

McAfee SpamKiller for Microsoft Exchange

Powered by McAfee SpamAssassin

O McAfee® Security SpamKiller® for Microsoft® Exchange, “powered by McAfee SpamAssassin™”, proporciona detecção e desempenho anti-spam inigualáveis, sem rival na proteção de servidores Microsoft Exchange. Ajustado para operar em alta velocidade, o McAfee SpamKiller pode ajudar a reduzir os custos associados ao spam, realizando a varredura do e-mail que entra logo que ele chegar ao servidor Microsoft Exchange. Logo após a varredura, é possível colocar o e-mail de spam em quarentena em uma pasta de lixo eletrônico do servidor ou do próprio usuário. Detectando o spam, você impede que os seus usuários precisem lidar com mensagens indesejáveis, ajudando-os a aumentar a sua produtividade.

O Que É o Spam?

Definindo um problema crescente

Existem muitas maneiras diferentes de descrever o spam, e o que é spam para uma pessoa pode ser informação útil para outra. Para simplificar a questão, a McAfee Security classifica o spam em três grupos: spam mal-intencionado, spam de propaganda e spam amistoso. O spam mal-intencionado consiste em mensagens que podem incluir conteúdo inadequado ou ameaças à segurança; o spam de propaganda consiste em mensagens de empresas legítimas tentando vender produtos ou serviços; e o spam amistoso consiste em mensagens contendo piadas, correntes ou links para páginas de humor. Todos os estudos recentes do ramo indicam que o volume do spam está crescendo. Aproximadamente 25% a 50% de todos os e-mails que as organizações recebem são spam.

O Spam é Apenas um Pequeno Inconveniente? Não!

O Spam é uma ameaça devastadora

Calcula-se que as mensagens indesejáveis custaram às empresas norte-americanas mais de US\$ 10 bilhões em 2003, e um recente estudo da Comissão Europeia nos mostra que o spam custa aos usuários europeus da Internet €10 bilhões anuais. Existem 4 áreas principais de aborrecimento nas quais o e-mail de spam custa dinheiro à sua organização.

Perda de produtividade — a quantidade de tempo gasta pelos usuários na leitura e no gerenciamento de mensagens indesejáveis. Estima-se que a perda de produtividade dos usuários seja o maior custo associado ao spam para as empresas.

Conteúdo inadequado — mensagens que, de algum modo, são consideradas ofensivas e, muito provavelmente, violam a política de RH. Esse tipo de

mensagem pode ofender pessoas ou grupos (por exemplo, a mensagem pode conter assuntos adultos).

Consumo de recursos de TI — a quantidade de largura de banda da rede ocupada pelo spam que realmente consegue chegar à rede.

Spam como uma ameaça à segurança — os e-mails de spam podem conter códigos mal-intencionados ou ataques de DDoS; os e-mails infectados por vírus podem usar métodos de distribuição semelhantes aos do spam (por exemplo, Sobig.F e envio de e-mails em massa).

Varredura do Spam

Reduzindo a ameaça

O McAfee SpamKiller for Microsoft Exchange reduz os custos do spam, varrendo as mensagens que entram, assim que chegam ao servidor Exchange. Após a varredura, o e-mail de spam pode ser colocado em quarentena em uma pasta de lixo eletrônico do servidor ou do próprio usuário. Detectando o spam, você impede que os seus usuários precisem lidar com mensagens indesejáveis, ajudando-os a aumentar a sua produtividade. Além disso, você ajudará a impedir que os seus funcionários recebam conteúdos inadequados em e-mails, permitindo uma melhor aplicação das suas políticas de RH. Você evitará o desperdício de largura de banda — transferência de arquivos e armazenamento no desktop — pois o material ofensivo ficará armazenado de forma segura em uma pasta residente no servidor. Você também reduzirá os riscos à segurança associados ao e-mail de spam.

Regras Predefinidas

Detecção instantânea

A tecnologia central da família de produtos McAfee SpamKiller é o engine McAfee SpamAssassin™, que opera com um sistema de classificação, atribuindo pontuações às mensagens de acordo com uma série de testes. É altamente preciso na identificação do spam, capturando até 95% de todo o spam, além de proporcionar uma taxa muito reduzida de identificação de falsos positivos (menos de 0,05%). A McAfee Security mantém as regras predefinidas que acompanham o produto. Não é necessária nenhuma configuração de regras, pois o McAfee SpamKiller é extremamente eficaz na detecção do spam, sem necessidade de ajuste.

Sistema de Pontuação

Pontuações diferentes para mensagens diferentes

O SpamAssassin utiliza um sistema de pontuação baseado em um amplo conjunto de regras, para determinar se uma mensagem de e-mail é um spam. Centenas de regras são aplicadas a cada e-mail e cada regra é associada a uma pontuação negativa ou positiva. Regras com pontuação negativa indicam atributos de e-mails legítimos e regras com pontuação positiva indicam atributos de mensagens não-solicitadas. Combinadas, essas pontuações individuais atribuem a cada e-mail uma "classificação geral de spam". Um algoritmo genético otimiza a pontuação, utilizando um arquivo de milhões de mensagens de spam e que não são spam para determinar as pontuações de cada regra. Agora que o e-mail é usado como uma parte crítica da infra-estrutura de negócios, é vital que todos os fabricantes de anti-spam ofereçam proteções contra mensagens incorretamente identificadas como spam. O uso de um sistema de pontuação é obrigatório hoje em dia, pois ele permite a detecção das áreas "cinzas" do spam.

