Material também disponível em:
www.projetoderedes.com.br
www.redesdecomputadores.com.br

ASPECTOS DE SEGURANÇA EM REDES VOZ SOBRE IP

White Paper

Última atualização em 3 de Dezembro de 2003

MSLAB (Módulo Security Lab)

Márcio Galvão (mgalvao@modulo.com.br)
Alexandre Zattar (azattar@modulo.com.br)

1. Introdução

O desenvolvimento de processadores de sinal digitais (DSPs) viabilizou a digitalização e compressão de sinais de voz e fax em pacotes de dados. Em paralelo, a evolução dos sistemas de transmissão possibilitou a criação de redes de pacotes de alta velocidade. A combinação destes desenvolvimentos tem permitido a evolução das redes convergentes, onde trafegam pacotes de dados "tradicionais" e pacotes de voz digitalizados.

Existem diversos tipos de redes de dados que permitem o tráfego de voz e fax, como por exemplo as redes baseadas em ATM, Frame Relay e TCP/IP. Embora destas três tecnologias apenas o ATM tenha sido projetado desde o início para transporte de voz e dados, o Frame Relay e o TCP/IP são mais utilizados, e o transporte de voz através destas redes doravante será chamado de VoFR e VoIP respectivamente.

De forma bastante resumida, as diferenças básicas entre VoIP e VoFR se referem ao fato de que VoIP está associado com a camada 3 no modelo OSI (roteamento), e portanto tem como características o baixo custo e a capacidade de operação em redes heterogêneas. Como desvantagens, podemos mencionar a qualidade de serviço (QoS limitado) e as questões relacionadas com a segurança.

Já VoFR (assim como Voz sobre ATM, ou VoATM) está associada com a camada 2 do modelo OSI (*data link*), e por isso tem custo mais elevado, pois requer redes homogêneas ou *gateways* Layer 2 especializados. Em contrapartida, oferece maior qualidade de serviço (QoS mais poderoso). O padrão principal é FRF.11/12.

Com relação aos protocolos para VoIP, há os utilizados para transporte (RTP, RTCP, SCTP) e os de sinalização (SIP, H.323, MGCP, etc). Uma descrição resumida de alguns destes protocolos e de outros conceitos relacionados com a tecnologia VoIP está disponível no Glossário.

Embora muitos conceitos da tecnologia de transmissão de voz em redes de dados se apliquem tanto ao VoIP quanto ao VoFR, neste trabalho vamos nos restringir ao VoIP, e em particular, aos seus aspectos de segurança. Em função da grande escalabilidade e baixo custo da utilização da Internet como meio de transporte de informação, as redes VoIP, embora ainda não estejam sendo implementadas em grande escala, estão ganhando importância cada vez maior, e muitas empresas já planejam a sua implementação para um futuro próximo.

Infelizmente, as facilidades e baixo custo da utilização das redes baseadas em IP (principalmente a Internet) para transmissão de voz são acompanhadas pela falta de padrões[1], que ainda causa dificuldades para a implantação, as limitações de qualidade de serviços e os problemas de segurança. A discussão dos principais aspectos de segurança das redes VoIP é o objetivo deste documento.

---

[1] Um dos motivos para a lentidão da tecnologia VoIP pelas corporações é a falta de padrões, o que torna os projetos mais caros e complexos, e os problemas de interoperabilidade mais difíceis de resolver. A maioria dos vendedores utiliza protocolos proprietários (por exemplo, a Cisco utiliza o "Skinny Station Protocol" para o controle de chamadas).

2. Conhecendo as Ameaças

Os protocolos de VoIP são relativamente novos e os hackers *ainda* não estão familiarizados com eles, o que explica o baixo número de ataques documentados. Entretanto, com a disseminação da tecnologia, a tendência é que, assim como ocorreu com as redes *wireless* baseadas no padrão 802.11, em breve estejam circulando na Internet farto material sobre as vulnerabilidades das tecnologias de VoIP e métodos para sua exploração, e assim o número de ataques visando obtenção de acesso indevido, fraudes ou negação de serviços aumentará significativamente.

