ANÁLISE DE SEGURANÇA DO ACESSO REMOTO VPN

Emilio Tissato Nakamura
Instituto de Computação
Universidade Estadual de Campinas
CP 6176 13083-970 Campinas-SP
emilio.nakamura@ic.unicamp.br

Paulo Lício de Geus
Instituto de Computação
Universidade Estadual de Campinas
CP 6176 13083-970 Campinas-SP
(19)788-5865 paulo@ic.unicamp.br

RESUMO

As redes privadas virtuais (Virtual Private Network – VPN) possuem uma importância cada vez maior para os negócios das organizações, porém possuem sérias implicações de segurança. O acesso remoto VPN, onde o cliente pode acessar as informações remotamente através de um software cliente, possui implicações de segurança específicas que precisam ser consideradas, onde a principal delas é a possibilidade de utilizar o cliente como uma ponte entre a Internet e a rede da organização. Este artigo visa analisar as possibilidades de ataques que podem ser exploradas contra os clientes VPN, e apresenta algumas sugestões de defesa contra esses riscos.

ABSTRACT

The importance of Virtual Private Network (VPN) to organizations' businesses has been steadily increasing despite its serious security implications. The remote access VPN, which may be used to provide information access remotely through a client software, has specific security concerns that need to be considered. The main problem is the possibility to use the client as a bridge between the Internet and the organization network. This paper presents an analysis of possible attacks against the VPN clients and presents some defense suggestions against those risks.

1 INTRODUÇÃO

O ambiente cooperativo pode ser caracterizado pelo alto nível de conectividade entre as organizações, onde a necessidade cada vez maior de segurança implica na utilização de diversas tecnologias, sejam elas para permitir a continuidade dos negócios, ou para prover a segurança necessária para essas conexões.

As redes privadas virtuais (*Virtual Private Network* – VPN) constituem uma das tecnologias que possibilitam, além da economia com os custos de comunicação, que essa comunicação seja realizada com segurança. A efetividade da segurança porém é colocada sob questionamento, uma vez que o *backbone* da comunicação é uma rede pública, e o que está em jogo são as informações e os recursos da organização.

Este artigo tem como objetivo analisar as possibilidades de ataques contra as organizações que podem ser realizadas quando o acesso remoto VPN é utilizado, e apresentar as sugestões de medidas que podem ser tomadas para que os riscos de ataques sejam minimizados.

2 O ACESSO REMOTO VPN

A VPN possibilita a conectividade em níveis globais a custos relativamente baixos, permitindo assim que as comunicações das organizações sejam realizadas de modo a tornar possível a adoção de um modelo de negócio mais rápido e mais dinâmico.

Além disso, a VPN possui também importantes aspectos econômicos, principalmente com relação à desnecessidade de se manter uma infra-estrutura de comunicação própria. No caso do acesso remoto VPN, não é mais necessário que a própria organização mantenha a sua estrutura de acesso remoto, já que os usuários passam a utilizar os provedores de acesso, ao invés de discarem para a própria organização.

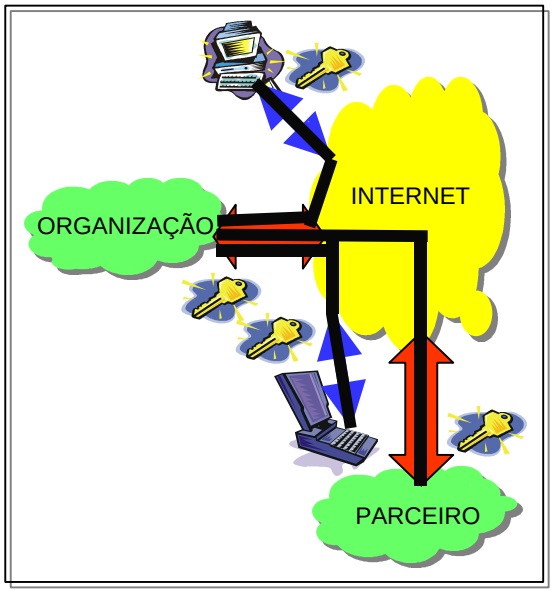

Fig. 1 – Acessos à organização via VPN, que utiliza uma rede pública como a Internet, eliminando a necessidade de uma conexão dedicada ou de uma estrutura de acesso remoto.

O acesso remoto VPN possui a vantagem de poder ser utilizado pelos clientes ou pelos pequenos parceiros que ainda não possuem uma conexão direta com a Internet, e que portanto necessitam utilizar os provedores de acesso. Além desses

usuários externos, existe ainda o grande número de funcionários que trabalham de suas próprias residências, e de *telecommuters*, que estão sempre viajando e possuem pontos de conexões diferentes a cada momento. O acesso remoto VPN objetiva solucionar os problemas de conexões desses usuários, e devido ao seu grande potencial de uso, a sua importância para o mundo atual é bastante grande. O tunelamento – criação do túnel virtual entre o cliente, nesse caso, e a rede da organização – é iniciado a partir de um software cliente instalado no equipamento do usuário. Outros tipos de VPN, como os que conectam redes diferentes (*gateways VPN*), não serão considerados neste artigo.

