Introdução

Atualmente, a necessidade de segurança vem crescendo cada dia mais. Quanto mais algo evolui, sua segurança deve evoluir também.

Em relação à segurança de redes, serão mostrados aqui itens mais comuns e imprescindíveis para uma boa segurança.

Ter segurança envolve muita criatividade e conhecimento do que esta ocorrendo em determinados momentos.

O objetivo da política de segurança é mostrar a sua importância e tratar mais profundamente assuntos específicos.

Segurança de Redes

TCP/IP

O TCP/IP na verdade é um conjunto de muitos protocolos. Usando uma arquitetura cliente-servidor quase perfeita, esse conjunto de protocolos possibilitam praticamente todo tipo de sistema operacional e rede de se comunicarem entre si, possibilitando até a criação da Internet. Ora, como seria possível um monte de computadores usando Macintosh, Unix, Linux e Windows comunicarem-se sem maiores problemas? É a tecnologia a nosso serviço. E o melhor de tudo, é um protocolo aberto.

Para começarmos o nosso estudo sobre os protocolos que compõem o TCP/IP, analisemos um a um os mais importantes deles. Ou em outras palavras, os que mais iremos utilizar. Não dá para vermos todos pois além de serem muitos, têm de ser estudados a fundo.

IP

O IP (Internet Protocol) é o responsável por rotear e entregar os pacotes contendo as informações que serão enviadas. O endereço IP contém um cabeçalho onde estão indicados os endereços de redes e de hosts. Esse endereço é representado por quatro bytes separados por pontos. Por exemplo:

200.202.36.251

As duas primeiras partes (200.202) indicam o endereço da rede. Ou seja, provavelmente todos os hosts dessa rede começam com esse endereço. O que vai mudar de host para host é a parte final do endereço (36.251). Claro que isso não é uma regra, existem redes gigantescas em que

essas propriedades podem mudar. Para saber se qual o endereço de rede e o endereço de host de uma rede, verifique a máscara de sub-rede.

A máscara de sub-rede (subnet mask) nos informa quais áreas do ip são mutáveis (usadas por hosts) e quais não mudam. Exemplo:

255.255.255.0

O que isso significa? Quando uma área da máscara de sub-rede tiver o número 255, significa que aquela área é imutável e quando for 0 a área pode mudar. Achou difícil? Não é. Preste atenção: observando o endereço acima, dá para notarmos o quê? Que somente a última parte do endereço IP está com o zero. Supondo que o endereço IP de uma máquina da rede seja 200.131.16.1

Portas

Se você quisesse colocar um servidor de homepage e um servidor de jogos em um host tendo um só endereço IP seria impossível. Como o cliente saberia identificar qual dos servidores precisa se conectar? Para isso criaram as portas. Elas identificam conexões utilizando números de 0 a 65536. Alguns serviços já possuem até suas portas padrões, como é o caso do Telnet (porta 23) e do FTP (porta 21).

DNS

Nosso próximo passo no estudo do TCP/IP é o Domain Name Server (DNS) ou Servidor de Nome de Domínio, em português. A função dessa belezinha é extremamente útil. Já imaginou se você tivesse que decorar o endereço IP de todas as página que visita na Internet? No máximo uns 10 você decoraria, mas e o resto? Para acabar com esse problema surgiu o DNS. A sua função é procurar em um banco de dados um nome que corresponda a um IP. Quando digitamos www.yahoo.com por exemplo, não precisamos saber o endereço IP. O DNS do nosso provedor de acesso vai checar esse nome em seu banco de dados e se encarregar de nos direcionar ao IP encontrado. Olha que protocolo bonzinho =) .

Nós mesmos podemos configurar e ligar alguns nomes a endereços IP. O método mais fácil de se fazê-lo é utilizar o arquivo HOSTS. O processo é o mesmo do LMHOSTS do NetBIOS, e o arquivo é encontrado no mesmo local. O interessante do HOSTS é que você pode pregar peças nos seus amigos, direcionando endereços como www.fbi.gov para o IP de alguma homepage hackeada ou até seu endereço IP local e contar vantagem de que invadiu o FBI. Muitos “hackers” hoje em dia usam isso para aparecerem na televisão e “hackear” ao vivo.

