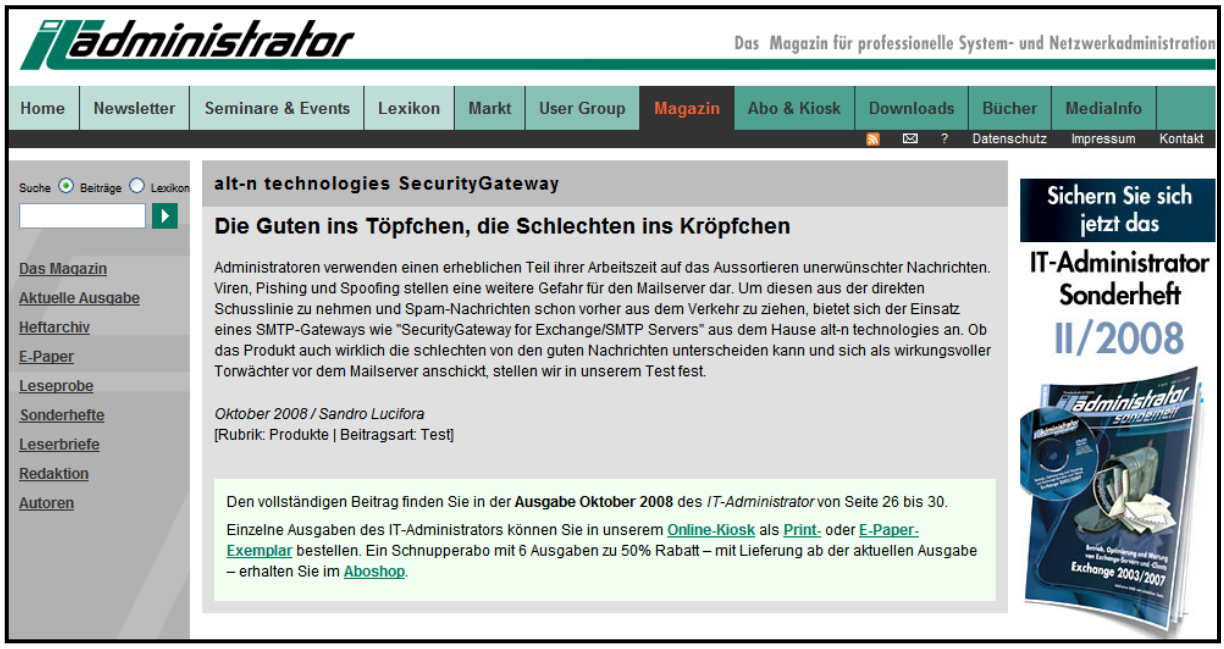
Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008



Teste: Alt-N Technologies SecurityGateway

Os administradores de servidores de e-mail usam uma boa parte de seu tempo tentando eliminar mensagens indesejadas. Vírus, Phishing e Spoofing são também ameaças. Na tentativa de retirar o servidor de e-mail da linha de fogo, e para eliminar os “spams” antes que cheguem ao servidor, a solução mais lógica é o uso de “gateways” como o “SecurityGateway para MS Exchange/SMTP” da Alt-N Technologies. Em nosso teste iremos determinar se este produto pode realmente discernir as mensagens boas das indesejáveis, e se o produto realmente age como um competente “porteiro” na proteção do servidor de e-mail.

Mensagens eletrônicas são transferidas de um servidor SMTP para outro. Para que essa transferência de dados funcione de modo correto, um servidor SMTP deve estar sempre acessível na Internet em sua porta 25. Se o mesmo servidor também disponibiliza acesso POP3 ou armazena

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

mensagens, a área vulnerável para um ataque cresce na mesma proporção. Para que se possa continuar a receber e-mails diretamente e ter o servidor na Intranet, a instalação de um gateway SMTP parece ser a melhor opção. Somente o gateway SMTP ficará diretamente acessível via Internet, agindo como um servidor SMTP. Além disso, o gateway trabalha varrendo as mensagens recebidas, filtrando spam e vírus.

É exatamente essa funcionalidade que o SecurityGateway da Alt-N Technologies oferece. O software recebe os e-mails, verifica sua validade e qualidade em um processo de varredura em camadas, transmitindo as mensagens que considera legítimas para o servidor de e-mail principal na rede interna da empresa. As vantagens deste processo são claras: o gateway pode ser integrado ao sistema de e-mail existente não importando a marca do mesmo, e o administrador não precisa adaptar ou ajustar as configurações existentes no servidor de e-mail principal.