As redes de voz representam um alvo importante para os hackers por diversos motivos. Afinal, voz encapsulada em pacotes de dados ainda é informação, e esta informação pode valer muito dinheiro. O simples acesso na caixa-postal de "voice-mail" do CFO *Chief Financial Officer's* (CFO's) pode permitir acesso indevido a informações financeiras estratégicas, cuja utilização pode gerar grandes prejuízos tanto para a própria corporação quanto para terceiros.

É importante ressaltar que na convergência das redes de voz com as redes de dados baseadas em TCP/IP, houve também a *convergência das vulnerabilidades* inerentes as duas tecnologias.

Ou seja, agora, um computador com telefone IP-compatível precisa ser protegido tanto das ameaças relacionadas aos computadores quanto das ameaças relacionadas com a telefonia. Por exemplo, um telefone IP instalado em uma estação de trabalho com o sistema operacional Windows está suscetível às vulnerabilidades do Windows.

Esta questão se tornará mais clara em seguida, na discussão sobre as principais ameaças ao VoIP.

Captura de Tráfego e Acesso Indevido a Informações

No VoIP, o conteúdo das conversas telefônicas está trafegando na rede de dados, encapsulado em pacotes IP, e a captura de pacotes de dados em uma rede IP através de técnicas de "*Sniffing*" é relativamente trivial (ver Figura 1). Já existem na Internet ferramentas como o **VOMIT**[2] ("*Voice Over Misconfigured Internet Telephones*"), que utiliza a ferramenta **tcpdump** do Unix para capturar pacotes de uma conversa telefônica e consegue remontá-los e convertê-los em um formato comum de áudio (*.wav). Ou seja, trata-se de uma espécie de "grampo telefônico" em plena rede de dados!

Embora o VOMIT não seja compatível com todos os padrões existentes (apenas com o CODEC G.711 utilizado pela Cisco), é questão de tempo para que ferramentas ainda mais poderosas sejam desenvolvidas. Vale ressaltar que os mecanismos de transporte de voz não utilizam criptografia, de forma que os pacotes podem ser facilmente capturados e remontados utilizando-se software especializado (como o VOMIT).