SMTP

O Simple Mail Transfer Protocol é o protocolo responsável por entregar mensagens de e-mail a um destinatário. Toda vez que seus e-mails são enviados, um servidor smtp se encarrega de levá-los ao seu destino. Esse servidor geralmente se aloja na porta 25. O interessante do SMTP é que ao contrário do POP3 (visto a seguir), não é necessário senha para enviar um e-mail. Eu posso abrir o Microsoft Outlook e mandar e-mails como se fosse Justin Bieber ou Robert Downey Jr. A falta de segurança no envio de mensagens é o ponto de partida para a facilidade de se enviar e-mails anônimos (como visto em anonimidade). O SMTP ainda permite anexar à uma mensagem de texto conteúdos binários (programas por exemplo), utilizando o MIME.

1.7 POP3

Outro protocolo de mensagens, só que agora é o responsável por o recebimento dessas mensagens. O POP3 já necessita de senhas para poder habilitar o acesso dos usuários às suas caixas postais, além de saber "re-montar" os arquivos enviados em formato MIME com o SMTP. O POP3 geralmente se localiza na porta 113. Uma grande desvantagem dele é que fica muito fácil fazer um ataque de bruteforce para tentar descobrir as senhas, já que a maioria dos servidores possui falhas que possibilitam softwares maliciosos de serem rodados.

1.8 TELNET

Telnet, ou terminal remoto é um modo de se acessar remotamente sistemas como se você os estivesse operando localmente. Por exemplo: usando o telnet (e um trojan instalado) podemos ter acesso ao MS-DOS de qualquer um. Do mesmo modo que poderíamos digitar comandos para listar, copiar e apagar dados, conectados a outro computador também podemos. Na verdade, todos os trojans são clientes telnet. Apenas são disfarçados com botõezinhos bonitinhos, pois, geralmente quem precisa de trojans para invadir sistemas são pessoas que não possuem um bom conhecimento de segurança. Se você encontrar alguma porta ativa em algum sistema (qualquer uma, seja de trojan, SMTP, POP3, etc...), pode se conectar a ela por telnet.

Resumindo, se você souber usar bem telnet não precisa mais de outros programas no computador. Ele acessa servidores utilizados pelos browsers (como Safari, Mozilla,Internet Explorer...), clientes de E-mail, absolutamente tudo.

FTP

File Transfer Protocol é seu nome real. O protocolo de transferência de arquivos serve única e exclusivamente para ser um banco de software. Não se pode executar programas remotamente como no caso do telnet, apenas pegar e colocar arquivos. Desde a criação da Internet, o ftp é largamente usado. Uma de suas vantagens é, como ele é usado somente para transferências de arquivos, sua velocidade pode chegar a ser muito maior do que pegar arquivos em HTTP (visto mais à frente).

HTTP

Esse sem dúvida é conhecido por muitos. Afinal, quem nunca viu na frente do endereço de uma homepage esse nome? http://www.altavista.com/. O Hyper Text Transfer Protocol é o protocolo responsável de transmitir textos, imagens e multimídia na Internet. Sempre que você abre uma homepage (mesmo que ele só contenha textos), você está usando esse protocolo. Achei interessante comentar sobre ele para que se entenda melhor como a Internet não funciona isolada com um só protocolo. HTTP, FTP, TELNET e os outros muitas vezes trabalham em conjunto e nem percebemos. Quando você for baixar um arquivo, preste atenção no link. É muito provável que de uma página navegada por HTTP, se envie a um servidor FTP.

Tipos de rede: LAN e WAN

Atualmente podemos contar com alguns tipos de rede quando a sua disposição física ,vamos as principais.

LAN – Local Area Network - Rede de alcance local

Redes locais (LAN's) são basicamente um grupo de computadores interconectados e opcionalmente conectados a um servidor.

Os usuários executam tarefas a partir de seus computadores. Entre as tarefas podemos destacar os banco de dados, planilhas e editores de texto. Normalmente temos um grupo destes usuários executando uma operação no servidor.

WAN – Wide Area Network - Rede de alcance remoto

Interligação de computadores geograficamente distantes. As WAN'S utilizam linhas de transmissão oferecidas por empresas de telecomunicações como a Embratel, e suas concessionárias.

A necessidade de transmissão de dados entre computadores surgiu com os mainframes, bem antes do aparecimento dos PC's. Com os PC's houve um aumento da demanda por transmissão de dados a longa distância.

