Aspecto de Segurança para uma Arquitetura Web

Luciano dos Santos Gonçalves

lucfab@cemib.unicamp.br

Resumo

A evolução da Internet tem facilitado extraordinariamente a comunicação entre instituições e pessoas no mundo inteiro. Entretanto, uma grande preocupação voltou a surgir nesse ambiente: como lidar com a segurança e o armazenamento de Informações de uma rede web. Atualmente, este é um dos assuntos mais comentados nos meios de tecnologia da informação, Por este motivo, propõem-se aqui um estudo de medidas para avaliação de serviços de uma rede web.

Palavras-chaves: DoS, Roteador, Firewalls.

Introdução

Tradicionalmente, as instituições - bancos, governos, empresas grandes ou pequenas dedicavam grande atenção à proteção de seus meios físicos e financeiros, mas pouco ou até mesmo nenhuma atenção às informações que possuíam. A tecnologia da informação atuava na retaguarda ou na melhoria de processos, mas muito dificilmente era um elemento que recebia ênfase das instituições.

Hoje, as instituições dependem da tecnologia da informação para o seu funcionamento, devido à automatização e ao mesmo tempo agregação de valores aos processos organizacionais. As redes de computadores têm simplificado muito a comunicação entre instituições e pessoas no mundo inteiro. Entretanto, com o fenômeno da globalização, surgiu uma grande preocupação com a segurança das informações a partir da década de 90.

Mas com toda essa evolução começaram a surgir os problemas. A facilidade de comunicação tornou as empresas mais vulneráveis, o ambiente passou a ser heterogêneo e mais distribuído, difícil de ser controlado. Os ataques e invasões acontecem a todo instante, as suas conseqüências cobrem uma enorme gama de possibilidades: perda de tempo recuperando a situação anterior, queda de produtividade, perda significativa de dinheiro, horas de trabalho, devastação de credibilidade ou oportunidades de marketing, empresa não habilitada a competir etc.

Em função de todos esses problemas, e da necessidade de se garantir um nível maior de segurança para os dados e privacidade para seus “donos”, serão desenvolvidas atividades que adequam a estrutura tecnológica da empresa para dar sustentação à segurança tanto das transações efetuadas como da própria organização, eliminando vulnerabilidades e ao mesmo

tempo criando um ambiente que possa ser mais facilmente controlado e monitorado. Enfim, criando uma infra-estrutura de rede que seja eficiente e, sobretudo confiável.

2. Princípios da Segurança da Informação

A segurança da informação é o bem mais valioso de uma instituição ou empresa, ela busca reduzir no máximo possível os riscos de vazamentos de informações, fraudes em arquivos, Banco de Dados, erros humanos e operacionais, uso indevido do sistema por falta de treinamento, sabotagens, paralisações de rede ou serviços, roubo de informações ou qualquer outra ameaça que possa prejudicar a instituição ou equipamentos da mesma.

Qualquer solução de segurança da Informação deve satisfazer os seguintes princípios:

- ✓ **Confidencialidade:** Significa proteger informações contra sua revelação para alguém não autorizado (interna ou externamente) e leitura e/ou cópia não autorizado. A informação deve ser protegida independentemente da mídia que a contenha (mídia impressa ou digital). Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas.
- ✓ **Autenticidade:** O controle de autenticidade está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema. Ela é a medida de proteção de um serviço/informação contra a personificação por intrusos.

- ✓ **Integridade:** A integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos ou fitas de backup. Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é assegurada evitando-se alteração não detectada de mensagens (Ex: tráfego bancário) e o forjamento não detectado de mensagem (aliado à violação de autenticidade).
- ✓ **Disponibilidade:** Consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

3. Ataque de Senhas

A utilização de senhas seguras é um dos pontos fundamentais para uma estratégia efetiva de segurança. A senha tem como objetivo permitir que somente as pessoas autorizadas tenham acesso a um sistema ou à rede, e são criadas e implementadas pelos próprios usuários ou pelos sistemas que gera a senha automaticamente. Palavras, símbolos ou datas fazem com que as senhas tenham algum significado para os usuários, permitindo que eles possam facilmente lembrá-las. Neste ponto é que existe o problema, pois muitos usuários priorizam a conveniência ao invés da segurança. Como resultado, eles escolhem senhas que são relativamente simples, para que possam lembrar facilmente, facilitando o trabalho dos *hackers*. Em virtude disso, invasores em potencial estão sempre testando as redes e sistemas em busca de falhas para entrar.