---

[2] Ver http://vomit.xtdnet.nl/

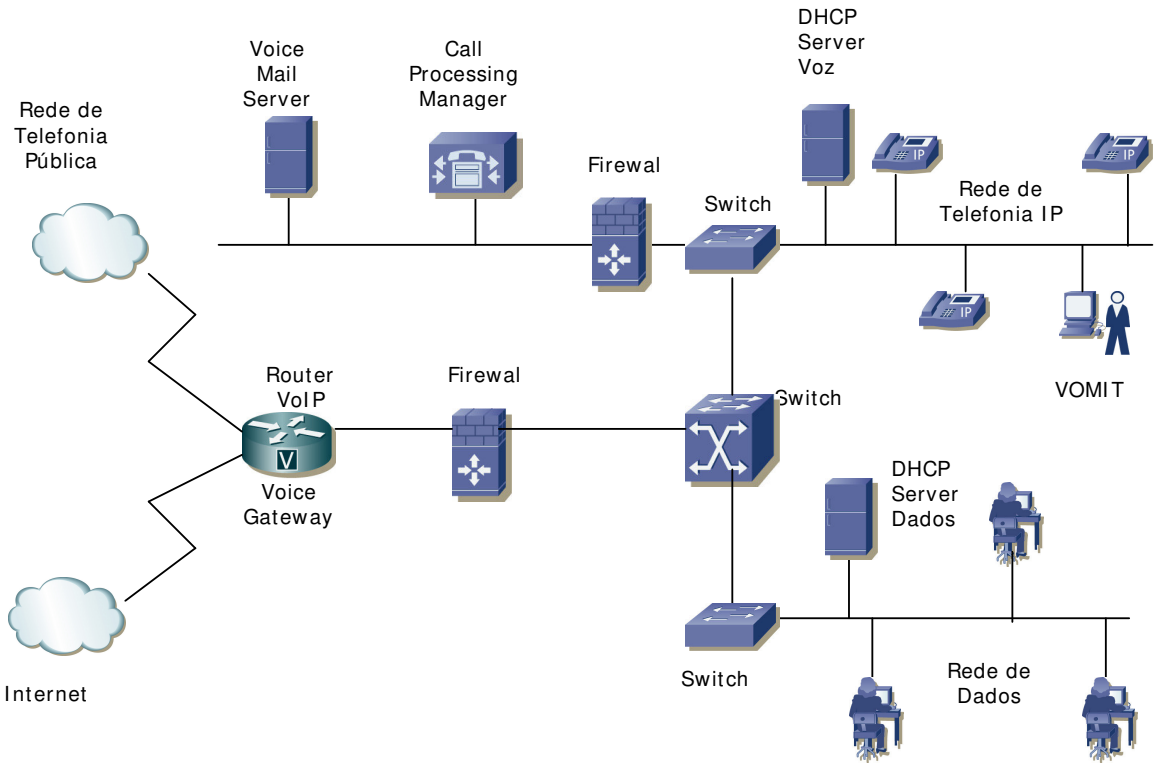

Figura 1 - Principais Componentes da Infra-estrutura VoIP

Outras técnicas mais complexas podem ser utilizadas pelos atacantes para obtenção de acesso indevido às informações corporativas que trafegam pela infra-estrutura de VoIP. Por exemplo, no ataque de "*Caller Identity Spoofing*" (algo como "falsificação da identidade do usuário que iniciou a chamada"), o atacante induz um usuário remoto a pensar que ele está conversando com alguma outra pessoa, ou seja, finge ser alguém que não é para obter informações sigilosas.

Vale ressaltar que este tipo de ataque requer apenas que o atacante obtenha acesso físico à rede e conseguir instalar um telefone IP não autorizado. Em seguida, utilizando uma outra técnica ("*MAC Spoofing*"), o atacante em muitos casos conseguirá sem maiores dificuldades fazer com que seu telefone IP assuma a "identidade" de um telefone IP válido da rede empresa. O resto é engenharia social.

Como se vê, o controle de acesso físico à rede de dados, que sempre foi uma boa prática importante, se torna ainda mais necessário nas redes convergentes. Pontos de rede ativos nos Hubs e Switches e não utilizados são uma porta aberta para ataques e fraudes diversas.

Código Malicioso

Os vírus, "*Trojan Horses*" e outros tipos de códigos maliciosos podem infectar os sistemas de telefonia IP baseados em PCs, e também os "*Gateways*" e outros componentes críticos da infra-estrutura. Desta forma, até mesmo vírus que não foram concebidos para afetar redes VoIP podem causar a paralisação de serviço nestas redes.

Por exemplo, quando ocorreu a grande infestação dos "worms" Nimda e Code Red, o tráfego gerado foi tão grande que as aplicações de VoIP que residiam nas redes de dados infectadas tiveram suas funcionalidades seriamente comprometidas. Telefones IP que suportam aplicações em Java também podem ser alvos de código malicioso que explore vulnerabilidades desta tecnologia.

Fraude Financeira, Uso Indevido de Recursos Corporativos

A ameaça de "*Toll Fraud*" se relaciona aos ataques que visam o uso não autorizado dos serviços de telefonia IP ou métodos de fraude para iludir os mecanismos de bilhetagem e cobrança das ligações realizadas. Os métodos variam. Um tipo de fraude se relaciona com a utilização indevida de um telefone IP para realização de chamadas que sejam contabilizadas como tendo sido originadas pelo endereço do telefone IP de algum funcionário (que seria eventualmente responsabilizado pelo custos!).

Um ataque ainda mais sofisticado envolve a instalação de um "*Voice Gateway*" falsificado pelo atacante. De forma muito simplificada, este "*host*" é o ponto de convergência entre a rede de telefonia pública com a rede de dados, e às vezes com a Internet ou a WAN corporativa. Todas as ligações discadas ou recebidas passam por este dispositivo, o que faz com que ele seja um dos ativos mais críticos em um ambiente de TI, e portanto um dos principais alvos dos hackers. Quando o "*Voice Gateway*" oficial não é comprometido diretamente, o atacante tenta instalar na rede um segundo "*Gateway*" e tenta redirecionar para ele o tráfego destinado ao "*host*" original. Desta forma, consegue bloquear, desviar e até mesmo escutar ligações.

