Proteção inteligente: como combater ameaças por e-mail com o Zoho Mail

INTRODUÇÃO

Desde a comercialização da Internet em meados dos anos 1990, o e-mail tem sido uma das ferramentas de comunicação de maior confiança das empresas.

No entanto, ele também se tornou o vetor de ataque cibernético mais comum nos últimos anos. Os invasores aprimoram cada vez mais seu mecanismo de ataque para entregar spam, injetar malware e lançar ataques de phishing ou outras ameaças de e-mail de forma não detectada com a intenção de roubar, alterar ou destruir dados importantes e sistemas de informação.

De acordo com o SpamLaws, cerca de 14,5 bilhões de e-mails de spam são enviados diariamente. Isso representa 45% do tráfego de e-mails diário do mundo todo. Embora essa informação seja de consenso geral, algumas estatísticas de tráfego de spam sugerem que até 73% dos e-mails são promoções indesejadas ou maliciosos por natureza. Para uma empresa de pequeno a médio porte, isso significa receber milhares de e-mails de spam anualmente, com potenciais variáveis de perda financeira ou reputação.

Com este white paper, a Zoho pretende conscientizar a respeito das ameaças mais comuns de e-mails que as empresas enfrentam atualmente e ajudar você a se aprofundar nas ferramentas de defesa que o mecanismo de spam do Zoho Mail implanta para garantir a comunicação por e-mail e a continuidade dos negócios dos clientes.

INTRODUÇÃO ÀS AMEAÇAS DE E-MAIL

De acordo com o Internet Crime Complaint Center (IC3) do FBI, só em 2019, o crime cibernético gerou perdas no valor de US$ 3,5 bilhões, sendo o comprometimento de e-mails corporativos (BEC) o maior responsável pelos danos. Para proteger os negócios e os dados pessoais e corporativos, é essencial conhecer os tipos comuns de ameaças de e-mail. Isso pode ajudar a evitar vulnerabilidades e riscos associados tomando as medidas preventivas necessárias.

As oito ameaças de e-mail típicas que você precisa conhecer

Spam: E-mail comercial não solicitado, ou spam, é um lixo eletrônico não desejado enviado em massa. Normalmente, o spam tem fins comerciais ou publicitários, embora alguns invasores o utilizem para distribuir vírus e malware. As empresas-alvo podem esperar ver um alto fluxo de spam, o que prejudica a produtividade, gera violações de segurança, maiores gastos com largura de banda e armazenamento e com recuperação de desastres, além de outros problemas.

Phishing: Phishing é a prática de enviar comunicações fraudulentas, mais comumente direcionada a centenas ou milhares de destinatários por alguém se passando por uma instituição legítima, normalmente por e-mail. O objetivo é obter informações confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito, normalmente com intenções maliciosas. Um nível avançado dessa tática é chamado de “spear phishing”.

Spear phishing: Esta ameaça é altamente direcionada a indivíduos para roubar informações confidenciais como senhas, números de conta, IDs de usuário, códigos de acesso, PINs ou informações financeiras de uma vítima específica, normalmente com intenções maliciosas. Para adquirir esses detalhes, os invasores se disfarçam de um indivíduo, entidade, amigo ou conhecido de confiança, normalmente por e-mail ou outro sistema de mensagens on-line.

Malware: Software malicioso, comumente chamado de malware, é um software desenvolvido e distribuído como um script, normalmente para explorar o funcionamento normal de um dispositivo eletrônico. Um malware normalmente assume o controle do dispositivo e começa a excluir, corromper ou criptografar arquivos para pedir resgate.

Vírus: Os vírus são um tipo de programa de malware que pega carona no código de um aplicativo legítimo e se espalha a partir dele. Os vírus de software são carregados para o computador de um usuário sem o conhecimento dele e realiza ações maliciosas, destrói dados e reduz a velocidade dos recursos do sistema.

Ransomware: Ransom malware, ou ransomware, é um tipo de malware com apenas um objetivo: extorquir dinheiro das vítimas. Ele impede que os usuários acessem os próprios sistemas ou arquivos pessoais e exige resgate para devolver o acesso.

