1

Segurança do Ambiente Lógico

Segurança e Auditoria de Sistemas

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Firewalls

Com o avanço das redes de computadores e a possibilidade de conectar praticamente qualquer computador a outro, um grande problema surgiu aos administradores de rede, a possibilidade de um intruso acessar uma rede privada se passando por um usuário legítimo e ter acesso a informações sigilosas. (CARUSO & STEFFEN, 2006). Além disso, conforme TANEMBAUM (2003), existe ainda o problema dos vírus e worms, que podem burlar a segurança e destruir dados valiosos.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Firewalls

Para ajudar a manter as redes mais seguras, os *Firewalls* remetem à idéia de uma única passagem para os dados, onde todos são analisados antes de serem liberados e, de fato, o que acontece é exatamente isso, todo o tráfego de uma rede passa obrigatoriamente por uma estação de controle para ser analisado, caso não encontre nenhuma restrição, o *Firewall* libera o pacote e este segue para seu destino, caso contrário, é sumariamente descartado.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Firewalls

CARUSO & STEFFEN (2006, p. 218) afirmam que:

"Normalmente, um Firewall é instalado no ponto de interligação de uma rede interna com a Internet. Todo o tráfego, nos dois sentidos, tem de passar por este ponto e, dessa forma, atender aos requisitos da política de segurança da instalação."

O administrador da rede pode definir políticas específicas para a filtragem do tráfego da rede, por exemplo, pode indicar que todo o tráfego endereçado para a porta 23 seja bloqueado. Desta forma o atacante, ao enviar pacotes de fora da rede para a porta 23, será automaticamente ignorado pelo destino e ainda, o administrador poderá ser alertado sobre a tentativa.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Firewalls

O Firewall se divide em dois componentes: o **filtro de pacotes**, que faz exatamente a função exemplificada anteriormente, inspecionando cada pacote de entrada e saída, e identificando a origem e o destino de cada um. E o **gateway** de aplicação que, conforme TANEMBAUM (2003), em vez de apenas examinar os pacotes brutos, o gateway toma a decisão de transmitir ou descartar a mensagem através da análise dos campos de cabeçalho, do tamanho da mensagem e até do seu conteúdo (em busca de palavras-chave). Esta última situação é bastante útil quando se deseja bloquear o acesso a conteúdos que não têm uma fonte específica, ou que são providos por um serviço onde as portas são atribuídas dinamicamente. Neste caso os pacotes passariam pelo filtro de pacotes, porém seriam bloqueados pela análise do gateway de aplicação.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Firewalls

Muitos Firewalls já identificam os ataques antes que consigam causar algum dano sério. Porém, um dos ataques mais comuns e que ainda é a causa de muitas indisponibilidades de serviços é o ataque de negação de serviço (DoS), onde o atacante envia milhares de pedidos de conexão ao servidor, que por sua vez responde a cada um deles, normalmente cada pedido fica retido por um tempo até que seja eliminado automaticamente pelo servidor, porém, até que isso aconteça o limite de conexões do servidor pode ser excedido, e a partir daí nenhuma conexão nova poderá ser aceita, deixando o serviço em questão indisponível para outros usuários. Para se proteger contra esse ataque o Firewall deve ser configurado para limitar a quantidade de conexões estabelecidas por cada usuário, desta forma, mesmo que o atacante utilize vários endereços de origem diferentes para conseguir várias conexões, será mais trabalhoso conseguir a negação do serviço para usuários legítimos.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Firewalls

Muitos Firewalls já identificam os ataques antes que consigam causar algum dano sério. Porém, um dos ataques mais comuns e que ainda é a causa de muitas indisponibilidades de serviços é o ataque de negação de serviço (DoS), onde o atacante envia milhares de pedidos de conexão ao servidor, que por sua vez responde a cada um deles, normalmente cada pedido fica retido por um tempo até que seja eliminado automaticamente pelo servidor, porém, até que isso aconteça o limite de conexões do servidor pode ser excedido, e a partir daí nenhuma conexão nova poderá ser aceita, deixando o serviço em questão indisponível para outros usuários. Para se proteger contra esse ataque o Firewall deve ser configurado para limitar a quantidade de conexões estabelecidas por cada usuário, desta forma, mesmo que o atacante utilize vários endereços de origem diferentes para conseguir várias conexões, será mais trabalhoso conseguir a negação do serviço para usuários legítimos.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Antivírus