Parte da responsabilidade dos administradores de sistemas é garantir que os usuários estejam cientes da necessidade de utilizar senhas seguras. Isto leva a dois objetivos a serem alcançados: educar os usuários sobre a importância do uso de senhas seguras; e implementar medidas que garantam que as senhas escolhidas pelos usuários sejam efetivamente adequadas (pelo menos oito caracteres, não iniciando com números, terem letras e números misturados e incluir pelo menos um caractere especial como por exemplo: **./<>;':"[]\{}|~!@#$%^&*()_+`-=**). Para alcançar o primeiro objetivo, a educação do usuário é o ponto chave. Já para alcançar o segundo objetivo, é necessário que o administrador de sistemas esteja um passo à frente, verificando possíveis senhas inseguras.

CLIFF [1], descreve as duas técnicas de ataque de senhas:

- **Ataque de Dicionário:** Nesse tipo de ataque são utilizados combinações de palavras, frases, letras, números, símbolos, ou qualquer outro tipo de combinação geralmente que possa ser utilizada na criação das senhas pelos usuários. Os programas responsáveis por realizar essa tarefa trabalham com diversas permutações e combinações sobre essas palavras. Quando alguma dessas combinações se referir à senha, ela é considerada como quebrada (Cracked). Geralmente as senhas estão armazenadas criptografadas utilizando um sistema de criptografia HASH. Dessa maneira os programas utilizam o mesmo algoritmo de criptografia para comparar as combinações com as senhas armazenadas. Em outras palavras, eles adotam a mesma configuração de criptografia das senhas, e então criptografam as palavras do dicionário e comparam com senha.

- **Força-Bruta:** Enquanto as listas de palavras, ou dicionários, dão ênfase a velocidade, o segundo método de quebra de senhas se baseia simplesmente na repetição. Força-Bruta é uma forma de se descobrir senhas que compara cada combinação e permutação possível de caracteres até achar a senha. Este é um método muito poderoso para descoberta de

senhas, no entanto é extremamente lento porque cada combinação consecutiva de caracteres é comparada.

Ex: *aaa, aab, aac ..... aaA, aaB, aaC... aa0, aa1, aa2, aa3... aba, aca, ada...*

4. Métodos e Ferramentas de Segurança

Uma vez conhecidos as principais ameaças e técnicas utilizadas contra a segurança da Informação, pode-se descrever as principais medidas e ferramentas necessárias para eliminar essas ameaças e garantir a proteção de um ambiente computacional. É nesse sentido que essa nova seção será apresentada.

4.1. Instalação e Atualização

A maioria dos sistemas operacionais, principalmente Unix, vem acompanhada de muitos aplicativos (Pacotes), que são instalados opcionalmente. Sendo assim, torna-se necessário que vários pontos sejam observados para garantir a segurança desde a instalação do sistema, dos quais podemos destacar:

- **Seja minimalista:** Instale somente os aplicativos (Pacotes) necessários, aplicativos com problemas podem facilitar o acesso de um atacante. Quanto mais aplicativos existirem na máquina, mais difícil é para o administrador mantê-los atualizados e informado sobre novos bugs e correções.
- **Devem ser desativados todos os serviços de sistema que não serão utilizados:** Muitas vezes o sistema inicia automaticamente diversos aplicativos que não são necessários, esses aplicativos também podem facilitar a vida de um atacante. Mais uma vez, quanto mais aplicativos inutilizados na máquina, maiores serão as chances de um atacante encontrar

uma porta aberta de seu sistema e invadi-lo. Ex. FTP se este serviço não é utilizado pela máquina não é necessário manter este aplicativo disponível no servidor.

- **Use partições diferentes para os diferentes tipos de dados:** A divisão física dos dados facilita a manutenção.

  Em meu projeto eu crie uma partição **/HOME.** Nela, serão criadas todas as contas dos Funcionários da Instituição e dos Colaboradores. E para o Banco de Dados criei uma partição **/BD,** nela ficará o Banco de Dados sendo assim ficará mais fácil de administrá-los e efetuar as devidas correções e de aplicativos e segurança da mesma.

- **Remova todas as contas de usuários não utilizadas:** Contas de usuários sem senha, ou com a senha original de instalação, podem ser facilmente exploradas para obter-se acesso ao sistema.

Grande parte das invasões pela Internet acontece devido à falhas conhecidas em aplicações de rede, as quais os administradores de sistemas não foram capazes de corrigir a tempo. Essa afirmação pode ser confirmada facilmente pelo simples fato de que quando uma nova vulnerabilidade é descoberta, um grande número de ataques é realizado com sucesso. Por isso, é extremamente importante que os administradores de sistemas se mantenham atualizados sobre os principais problemas encontrados nos aplicativos utilizados, através dos sites dos desenvolvedores ou específicos sobre segurança da Informação. As principais empresas comerciais desenvolvedoras de software e as principais distribuições Unix possuem boletins periódicos informando sobre as últimas vulnerabilidades encontradas e suas devidas correções. Alguns sistemas chegam até a possuir o recurso de atualização automática, facilitando ainda mais o processo.