Engenharia social: É a arte de manipular as pessoas para que entreguem informações confidenciais. Esse ataque acontece em uma ou mais etapas, embora comece ganhando a confiança da vítima por telefone, e-mail ou até pessoalmente. Criminosos usam táticas de engenharia social porque costuma ser mais fácil se aproveitar da sua inclinação natural de confiar do que encontrar maneiras de invadir seu software.

Comprometimento de e-mails corporativos: Em ataques BEC, scammers imitam um funcionário da organização para defraudar a empresa, os funcionários, clientes ou parceiros. Os invasores miram nos funcionários que têm acesso aos dados financeiros ou confidenciais da empresa, enganando-os para que realizem transferências bancárias ou divulguem informações sensíveis. Isso começa com um e-mail, normalmente seguido por táticas de engenharia social e contas comprometidas, que não envolvem vírus, links ou anexos maliciosos, dificultando a detecção.

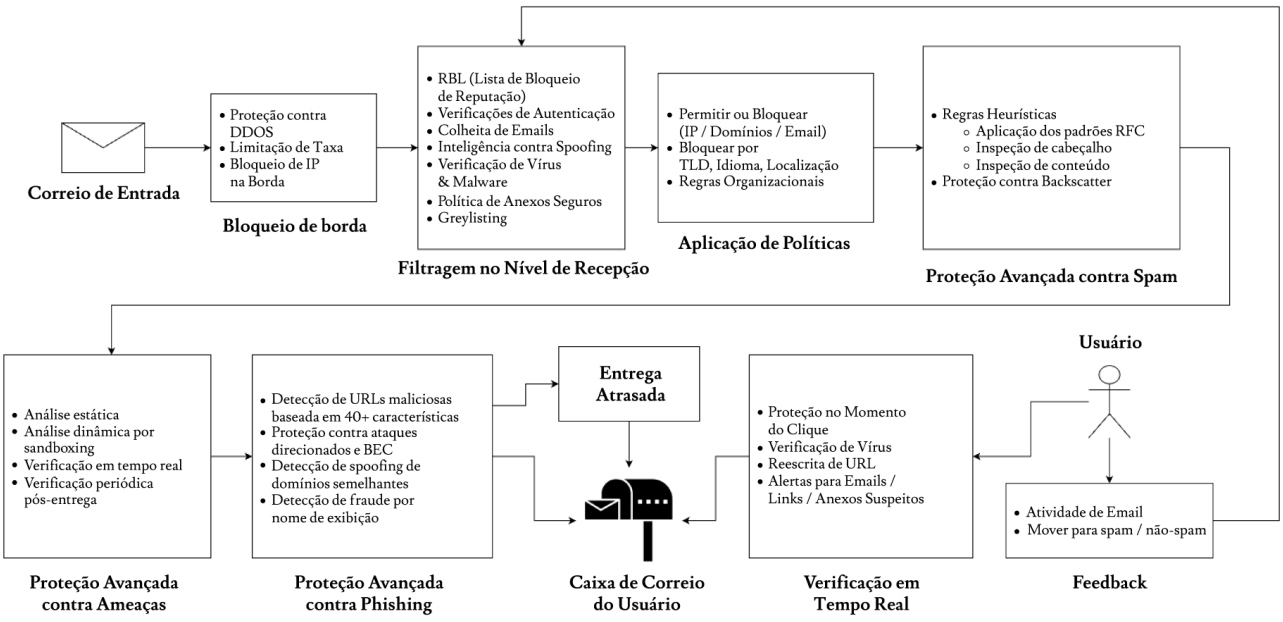
Essa crescente variedade de ameaças e a dinâmica dos ataques cibernéticos atuais exigem uma linha de frente de defesa sofisticada e adaptável para proteger sua organização de tais ameaças de e-mail.