2.1 Como Funciona

O software cliente na qual se baseou a análise funciona da seguinte maneira, lembrando que as outras soluções de acesso remoto VPN funcionam de modo similar: o usuário precisa instalar em seu equipamento um software, o cliente VPN, que é o responsável pela inicialização do tunelamento, que é baseado no *IP Security* (IPSec). A configuração desse software é feita através de um arquivo que contém todos os parâmetros de tunelamento necessários, que deve ser importado para o software mediante a utilização de uma chave simétrica. Essa chave e o arquivo de configuração são gerados pela entidade certificadora, e a chave simétrica utilizada no processo de importação aumenta o nível de segurança do processo, ao evitar que o arquivo de configuração seja capturado e utilizado indiscriminadamente. A segurança desse processo será analisada posteriormente.

Resumidamente, os passos do funcionamento do acesso remoto VPN são:

1. O usuário instala o software cliente;
2. A entidade certificadora gera um arquivo contendo os parâmetros necessários para a conexão IPSec, entre eles o certificado digital, a chave assimétrica e os algoritmos criptográficos a serem utilizados;
3. A entidade certificadora gera uma chave simétrica que deve ser utilizada pelo usuário para a importação do arquivo de parâmetros no software cliente;
4. O usuário deve configurar o software cliente através da importação do arquivo de parâmetros utilizando a chave simétrica, gerados pela entidade certificadora;
5. O usuário recebe o arquivo de parâmetros e a chave simétrica;
6. O usuário utiliza a chave simétrica para importar o arquivo de parâmetros;
7. O usuário configura o software cliente através da importação do arquivo de parâmetros, e assim está apto a iniciar um tunelamento IPSec para a rede da organização;
8. A conexão IPSec é negociada entre o usuário e a rede da organização de acordo com os parâmetros do usuário e do servidor, que possui uma lista dos recursos que cada usuário pode acessar.

Um ponto interessante é que, uma vez configurado o software cliente VPN, através da importação dos parâmetros do túnel IPSec, a autenticação é feita baseada no equipamento, e não necessariamente no usuário. Isso cria algumas aberturas na segurança da rede da organização, como será visto adiante.

3 A SEGURANÇA DO ACESSO REMOTO VPN

Ataques do tipo *Denial of Service* (DoS) certamente são um grande fardo que podem resultar em grandes prejuízos. Porém, nesta análise o enfoque está em garantir a segurança da rede interna da organização, ou seja, garantir que o uso do acesso remoto VPN não resulte em uma brecha de segurança e conseqüentes quebras de confidencialidade ou de integridade dos recursos da organização. O enfoque da análise será dado em cima desta possibilidade, em pontos que incluem o protocolo IPSec, as configurações do software cliente, a possibilidade do cliente ser utilizado como ponte para a rede da organização, o compartilhamento de arquivos do Windows e a utilização de modems. É sabido, contudo, que ataques DoS são muitas vezes armados como parte de um ataque ativo a um recurso.

3.1 IPSec

A segurança da conexão é baseada fundamentalmente no IPSec, que é reconhecidamente um protocolo seguro, e padrão *de facto* das VPNs. A autenticação do cliente, a autenticação do servidor e a confidencialidade e integridade dos dados são providas por esse protocolo e pelos algoritmos criptográficos negociados pelo mesmo. Porém, não se deve esquecer que o fato de um protocolo ser seguro não garante a segurança do sistema, já que essa segurança depende da correta implementação do protocolo. Diversos casos de erros na implementação que comprometiam a segurança foram descobertos, principalmente em algoritmos criptográficos. Portanto, uma falha na implementação do IPSec pode comprometer o sistema, e deve ser verificado através de insistentes testes e análises de todas as possibilidades de conexões possíveis. Mesmo a implementação e o projeto do cliente VPN podem ter problemas que podem comprometer totalmente a segurança.

Ataques teóricos contra o IPSec foram demonstrados em [BEL 97], porém implementar

essas técnicas seria bastante improvável, devido à complexidade dos cenários necessários, que exigem análise constante e rápida de todos os pacotes da conexão.

3.2 Segurança do Certificado Digital e da Chave Assimétrica

Foi visto que o certificado digital e a chave assimétrica, além dos parâmetros necessários para a criação do túnel IPSec, são armazenados em um arquivo, que deve ser importado pelo cliente.

Os riscos existentes com relação à apropriação indevida do certificado digital e da chave assimétrica estão relacionados com a captura desse arquivo de configuração da VPN, e também com o uso não autorizado ou com o roubo do equipamento do usuário. Esses riscos serão vistos a seguir.