4.2. Desenvolvimento de Aplicações WEB

O desenvolvimento de aplicações que irão utilizar a internet como interface, comentada aqui como Aplicações WEB, exige uma maior preocupação com a segurança no processamento e armazenamento dos dados. Esse tipo de aplicação fica exposto um grande número de usuários e ameaças. Hackers estão constantemente testando as aplicações em busca de vulnerabilidades que possam facilitar o acesso a um sistema, ou simplesmente falhas, que possam negar um serviço.

PUTTINI [2], podemos destacar algumas das principais práticas para o desenvolvimento seguro de aplicações WEB:

- **Não use mais poder do que o necessário:** As aplicações devem rodar num nível de acesso suficiente para utilizar somente os recursos necessários do servidor, não em níveis superiores, pois em caso de falhas na aplicação, ela somente terá acesso aos seus recursos e não aos pertencentes a outros processos.
- **Nunca confie nas informações fornecidas pelo usuário:** As aplicações sempre devem validar as informações enviadas pelo usuário, verificando o formato e tamanho dos dados para evitar possíveis sobrecargas de armazenamento (*Buffers Overflows).*
- **Não guarde as senhas de acesso ao banco de dados ou outros recursos dentro de páginas pré-processadas ou scripts CGI:** Muitas vezes é possível obter o seu código fonte, obtendo-se assim senhas e outras informações sensíveis.

- **Use criptografia para armazenar informações sensíveis no servidor:** Dessa maneira é possível proteger números de cartão de crédito em sites de comércio eletrônico, ou qualquer outra informação importante.
- **Não deixe comentário no código de produção:** Caso possam ser visualizados, eles podem auxiliar muito o trabalho de algum invasor.
- **Verifique e personalize as mensagens de erro:** Muitas vezes as mensagens de erro padrão de uma linguagem podem fornecer informações valiosas sobre o servidor.

- **Utilize ferramentas, linguagens e bibliotecas atualizadas:** Caso elas possuam algum problema de segurança todo o sistema estará comprometido.

5 Firewalls

HAZARI [3], define firewall como sendo uma barreira inteligente entre duas redes, geralmente a rede local e a Internet, através da qual passa tráfego autorizado. Este tráfego é examinado pelo firewall em tempo real e a seleção é feita de acordo com um conjunto de regras de acesso. É tipicamente um roteador (equipamento que liga as redes com a Internet), um computador filtrando pacotes, um software proxy, um firewall-in-a-box (um hardware proprietário específico para função de firewall), ou um conjunto desses sistemas.

Pode-se dizer que firewall é um conceito ao invés de um produto. Ele é a soma de todas as regras aplicadas à rede. São elaboradas considerando as políticas de acesso da instituição.

Podemos descrever o modelo mais comumente utilizado para implementação de um firewall, apresentado na Figura 1.

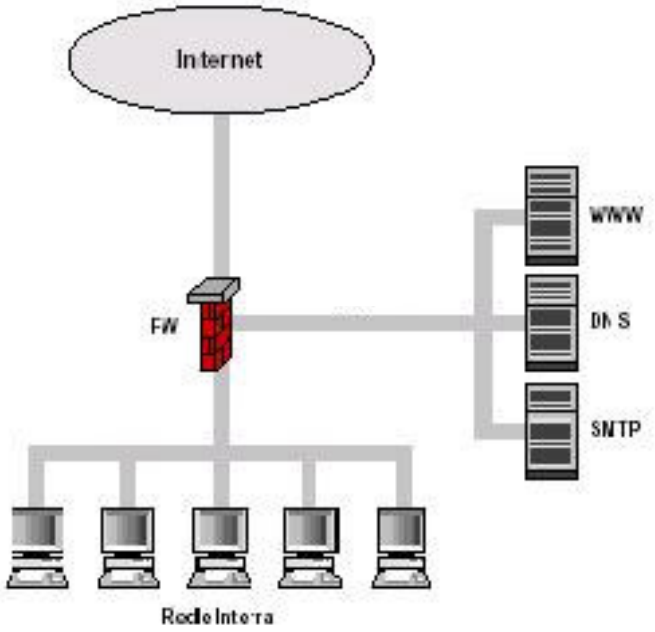

Figura 1: Modelo de Firewall

Podemos observar que o firewall é único ponto de entrada da rede. Quando isso acontece também pode ser designado como *ponto de checagem.*

