Arquiteturas de Firewall: Propostas para ambientes empresariais

POSSARI, Mauricio Rafael – mauricio.possari@gmail.com[1]
ZEM, José Luís Zem (Orientador) – jose.zem@fatec.sp.gov.br

RESUMO

O firewall é um instrumento de segurança de rede bastante eficiente e que apresenta uma boa relação custo-benefício, além de ser possível encontrar no mercado soluções bastante confiáveis e, ainda, com softwares livres. Apesar disso, nem sempre ele é usado da maneira correta, pois, geralmente, é configurado apenas para separar a Internet da rede interna da empresa, subutilizando, assim, essa ferramenta. Este estudo busca demonstrar como uma Arquitetura de Firewall eficiente pode evitar problemas de segurança e limitar o campo de ação de um eventual invasor.

Palavras Chaves: firewall segurança perímetro

ABSTRACT

The firewall is a tool for network security that provides an efficient and cost-benefit relationship and be able to find solutions on the market and very reliable, even with free software. Nevertheless it's not always used the right way, because usually it's configured just to separate Internet from the company's internal network, underdoing this powerful tool. This paper seeks to demonstrate how an efficient Firewall Architecture can avoid security problems and limit the purview of an attacker.

Keywords: firewall security perimeter

[1] Aluno do Curso de Segurança da Informação. 1S/2011.

INTRODUÇÃO

O objetivo geral deste estudo é o de mostrar o ganho, em termos de segurança, obtidos quando se adota uma arquitetura de Firewall eficiente e adequada ao ambiente que deverá ser protegido.

Como objetivos específicos podem ser destacados o de apresentar as definições conceituais dos assuntos tratados, explicar o motivo da escolha de um Sistema Operacional seguro para a configuração dos bastion hosts, descrever as principais características das arquiteturas de firewall mais conhecidas, mostrar quais são as maneiras mais comuns de configuração de firewall nas empresas, mostrar exemplos de configurações seguras de rede.

O método científico de pesquisa utilizado foi o estudo teórico dos modelos clássicos de firewall e alguns outros modelos eficientes propostos por profissionais de segurança da informação. Será feita uma análise sobre alguns modelos de firewall comumente instalados nas empresas, de forma a verificar se há falhas de configuração que possam ocasionar problemas de segurança. Após a verificação dos possíveis erros serão propostos modelos de firewall que possam eliminar ou diminuir ou até mesmo eliminar tais problemas de segurança.

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES EMPRESARIAIS

A preocupação com segurança nos ambientes empresariais tem crescido em ritmo acelerado. Nos últimos anos, devido à melhora e ao barateamento dos serviços de banda larga no Brasil, a quantidade de empresas com acesso à Internet tem crescido muito. Contudo, os riscos estão lado a lado com as facilidades e os benefícios que a Internet proporciona.

É preciso ter em mente que o ativo mais importante no ambiente digital é a informação, logo, todos os esforços precisam ser empregados para protegê-la. A informação pode ser armazenada sob diversas formas, como, por exemplo,

impressa ou escrita em papel ou mesmo em algum dispositivo de armazenamento eletrônico. O foco desse trabalho é a proteção da informação armazenada digitalmente.

Para a informação ser protegida de maneira apropriada é necessário que haja um documento que defina como essa proteção será feita. Esse documento é denominado Política de Segurança da Informação e toda empresa que pretende resguardar as informações contra as ameaças deveria ter essa política bem definida.

A NBR ISO/IEC 27002 é um guia para a organização que deseja iniciar, manter ou melhorar as diretrizes e princípios gerais da gestão de segurança da informação de uma organização e, com isso, criar um documento sobre a política de segurança da informação mais adequado à realidade da empresa.

Em ambientes empresariais com acesso à Internet, a informação pode ser acessada pela rede. Uma primeira linha de proteção contra as ameaças virtuais é o Firewall. Essa ferramenta é definida por Nakamura (2000:105-106) da seguinte forma:

> (...) *firewall* é um ponto entre duas ou mais redes, ponto este que pode ser um componente ou um conjunto de componentes, por onde passa todo o tráfego, permitindo que o controle e/ou autenticação e registro de todo o tráfego seja realizado. Assim, esse ponto único constitui um mecanismo utilizado para proteger, geralmente, uma rede confiável de uma rede pública, não-confiável. Um *firewall* pode ser utilizado também para separar diferentes sub-redes, grupos de trabalhos ou LANs dentro de uma organização (...)

Ele ainda oferece outra definição:

> (...) é um sistema ou um grupo de sistemas que reforça a política de controle de acesso entre duas redes, e portanto pode ser visto como uma implementação da política de segurança.

A Política de Segurança da Informação de uma empresa é tão importante que Nakamura (2000:106) enfatiza dizendo:

> O *firewall* é tão seguro quanto à política de segurança que ele suporta (...)