As redes WAN's estão passando por uma evolução muito grande com a aplicação de novas tecnologias de telecomunicações com a utilização de fibra ótica (Optical fiber). Novos padrões estão surgindo como a ATM (Asynchronous Transfer Mode) que disponibiliza a transmissão de dados, som e imagem em uma única linha e em altíssima velocidade. A velocidade passa a ser determinada pelos equipamentos que processam as informações (Clientes/Servidores) e não do meio físico.

Diferenças – TCP/IP e OSI

O TCP/IP combina os aspectos das camadas de apresentação e de sessão dentro da sua camada de aplicação.

O TCP/IP combina as camadas física e de enlace do OSI em uma camada.

O TCP/IP parece ser mais simples por ter menos camadas .

Os protocolos TCP/IP são os padrões em torno dos quais a Internet se desenvolveu, portanto o modelo TCP/IP ganha credibilidade apenas por causa dos seus protocolos. Ao contrário, geralmente as redes não são desenvolvidas de acordo com o protocolo OSI, embora o modelo OSI seja usado como um guia.

Camadas OSI

•Cada camada OSI individual tem um conjunto de funções que ela deve executar para que os pacotes de dados trafeguem de uma origem a um destino em uma rede.

Camada de Aplicação

: Disponibiliza serviço rede para processos de aplicativos.

Camada de Apresentação: Garante que o dados sejam legíveis, formato de dados.

Camada de Sessão : Estabelece, gerencia e termina sessões entre aplicativos.

Camada de Transporte: Trata entre questões de transporte.

Camada de Rede: Fornece conectividade e seleção de caminhos.

Camada Enlace de Dados: Fornece transferência de dados confiáveis

Camada Física: Fios , conectores, voltagens, taxa de dados.

Camadas TCP/IP

TCP/IP - Camada de aplicação

•Os protocolos de mais alto nível incluem os detalhes da camada de apresentação e de sessão.

•trata de protocolos de alto nível, questões de representação, codificação e controle de diálogo.

•O TCP/IP combina todas as questões relacionadas a aplicações em uma camada.

•TCP/IP - Camada de transporte

•Qualidade de serviços de confiabilidade, controle de fluxo e correção de erros.

•Transmission Control Protocol (TCP), fornece formas excelentes e flexíveis de se desenvolver comunicações de rede confiáveis com baixa taxa de erros e bom fluxo, é um protocolo orientado para conexões. Ele mantém um diálogo entre a origem e o destino enquanto empacota informações da camada de aplicação em unidades chamadas segmentos.

TCP/IP - Camada de Internet

•Sua finalidade é enviar pacotes da origem de qualquer rede na internetwork e fazê-los chegar ao destino, independentemente do caminho e das redes que tomem para chegar lá.