Instalação e Configuração

Após a instalação do produto, o primeiro passo é definir o método de verificação. Ao explorar esta função identificamos a primeira vantagem do gateway: esta opção permite definir com antecipação quais serão os destinatários para os quais o gateway estará recebendo mensagens. Os destinatários poderão ser identificados manualmente no gateway. Entretanto, o usual é que esses destinatários já estejam definidos em algum outro local. Em grandes instalações – ou mesmo para eliminar trabalho desnecessário – o método escolhido é a verificação via Active Directory, um servidor Exchange, ou qualquer outro servidor LDAP. Se outra solução de groupware é utilizada, a verificação via “SMTP Call Forward” elimina a necessidade de configuração manual. Usando o protocolo SMTP, esta ferramenta verifica, em cada mensagem recebida, se o destinatário possui uma caixa postal válida no servidor de e-mail principal da organização.

Após configurar os domínios de e-mail e o método de verificação, definimos o endereço IP ou o “host name” do servidor de correio eletrônico que deverá receber as mensagens após a verificação. Aqui também definimos a porta SMTP. Esta configuração é importante se o SecurityGateway e o servidor principal de correio eletrônico encontram-se instalados no mesmo hardware. Neste caso, os dois serviços estarão monitorando a porta 25 no mesmo endereço IP, o que pode prejudicar o bom funcionamento do sistema de correio eletrônico. Será então necessário configurar o servidor SMTP principal para uma porta diferente: 10025, por exemplo, (veja fig. 2). Isto faz com que o gateway

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

receba as mensagens na porta 25, as quais serão então verificadas e encaminhadas para, por exemplo, um servidor Exchange na porta 10025. Nesta situação é importante configurar o servidor de e-mail principal para somente aceitar mensagens do mesmo IP, o do gateway, exigindo autenticação SMTP. Isto garante que o servidor de e-mail principal não seja utilizado como um servidor de repasse (relay). Após efetuar os passos acima a instalação está concluída, e o serviço é iniciado.

O SecurityGateway tem uma interface de administração que utiliza seu próprio servidor Web interno, e que pode operar em paralelo a um servidor IIS existente. A interface pode ser utilizada pelos principais navegadores do mercado. Se a verificação de destinatários válidos é feita através de Active Directory – em um servidor Exchange, por exemplo – então a única configuração necessária antes da utilização do gateway é a dos domínios dos destinatários válidos. Além disso, o gateway deve saber em qual servidor deverá verificar as caixas postais, e onde deverá entregar as mensagens. No nosso teste configuramos diferentes servidores de correio eletrônico para vários domínios diferentes.

Segurança em Múltiplas Camadas

O menu de Segurança do gateway é dividido em “Spam”, “Vírus”, “Spoofing” e “Abuse”. As ferramentas Anti Spam são baseadas no já conhecido “SpamAssassin” e trabalham com Regras Heurísticas e Filtro Bayesiano. O software pode utilizar o SpamAssassin que já vem integrado ao produto ou mesmo uma sessão remota do SpamAssassin. A segunda opção tem a vantagem de se ter um único SpamAssassin centralizado e configurado para múltiplos gateways. A “Lista Negra DNS” utiliza as bases de dados “spamhaus.org” e “spamcop.net”. Bases de dados adicionais podem ser incluídas. A “Lista Negra de URLs” complementa as rotinas de identificação de Spam, tendo por base o conhecido site URIBL.

Proteção Efetiva contra Spam através de Greylisting

Greylisting é uma das ferramentas mais recentes dos Filtros de Spam. Esta ferramenta faz com que o SecurityGateway recuse temporariamente a primeira mensagem recebida de um remetente desconhecido. Se uma segunda tentativa é feita para entregar a mensagem (servidores SMTP que operam de acordo com RFC são configurados deste modo), a mesma é finalmente aceita. As ferramentas de envio de Spam não tentarão enviar uma mensagem duas vezes porque não recebem

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

nenhuma mensagem de rejeição vindas do diálogo no protocolo SMTP. Após a segunda entrega da mensagem o SecurityGateway trata o servidor remetente como “bom” e armazena esta informação na base de dados local. Se o gateway receber novas mensagens de um mesmo servidor previamente verificado, as mensagens serão aceitas sem nenhuma restrição.

A ferramenta Clam Antivírus se encarrega da verificação de vírus. É possível adicionar o aplicativo opcional ProtectionPlus, que opera com um engine Kaspersky para proteger o sistema das mensagens que possam estar infectadas. É possível configurar o intervalo de atualização do antivírus para uma vez por hora ou uma vez por dia, mas o método de atualização a cada hora deve ser o escolhido.