3.2.1 Capturando o Arquivo de Configuração da VPN

Um ataque visando a captura do arquivo de configuração não surtiria efeito, pois para que ele possa ser utilizado, é necessário utilizar uma chave simétrica para importá-lo no software cliente do usuário. Assim, o ataque teria sucesso apenas se o hacker capturar também a chave de importação do arquivo. Essa abordagem, de tornar imprescindível a utilização de dois elementos (arquivo de configuração e chave de importação), aumenta o nível de segurança do esquema, já que é mais difícil o hacker obter esses dois elementos distintos que se relacionam entre si.

A grande questão está no modo em que esses elementos são enviados ao cliente. É essencial que um canal seguro seja utilizado para a transferência do arquivo de configuração e da chave de importação. Caso não seja possível utilizar um canal seguro, o nível de segurança do processo de transferência pode ser incrementado utilizando-se dois canais diferentes, como por exemplo, o telefone e o *e-mail*, um para a transferência do arquivo de configuração, e o outro para a transferência da chave de importação.

3.2.2 Roubo ou Utilização Indevida do Equipamento do Usuário

Uma outra possibilidade é o roubo do equipamento do usuário. Roubando-se o equipamento, o acesso à rede interna torna-se praticamente automático, pois o software cliente já está apropriadamente configurado para o seu uso. Essa é uma possibilidade que deve ser analisada com cuidado, já que tem sido observado um aumento significativo na criminalidade envolvendo roubos de *notebooks*.

Além disso, ainda é possível roubar o disco rígido de *desktops* de maneira relativamente simples. Alguns equipamentos possuem até mesmo uma gaveta removível para o posicionamento do disco rígido, tornando assim mais fácil a ação de quem tem a intenção de roubá-lo.

Outra oportunidade perigosa ocorre quando um equipamento contendo o software cliente VPN é enviado para a assistência técnica. É possível recuperar e copiar diversos tipos de informações desse equipamento, o que pode comprometer a segurança do sistema. O que também pode ocorrer com o cliente VPN é alguém usar o equipamento "emprestado" em momentos de ausência do dono para fazer a conexão VPN.

Esses problemas podem ser minimizados de uma maneira simples, através da utilização de uma senha de acesso no software cliente VPN. O seu nível de segurança, no entanto, depende do método de armazenamento da senha e do algoritmo criptográfico utilizado pelo software. Uma análise com relação a isso é importante, pois diversos casos de senhas fáceis de serem descobertas já foram relatados, como são os casos das utilizadas em documentos do Word ou do Excel, e até mesmo das senhas de *login* da rede Microsoft e dos protetores de tela. Além dos problemas com os algoritmos, diversos métodos de recuperação de senhas são conhecidos. Um desses métodos pode ser visto em [SHA 98], onde são descritos sofisticados ataques algébricos e estatísticos utilizados para localizar chaves de criptografia escondidas em uma grande *string* ou em grandes arquivos.

3.3 Uma Possibilidade Perigosa – Cliente VPN como Gateway

Uma característica que abre um grande leque de possibilidades de ataques é a utilização do cliente VPN como um *gateway* entre a Internet e a rede interna. Isso pode ocorrer porque o equipamento do usuário passa a ter duas conexões, uma com a Internet e outra, via tunelamento IPSec, com a rede da organização. Deste modo, o hacker pode utilizar uma conexão (Internet) para passar para a outra (túnel IPSec), alcançando assim a rede da organização. O nível de segurança envolvido aqui é portanto bastante preocupante, já que o cliente está disponível (porém não aberto) a todo o universo da Internet.

Essa "ponte" pode ser caracterizada porque o cliente VPN age sobre a pilha TCP/IP do cliente, de modo que todo pacote endereçado à rede da organização é transformado em um pacote IPSec, que são pacotes válidos e autenticados.

Será analisada a seguir como isso é possível, e se um ataque dessa natureza pode mesmo ser

utilizado contra a organização. Será visto que é necessário que o hacker seja capaz de rotear pacotes através desse cliente VPN, ou que ele tenha o controle sobre essa máquina, seja ele fisicamente, através de vírus ou cavalos-de-tróia, ou ainda através de ataques para dominá-la.

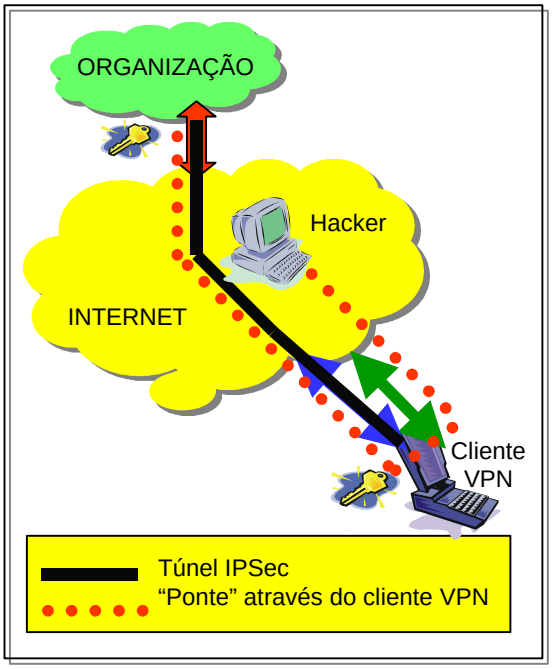

Fig. 2 – Utilizando o cliente VPN como uma ponte entre a Internet e a rede da organização.