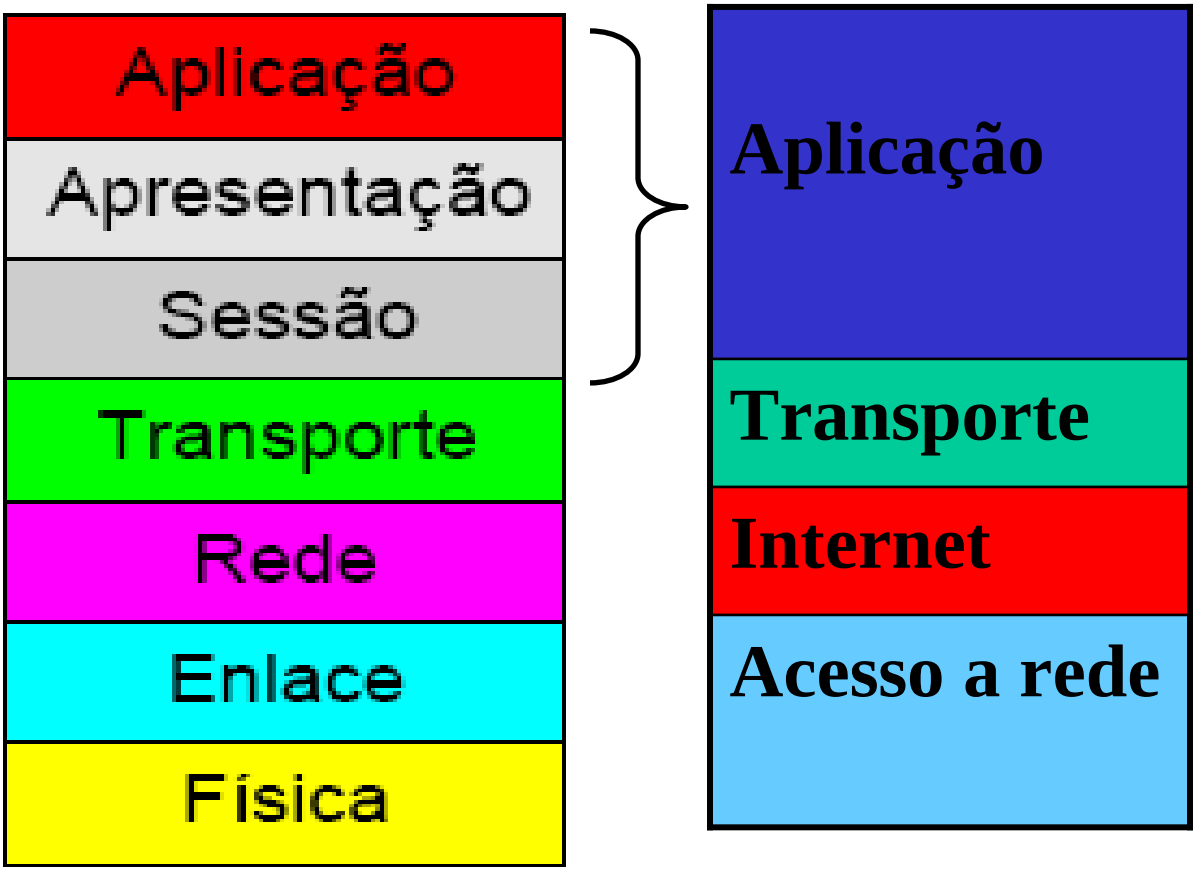
•O protocolo específico que governa essa camada é chamado Internet protocol (IP). A determinação do melhor caminho e a comutação de pacotes acontecem nessa camada. Igual ao sistema postal (não sabe como a carta vai chegar ao seu destino).

TCP/IP - Camada de acesso à rede

•O significado do nome dessa camada é muito amplo e um pouco confuso.

•É também chamada de camada host-rede. É a camada que se relaciona a tudo aquilo que um pacote IP necessita para realmente estabelecer um link físico e depois estabelecer outro link físico. Isso inclui detalhes de tecnologia de LAN e WAN e todos os detalhes nas camadas física e de enlace do OSI.

Comparação entre os modelos TCP/IP e OSI



Encapsulamento

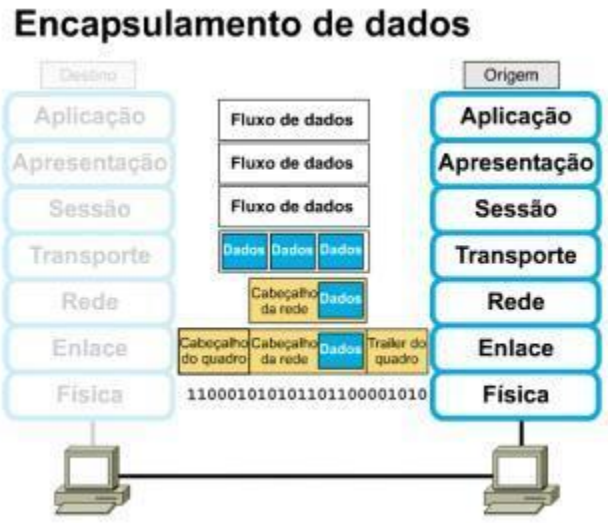
Como você sabe, todas as comunicações em uma rede têm uma origem e são enviadas para um destino, e as informações emitidas em uma rede são chamadas de dados ou pacote de dados. Se um computador (host A) desejar enviar dados para outro computador (host B), os dados devem primeiro ser empacotados através de um processo chamado encapsulamento.

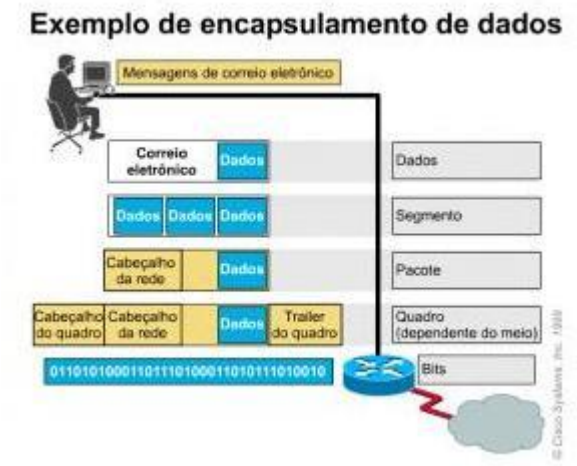
O encapsulamento empacota as informações de protocolo necessárias antes do trânsito pela rede. Assim, à medida que o pacote de dados desce pelas camadas do modelo OSI, ele recebe cabeçalhos, trailers e outras informações. (Observação: A palavra "cabeçalho" significa que informações de endereço foram adicionadas.)