Os vírus de computador se tornaram uma praga no mundo digital e as empresas têm gasto milhares de Dólares na busca por formas de combatê-los. Basicamente um vírus é um código malicioso que se hospeda em outro programa do computador. Segundo TANENBAUM & WOODHULL (2000), quando um programa infectado é iniciado, este começa uma varredura no disco rígido em busca de outros arquivos executáveis, quando um programa é localizado, ele é infectado anexando-se código do vírus no final do arquivo e substituindo a primeira instrução por um salto para o vírus. Desta maneira, toda vez que o usuário tenta executar um programa infectado, irá, na verdade, executar o código do vírus e estará, cada vez mais, propagando o código malicioso para outros arquivos.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Antivírus

Combater um vírus não é uma tarefa fácil (TANEMBAUM, 2003), principalmente devido ao fato de que ele pode ter embutido em seu código uma característica de mutação própria, transformando-se novamente em uma estrutura desconhecida pelo antivírus. CIDALE (1990) cita quatro formas diferentes de detecção possíveis para antivírus:

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Antivírus

1. **Escaneamento de vírus conhecidos**: Apesar de ser bastante antigo, este ainda é o principal método de detecção de códigos maliciosos. Assim como, na área da saúde, os médicos e infectologistas precisam conhecer parte do vírus (biológico) para desenvolver uma vacina que será aplicada em humanos, na área computacional, as empresas desenvolvedoras dos antivírus (digitais) precisam também conhecer o código malicioso para poder criar uma vacina e proteger os computadores. Uma vez que as empresas recebem o vírus, uma parte do código é separada (string) e tomada como "assinatura" ou impressão digital do vírus, que por sua vez, passa a integrar uma lista de vírus conhecidos. Esta lista é distribuída por meio de atualizações via internet para os computadores pessoais. A partir daí, sempre que o antivírus identificar em um programa a string de um vírus, este será bloqueado.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Antivírus

2. **Análise Heurística:** Este processo consiste em uma análise, por parte do antivírus, em programas que estão sendo executados em busca de indícios de ações que seriam executadas comumente por vírus. Por exemplo, uma função de escrita em um arquivo executável, ou em vários arquivos executáveis de forma seqüencial, isso poderia ser um indício de que um código malicioso estaria tentando se propagar, atribuindo seu código à outro executável. Neste caso a análise Heurística do antivírus deve bloquear a ação e alertar o usuário sobre o evento. Este é um processo complexo e que nem sempre funciona como deveria, conforme CIDALE (1990), algumas funções que seriam identificadas como suspeitas podem ser totalmente normais em determinadas circunstâncias, gerando o que o próprio chama de falso positivo, que é quando um alerta de vírus é dado para um arquivo legítimo.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Antivírus

3. **Busca Algorítmica:** Em comparação com o primeiro método, este processo de identificação é um pouco mais preciso, pois utiliza um conceito de busca mais complexo. Uma série de condições pode ser imposta para que o vírus seja identificado, como a extensão do arquivo, o tamanho, a string, e outros mais. Devido à sua maior complexidade, torna a pesquisa mais lenta e, por isso, acaba sendo utilizado apenas em casos onde o método de comparação de string não é eficaz.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Antivírus

4. **Checagem de Integridade:** Diferentemente dos outros métodos, nesta técnica não é necessário conhecer o código do vírus anteriormente para se proteger dele. Consiste basicamente em criar um registro com os dígitos verificadores de todos os programas instalados no computador, TANENBAUM (1999) afirma que tal registro deve ser feito logo após uma formatação completa e armazenado em um local seguro no computador e criptografado. Posteriormente, quando executada uma verificação, o código verificador do programa em execução será comparado com o código armazenado no banco de dados do antivírus, caso haja alguma alteração significa que o programa foi alterado sem permissão. Tal abordagem não impede a infecção, mas permite detectar cedo a sua presença.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Antivírus

Como podemos perceber nenhum dos métodos disponíveis até hoje é completamente eficaz contra as pragas virtuais. O mais certo é utilizar um antivírus que esteja sempre atualizado e que possua métodos de detecção próprios eficientes como a Análise Heurística e a Checagem da Integridade, mesmo assim, deve-se sempre instalar softwares originais e de fontes confiáveis (TANEMBAUM, 1999).