3.3.1 Roteamento de Pacotes através do Cliente VPN

Um dos métodos para fazer com que o cliente VPN atue como um *gateway* entre a Internet e a rede da organização é através do roteamento de pacotes por esse cliente. Caso esse cliente possua a capacidade de roteamento, então um hacker pode enviar pacotes para o cliente da Internet, que por sua vez rotearia esses pacotes para a rede da organização.

A capacidade de roteamento depende do sistema operacional em uso pelo cliente. Pode-se afirmar que os usuários que utilizam o Windows 9x ou o Windows NT Workstation estão imunes a esse tipo de ataque, pois esses sistemas operacionais não possuem essa capacidade. O mesmo não se pode dizer daqueles que utilizam o Windows NT Server, o Linux ou os sabores de Unix em geral, que são capazes de rotear pacotes.

Porém, pela lógica, esses clientes não devem rotear pacotes para a rede interna da organização, ou seja, rotas padrões para a rede interna devem ser evitadas a todo custo. Portanto, primeiramente uma rota com destino à rede interna da organização deve ser incluída, o que pode ser considerado difícil, porém possível mediante um ataque a esse equipamento.

Uma possibilidade de forçar o roteamento é a utilização de uma funcionalidade do TCP/IP, o *source routing*. Através dele é possível criar pacotes com informações de roteamento, ou seja, é possível enviar um pacote para o equipamento do cliente VPN com informações sobre qual rota esse pacote deve seguir, que nesse caso seria para a rede da organização. Essa é uma funcionalidade com enormes implicações de segurança, já que permite que um hacker envie pacotes com informações de roteamento para qualquer destino desejado, sendo que essa rota normalmente seria proibida. Além disso, o *source routing* é utilizado também para que firewalls sejam driblados, e para que uma rota de retorno dos pacotes seja definida, o que pode ser utilizado em ataques mais sofisticados, que dependem de uma resposta da vítima, e que são geralmente utilizados em conjunto com o *IP Spoofing*.

Um ponto com relação ao *source routing* é que essa funcionalidade pode ser utilizada tanto por *hosts* roteadores quanto por *hosts* que não atuam como roteadores. Por isso a preocupação que se deve ter também com o Windows NT Workstation e com o Windows 9x [MIC 99-4]. No Windows NT essa opção não podia ser desabilitada, o que é possível somente agora, através do *Service Pack 5* [MIC 99-1]. Mesmo assim, foi descoberto uma vulnerabilidade no Windows que permitia a utilização do *source routing*, mesmo ela estando desabilitada [NAI 99]. O *patch* de correção da vulnerabilidade está disponível, menos para o Windows 9x e o Windows NT 4.0 Server, Terminal Server Edition [MIC 99-2].

3.3.2 Ataques ao Sistema Operacional, aos Aplicativos e aos Serviços

Uma outra possibilidade de invadir a rede interna é através do controle da máquina do usuário. Existem diversos ataques conhecidos que tiram proveito de falhas nos sistemas operacionais, nos aplicativos ou nos serviços. Uma dessas inúmeras falhas poderia ser utilizada para que o hacker assumisse o controle da máquina ou roubasse arquivos que seriam utilizados no ataque à rede interna. Esse mesmo tipo de ataque poderia ainda ser utilizado para se alterar tabelas de roteamento, que teve a sua possibilidade descrita na seção anterior.

Geralmente o Windows 9x e o Windows NT Workstation não disponibilizam muitos serviços, e portanto são menos susceptíveis a ataques. Um *port scanning* revelou as seguintes portas abertas nos sistemas operacionais da Microsoft em uma instalação padrão:

- Windows 9x – porta 139;
- Windows NT Workstation – portas 135 e 139;
- Windows NT Server (funcionando como servidor proxy) – portas 7, 9, 13, 17, 19, 135, 139, 1080.

As portas 135 e 139 podem ser exploradas para ataques do tipo DoS, que é o único método de ataque possível conhecido para essas portas. Com isso, pode-se considerar que máquinas com Windows 9x ou Windows NT Workstation em sua instalação típica, sem nenhum serviço adicional e, principalmente, sem estar contaminado com um vírus ou cavalo-de-tróia, possuem menores chances de serem explorados em um ataque do que o Linux, o Unix ou o Windows NT Server.