Nenhuma Mudança no Spoofing

Spoofing é a tentativa de um servidor de correio eletrônico de mascarar sua real identidade, por exemplo, através de endereços forjados. O SecurityGateway possui várias armas eficientes na verificação antecipada da identidade dos remetentes. Além deste primeiro passo, a verificação reversa, a verificação DKIM e o SPF (Sender Policy Framework), em conjunto com a verificação da identidade do remetente (Sender ID), são utilizados em cada mensagem. A verificação “call-back” é mais um obstáculo adicional para as mensagens de Spam. Essas mensagens são usualmente enviadas sem nenhum dado no cabeçalho “DE”. Se, por esta razão, o remetente não puder ser verificado, o gateway irá recusar a mensagem.

Nós configuramos a proteção contra o uso do servidor como repasse (“Relay Server” e, portanto, um Servidor Spam) através da definição dos endereços dos remetentes autorizados. A ferramenta adicional de autenticação SMTP é mais uma alternativa contra o uso indevido do servidor.

Filtros personalizados podem também ser criados a partir de regras de conteúdo para mensagens e anexos. No nosso teste poderíamos, por exemplo, ter arquivos executáveis bloqueados e arquivos de áudio sendo automaticamente transferidos para a quarentena. Estas configurações podem ser aplicadas de modo global para todos os domínios, ou para domínios específicos. Listas negras e brancas individuais, passíveis de configuração manual para um único endereço de e-mail, domínio ou endereço IP, completam a poderosa configuração de segurança.

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

A Varredura das Mensagens enviadas aumenta a taxa de detecção

Além do tráfego de mensagens que entram no servidor, também é monitorado o tráfego de saída de mensagens. O pré-requisito para o uso desta ferramenta foi que instruímos nosso servidor para não mais entregar mensagens diretamente ou via um “smarthost”, mas somente via o SecurityGateway.

O gateway pode analisar o tráfego externo e aprender com isso. Os exemples clássicos são as palavras “sexo” e “Viagra” no corpo da mensagem. No recebimento, tais palavras usualmente fazem com que as mensagens sejam classificadas como spam e isoladas. Entretanto, o uso dessas palavras pode ser parte do dia-a-dia de negócios para, por exemplo, empresas do ramo farmacêutico ou de comercialização de produtos eróticos. Quando o gateway reconhece que mensagens contendo tais palavras-chave são enviadas, ele automaticamente ajusta de acordo os critérios de recebimento de mensagens. Isto também se aplica a remetentes cujos domínios ou servidores – que por qualquer razão – estejam incluídos em uma lista negra. O gateway normalmente recusa tais mensagens. Ao mesmo tempo em que o software reconhece no tráfego de saída que mensagens estão sendo enviadas para o domínio na lista negra, as mensagens originadas desse domínio serão encaminhadas aos destinatários.

Excelentes Índices de Detecção

Em nosso teste, utilizamos um serviço web para encaminhar spam e mensagens com vírus ao nosso domínio de teste. Também colocamos na lista negra da spamhaus.org um domínio acessível via Internet. Com esses preparativos poderíamos receber mensagens reais e manipuladas por várias semanas, testando a eficiência da plataforma. O resultado foi que nenhuma mensagem indesejada passou pelo nosso domínio de teste sem ser colocada previamente em quarentena. Somente quando deliberadamente enviamos mensagens para aquele domínio através do nosso gateway foi que o SecurityGateway identificou que o recebimento de mensagens desse domínio era desejado.

Como já mencionamos, o aplicativo ProtectionPlus, adquirido em separado, amplia as ferramentas de segurança do SecurityGateway através do Kaspersky Antivirus. Apesar do Clam Antivírus não ter falhado nenhuma vez em nossos testes, pode-se concluir que, numa comparação direta, o mesmo teria maiores dificuldades com novos vírus. Com relação à atualização das bases de informação sobre vírus, a solução Kaspersky é reconhecidamente tão boa quanto imbatível.

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

Conclusão

Como regra, o uso de um gateway SMTP faz sentido na complementação de um sistema de correio eletrônico existente pela adição de poderosos filtros de Spam e Vírus, e para remover o servidor de correio eletrônico da DMZ da rede. Durante nosso teste, conduzido durante várias semanas, o SecurityGateway não demonstrou nenhuma fraqueza e bloqueou de maneira segura spam, vírus e mensagens forjadas (“phishing”). A ferramenta de aprendizado mostrou toda a sua eficácia após o envio de aproximadamente duzentas mensagens. As opções de configuração são versáteis, mas podem “fazer o tiro sair pela culatra”. Se as configurações de segurança do gateway forem definidas com muita rigidez, mensagens legítimas poderão ser bloqueadas. Sendo assim, é necessário, especialmente durante as primeiras semanas ou meses, revisar regularmente as regras e os arquivos de log de modo a adaptar as configurações às necessidades da organização. Ao contrário de regras usadas em um firewall, a estratégia de não aceitar nada no início da instalação e gradualmente ir abrindo aos poucos portas específicas, no caso do SecurityGateway, é recomendável inicialmente confiar na configuração padrão (default) do produto e só então gradualmente adaptá-la, após várias semanas de aprendizado e análise dos arquivos de log.