Para um firewall ser eficiente, os elementos que o compõem (software e hardware) precisam ser posicionados em locais estratégicos da rede. O posicionamento dos componentes de firewall na rede visando criar uma seqüência de barreiras e controles para dificultar o tráfego malicioso nessa rede é conhecido como Arquitetura de Firewall.

Há diversos tipos de Arquiteturas de Firewall, algumas são consideradas clássicas devido a ampla aceitação dos profissionais de segurança da informação, que freqüentemente as implantam em ambientes empresariais. Porém é preciso analisar qual dessas arquiteturas é a mais indicada ao ambiente que se deseja proteger.

Também é possível realizar algumas modificações nessas arquiteturas clássicas de forma a adaptá-las às necessidades da empresa. Por exemplo, em alguns casos pode-se substituir um roteador por um computador, chamado de bastion host. Isso é feito, principalmente, para reduzir os custos com hardware. Porém nem sempre é possível realizar esse tipo de troca, pois, dependendo do arranjo dos componentes na rede, essa modificação pode acarretar em problemas de segurança.

Além do firewall há outros mecanismos de segurança, como o Proxy, a Virtual Private Network (VPN), o Sistema de Detecção de Intrusões (IDS), o Sistema de Prevenção de Intrusões (IPS), a Infra-estrutura de Chaves Públicas (ICP) e a autenticação.

O ambiente configurado com o serviço de Proxy é composto por clientes proxies e por servidores proxies. Em sua configuração convencional, o servidor Proxy recebe as requisições dos clientes, que estão na rede interna, e as retransmitem para servidores externos. O servidor pode atuar apenas como um relay, retransmitindo os pedidos dos clientes, ou pode realizar uma filtragem mais profunda dos pacotes.

Conforme SCOTT (1999:2) a VPN é uma forma de simular uma rede privada tendo como base uma rede pública, como por exemplo, a Internet. É chamada de

virtual porque depende do uso de conexões virtuais, ou seja, conexões temporárias que não são estabelecidas fisicamente. Ela é usada para criar uma conexão protegida entre dois pontos para o tráfego seguro de dados, além de reduzir os custos, por não precisar de um link de dados dedicado.

O Sistema de Detecção de Intrusões (IDS) é, conforme KORFF (2005:336), um programa ou máquina que procura por sinais que indicam que o meio está sendo atacado. O IDS é um sistema que age em modo passivo, monitorando o tráfego e alertando o usuário quando um ataque é detectado. Contudo, ele não realiza nenhuma ação para bloquear o ataque, apenas manda um sinal de alerta. A ação precisa partir do administrador, que deve analisar o alerta e tomar providencias para bloquear o ataque.

Já o Sistema de Prevenção de Intrusões (IPS) é a versão ativa do IDS. O IPS não apenas reporta um ataque, mas também bloqueia o tráfego malicioso. O problema dessa solução é que no caso de falso-positivos, o tráfego legítimo pode ser bloqueado, portanto, é preciso avaliar se a instalação de um IPS compensa o risco de bloqueio do tráfego legítimo da rede.

A Infra-estrutura de Chaves Públicas (ICP) permite que os usuários de uma rede pública insegura como a Internet possam de maneira segura e privada trocar dados através dos pares criptográficos de chaves públicas e privadas, compartilhando as chaves públicas através de uma autoridade confiável. A ICP possui sistemas para emitir, armazenar, determinar a autenticidade e revogar certificados cujas chaves foram comprometidas. Além disso, para efetivamente utilizar a criptografia de chave pública e assinaturas digitais, ele também provê o não-repúdio. A ICP garante que esses serviços trabalhem em conjunto e tenham uma compreensão comum de formatos e protocolos necessários para atingir os seus objetivos

Segundo VACCA (2004), uma boa implementação de ICP precisa satisfazer os seguintes requisitos:

- Não-repúdio: Para uma transação de negócio ser válida, nenhuma das partes pode mais tarde negar a existência ou a execução dessa transação. A ICP usa assinaturas digitais para satisfazer esse requisito.

- Privacidade: A privacidade é obtida através da criptografia de chaves pública e privada.

- Integridade: Na ICP a integridade é obtida através da assinatura digital, que é usada para provar que os dados não foram adulterados durante o transito.

- Responsabilização: A ICP oferece responsabilização, verificando a identidade dos usuários através de assinaturas digitais. Como as assinaturas digitais são mais seguras do que a combinação nome de usuário e senha, os usuários estão mais propensos a ser responsabilizados pelas suas ações.

- Confiança: Todo o conceito de ICP tem como base a confiança. Você confia na autoridade (AC) emissora. Se você não tem fé na AC emissora, então você não pode confiar em nenhum dos certificados emitidos por ela, ou nas organizações que os emitiram. Isso não significa que a organização não é confiável, mas que a AC da organização não o é.

Segundo Nakamura (2000:192-193), para um usuário ter acesso aos recursos da organização ele precisa passar por um processo de verificação. Esse processo tem por finalidade validar a identidade do usuário, para tanto, é necessário verificar a identificação do usuário e realizar a autenticação.