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Segregação de Redes

A norma NBR ISO/IEC 17799 (2005) afirma, em um dos seus controles, que um método de controlar a segurança da informação em grandes redes é dividi-la em domínios de redes lógicas diferentes. De fato, esta é uma prática comum em redes de computadores estruturadas que garante acesso restrito a certos serviços. Por exemplo, uma instituição de ensino como uma faculdade, que possui laboratórios de informática utilizados por seus alunos, não seria conveniente que eles estivessem desenvolvendo suas pesquisas na mesma rede onde se encontra o servidor de banco de dados com suas notas, faltas e vida financeira. Tais dados poderiam estar em risco. Porém, também não seria conveniente para a instituição manter uma infra- estrutura física separada para atender apenas aos laboratórios, isso sairia caro, portanto com a divisão lógica da rede é possível manter apenas uma estrutura física impondo limites logicamente.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Segregação de Redes

“Tal perímetro de rede pode ser implementado instalando um gateway seguro entre as duas redes a serem interconectadas para controlar o acesso e o fluxo de informação entre os dois domínios. Convém que este gateway seja configurado para filtrar tráfico entre estes domínios e bloquear acesso não autorizado conforme a política de controle de acesso da organização". (NBR ISO/IEC 17799, 2005, p. 74).

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Segregação de Redes

Outra situação onde a segregação de rede se faz necessária é quando máquinas da rede precisam receber acessos externos, como é o caso de servidores Web e email, por exemplo. O fato de deixá-las no mesmo segmento de rede de outras máquinas não impediria que o serviço que elas executam funcionasse corretamente, porém, em caso de invasão todo o segmento de rede estaria em risco. O atacante poderia se utilizar de uma falha no servidor Web para ter acesso ao servidor de banco de dados da empresa e roubar informações sigilosas, além é claro, de ter controle sobre o primeiro servidor.

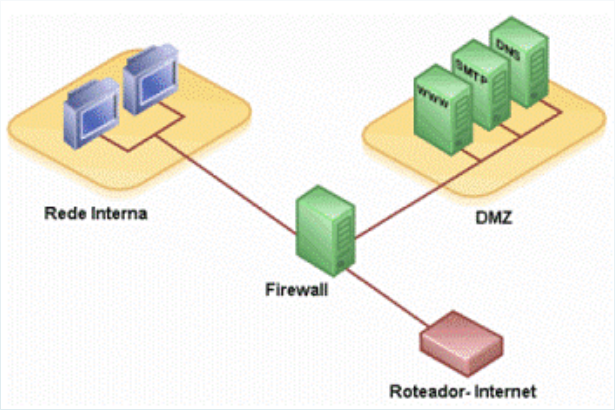
Neste caso, seria criada uma divisão lógica, ou uma sub-rede, chamada de DMZ (Zona Desmilitarizada). Este segmento seria protegido por um Firewall, porém, permitiria o acesso de clientes externos conforme demandam os seus serviços.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Segregação de Redes

Segundo SÊMOLA (2003), o conceito de Firewall, e que se aplica muito bem nessa situação, está ligado às paredes internas de uma construção que impedem que o fogo se propague de uma sala para outra. Caso o atacante consiga explorar uma falha em um dos serviços da DMZ, ainda não teria acesso à rede interna da corporação. A recomendação da norma NBR ISO/IEC 17799 (2005, p. 73) é que "os domínios sejam definidos de acordo com uma análise de riscos e requisitos de segurança diferentes". Esta análise pode determinar a divisão da rede em vários segmentos, como sistemas publicamente acessíveis, redes internas e ativos críticos [19].



Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Controle de Acessos de Usuários

O objetivo do controle de acessos de usuário é controlar o acesso à informação. (NBR ISO/IEC 17799, 2005). CARUSO & STEFFEN (2006) afirmam que o controle de acessos leva em consideração, basicamente, duas questões que devem se respondidas antes de qualquer coisa:

- Quem irá acessar?
- Quais recursos serão acessados?