Repúdio

A questão do repúdio tem a ver com a negação, por parte de um usuário que utilizou os serviços de VoIP para fazer uma ligação, de que ele tenha efetivamente feito tal ligação. Como isso poderá ser comprovado ? A menos que se tenha algum mecanismo eficiente para autenticação, não será possível identificar os usuários dos serviços, discriminando quem executou quais chamadas a partir de quais telefones IP.

Indisponibilidade de Serviços

Como mencionado anteriormente, a convergência de voz e dados em rede IP traz também a convergência de alguns problemas de segurança. No caso, todos os ataques de DoS ("*Denial of Service*") capazes de paralisar os serviços em redes TCP/IP irão afetar "por tabela" os serviços de voz, fax e vídeo que dependam deste transporte.

Infelizmente para os responsáveis pelas áreas de TI, o cardápio de ataques de DoS é bastante variado, incluindo por exemplo o "*TCP SYN Flood*" e suas variações, e também a exploração de falhas nas pilhas de protocolo dos sistemas operacionais, como no "*Ping of Death*", "LAND", "*Teardrop*" e vários outros ataques que podem tornar os serviços do VoIP indisponíveis.

Nas redes VoIP, os equipamentos de PBX ("*Private Branch Exchanges*") tradicionais são substituídos por aplicações PBXs IP-compatíveis que são executadas, por exemplo, em servidores Windows NT. Estas aplicações de "*Call Management*" são críticas para a infra-estrutura de VoIP, e no entanto estão sujeitas aos ataques que exploram vulnerabilidades não só das próprias aplicações como também do sistema operacional.

3. Reduzindo os Riscos

Vamos apresentar em seguida algumas boas práticas genéricas para a implantação de uma estrutura VoIP segura.

1. Segmentar tráfego de voz e dados

Se possível, convém segmentar as redes de voz e dados utilizando Switches. A segmentação contribui para uma melhor gestão do QoS e facilita a gerência da rede de voz e simplifica a sua manutenção (por exemplo, a instalação de telefones IP). Além disso, do ponto de vista da segurança, a separação dos segmentos de voz e dados reduz os riscos de ataques de "*eavesdropping*" (captura não autorizada do tráfego de conversas telefônicas que trafegam na rede encapsuladas em pacotes IP) realizados com o VOMIT e outras ferramentas semelhantes.

A segmentação também protege a rede de voz de alguns ataques baseados em TCP/IP que, mesmo destinados a outros alvos que não estejam diretamente relacionados com a infra-estrutura de VoIP, podem tornar estes serviços indisponíveis caso todo o tráfego esteja no mesmo segmento. Por exemplo, os telefones IP normalmente utilizam o protocolo UDP com portas acima de 16384 para sua comunicação. Sendo assim, um ataque de negação de serviços baseado em "*UDP Flood*" no segmento de dados poderia afetar também os serviços de voz se as redes não estiverem adequadamente segmentadas.

Como boa prática, recomenda-se que os segmentos de rede de voz e dados sejam separados em VLANs distintas quando possível. Naturalmente, os detalhes da implementação vão variar em função das características do ambiente. Como referência, em uma instalação de pequeno porte, uma VLAN dedicada ao tráfego de voz seria suficiente, onde seriam instalados o "*Call Manager*" e os telefones IP. Outros componentes como estações de gerenciamento e sistemas de "*Voice/Mail*" podem residir no segmento de dados. Já em instalações de grande porte, várias VLANs podem ser criadas, tanto para voz quanto para dados. Por exemplo, os serviços de "*voice mail*" podem ocupar uma VLAN dedicada.

2. Controlar o acesso ao segmento de voz com um Firewall especializado.

Adicionalmente, convém que o acesso ao segmento de rede onde está instalado o "*Call Manager*" seja protegido por um Firewall especializado, com o objetivo de filtrar todo o tipo de tráfego que seja endereçado à rede de voz e não seja necessário para o funcionamento destes serviços. O FireWall vai proteger o "*Call Manager*" de acessos indevidos por parte de telefones IP não autorizados que sejam instalados em outros segmentos.