3.3.3 Vírus e Cavalos-de-Tróia

Os vírus e os cavalos-de-tróia são uma das maiores ameaças ao esquema de segurança da VPN. Esse pode ser considerado o ponto mais crítico dentro do sistema de segurança do acesso remoto VPN, já que os usuários (o elo mais fraco da segurança de uma organização) podem contaminar seus próprios equipamentos através da execução de programas maliciosos, que geralmente adotam doses de engenharia social, como a que se iniciou com o vírus Melissa, que induzia o usuário a abrir o *e-mail* contaminado.

Um cavalo-de-tróia instalado, combinado com a possibilidade de existência da conexão com a Internet e com o túnel VPN, torna possível o mais perigoso dos ataques contra a rede interna da organização, já que o hacker pode ter acesso a todos os dados da rede interna da organização acessíveis através da VPN. Mesmo a necessidade de uma chave para a inicialização do túnel perde a sua efetividade, já que um cavalo-de-tróia, como o *Back Orifice*, pode capturar tudo o que o usuário digita, além de ser possível ainda capturar a tela do usuário.

3.4 Problemas com Compartilhamento de Arquivos do Windows

Um outro ponto a ser considerado são os compartilhamentos de arquivos do Windows. Uma configuração equivocada do sistema operacional pode permitir que seus arquivos sejam acessíveis não apenas pelos demais equipamentos da sua rede, mas também pela Internet (através da opção NetBEUI over TCP/IP). Com isso, as informações residentes na máquina do cliente podem ficar disponíveis através desse compartilhamento. Essas informações podem ser confidenciais, tendo sido armazenadas no equipamento do cliente depois de uma conexão segura através de IPSec.

3.5 Problemas com Modems

O perigo dos modems foi analisado por Brian McWilliams em [McW 97], onde foi utilizado a técnica de *war dialing*. Através dele, é possível discar para diversos números de telefones em busca de conexões abertas, que podem servir de ponto de entrada para sistemas de computadores ou de telecomunicações. Caso um equipamento com o software cliente VPN responda a uma dessas chamadas, ele pode ser explorado para que uma conexão à rede da organização seja iniciada.

4 SOLUÇÕES

Foi visto que os problemas de segurança aparecem principalmente devido à existência de duas conexões no cliente, uma com a Internet e outra, via túnel IPSec, com a rede da organização. Outros problemas são a segurança do certificado digital armazenado no equipamento do cliente, a possibilidade de ataques através de vírus e cavalos-de-tróia, o compartilhamento de arquivos do Windows, e a utilização indiscriminada de modems.

Todas essas possibilidades de ataques podem ser minimizadas através de uma boa política de segurança. É esse o principal elemento de um sistema de segurança, e é através da sua correta implementação e gerenciamento que muitos dos problemas podem ser eliminados. Além da política de segurança bem definida, uma defesa mais ativa também deve ser utilizada, como por exemplo, a utilização de *port scannings* ou de firewalls individuais nos clientes, como serão discutidas nas próximas seções. O papel do firewall dentro do esquema de acesso remoto VPN também é discutido brevemente.

4.1 Firewall

O firewall é um elemento essencial na arquitetura de segurança de qualquer organização. Ele é essencial porque atua na borda da rede da organização, realizando um controle de acesso onde apenas os usuários legítimos podem atravessar essa barreira. Na solução que inclui não somente o acesso remoto VPN, mas a VPN em geral, o firewall tem a função de aceitar somente os pacotes relativos aos serviços disponíveis (internamente e externamente), e os pacotes IPSec relativos à VPN. A autenticação dos usuários é baseada no IPSec, e como o posicionamento do *gateway* IPSec com relação ao firewall é um tópico extenso e complexo, ele não será analisado neste artigo.

4.2 Política de Segurança

A política de segurança é fundamental para todas as organizações, e deve tratar de diversos aspectos técnicos, operacionais e organizacionais. Alguns dos aspectos que devem ser tratados pela política de segurança, com relação ao acesso remoto VPN, são:

- Segurança física, como por exemplo, o estabelecimento de regras para o acesso aos equipamentos, que evitam que eles sejam roubados ou sejam acessados temporariamente de modo indevido;

- Procedimentos em caso de roubo ou perda. Caso um *notebook* seja roubado, por exemplo, esse roubo deve ser notificado imediatamente, de modo que o seu certificado digital seja revogado nesse mesmo instante;

- Utilização de senha no protetor de tela para evitar que terceiros utilizem o equipamento em horários oportunos, como a hora do almoço, para ter o acesso à rede da organização via túnel IPSec.