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Controle de Acessos de Usuários

Essas duas questões irão gerar um inventário com todos os usuários e os recursos disponíveis no ambiente da empresa. Conhecendo os usuários, deve-se organizá-los em grupos por departamentos ou por funções relacionadas. A seguir, os direitos de acesso devem ser dados por pessoas autorizadas de dentro da empresa. “Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços". (NBR ISO/IEC 17799, 2005, p.66).

Vários usuários poderão receber as mesmas designações de acesso às informações, por isso, devem ser agrupados em entidades, e as permissões atribuídas à entidade, facilitando o gerenciamento dos privilégios.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Monitoramento

O monitoramento das atividades em um ambiente de tecnologia da informação tem como objetivo principal detectar atividades não autorizadas realizadas por usuários internos ou externos. (NBR ISO/IEC 17799, 2005). O registro das atividades deve ser feito de forma automática pelos sistemas, gerando um arquivo chamado de log. Este arquivo deve ser protegido contra falsificação e acesso não autorizado, mantendo a sua integridade e confiabilidade caso seja necessário utilizá-lo. (TANEMBAUM, 1999).

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Monitoramento

Muitos dos logs gerados trazem informações referentes não só aos acessos de usuários, mas também, informações técnicas referentes aos recursos do sistema. Essas informações podem ser úteis na resolução de problemas, pois muitos sistemas emitem alertas sobre deficiências encontradas na execução de tarefas. Desta forma registros de log geralmente contêm um grande volume de dados, tornando difícil para uma pessoa identificar eventos importantes. Por tanto, a norma NBR ISO/IEC 17799:2005 recomenda o uso de ferramentas de auditoria para a análise adequada desse material.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Monitoramento

Alguns sistemas, como o Microsoft Windows Server 2003, por exemplo, possuem uma ferramenta de análise de logs própria, que em caso de eventos considerados relevantes envia uma mensagem para o administrador informando sobre o problema.

As atividades de todos os usuários (administradores ou operadores) devem ser registradas sejam estas realizadas em um sistema operacional ou em um software ERP [20]. CARUSO & STEFFEN (2006) definem alguns dados como indispensáveis em um log:

- Identificação do usuário;
- Data, horário;
- Informações sobre o evento;
- Identificação do terminal utilizado.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Monitoramento

O monitoramento pode ser feito não só através de logs, mas, também em tempo real, como é o caso dos sistemas de monitoramento de serviços. Basicamente, o administrador tem acesso às condições de operação de um ativo mesmo este estando em uso, seja um software ou hardware. E através da emissão de relatórios é possível identificar problemas, planejar melhorias ou, definir regras para uma melhor utilização da ferramenta.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Criptografia

Com a vulnerabilidade dos mecanismos de comunicação utilizados atualmente sempre existe a possibilidade de interceptação dos dados trafegados. CARUSO & STEFFEN (2006, p. 172) afirmam que “enquanto as linhas de comunicação fizerem uso de sinais elétricos para a transmissão de sinais, elas continuarão a ser vulneráveis à penetração não autorizada". Isso se deve ai fato de que interceptar um sinal elétrico é muito simples e pode ser difícil de identificar o intruso.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Criptografia

Como muitas vezes é impossível garantir a confiabilidade do meio de transmissão, passou-se a utilizar uma técnica para esconder a mensagem caso esta fosse interceptada durante o trajeto. A palavra criptografia tem origem grega, significa "escrita secreta", esta técnica já é utilizada a milhares de anos. (TANEMBAUM, 1999). Consiste basicamente na substituição ou transposição de caracteres de uma mensagem.

O emissor criptografa o texto utilizando um padrão estabelecido pela chave de cifragem e envia a mensagem ininteligível. Chegando ao destino, o texto cifrado precisa ser descriptografado, realizando o processo inverso, e seguindo o mesmo padrão estabelecido pelo emissor. As chaves de cifragem dividem-se em simétricas e assimétricas.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Criptografia