Naturalmente, as portas e protocolos que devem ser configuradas no FireWall vão depender do tipo de solução / fabricante de solução VoIP em uso. Por exemplo, no caso da solução Cisco, as seguintes portas podem ser utilizadas: UDP 67/68 (DHCP), TCP 80 (HTTP), UDP 16384-32767 (RTP), TCP 2748 (TAPI/JTAPI), TCP 389/8404 (Cisco Softphone Directory Lookup), TCP 2000 (Cisco Skinny Protocol), TCP 5000 (HDIS Management), TCP 8404 (DCD - Directory Access).

Também é preciso estar atento para o fato de que o Firewall deve ser compatível com o protocolo H.323, utilizado pela telefonia IP. Ocorre que algumas aplicações que utilizam o protocolo H.323 alocam portas dinamicamente para canais de áudio, vídeo e dados. Por este motivo, o Firewall escolhido deve ser capaz de lidar com o tráfego H.323, ou através de um "*proxy*", ou utilizando algum método para determinar que portas estão sendo alocadas para as sessões H.323, de forma a permitir a passagem do tráfego autorizado durante a duração das sessões.

Alguns fabricantes oferecem "*appliances*" de FireWall/VPN customizados para suas tecnologias, como por exemplo o "Contivity Secure IP Services Gateway" da NORTEL.

3. Evitar o uso de aplicações de telefones para microcomputadores (PC-Based IP phones), utilizando preferencialmente telefones IP que suportem VLAN

Se possível, convém utilizar telefones IP que suportem VLANs, em vez de aplicações de *IP Phone* para computadores pessoais ("*PC-based IP Phones*"), já que estas últimas estão sujeitas a um número maior de ataques que os aparelhos de telefonia IP baseados em hardware.

Além do risco de falhas em seu próprio código, as aplicações de telefone IP para PCs estão sujeitas às vulnerabilidades do sistema operacional e também de outras aplicações que residem no computador onde estão instaladas, bem como vírus, worms e outros códigos maliciosos.

Já os telefones IP executam sistemas operacionais proprietários com serviços limitados (e portanto menos vulneráveis). Além disso, como as aplicações de telefone IP para PC precisam residir no segmento de dados da rede, elas são susceptíveis a ataques de negação de serviços (como "*floods*" baseados em UDP ou TCP) que sejam destinados ao segmento como um todo, e não apenas ao computador em que estão instalados.

4. Usar endereços IP privativos e inválidos (compatíveis com RFC 1918) nos telefones IP.

O uso de endereços IP válidos em telefones IP não é necessário e deve ser evitado, para reduzir a possibilidade de que o tráfego de voz possa ser monitorado de fora da rede interna e para evitar que hackers consigam mapear o segmento de voz em busca de vulnerabilidades.

Para facilitar a configuração de filtros e a monitoração, convém utilizar endereços IP privativos e preferencialmente de classes diferentes nos segmentos de voz e dados, de acordo com a orientação do RFC 1918 ("*Address Allocation for Private Intranets*"). As conexões com redes externas devem utilizar endereços IP válidos fornecidos por um Firewall, através do serviço NAT ("*Network Address Translation*").

5. Configurar os telefones IP com endereços IP estáticos, associados ao MAC Address.

O MAC Address é um parâmetro importante para permitir a autenticação dos telefones IP. Quando um telefone IP tenta obter configurações da rede do "*Call Manager*", seu *MAC Address* pode ser verificado em uma lista de controle de acesso. Se o endereço for desconhecido, o dispositivo não receberá a configuração (desde que o recurso de registro automático não esteja habilitado).

Sempre que possível, é uma boa prática ceder endereços IP estáticos para os telefones IP, e associar este endereço IP ao "*MAC Address*" do dispositivo. Desta forma, cada telefone IP terá sempre o mesmo endereço IP associado ao endereço MAC. Desta forma, para conseguir instalar um telefone IP não autorizado na rede, um atacante teria que forjar tanto um endereço IP válido para o segmento de voz quanto o endereço MAC a ele associado, o que dificulta bastante este tipo de ataque. Entretanto, dependendo da escala da implantação, a associação endereço IP estático x "*Mac Address*" nos telefones IP pode ser de difícil gerenciamento, de forma que é preciso avaliar sua aplicabilidade em função das características do ambiente.