De acordo com os mecanismos de funcionamento podemos destacar alguns tipos principais:

- Filtros de pacotes;
- Firewalls em Nível de Aplicação.
- Considerações sobre o uso de Firewalls

5.1. Filtros de Pacotes

Esse é o tipo de firewall mais conhecido e utilizado, pois controla a origem e o destino dos pacotes de mensagens da Internet. Quando uma informação é recebida, o firewall verifica as informações através do endereço IP de origem e destino do pacote e compara com uma

lista de regras de acesso (em meu projeto seria o arquivo **rc.firewall** que se localiza no **/etc**), para determinar se o pacote está autorizado ou não a ser repassado através dele.

Atualmente, a filtragem de pacotes é implementada na maioria dos roteadores e é transparente aos usuários.

5.2. Firewalls em Nível de Aplicação

Nesse tipo de firewall, o controle é executado por aplicações específicas, denominadas proxy, para cada tipo de serviço a ser controlado. Essas aplicações interceptam todo o tráfego recebido e o envia para as aplicações correspondentes; assim, cada aplicação pode controlar o uso de um serviço.

Apesar desse tipo de firewall ter uma perda maior de desempenho, já que analisa toda a comunicação utilizando proxy, ele permite uma maior auditoria sobre o controle no tráfego, já que as aplicações específicas podem detalhar melhores os eventos associados a um dado serviço.

Guia Internet de Conectividade [4], O endereço IP do proxy é a única informação realmente necessária. Instituições usando endereços, por exemplo, classe A (como 10.*.*.*), em suas redes particulares podem ainda acessar a internet contanto que o proxy seja visível tanto para a rede particular como para a Internet.

Proxy permite um alto nível de log das transações de clientes, incluindo endereço IP, data e hora, URL, contagem de bytes e código de sucesso. Qualquer campo (seja de meta-informação, ou seja, comum) em uma transação WEB é um candidato para log. Isto não é possível com log no nível IP ou TCP.

Também é possível fazer a filtragem de transações de clientes no nível do protocolo de aplicação. O proxy pode controlar o acesso a serviços por métodos individuais, servidores e domínios.

5.3. Considerações sobre o uso de Firewalls

Embora os firewalls garantam uma maior proteção, e são inestimáveis para segurança da informação, existem alguns ataques que os firewalls não podem proteger, como a interceptação de tráfego não criptografado, como e-mail. Além disso, embora os firewalls possam prover um único ponto de segurança e auditoria, eles também podem se tornar um único ponto de falha – o que quer dizer que os firewalls são a última linha de defesa. Significa que se um atacante conseguir quebrar a segurança de um firewall, ele vai ter acesso ao sistema, e pode ter a oportunidade de roubar ou destruir informações. Além disso, os firewalls protegem a rede contra os ataques externos, mas não contra os ataques internos. No caso de funcionários mal intencionados, os firewalls não garantem muita proteção, devido ele já está dentro da rede, onde ira tentar atacar os Servidores de Rede e achar pontos falhos nos Servidores de Aplicação WEB.

6 Política de Segurança

FONTES [5], “A política de segurança da informação é o conjunto de diretrizes que deve expressar o pensamento da alta administração da instituição em relação ao uso da informação por todos aqueles que têm acesso a esse bem. Neste caso, a administração está representando os proprietários que, como donos, devem decidir os destinos de todos os recursos da instituição.”

Dessa maneira, podemos definir a política da segurança como sendo sistemáticas gerenciais que visam determinar o nível de segurança de uma rede ou sistemas de informação de uma instituição, suas funcionalidades e a facilidade de uso.

Essas sistemáticas são reunidas em um documento formal com regras pelas quais as pessoas deverão aderir para ter acesso à informação e à tecnologia da instituição.

Para se estabelecer uma política de segurança é necessário conhecer os objetivos da instituição, para depois poder medi-los e verificar as ameaças.

Algumas características da política de segurança:

Algumas características de LIMA [6], abaixo:

- **Ser verdadeira:** A política deve realmente exprimir o pensamento da instituição e deve ser coerente com as ações dessa instituição. Deve ser possível o seu cumprimento.
- **Ser curta:** Duas a três páginas são suficientes para se formalizar uma política. Não devemos confundir política com normas e procedimentos de segurança. A política não deve ser um “Manual de Procedimentos”. Este manual pode até existir, mas terá vida própria.
- **Ser válida para todos:** A política deve ser cumprida por todos os usuários que utilizam a informação da instituição. Ela é válida para o diretor e para o estagiário recém contratado. Normalmente o "rei" não causa maiores problemas. Os problemas deste tipo são causados pelos "amigos do rei".
- **Ser simples:** A política deve ser entendida por todos. Deve ser escrita em linguagem simples e direta. A política não deve conter termos técnicos de difícil entendimento pelos "mortais".
- **Ter o patrocínio da alta direção da instituição:** O documento normativo que formalizará a política deve ser assinado pelo mais alto executivo, explicitando assim o seu total apoio à política.

