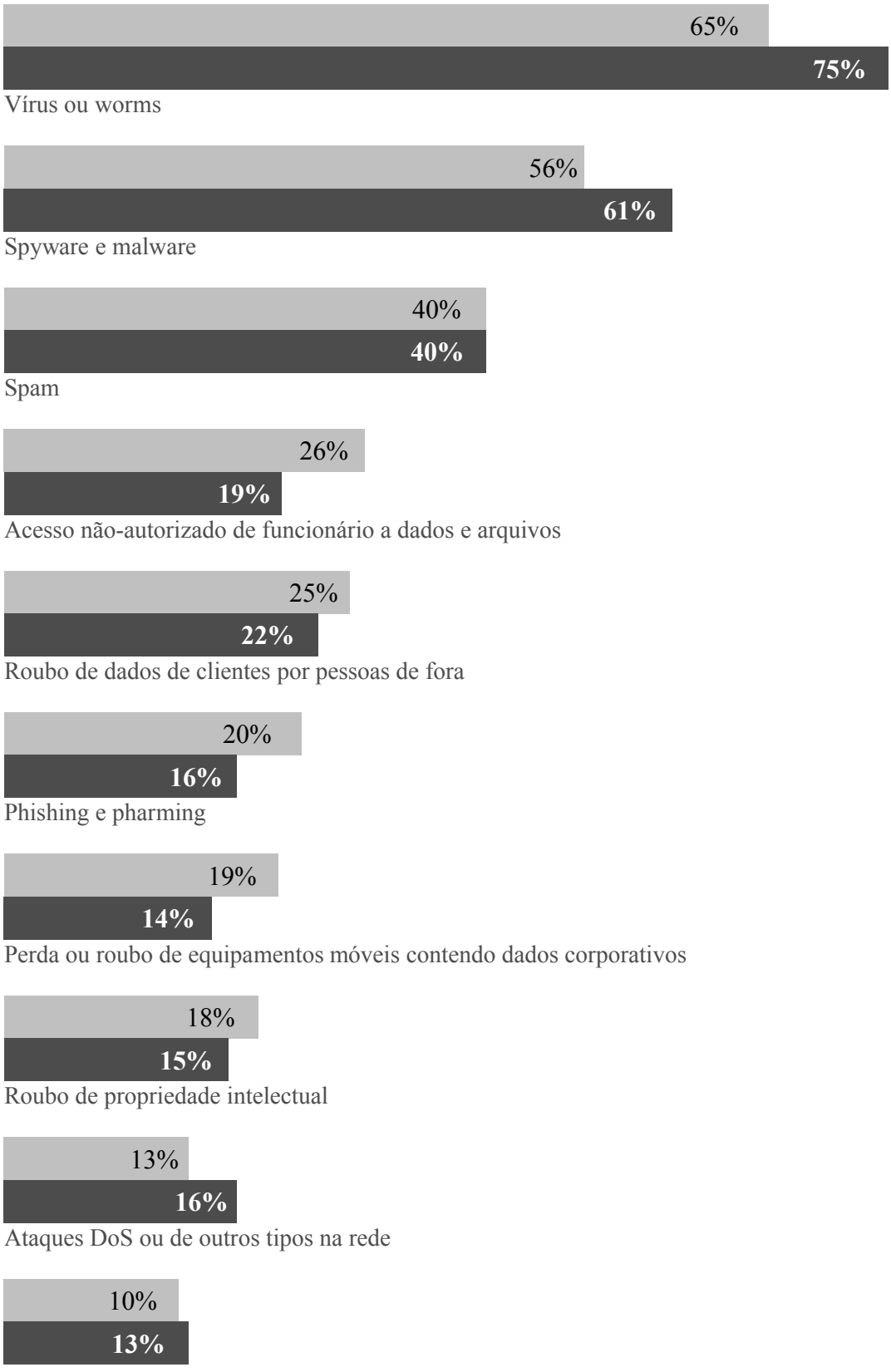
SYN FLOOD – Para entendermos este ataque precisamos ver como funciona uma conexão TCP entre 2 máquinas A e B, que é realizada em 3 etapas.
Primeiramente, a máquina A envia um pacote SYN. A máquina B então responde com outro pacote SYN/ACK que ao chegar a máquina A, reenvia um pacote ACK e então a conexão é estabelecida. A vulnerabilidade explorada é que a maioria dos sistemas aloca uma quantidade finita de recursos para cada conexão potencial. Mesmo que um servidor seja capaz de atender muitas conexões concorrentes para uma porta específica (por exemplo, porta 80), o que o atacante explora é que apenas cerca de algumas conexões potenciais são tratáveis. Iniciando o ataque, o cracker envia um pacote SYN com origem falsificada (buraco negro), o que deixará a vítima procurando por algum tempo (que varia de acordo com o sistema) a origem para enviar o pacote SYN/ACK. Sendo assim, esta possível conexão fica alocada na fila, que é bastante limitada.

Detectando e evitando:
Há dois tipos de tráfego gerado por DDoS: tráfego de controle (entre cliente e servidor) e tráfego “flood” (entre servidor DDoS e a vítima). Para habilitar uma eficiente detecção deve-se procurar por sinais gerais (assinaturas), alguns óbvios, outros pelo volume de tráfego e que causam suspeita.

Ainda não existe uma solução para bloquear um ataque DoS/DDoS. O que se pode fazer é tentar minimizar seu impacto, para fazer isso temos que primeiro identificar corretamente um ataque de DoS e depois criar soluções para “escoar” o fluxo de pacotes, seja através de um firewall na fronteira ou algum esquema de alteração de endereçamento IP ou DNS.

Pesquisa

Em segurança, quais são as principais prioridade da sua companhia ?
Fonte: pesquisa InformationWeek Brasil-Agosto/07-Nr 186



Botnets que se apoderam remotamente dos recursos de TI

6%

5%

Ataques contra sistemas sem fio e de RFID

3%

4%

Intrusão no VoIP

China EUA