6. Utilizar servidores DHCP separados para voz e dados.

Adicionalmente, tal como foi representado na Figura 1, convém utilizar servidores DHCP separados para os segmentos de voz e dados. Desta forma, os ataques de negação de serviços e outros lançados contra o servidor DHCP no segmento de dados não vai interferir com a alocação de endereços IP para os telefones no segmento de voz, e vice-versa, o que aumenta a tolerância da rede.

7. Monitorar os endereços MAC no segmento de voz.

Convém utilizar ferramentas como o ARPWATCH para monitorar os "MAC Addresses" de todos os dispositivos instalados no segmento de voz. O ARPWATCH é capaz de registrar alterações não autorizadas na associação entre endereço IP e endereço MAC. Para informações adicionais, ver http://www-nrg.ee.lbl.gov/nrg.html.

8. Implementar mecanismos que permitam autenticar os usuários dos telefones IP

Quando suportado pela tecnologia em uso, convém implementar os recursos de autenticação dos usuários dos telefones IP, além de autenticar apenas os dispositivos através de seus endereços MAC. Alguns modelos de telefone IP exigem que o usuário faça um "login" informando uma senha ou número de identificação (PIN) válidos para que possam utilizar o dispositivo. A autenticação do usuário reduz os riscos de uso indevido dos recursos da rede de voz, e permite maior rastreabilidade no uso dos serviços, além de um certo nível de não repúdio.

Algumas aplicações de telefone IP para a plataforma Windows suportam autenticação integrada ao sistema operacional, enquanto outros modelos utilizam uma combinação de nome de usuário / PIN. Em qualquer caso, as senhas utilizadas devem ser trocadas periodicamente e devem ser de difícil dedução.

9. Implementar um sistema IDS

Embora os sistemas atuais de detecção de intrusos (IDS) ainda não contenham assinaturas específicas de ataques para os protocolos de VoIP, eles podem ser úteis para monitorar ataques baseados em UDP e HTTP que podem ser executados contra os componentes da infra-estrutura.

Por este motivo, convém que uma aplicação ou *appliance* de IDS seja instalado no segmento onde estiver instalado o "*Call Manager*", visando a detecção de ataques originados principalmente no segmento de dados, onde estão localizadas as estações de trabalho dos usuários.

Naturalmente, é necessário fazer o *tunning* do IDS para maximizar sua eficiência. Esta operação é dependente do tipo de tecnologia e protocolos de VoIP em uso. De qualquer forma, se tiverem sido separados os segmentos de voz e dados como recomendado, o tráfego esperado no segmento de voz estará obrigatoriamente associado a um número limitado de protocolos e portas, o que facilita a configuração do IDS e reduz o número de falsos positivos. Qualquer tráfego TCP/IP que não esteja relacionado aos protocolos utilizados pela tecnologia VoIP em uso deve gerar alarmes no sistema IDS.

10. Fazer o *hardening* do "host" onde está instalado o call manager

O C*all Manager* é um alvo preferencial para atacantes interessados em explorar vulnerabilidades da infra-estrutura de VoIP. Existem muitos vetores de ataque, em função do grande número de serviços que podem estar sendo oferecidos por estas aplicações.

Por exemplo, o C*all Manager* normalmente disponibiliza aplicações para controle de chamadas, permite a configuração via Web, dá suporte a serviços de localização de telefones (*IP phone browsing*), serviços de conferência, e gerenciamento remoto por SNMP.

Por este motivo, convém que sejam implementados procedimentos para a configuração segura ("*hardening*") do servidor onde o call manager está instalado. Como recomendações genéricas, convém desabilitar todos os serviços desnecessários, instalar os patches do sistema operacional e um bom antivírus. Os serviços inicializados pelo *call manager* devem utilizar contas de baixo privilégio, e o acesso físico ao servidor deve ser restrito a usuários autorizados.