- Procedimentos a serem tomados em caso de envio do equipamento à assistência técnica também devem ser bem descritos, para se evitar a cópia dos dados do disco rígido;

- Definição de quais serviços podem rodar nesses equipamentos. Foi visto que cada serviço funciona como uma porta de entrada que o hacker pode explorar para a realização de um ataque. Quanto menos portas abertas existirem, menores as possibilidades de ataques. Serviços não essenciais devem ser portanto desabilitados;

- Uma política de atualização dos sistemas operacionais/aplicativos/serviços é essencial, já que são essas atualizações que trazem soluções para *bugs* e vulnerabilidades que podem ser explorados pelos hackers;

- Procedimento para as conexões VPN. Uma das regras necessárias é desconectar o cabo de rede no momento da conexão VPN, caso esse equipamento faça parte de uma outra rede. Na realidade, essa prática deve ser utilizada sempre que um modem é utilizado, para evitar que alguém da Internet tenha acesso aos outros pontos dessa rede. No esquema do acesso remoto VPN, a desconexão do cabo de rede evita também que outros usuários da mesma rede desse cliente consigam entrar na rede interna da organização via VPN;

- Uma política de prevenção contra vírus e cavalos-de-tróia é essencial, tanto com relação à educação dos usuários, que precisam saber quais tipos de arquivos podem ser abertos e executados em seu equipamento, quanto para a utilização e atualização dos anti-vírus;

- Política de utilização de modems, principalmente não deixar o modem em espera, já que uma conexão externa pode comprometer não apenas a segurança da VPN, mas também da própria rede da organização;

- Política que trata do roteamento, que determina quais máquinas trabalham como roteadores ou se existe mesmo a necessidade de deixar a opção de *source routing* habilitada, o que é uma situação extremamente rara.

A política de segurança é assim imprescindível para a organização. Porém, no caso do acesso remoto VPN, uma série de complicações vem à tona – Como implantar uma política de segurança em equipamentos de terceiros, que geralmente são utilizados também para outros fins? Como controlar, por exemplo, o equipamento de um revendedor que é utilizado para controle das vendas, acesso à Internet e leitura de *e-mails*, além da conexão VPN? Como exigir que uma política de segurança seja seguida por esse usuário? Como garantir que essa política estará sendo seguida? Essa política poderia ser mais facilmente implementada caso os equipamentos pertencessem à própria organização que disponibiliza o serviço, já que permitiria um controle mais refinado do equipamento, podendo-se controlar o que o usuário pode instalar, o que o usuário pode acessar, o que o usuário pode apagar, etc. Porém, essa não é uma situação que pode ser considerada normal, sendo portanto necessário grandes esforços adicionais, como um acompanhamento eficiente e uma auditoria constante. Além disso, medidas mais proativas também devem ser adotadas. Elas auxiliam na segurança da solução, e algumas delas serão apresentadas a seguir.

4.3 Sem Acesso Simultâneo com a Internet e com a VPN

Foi visto que as possibilidades de ataques mais concretas são devidas ao fato do cliente VPN possuir uma conexão direta com a Internet e outra com a organização, via túnel VPN.

A utilização do cliente VPN como *gateway* depende do *source routing*, portanto essa opção deve ser imediatamente desabilitada. Essa medida porém não elimina os riscos com os vírus e cavalos-de-tróia, que devem ser combatidos de outra forma, principalmente através de uma política de segurança eficiente.

Os riscos podem ser eliminados se o cliente aceitar somente conexões IPSec. Isso eliminaria os

riscos de ataques ao sistema operacional/aplicativos/serviços do cliente, além de tornar a conexão VPN segura mesmo se o cliente VPN estiver contaminado com um vírus ou cavalo-de-tróia, já que os comandos enviados ao equipamento contaminado seriam todos descartados. Mesmo se alguém conseguir enviar pacotes IPSec ao equipamento, os certificados digitais serão sempre verificados, e como o cliente VPN não troca certificados com o hacker, essa conexão não será permitida. Portanto, caso o cliente VPN possua essa opção de aceitar somente conexões IPSec, ela deve ser habilitada. Porém, o que se tem observado é que essa possibilidade não é implementada nos clientes VPN, principalmente devido à complexidade envolvida quando uma conexão PPP discada é utilizada.

Uma alternativa poderia ser configurar o cliente VPN para que ele envie todos os seus pacotes somente através desse túnel IPSec, ou seja, todos os pacotes que são enviados através de seu modem devem ser transformados em pacotes IPSec para a rede da organização. Isso faria com que um hacker da Internet consiga enviar pacotes ou comandos para o cliente VPN, porém ele não receberia de volta os pacotes de resposta, que seriam enviados à rede da organização, em vez de serem enviados ao hacker. Assim, o hacker não teria acesso a nenhuma informação da organização. Essa solução pode funcionar, porém com o custo de maior tráfego na rede da organização, e a possibilidade de ataques DoS. Do ponto de vista do usuário, a sua largura de banda com o provedor seria esgotado, e do ponto de vista da rede da organização, seu canal com a Internet poderia ser comprometido caso haja um ataque coordenado, onde diversos clientes VPN enviam ao mesmo tempo uma quantidade muito grande de pacotes para a rede da organização. Assim a rede da organização ficaria inacessível, o que resultaria em prejuízos.