Para ver como o encapsulamento ocorre, vamos examinar a forma como os dados viajam pelas camadas, como ilustrado na figura 1. Uma vez que os dados são enviados da origem, como ilustrado na figura, eles viajam através da camada de aplicação em direção às outras camadas. Como pode ver, o empacotamento e o fluxo dos dados que são trocados passam por alterações

à medida que as redes executam seus serviços para os usuários finais. Como ilustrado nas figuras, as redes devem efetuar as cinco etapas de conversão a seguir para encapsular os dados:

1. **Compilar os dados.**
   Quando um usuário envia uma mensagem de correio eletrônico, os seus caracteres alfanuméricos são convertidos em dados que podem trafegar na internetwork.
2. **Empacotar os dados para transporte ponto a ponto.**
   Os dados são empacotados para transporte na internetwork. Usando segmentos, a função de transporte assegura que os hosts da mensagem em ambas as extremidades do sistema de correio eletrônico possam comunicar-se com confiabilidade.
3. **Anexar (adicionar) o endereço da rede ao cabeçalho.**
   Os dados são colocados em um pacote ou datagrama que contém um cabeçalho de rede com endereços lógicos de origem e destino. Esses endereços ajudam os dispositivos da rede a enviar os pacotes através da rede por um caminho escolhido.
4. **Anexar (adicionar) o endereço local ao cabeçalho do link de dados.**
   Cada dispositivo da rede deve colocar o pacote dentro de um quadro. O quadro permite a conexão com o próximo dispositivo da rede diretamente conectado no link. Cada dispositivo no caminho de rede escolhido requer enquadramento em seqüência para conectar-se ao dispositivo seguinte.
5. **Converter em bits para transmissão.**
   O quadro deve ser convertido em um padrão de 1s e 0s (bits) para transmissão no meio (normalmente um cabo). Uma função de sincronização permite que os dispositivos diferenciem esses bits à medida que trafegam no meio. O meio na conexão física das redes pode variar de acordo com o caminho usado. Por exemplo, a mensagem de correio eletrônico pode ser originada em uma LAN, atravessar um backbone do campus e sair por um link da WAN até alcançar seu destino em outra LAN remota. Cabeçalhos e trailers são adicionados enquanto os dados se movem pelas camadas do modelo OSI.





Segurança da Informação

A fragilidade dos sistemas informatizados não é nenhuma novidade. Há décadas, celebridades como Robert Morris Jr., Capitão Crunch, Kevin Poulsen e Kevin Mitnick (esses últimos dois mais recentes), fazem com que as pessoas se preocupem e tenham um medo maior do computador.

Diariamente páginas são tiradas do ar por piratas digitais. Grupos de hacker e crackers realizam façanhas extraordinárias, como invadir sites da Microsoft, da Nasa, FBI, Interpol entre muitos outros. Os grupos brasileiros atualmente, são os que mais se destacam em todo o mundo, fazendo com que à própria Nasa, restrinja acesso aos usuários Brasileiros em algumas de suas páginas.

Invasores digitais (Nomenclatura e definição)

Todos os dias surgem notícias sobre piratas digitais na televisão e na Internet. Um pirata invadiu o computador de um sistema de comércio eletrônico, roubou os números de cartão de crédito dos usuários.

Mais recentemente um grupo estrangeiro conseguiu tirar mais de 650 sites do ar em um minuto. Para entender como se organiza a hierarquia virtual da Internet, vamos estudar seus principais integrantes:

Hacker

Os Hackers usam sua inteligência para o bem, quando não, não visam prejudicar ninguém, promovem invasões apenas pra provar sua capacidade, entrando e saindo sem causar nenhum dano, mas sempre deixando um alerta do dono do site ou do serviço invadido. Infelizmente a imprensa confunde os termos e toda notícia referente a baderneiros digitais são erroneamente atribuídas aos Hackers.