11. Monitorar a performance e status dos serviços de VoIP

O objetivo deste controle é permitir a monitoração periódica, se possível em tempo real, do desempenho da rede de voz, e detectar instabilidades, atrasos e latências que possam comprometer a performance ou disponibilidade dos serviços. A monitoração pode ser feita através de soluções proprietárias disponibilizadas pelos fabricantes (Cisco, etc), ou de soluções de mercado como o VoIP Manager da NetIQ ou o VoIP Test Suite da Brix Networks.

12. Montar uma estrutura de Help Desk capacitada para dar suporte em VoIP

Uma vez feitos os investimentos em uma rede convergente de voz e dados, os funcionários dependerão de sua boa operação para poder executar suas atividades, de forma que é importante manter disponíveis os serviços de voz. A tecnologia VoIP utiliza equipamentos especializados e requer configurações em Switches, Roteadores e aplicações, de forma que uma equipe de suporte técnico deverá ser treinada para a resolução de problemas ("*troubleshooting*") nos componentes da infra-estrutura da VoIP e para prestar atendimento aos usuários. Também é conveniente manter um contrato de Suporte Técnico com algum integrador qualificado, ou com o próprio fabricante dos equipamentos adquiridos.

13. Restringir o acesso físico

Obtendo acesso físico indevido na rede, um atacante pode por exemplo instalar um telefone IP não autorizado e utilizar técnicas de "*MAC Spoofing*" e "*Caller Identity Spoofing*" para enganar os usuários, fazendo-os pensar que estão conversando com alguma outra pessoa, quando na verdade estão conversando com o atacante. Desta forma informações sigilosas poderão ser obtidas através de engenharia social.

Naturalmente, o acesso físico indevido também expõe os componentes da infra-estrutura de VoIP a ameaças como fraudes, roubo, sabotagem ou danificação acidental ou proposital dos equipamentos, podendo causar a indisponibilidade dos serviços. Por estes motivos, convém que o acesso físico aos dispositivos mais críticos da rede (Switches, Roteadores, *Call Manager*, Firewalls, etc), seja restrito apenas para usuários autorizados.

14. Auditar o Uso dos Recursos

Para maior rastreabilidade da utilização dos serviços de VoIP, convém manter registros das informações sobre as sessões (data e hora do início e término, duração, origem, destino, etc). Informações relacionadas ao QoS (latência, perda de pacotes, uso de banda, etc) também podem ser coletadas para auditorias futuras. A auditoria pode ser implementada através de aplicações especializadas.

Nota: Para maior rastreabilidade, convém que seja implementado algum tipo de autenticação dos usuários dos telefones IP.

15. Criptografar o tráfego de VoIP

Quando possível, convém criptografar o tráfego entre o telefone IP e o "*Call Manager*". Isto impedirá o uso de ferramentas como o VOMIT para violação da confidencialidade das conversações. A criptografia pode ser feita, por exemplo, estabelecendo-se um túnel IPSec entre as estações com telefones IP e o "*Call Manager*". Nas comunicações externas (matriz com filiais, por exemplo), pode-se considerar a implementação de uma VPN ("*Virtual Private Network*") para criptografar o tráfego de VoIP.

4. Conclusão

Nas redes onde há convergência de voz e dados, há muitos "alvos" em potencial em risco, como telefones IP, roteadores, Switches, Gateways, sistemas de "*Voice/Mail",* FireWalls e outros. O fato é que *a convergência das redes traz também a convergência das ameaças*, de forma que a infra-estrutura de VoIP herda os perigos das redes de dados (mapeamentos, *TCP/IP Denial of Service*, exploração das vulnerabilidades dos sistemas operacionais, engenharia social, roubo de identidade e *spoofing*, etc) e também é sujeita as ameaças e problemas inerentes aos serviços de voz (*delay*, *jitter*, perda de pacotes, "*Toll Fraud*" (fraudes de pagamento), *IP Phone Spoofing*, etc).