A identificação é a função na qual o usuário declara uma determinada identidade para um sistema. Já a autenticação é a função responsável pela validação dessa declaração de identidade do usuário.

Conforme Nakamura (2000:192-203) a autenticação valida a identificação dos usuários e concede a autorização para acesso aos recursos. Há três maneiras de realizar a autenticação: mediante alguma informação que o usuário sabe, ou sobre algo que ele possui, ou ainda alguma característica do usuário. Todos esses

métodos possuem um ponto fraco. Dependendo do grau de segurança do sistema, usam-se dois desses métodos para autenticar o usuário.

Outro elemento importante na configuração de um ambiente de rede seguro é o bastion host. Conforme Chapman (1995:91-92) e Nakamura (2000:107), bastion hosts são equipamentos que disponibilizam serviços que podem ser acessados diretamente a partir da Internet. Essas máquinas possuem IP público, definido como categoria 3 na RFC 1918 REKHTER (1996:3), o que significa que elas são conhecidas e endereçáveis via Internet.

De acordo com Chapman (1995:92) há dois princípios gerais na configuração de um bastion host: mantê-lo simples e estar preparado caso ele seja comprometido.

A simplicidade na configuração do bastion host torna mais fácil mantê-lo seguro. Isso significa que poucos serviços devem ser instalados e com o menor número de privilégios possíveis, porém não se esquecendo que ele precisa cumprir o seu papel.

As redes encontradas nos ambientes empresariais, de acordo com Nakamura (2000:204-233), começam a partir da necessidade de compartilhar recursos internos da empresa. Um segundo passo seria a interligação entre a matriz e a filial. Na seqüência as empresas sentem a necessidade de ter acesso à Internet e finalmente decidem disponibilizar serviços para a Internet, como o site da empresa, por exemplo.

Os problemas de segurança das empresas aumentam significativamente quando elas passam a ter acesso à Internet, pois, geralmente, elas não têm o conhecimento necessário para realizar a proteção da rede interna e, conseqüentemente, de seus dados.

As Arquiteturas de Firewall e os componentes de segurança descritos acima visam justamente diminuir as vulnerabilidades da rede das empresas, permitindo que a Política de Segurança da Informação criada pela empresa possa ser implantada no ambiente virtual.

DISCUSSÃO

Este material tem o objetivo de dar uma visão macroscópica sobre a segurança digital em ambientes empresariais, focando em Arquiteturas de Firewall.

Para os empresários, este documento pode servir de guia para a implantação de soluções de segurança para a empresa. Pode-se implementar desde soluções básicas, empregando filtros de pacotes, até ambientes complexos utilizando Infra-estrutura de Chaves Públicas (ICP), Sistema de Detecção de Intrusões (IDS), autenticação por biometria entre outros.

Os estudantes da área de informática também podem utilizar esse material para obter informações importantes para futuros trabalhos acadêmicos e mesmo para aprender um pouco mais sobre redes seguras. Os assuntos tratados aqui podem ajudar os estudantes e funcionários da área de Tecnologia da Informação a proporem soluções de segurança nas empresas em que trabalham, ajudando a proteger as informações da organização e podendo, inclusive, ganhar maior destaque perante a direção da empresa.

CONSIDERAÇÕES FINAIS

Muitas empresas alegam que não possuem recursos para investir em segurança. Porém, para proteger a informação nem sempre é necessário gastar grandes somas. O primeiro passo é definir o que se quer proteger e então criar uma Política de Segurança clara e eficiente.

Com a política de Segurança pronta é necessário implementar tecnicamente o que foi definido por esse documento. Contudo, é possível usar técnicas eficientes de segurança usando soluções acessíveis, como softwares livres. Portanto, mesmo pequenas e médias empresas podem realizar, de forma segura, transações on-line e disponibilizar seu site, por exemplo, sem a necessidade de comprar soluções caras.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Código de prática para a gestão da segurança da informação: NBR ISO/IEC 27002/ago. 2005. Rio de Janeiro: ABNT, 2005.

CHAPMAN, D. Brent; ZWICKY, Elizabeth D. Building Internet Firewalls. O'Reilly & Associates, Inc. 1995.

KORFF, Y; HOPE, P; POTTER, B. Mastering FreeBSD and OpenBSD Security. O'Reilly Media, Inc. 2005.

NAKAMURA, E. T. Um modelo de Segurança de Redes para Ambientes Cooperativos. 2000. 286f. Dissertação (Mestrado em Ciência da Computação) – Instituto de Computação, Universidade Estadual de Campinas, Campinas. 2000.

SCOTT, C; WOLFE P; ERWIN M. Virtual Private Networks, Second Edition. 2 ed. O'Reilly & Associates, Inc. 1999.

STALLINGS, W. Criptografia e segurança de redes: Princípios e práticas. Tradução de Daniel Vieira. 4 ed. São Paulo: Pearson Prentice Hall, 2008. 492p.

VACCA, J. R. Public Key Infrastructure: Building Trusted Applications and Web Services. Auerbach Publications, 2004.