Crackers

Com um alto grau de conhecimento e nenhum respeito, invadem sistemas de todo o mundo, podendo apenas deixar a sua “marca”, tirar o sistema do ar ou destruí-los por completo.

Geralmente, Crackers são Hackers que querem se vingar de alguém. Hackers e Crackers costumam sempre estar em conflito. Guerras entre os grupos são comuns na rede.

Hoje para se protegerem as grandes empresas, contratam Hackers para protegerem seus sistemas.

Mitos e fantasias

O maior mito existente na Internet é que um Cracker pode invadir qualquer computador na hora que quiser. Não é bem assim. Invasões por Instant Messengers, por exemplo, são pura lenda, isso só era possível em versões antigas dos programas. Para invadir um computador pessoal, existem duas maneiras mais conhecida: trojans e netbios. A não ser que seja um computador que rode muitos serviços do tipo FTP, WWW e Telnet, o risco é mínimo.

Dicas

Faça sempre backup dos logs e uma varredura do sistema em busca de falhas ou programas desconhecidos e não foram instalados por você, a Microsoft, por exemplo, disponibiliza em seu site ferramentas para isso como o Windows defender.

Um bom antivírus também é indispensável.

Programas para segurança, como firewalls, detectores de intrusos entre outros, dê preferência para os mais conhecidos e de empresas conceituadas.

Invasão por portas TCP e UDP

Trojans

Definição de Trojan

O nome trojan é uma alusão à história do antigo cavalo de tróia, em que o governante da cidade de Tróia na antiga Grécia foi presenteado com um cavalo de madeira no qual havia escondido soldados inimigos. Conseguem ficar escondidos em arquivos de inicialização do sistema operacional e se iniciam toda vez que a máquina é ligada.

Perigo real

A popularização da Internet e a facilidade de se criar um programa cavalo de tróia fazem com que esse método de invasão seja atualmente o mais perigoso de todos. Ele não depende de falhas no seu sistema, é quase indetectável e pela sua facilidade de uso pode ser operado por crianças de 6 anos. Pode-se esconder um trojan em fotos, arquivos de música, aplicativos e jogos

Política de Segurança

A importância:

A política de segurança é o fundamento para as questões relacionadas à proteção da informação, um papel importante em todas as organizações.

O desenvolvimento é o primeiro e o principal passo da estratégia, no entanto, as maiores dificuldades estão mais na sua implementação do que em seu planejamento e elaboração.

Tem uma importante função como facilitadora e simplificadora do gerenciamento de todos os seus recursos. O gerenciamento de segurança é a arte de criar e administrar a política de segurança, pois não é possível gerenciar o que não pode ser definido.

O planejamento:

O planejamento da política da segurança deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que devem ser obedecidas por todos. Essas regras devem especificar quem pode acessar quais recursos, quais são os tipos de usos permitidos no sistema, bem como os procedimentos e controles necessários para proteger as informações.

A política de segurança também pode ser dividida em vários níveis, partindo de um nível mais genérico, passando pelo nível dos usuários, chegando ao nível técnico.

Os elementos:

Os elementos são essências para combater invasões, são eles:

Vigilância: o sistema deve ser monitorado a todo o momento.

Atitude: postura e conduta quanto à segurança; significa também o correto planejamento.

Estratégia: deve ser criativo quanto às definições da política e do plano de defesa contra intrusões.

Tecnologia: a solução tecnológica deve ser adaptativa e flexível, com o objetivo de suprir as necessidades estratégicas da organização.

Uma política de segurança de sucesso abrange sempre esses quatro principais itens.

Uma característica importante é que ela deve ser curta o suficiente para que seja lida e conhecida por todos os funcionários da empresa.

Considerações sobre a segurança:

É necessário que os responsáveis pelo desenvolvimento da política de segurança tenham o conhecimento dos diversos aspectos de segurança e também familiarização com as questões culturais, sociais e pessoais que envolvem o bom funcionamento da organização.

Aqui estão algumas considerações sobre a segurança, importantes para a definição de uma boa política de segurança.

Conheça seus possíveis inimigos.

Contabilize os valores.

Identifique, examine e justifique suas hipóteses.

Controle seus segredos.

Avalie os serviços estritamente necessários para o andamento dos negócios de organização.

Considere os fatores humanos.

Conheça seus pontos fracos.

Limite à abrangência do acesso.

Entenda o ambiente.

Limite à confiança.

Nunca se esqueça da segurança física.