Na **criptografia simétrica** a chave utilizada para cifrar uma mensagem é a mesma utilizada para voltar ao texto inteligível (CARUSO & STEFFEN, 2006). Neste caso o destinatário deve conhecer a chave utilizada pelo emissor para efetuar a troca. É um processo simples, muito utilizado pela maioria dos algoritmos, porém não muito seguro, já que se a chave for descoberta qualquer um poderá ler a mensagem cifrada. (CARUSO & STEFFEN, 2006). Um exemplo claro deste tipo de chave é a Cifra de César, onde cada letra da mensagem é substituída por outra do alfabeto, seguindo um número de troca de posições. Por exemplo, utilizando uma troca de quatro posições, a letra A seria substituída pela letra E, a letra B seria F e assim por diante. Juntamente com a mensagem cifrada, o emissor deve encontrar um meio de informar ao destinatário qual a chave para descriptografar a mensagem. Nesse caso, o número de troca precisa ser informado.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Criptografia

Já na **criptografia assimétrica**, a chave usada para criptografar não pode ser usada para reverter o processo; isto só é possível com uma chave complementar. (CARUSO & STEFFEN, 2006). Um dos poucos exemplos que temos é o método de chaves públicas RSA. Este método é baseado em cálculos com números primos, e se utiliza da dificuldade de fatorar tais números. Teoricamente, é perfeitamente possível quebrar a chave RSA, porém matemáticos têm tentando fatorar números extensos há pelo menos trezentos anos e o conhecimento acumulado sugere que o problema é extremamente difícil (TANEMBAUM, 1999). Na prática o algoritmo funciona da seguinte forma: primeiro um dos indivíduos (A) que participará da comunicação cria uma chave pública e envia para o outro indivíduo (B), na verdade estará enviando o algoritmo de encriptação. Depois A deve criar a chave privada que será conhecida apenas por ele próprio. B poderá enviar mensagens para A através da chave pública, porém apenas A terá a chave privada para fazer a leitura da mensagem.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Criptografia

CARUSO & STEFFEN (2006) fazem uma analogia comparando a chave pública como um cadeado e a chave privada como a chave do cadeado, todos podem fechá-lo, porém só um terá a chave para abri-lo. TANEMBAUM (1999) deixa claro que quanto maior for o número criptográfico escolhido pelo emissor, maior será a dificuldade em quebrar o algoritmo, de fato, a fatoração de um número de 500 dígitos levaria 1025 anos. Em contrapartida, maior também, será o tempo gasto no processo de encriptação, o que às vezes, pode não ser satisfatório. CARUSO & STEFFEN (2006) prevêem que a única forma de quebrar a criptografia RSA, e todas as outras técnicas de chave assimétrica, seria com a entrada de operação dos computadores quânticos:

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Criptografia

“Esses computadores terão velocidade de processamento milhões de vezes mais rápida do que os atuais computadores mais rápidos. Por possuírem (por enquanto teoricamente) a capacidade de realizar cálculos simultâneos, isso eliminaria a atual segurança de métodos de chave assimétrica, como o RSA, podendo realizar ataques de força bruta quase que instantaneamente." (CARUSO & STEFFEN, 2006, p. 182).

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Backup

O processo de backup consiste na realização de cópias de segurança de arquivos ou configurações.

A norma NBR ISO/IEC 17799 (2005, p. 48) afirma que o objetivo da realização de backups é “manter a integridade e disponibilidade da informação e dos recursos de processamento de informação". Para tanto, a norma ainda trás alguns itens que devem ser considerados durante o processo:

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Backup

- Definição da necessidade das cópias;
- Produção de registros das cópias efetuadas com documentação apropriada;
- As cópias de segurança sejam armazenadas em uma localidade remota com um nível apropriado de segurança;
- As mídias sejam testadas regularmente para garantir que elas são confiáveis;
- Em caso de confidencialidade dos dados, as cópias sejam criptografadas.

Segurança e Auditoria de Sistemas

Segurança do Ambiente Lógico

Backup

Devem ser feitas cópias de segurança de todos os trabalhos desenvolvidos nas estações dos usuários. CARUSO & STEFFEN (2006, p. 194) afirmam que “essa providência facilita a recuperação das informações, precavendo-se de algum dano ou sinistro nos arquivos originais". Conforme SÊMOLA (2003), várias cópias do mesmo arquivo podem ser feitas, dependendo da sua criticidade para a continuidade dos negócios.

Referências

https://www.teleco.com.br/tutoriais/tutorialitil/pagina_4.asp