Essa situação pode ainda provocar uma possibilidade mais séria, onde o hacker poderia criar pacotes com comandos maliciosos que seriam enviados automaticamente para a rede da organização via o cliente VPN. O hacker seria impossibilitado de obter respostas, porém a rede da organização poderia passar a negar serviços legítimos (ataque DoS).

Uma solução mais simples é através da alteração da tabela de roteamento do cliente. A idéia aqui é a de eliminar o roteamento padrão (*default gateway*), que é inserido na tabela no momento da conexão do cliente com o provedor, e inserir apenas duas rotas: uma para o provedor, enviando os pacotes através da conexão PPP, e outra para o *gateway* VPN, enviando os pacotes para o provedor. Desta forma, o cliente seria capaz de enviar pacotes apenas para o provedor e para o *gateway* VPN, passando por esse provedor. O envio de pacotes para outros destinos não seria possível apenas com essas duas rotas. Os problemas envolvidos na alternativa anterior, onde o hacker teria a chance de enviar pacotes maliciosos para o cliente, causando negação de serviços, ainda é válido para este caso. Ele apenas não é capaz de obter respostas a esses pacotes.

4.4 Port Scannings

Através da utilização de *port scannings* (varredura de portas TCP/IP) nos clientes VPN é possível verificar quais serviços estão rodando nos respectivos equipamentos, além de ser possível determinar também se ele está ou não contaminado com determinados vírus ou cavalos-de-tróia. Assim, caso uma contaminação ou serviços indevidos ou desnecessários sejam detectados, as devidas providências podem ser tomadas.

O *port scanning* poderia ser um requerimento para o estabelecimento de uma conexão VPN entre o cliente e a rede da organização. Uma regra que poderia ser utilizada é que a conexão só seja efetivada depois de uma varredura. Outra regra poderia ser que a varredura seja executada periodicamente, dependendo da política de segurança da organização.

Além do *port scanning*, que verifica as portas abertas, o *scanning* de vulnerabilidades também poderia ser utilizado, de acordo com as necessidades. Isso minimizaria as possibilidades de ataques, já que vulnerabilidades de sistemas operacionais, aplicativos e serviços seriam detectados e corrigidos, teoricamente, antes que os hackers mais comuns tirassem proveitos deles.

A dificuldade em se adotar essa prática está no processo de execução das varreduras, já que os endereços IPs dos clientes são dinâmicos. Varreduras em sistemas não autorizados podem resultar em diversos problemas éticos e legais, e por isso ele deve ser feito com extremo cuidado, e apenas em equipamentos nos quais se tenha a certeza que estão se conectando à rede da organização.

4.5 Firewall Individual

A utilização do firewall individual pode minimizar grande parte dos problemas de segurança. Esse tipo de firewall atua na camada de enlace de dados do equipamento do usuário, e filtra pacotes IP (TCP, UDP, ICMP), e outros como o NetBEUI, IPX, ARP. Através dele é possível controlar acessos aos recursos, monitorar todo o tráfego gerado ou que chega ao sistema, gerar regras de acordo com uma aplicação específica que

está funcionando, e gerar registros de todos os acessos do sistema [SIG 99].

É possível criar regras de acordo com as seguintes características [SIG 99]:

- Quando um aplicativo específico está funcionando;
- Em determinado dispositivo Ethernet ou serial;
- Quando um número de telefone específico é utilizado;
- Para serviços, arquivos ou compartilhamentos específicos;
- Para endereços IPs específicos;
- Para direção de fluxo dos pacotes;
- Para usuários específicos;
- Para conexões VPN ou conexões discadas.

Assim, através de um firewall individual é possível obter um controle sobre as conexões do cliente, de modo que uma política poderia definir a exigência de sua utilização. Isso eliminaria os problemas com cavalos-de-tróia, que poderiam ainda infectar o cliente. Porém o cliente não poderia ser controlado através dos comandos, que não chegariam a ele, já que eles seriam bloquados pelo firewall individual. Os problemas envolvendo o roteamento através do cliente também poderia ser contornado. Porém, não se deve esquecer que um vírus sempre pode reescrever essas regras do firewall individual, mesmo que isso exija um trabalho extra para o atacante. Além disso, basta que a solução fique conhecida para que ela passe a se tornar também alvos dos atacantes. Isso reforça novamente a importância de uma política de segurança bem definida.

CONCLUSÃO

O uso de VPNs é essencial para as organizações, por possibilitar as conexões entre seus clientes, fornecedores, parceiros e funcionários. Sua importância cresce porque a sua implantação é simples e o retorno econômico é grande. Porém, as implicações de segurança que aparecem quando se utiliza uma rede pública, como a Internet, são bastante relevantes, e incluem ainda a utilização de um firewall.