A segurança é complexa.

A segurança deve ser aplicada de acordo com os negócios das organizações.

Os pontos a serem tratados:

É de responsabilidade do administrador alertar sobre as questões de segurança e implementar as medidas definidas na política.

É essencial que exista sua participação no trabalho de desenvolvimento da política e também na definição das normas e procedimentos a serem adotados.

Uma política de segurança adequada deve tratar não só dos aspectos técnicos, mas principalmente daqueles relacionados ao trabalho. Ela deve abordar, especialmente, os aspectos do cotidiano, como por exemplo, a definição dos cuidados necessários como documentos em mesas de trabalho e ate mesmo com o lixo.

Os aspectos culturais e locais também devem ser considerados na elaboração da política de segurança, pois eles influenciam diretamente na sua efetividade.

A política de segurança deve definir também, do modo mais claro possível, as punições e os procedimentos a serem adotados, no caso do não-cumprimento da política definida.

Devem ser tomadas algumas atitudes:

A segurança é mais importante do que os serviços.

A política de segurança deve evoluir constantemente.

Aquilo que não for expressamente permitido será proibido.

Nenhuma conexão direta com a rede interna, originária externamente, deverá ser permitida sem que um rígido controle de acesso seja definido e implementado.

Os serviços devem ser implementados com a maior simplicidade possível.

Devem ser realizados testes.

Nenhuma senha deve ser fornecida em claro.

A implementação:

A implementação deve ser divulgada, como por exemplo, através de e-mails, painéis, páginas da internet.

Os esforços necessários para a implantação da segurança podem levar anos ate que se consiga o resultado esperado.

Seu desenvolvimento ajuda a diminuir, e não a aumentar, os custos operacionais.

A política de segurança deve ser aplicada de maneira rigorosa e a não-conformidade deve ser punida.

Alem da auditoria, o monitoramento e a revisão da política é importante para a melhoria contínua dos procedimentos de segurança da organização.

Os maiores obstáculos para a implementação:

Recursos financeiros insuficientes.

Dificuldade dos executivos em compreender os reais benefícios da política de segurança para a organização.

Os executivos podem aprovar uma política de segurança apenas para satisfazer os auditores, e isso acaba comprometendo a própria organização.

Dependências: as dependências existem nos diversos tópicos da política, por exemplo, os usuários irão reclamar que não conseguem trabalhar remotamente (comprometendo sua produtividade) e os executivos, por sua vez, irão reclamar que os usuários não podem trabalhar remotamente, porque não existe tecnologia que possibilita o acesso remoto seguro.

Alguns executivos podem resistir à implementação da política, por acharem que isso trará ameaças ao seu poder e prestígio.

Geralmente, os executivos não gostam de compartilhar e discutir os detalhes técnicos sobre a segurança.

“Não podemos lidar com isso, pois não temos um processo disciplinar.”: um processo disciplinar especifico para os casos de não-cumprimento da política definida é importante para a organização.

Política para senhas:

A provisão de senhas pelos administradores de sistemas e a utilização de senhas pelos usuários é uma parte especifica da política de segurança, de grande importância para as organizações. Elas são consideradas também perigosas, principalmente porque dependem do ‘elo mais fraco da corrente da segurança’ que são os usuários.

O ser humano consegue memorizar apenas senhas com tamanho curto, o que compromete sua eficiência.

A política de senhas é importante também porque diversos problemas de segurança das empresas estão relacionados a elas. O esquecimento das senhas é um fato comum, e apresenta cerca de 30% dos chamados ao help desk.

Uma boa política de senhas que auxilie os usuários na escolha das mesmas e balanceie os requisitos de segurança mínimos para reduzir os problemas de esquecimentos, portanto, significa também uma melhor produtividade dos usuários e menores custos com o help desk.

Um modo de comprometer as senhas é por meio do crack, um software que realiza a codificação de palavras do dicionário. O uso de composições entre letras, números e caracteres especiais minimiza a efetividade do ataque do dicionário.

Outro ataque que tem como objetivos descobrir senhas de usuários é a adivinhação de senhas (password guessing).

Deve-se auxiliar o usuário a escolher uma senha adequada.

A senha deve ser redefinida pelo menos a cada dois meses.

As informações sobre o ultimo acesso devem constar.

As senhas devem ser bloqueadas a cada três ou cinco tentativas sem sucesso.

A transmissão da senha deve ser feita de modo cifrado, sempre que possível.