Em muitos projetos, os mecanismos de autenticação ainda são deficientes, permitindo apenas a identificação *do telefone*, e não *do usuário*. Ferramentas como o VOMIT podem comprometer a confidencialidade das conversas telefônicas, permitindo ao hacker acesso indevido a informações sigilosas. Finalmente, nos ataques de negação de serviços, é preciso considerar que o impacto do *downtime* do sistema de telefonia, uma vez integrado na rede de dados, pode ser devastador para os negócios na maioria das corporações.

Infelizmente ainda não há uma solução única que ofereça proteção contra todas estas ameaças. Muitos projetos de VoIP ainda são baseados em componentes e produtos fornecidos por vários fornecedores, o que torna a infra-estrutura bastante heterogênea, e nenhum vendedor tem atualmente a solução perfeita e completa para todas as vulnerabilidades, até porque algumas são inerentes à própria tecnologia e protocolos em uso (como por exemplo as fragilidades do TCP/IP) e portanto podem ser minimizadas, mas não totalmente eliminadas. Além disso, os problemas de padronização e os desafios de integração das soluções oferecidas pelos diferentes fabricantes introduzem um grau de complexidade nos projetos que contribui ainda mais para a falta de segurança.

As soluções requerem de início um bom planejamento da infra-estrutura. O cabeamento deve ser adequado, os dispositivos devem suportar as demandas de QoS requeridas, a rede deve ser segmentada apropriadamente, os serviços como o DHCP devem ser bem planejados. A definição de uma Política de Segurança é muito importante, e deve preceder a configuração de Switches, Roteadores, FireWalls, soluções de IDS e outros dispositivos de proteção, cujo acesso físico deve ser restrito a usuários autorizados. O uso de criptografia do tráfego de voz encapsulado na rede IP é recomendado em certos contextos.

A escolha dos equipamentos (por exemplo, telefones IP que suportem VLAN e soluções que ofereçam recursos de autenticação mais sofisticados) é crítica para viabilizar um maior nível de segurança, bem como o treinamento do pessoal envolvido na instalação, suporte e auditoria dos serviços. Em alguns casos, até mesmo um plano de "*Disaster Recovery*" deve ser considerado, tal o impacto que a descontinuidade dos serviços de voz pode trazer para a corporação.

Finalmente, é preciso conscientizar os usuários dos serviços VoIP no ambiente corporativo sobre os riscos existentes, já que em muitos casos eles próprios poderão ser responsabilizados pelo uso indevido, fraude e outras ações maliciosas executadas por *hackers* e *phreakers*.

GLOSSÁRIO

IP Phone* ou dispositivo de telefonia IP:* É qualquer equipamento ou aplicação para PCs que suporte conversação através dos padrões de voz sobre IP. Isto inclui telefones propriamente ditos (IP phones) bem como softwares instalados nas estações de trabalho dos usuários, com microfones e alto-falantes.

Call-processing Manager*:* Servidor que gerencia o estabelecimento das conexões, gerencia e fornece configurações necessárias para o funcionamento dos telefones IP quando eles são inicializados, e também gerencia o roteamento do tráfego para outras redes quando necessário.

Voice-mail system*:* Servidor que faz o armazenamento das mensagens de voz baseadas em IP e permite que os usuários façam acessos a estas mensagens.

H.323: Protocolo do ITU que é uma extensão do padrão H.320, permite o transporte de tráfego de voz, imagem e dados em redes de pacotes.

Session Initiation Protocol (SIP): Padrão do IETF para vídeo e áudio conferência sobre IP. Trata-se de um protocolo de aplicação definido no RFC 2543 que trata das questões de sinalização e estabelecimento de sessões entre dispositivos da rede.

REFERÊNCIAS

RFC 2543—*SIP: Session Initiation Protocol*:
http://www.cisco.com/warp/public/788/voip/voice_rfcs.html

White Paper - SAFE: IP Telephony Security in Depth
Author - Jason Halpern
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm

White Paper - Security in SIP-Based Networks
Cisco Systems

SANS 2002 - Deploying Secure Converged Networks
Jason Halpern (Cisco Systems)

Securing your Voice Over IP Network
James Valentine & Rick Blum
INS - International Network Services