Além dos cuidados com possíveis problemas na implementação do IPSec, do cliente VPN e no projeto da VPN, uma política de segurança bem definida para os clientes que forem utilizar a VPN é essencial. Os problemas de segurança que podem existir são de natureza física (roubo do equipamento ou acesso físico a esse equipamento) e principalmente quanto à possibilidade de conexões múltiplas (com a Internet e com o túnel VPN), que podem tornar esse cliente um *gateway* entre a Internet e a rede interna da organização. Roteamento, vírus e cavalos-de-tróia são os elementos envolvidos nessas conexões múltiplas, que incluem ainda o *source routing*, relacionado com o roteamento.

O uso de *ports scannings* e *scannings* de vulnerabilidades regulares realizam uma auditoria de quem deseja se conectar à rede via VPN, de modo que serviços desnecessários, equipamentos contaminados com vírus ou cavalos-de-tróia, e vulnerabilidades possam ser identificados.

O firewall individual incrementa o nível de segurança do sistema ao atuar na camada de enlace de dados e permitir a criação de diversas regras que impedem a atuação de vírus, cavalos-de-tróia e a utilização do cliente como um *gateway*.

Assim, o acesso remoto VPN traz uma série de benefícios à organização e a seus usuários, porém incrementa as implicações de segurança na rede da organização. Abrir a rede interna para esses usuários requer que os cuidados citados acima sejam tomados para se evitar problemas maiores, que podem aparecer posteriormente. Os problemas discutidos são pertinentes a um ambiente cooperativo, principalmente devido à sua conexão com a Internet. Os ambientes cooperativos são um fato no mundo atual, onde a competitividade global exige novas soluções em seus processos de negócios. E essas novas soluções necessitam de segurança suficiente para que elas sejam justificáveis.

REFERÊNCIAS BIBLIOGRÁFICAS

[BAY 98] Bay Networks. *Understanding and Implementing Virtual Private Networking (VPN) Services*. http://www.baynetworks.com/products/Papers/2746.html. 29/01/99.

[BEL 97] BELLOVIN, Steven M. *Probable Plaintext Cryptanalysis of the IP Security Protocols.* AT&T Labs Research. Florham Park, NJ, USA: 1997.

[CHE 98] Check Point Software Technologies Ltd. http://www.checkpoint.com. 04/01/99.

[CHE 98-1] Check Point Software Technologies Ltd. *Redefining the Virtual Private Network.* March 4, 1998.

[CHE 98-2] Check Point Software Technologies Ltd. *Virtual Private Network –*

Security Components – A Technical White Paper. March 23, 1998.

[FOR 98] Forrester Research Inc. http://www.forrester.com. 04/01/99.

[GAR 98] GARFINKEL Simson L. *Advanced Telephone Auditing with PhoneSweep: A Better Alternative to Underground "War Dialers"*. 1999. 27/08/99. http://www.mids.org/mn/812/sim.html

[ISS 99] ISS – Internet Security Systems. *ISS X-Force White Paper – Back Orifice 2000 Backdoor Program*. September 1999.b

[McW 97] McWilliams, Brian. *Did You Forget to Lock the Back Door?*. PC World News Radio. September 19, 1997. 27/08/99. http://www.pcworld.com/news/daily/data/0997/970919181153.html

[MIC 99-1] Microsoft Corporation. *TCP/IP Source Routing Feature Cannot Be Disabled*. 18/08/99. http://support.microsoft.com/support/kb/articles/q217/3/36.asp

[MIC 99-2] Microsoft Corporation. *Microsoft Security Bulletin (MS99-038) – Patch Available for "Spoofed Route Pointer" Vulnerability*. September 20, 1999. 22/09/99. http://securityportal.com/topnews/ms99-038.html

[MIC 99-3] Microsoft Corporation. *Data in Route Pointer Field Can Bypass Source Routing Disable*. September 20, 1999. 22/09/99. http://support.microsoft.com/support/kb/articles/q238/4/53.asp

[MIC 99-4] Microsoft Corporation. *Microsoft Security Bulletin (MS99-038): Frequently Asked Questions*. September 20, 1999. 22/09/99. http://www.microsoft.com/security/bulletins/ms99-038faq.asp

[NAI 99] Network Associates, Inc. *Security Advisory – Windows IP Source Routing Vulnerability*. September 20, 1999. 22/09/99. http://securityportal.com/topnews/nai19990920.html

[SHA 98] SHAMIR, Adi; SOMEREN, Nicko van. *Playing Hide and Seek With Stored Keys*. September 22, 1998.

[SIG 99] SIGNAL 9 SOLUTIONS. *ConSeal PC Firewall*. 10/08/99. http://www.signal9.com.

[STU 98] STUTZ, Michael. *Wardialer Goes Corporate*. October 7, 1998. 27/08/99. http://www.jammed.com/Lists/ISN/1998-Oct/ISN-774