Aqueles que selecionarem a menor licença de 10 (dez) usuários, com certeza estarão buscando as mensagens em seu provedor internet via POP3. Através de um atalho e um conector POP3 adicional (veja dica 2) esta implementação poderá ser mantida. Seria recomendável, entretanto, que tal funcionalidade fosse incluída no gateway. Fora isso, podemos dizer que o SecurityGateway possui implementação rápida, a sintonia fina da configuração é poderosa, e tem preço extremamente competitivo. A um custo de EUR 50 por usuário no primeiro ano e EUR 10 nos anos seguintes, o investimento será rapidamente amortizado. (Nota do Tradutor: valores exclusivos para a Alemanha)

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

Resumo e Avaliação

Produto: SecurityGateway para filtro de Spam e defesa contra vírus

Preço: A licença para 10 usuários custa EUR 474 para o primeiro ano e EUR 100 para cada ano subseqüente. A proteção opcional do SecurityPlus adiciona EUR 143 para o primeiro ano e EUR 100 para cada ano subseqüente, considerando-se o mesmo número de usuários (caixas postais). Encontram-se também disponíveis licenças de 25, 50 e 100 usuários.

(Nota do Tradutor: valores exclusivos para a Alemanha)

Dados Técnicos: www.it-administrator.de/downloads/datenblaetter

Avaliação da IT-Administrator (máximo 10 pontos)

Confiabilidade dos Filtros: 10

Individualização dos Filtros: 8

Atualização das Definições: 8

Tempo e Esforço de Configuração: 8

Tempo e Esforço da Administração: 8

O Produto é...

Ideal para proteger sistemas de correio eletrônico baseados no MS Exchange, usando Active Directory.

Recomendável para proteção de sistemas de correio eletrônico sem Active Directory, usando um servidor LDAP ou a verificação SMTP “call-forward”.

Não adequado para uso em estações de trabalho.

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

Figuras

Fig. 1: Visão esquemática da implementação do SecurityGateway

Fig. 2: Configuração do gateway se o servidor de correio eletrônico encontra-se instalado no mesmo hardware

Fig. 3: A interface web abrangente permite a configurações de segurança individuais

Fig. 4: Extrato de um arquivo de log que registra tentativa mal sucedida de utilizar o SecurityGateway para enviar Spam

Fig. 5: Exemplos de configuração do “Small Business SMTP Connector, para que se possa usar o SecurityGateway também no tráfego de saída de mensagens

Dicas

Dica 1: Discos Rígidos Rápidos

Como o SecurityGateway utiliza constantemente o disco rígido, a velocidade na entrega de mensagens poderá ser otimizada instalando-se discos de maior velocidade. Discos rígidos específicos para a base de dados e para os arquivos de log aumentarão também seu desempenho.

Dica 2: Retirar Mensagens no Caso de Endereços IP Dinâmicos

Para aqueles que não possuem seus servidores de correio eletrônico como um registro MX em seus domínios, ou que utilizem endereços IP dinâmicos, sugerimos acessar caixas postais externas através de um conector POP3, encaminhando suas mensagens para o SecurityGateway via protocolo SMTP. Apesar de existirem várias opções comerciais no mercado, o software gratuito “PullMail” é ideal para essa tarefa. Esta ferramenta provavelmente não terá seu desenvolvimento continuado, mas a mesma pode ser obtida via link [1].

Tradução para o Português

SecurityGateway para Servidores MS Exchange/SMTP

Fonte: www.IT-Administrator.de

Data da Publicação: Outubro 2008

Requisitos de Sistema

Os requisitos de sistema para o SecurityGateway vão depender do volume de tráfego de correio eletrônico a ser gerenciado. Para um tráfego médio de 10 a 25 usuários, e no caso de uso exclusivo do hardware, o fabricante especifica os seguintes requisitos mínimos de sistema: Sistema Operacional Microsoft Windows 2000, XP, Vista ou Server 2003. O servidor deverá ser equipado com processador Pentium 4 (recomendável multi-core) e um mínimo de 512 MB de memória RAM (2 GB é recomendável) e uma partição NTFS com um mínimo de 500 MB de espaço disponível. Os clientes devem utilizar navegadores como o Microsoft Internet Explorer 6.0, Firefox 1.5, Opera 8.5, Safari, 3.5, além do Adobe Flash Player, a partir da versão 8.

Testamos o gateway em uma máquina virtual rodando VMWare, com Windows Server 2008 como sistema operacional.