As políticas de segurança podem variar muito, mas em geral sempre existem alguns pontos em comum.

- ✓ A Informação como um Bem da instituição - uso profissional;
- ✓ Controle do acesso à Informação;
- ✓ Responsabilidades – usuário e gerência;

- ✓ Preparação para situações de contingência - continuidade operacional;
- ✓ Privacidade do usuário - arquivos pessoais, correio eletrônico;
- ✓ Medidas disciplinares que serão utilizadas caso a Política não seja cumprida.

A política de segurança proporciona o direcionamento para as implementações técnicas. Implementar procedimentos de segurança sem uma política definida é equivalente a navegar sem saber onde se quer chegar. Porém, a política deve ser um elemento de um conjunto de ações que compõem o Processo de Segurança da instituição.

7 DoS - Denial-of-Service

Ter as informações acessíveis e prontas para uso representa um objetivo crítico para muitas empresas. No entanto, existem ataques de negação de serviços (DoS – Denial-of-Service Attack), onde o acesso a um sistema/aplicação é interrompido ou impedido, deixando de estar disponível; ou uma aplicação, cujo tempo de execução é crítico, é atrasada ou abortada.

Conclusão

Para se ter um sistema estável e com poucas vulnerabilidades, é necessário apenas mantermos na máquina aplicativos que estarão realmente sendo usados, pois quanto mais aplicativos sem uso, mais fácil é de se encontrar vulnerabilidades através destes aplicativos. Sempre devemos estar atentos a novas correções disponíveis do software nos mercados para podermos aplicá-las antes que alguém que saiba do problema tire proveito da situação.

A Instituição também deve se preocupar com sua segurança interna, pois a falta dela é, na maioria das vezes, o motivo causador de danos. Para tal, uma política de segurança clara e bem definida e, principalmente, sem exceções a qualquer tipo de pessoa é essencial para termos uma política bem sucedida.

Observando a parte de comunicação da Instituição, recomendamos que o firewall existente bloqueie todo o tipo de comunicação externa aos interesses da empresa como MSN e ICQ. Estes programas deixam as portas que utilizam para sua comunicação totalmente abertas a algum tipo de invasor. Sempre devemos nos preocupar em manter fechadas todas as portas não utilizadas pelo firewall.

A criptografia também é outra ferramenta muito útil e necessária quando falamos de segurança. Em todas as transações, ela deve ser utilizada para prevenir de alguma forma a ação do invasor conseguir entrar na Instituição, não conseguirá ver as informações contidas nos pacotes, pois os mesmos estarão criptografados. No acesso remoto via SSH a mesma é necessária para evitar que algum “espião” possa tirar proveito do acesso remoto e ver as informações que estão sendo trafegadas.

Hoje, existem muitos métodos de segurança disponível. Devemos ter a consciência que nenhum método é eficaz sozinho e sem as devidas correções. Segurança também é uma questão de preço. A Instituição que desejar uma boa política de segurança deve investir muito

em treinamento de seus funcionários e deixar sempre bem claro a todos que utilização recursos de sua rede, para que não aja nenhum imprevisto desagradável no parque computacional da Instituição.

Referências Bibliográficas

[1] CLIFF, A. **Password Crackers – Ensuring the Security of Your Password,** Obtido através da Internet. http://www.securityfocus.com/, 09 abr. 2001.

[2] PUTTINI, Ricardo S.; SOUZA, Rafael T. de. **Principais Aspectos da Segurança,** obtido através da Internet. Obtido através da Internet. http://webserver.redes.unb.br/security/introducao/aspectos.html, 12 fev. 2001.

[3] HAZARI, Sunil. **"Firewalls for Beginners"**. Obtido através da Internet http://www.securityfocus.com/. 22 nov. 2000.

[4] **Guia Internet de Conectividade.** 2. ed. São Paulo: Cyclades Brasil, 1999.

[5] FONTES, Edison. **Política da Segurança da Informação.** Obtido através da Internet. http://www.modulo.com.br/, 03 nov. 2000.

[6] LIMA, Marcelo B. Firewalls – **"Uma Introdução à Segurança"**. Revista do Linux. nº2, pg. 16, Fev. 2000.