As atividades de autenticação devem ser registradas e verificadas.

As senhas e as informações relativas a contas devem ser armazenadas de modo extremamente seguro.

Política para Firewall:

Um dos principais elementos da política de segurança para o firewall é a definição das regras de filtragem, que, por sua vez, têm como base a definição dos serviços a serem fornecidos para os usuários externos e a dos serviços que os usuários internos podem acessar.

O firewall geralmente resulta em diversos questionamentos para as organizações. Por exemplo, no Brasil, os cidadãos costumam entregar suas declarações de imposto de renda via internet. Como o software para a entrega da declaração utiliza um protocolo proprietário, ele não funciona normalmente em um ambiente comum, necessitando, assim de uma regra especifica no firewall para que ele possa funcionar adequadamente.

Política para acesso remoto:

Outro aspecto importante que deve ser considerado na política de segurança é o acesso remoto. O crescimento da necessidade de acesso remoto, advindos do trabalho remoto e da computação móvel, transforma esse aspecto em uma das principais prioridades das organizações atuais.

Firewall

O que é um firewall

É um software que trabalha nas camadas de transporte e de rede do modelo TCP/IP, tendo como principal finalidade a filtragem de pacotes. Ele analiza todos os pacotes que entram ou saem de todas as interfaces de rede a ele conectado, ou seja, analiza tanto pacotes destinados diretamente ao Firewall, quanto aqueles destinados a qualquer host conectado a ele por meio de alguma de suas interfaces de rede. Sua principal função também é bloquear todas as portas quem não estejam sendo utilizadas.

História

Na Decada de 80, a AT&T precisava de um software que analizace e filtrace todos os pacotes que trafegassem em sua rede corporativa, então a Bell Labs, a pedido da AT&T, desenvolveu o primeiro Firewall do mundo e que mesmo com toda a evolução tecnologica, mantem os mesmos principios de quado foi criado.

Desde sua primeira geração, ainda na v.1.x de seu Kernel, o Linux insere a propriedade de filtragem de pacotes, mas isso porque foi agregado a ele o NetFilter, criado por Marc Boucher, James Morris, Harald Welte e Rusty Russell.

Outros softwares que podemos associar aos Firewalls

Proxy

Os Proxies tem como função principal, analisar o que chamamos pacotes de Internet, FTP e HTTP por exemplo. Os Proxies também têm a função de fazer cache do tráfego Internet, alem de prover controle de acesso por meio de autenticação, as empresas costumam usá-los para controle e monitoramento do acesso à Internet.

IDS (Intrusion Detection System)

Os IDS's são desenvolvidos baseando-se nos tipos conhecidos de ataques e também verificando alterações de comportamento do tráfego TPC/IP. Sempre que é detectada alguma alteração no comportamento do tráfego, ou identificando algum tipo de ataque, ele pode enviar alertas aos administradores, contra atacar ou simplesmente se defender baseado em alguma configuração pré-definida.

Aplicabilidade

Os Firewalls são usados basicamente para analisar e filtrar pacotes destinados e ele mesmo, uma característica comum nos Firewalls pessoais.

Quando falamos de ambientes corporativos, o Firewall trabalha sendo o ponto central de conexão entre as redes, analisando e filtrando todos os pacotes destinados a qualquer uma das redes a ele conectado.

Nos ambientes corporativos, sempre são usados Firewalls do tipo Híbrido e sempre associando eles a outros softwares (Proxy ou IDS).

Conclusão

Você viu que apesar de existirem pequenas organizações a grandes, o padrão de segurança sempre deve ser o mesmo, até porque os ataques de hackers, na maioria das vezes, utilizam mesmo método para qualquer tipo de organização.

Foi visto que em relação à política de segurança, é importante que cada organização deve ter sua própria política, visando assim, um melhor desempenho. Essa política deve ser abrangente e flexível o suficiente para que não sofra alterações freqüentes.

Um Firewall é um equipamento essencial e fundamental para qualquer projeto de Segurança da Informação, pois obrigatoriamente, tem que estar incluído na interconexão entre redes, sempre analisando, filtrando pacotes e bloqueando as portas que não estejam sendo utilizadas, minimizando assim os meios de invasão em uma rede.

No protocolo TCP/IP existe uma área responsável pelo controle de dados e a outra que são os dados em si, o empacotamento nada mais é que a junção do controle e dos dados em um único pacote.