Edição de regras

Ajuste das regras por meio da interface de usuário

Se o administrador quiser aumentar as regras predefinidas, poderá fazê-lo por meio da interface administrativa. Personalizar as regras em cada organização permite que o administrador ajuste com precisão o sistema às suas necessidades.

Vários Níveis de Proteção Contra Spam

Seis níveis que garantem a detecção

Utilizando o processo subjacente de conjuntos de regras predefinidas, o McAfee SpamKiller verifica, por meio de cinco métodos diferentes de detecção, cada e-mail recebido.

- **Análise de Integridade** — O SpamKiller examina o cabeçalho, o layout e a organização de cada mensagem de e-mail para identificar as características comuns do spam. Um avançado engine de comparação de padrões aplica simultaneamente centenas de algoritmos durante uma única passagem, determinando uma classificação de probabilidade que define se a mensagem é spam ou não. Este é um método altamente preciso de detecção de spam.

Método de Detecção Heurística—Este método utiliza uma série de testes internos para determinar a probabilidade de que uma mensagem seja spam. Cada teste atribui uma pontuação para ajudar a reduzir falsos positivos. Isso assegura que o McAfee SpamKiller funcionará de maneira proativa para proteger o seu ambiente contra o spam.

Bayesian Filtering—McAfee SpamKiller provides Bayesian filtering technology to allow e-mail messages to be "intelligently assessed for spam and non-spam criteria. The Bayesian filtering provided includes a pre-taught database of Bayesian filters, as well as proactive technology to automatically learn what types of messages should be classed as spam and non-spam in your organization.

- **Filtragem de conteúdo** — Esta função pode ser usada para ajudar a identificar as palavras ou expressões chaves presentes em um e-mail e que podem indicar que a mensagem se trata de spam. O administrador ou o usuário (dependendo do tipo de software que está sendo usado – servidor ou cliente) pode incluir palavras ou expressões em um banco de dados para definir o conteúdo inadequado.
- **Blacklists e Whitelists** — O administrador é capaz de estabelecer os padrões no nível do servidor para determinar e-mails de spam para todos na organização, utilizando configurações globais de whitelists e de blacklists. Personalizar as blacklists e whitelists permite que os usuários vejam e editem as suas próprias listas. Esta poderosa função transfere para os seus usuários finais a decisão final sobre o que é spam ou não, liberando o tempo do administrador de sistemas para outras tarefas.
- **Auto-Ajuste** — O McAfee SpamAssassin é capaz de aprender as características dos e-mails que você recebe. Ele é capaz de usar a informação para ajustar a "classificação geral de spam" de novas mensagens enviadas por um remetente conhecido. O auto-ajuste ajuda a reduzir a identificação de e-mails falsos positivos e aumentar a taxa de detecção de spam sem que o administrador ou o usuário precisem configurá-la. Portanto, o McAfee SpamAssassin é essencial na batalha para reduzir o custo total de propriedade.

McAfee System Protection Solutions

Várias Opções de Quarentena

Quando o spam é detectado, o McAfee SpamKiller o coloca em quarentena no servidor e marca as mensagens como spam antes de transferi-las à caixa de correio do usuário. Os administradores também têm a opção de usar o utilitário incorporado ou transferir o spam para pastas de lixo eletrônico especificadas na rede (por exemplo, as pastas pessoais de lixo eletrônico do usuário e áreas de quarentena do sistema).

Relatórios Detalhados e Gerenciamento Centralizado

Analise a detecção do spam

O McAfee SpamKiller for Microsoft Exchange será integrado ao McAfee ePolicy Orchestrator® para centralizar o gerenciamento e a emissão de relatórios. Os administradores procuram e avaliam as vulnerabilidades do sistema, mantêm atualizada a proteção, configuram e fiscalizam as políticas de proteção e geram relatórios gráficos detalhados.

Compatibilidade Total com o McAfee GroupShield for Microsoft Exchange

O McAfee SpamKiller for Microsoft Exchange é um complemento da tecnologia McAfee GroupShield® for Exchange existente, que proporciona proteção de primeira classe contra o spam em ambientes de computação colaborativa. Se for instalado no mesmo servidor que o McAfee SpamKiller e o GroupShield for Microsoft Exchange, ele poderá compartilhar o console de gerenciamento do ePolicy Orchestrator.

Anti-Phishing

O McAfee SpamKiller inclui regras específicas que ajudam a identificar os “phishing attacks” observando certas características específicas de phishing presentes em e-mail. Uma vez aplicadas, o Spamkiller atribui uma pontuação, que resulta em bloqueio na maioria dos casos. Em conjunto com o Anti-Phishing Working Group (APWG), a McAfee reuniu um considerável Banco de Dados de phishing attacks que é utilizado para criar regras efetivas de filtragem destes ataques.

Requisitos de Sistema

É importante notar que é possível instalar o McAfee SpamKiller em servidores Exchange que já executam um software antivírus.

- **Plataforma de e-mail** — Microsoft Exchange 2000 ou 2003 Server, ou Advanced Server
- **Sistema operacional** — Microsoft Windows 2000 ou 2003
- **Limite da caixa de correio** — Ilimitado
- **Espaço em disco** — 200MB de espaço livre no disco rígido ou mais
- **Memória** — 512MB de memória ou mais
- **Processador** — Pentium II de 400MHz ou mais veloz