AMPLA DEFESA DE E-MAILS DO ZOHO MAIL

O Zoho Mail conta com um mecanismo de várias camadas de proteção de e-mail e antispam criada para detectar e-mails indesejados e não solicitados e proteger as redes contra ameaças de e-mail. Nossa abordagem de proteção contra spams começa com a *proteção do perímetro/da edge* e vai até a *proteção contra spam no momento do clique* na caixa de entrada do usuário, garantindo que sua organização não apenas se mantenha produtiva, mas também protegida contra ameaças vindas de e-mails.

Resiliência cibernética para e-mails – abordagem do Zoho Mail para a segurança de e-mails

O Zoho Mail oferece uma proteção robusta e simples de gerenciar contra spam, combinando as melhores tecnologias para eliminação de spam em um único sistema coeso e intuitivo. Ele combina análise de conexão, reputação local e global e técnicas avançadas de análise de conteúdo e estatística que inspecionam todos os e-mails enviados e recebidos para proteger os usuários de diversas ameaças cibernéticas.



FILTRAGEM NO NÍVEL DA CONEXÃO

A. Bloqueio da edge

- **Proteção de negação de serviço distribuída (DDOS)**

Um ataque de DDoS é um tipo de ameaça de DoS em que vários sistemas sequestrados são usados para sobrecarregar recursos do sistema ou larguras de banda da rede. Elas podem deixar o serviço de e-mail indisponível, interrompendo a acessibilidade do e-mail. O Zoho Mail atua como sua primeira camada de defesa contra essas ameaças, recebendo todos os e-mails que entram e garantindo que as ameaças nunca cheguem ao parâmetro da sua rede.

- **Limitação de taxa**

O software de spam automatizado costuma ser usado para enviar e-mails em massa a um único servidor. Para proteger a infraestrutura contra inundação de e-mails, nosso mecanismo de spam restringe e-mails recebidos por um período depois que o limite de taxa é excedido. Ele também bloqueia qualquer nova tentativa de conexão de infratores conhecidos.

A limitação de taxa garante a disponibilidade do serviço sem que a caixa de entrada do usuário seja inundada por spams.

- **Bloqueio de IP da edge**

Em seguida, compara endereços IP de e-mails recebidos com as listas de infratores conhecidos, como:

- Bloqueio de IP dinâmico
  A lista de bloqueio de IP dinâmico é uma lista pública de endereços IP ou intervalos de endereços ou endereços IP maliciosos. Em vez de bloquear a conta do usuário, o mecanismo de spam bloqueia o endereço IP de origem do e-mail malicioso ou tentativa de login malsucedida usando um nome de usuário diferente e senhas normalmente usadas por um período específico.
- Verificação da reputação de terceiros
  Os serviços de reputação de terceiros compila e gerencia listas de endereços IP desejáveis ou indesejáveis. O mecanismo de spam usa essas listas de bloqueio e serviços de reputação de terceiros como parte de seu sistema de proteção.

B. Filtragem no nível da recepção

Depois que os e-mails são recebidos para processamento, as verificações no nível da recepção seguintes são feitos para rejeitar, colocar em quarentena ou marcar e-mails espúrios.

- **Lista de bloqueio em tempo real**

A lista de bloqueio em tempo real (LBTR) SMTP é um mecanismo para publicar os endereços IP de spammers de SMTP. Você pode configurar o mecanismo de spam do Zoho Mail para utilizar servidores RBL para verificar os endereços IP de solicitações de entrada em relação a endereços IP conhecidos ou suspeitos de gerar spam.

Observação: a LBTR SMTP é uma técnica de filtragem de spam agressiva e pode mostrar resultados falso-positivos, pois é compatível com a atividade de spam relatada. Para evitar que e-mails de fontes confiáveis sejam bloqueados por LBTR, adicione-os a uma Lista de permissões.

- **Verificação de autenticidade**

A camada de autenticação do remetente usa muitos frameworks, como SPF e DKIM, ao mesmo tempo em que analisa e-mails com base na política DMARC para validar a autenticidade do remetente com verificações de protocolo padrão e analisar se há falsificação de nome de domínio ou outras técnicas de camuflagem. Os e-mails que reprovarem nessas verificações são classificados como spam ou e-mails falsificados e a ação adequada é acionada para isolá-los.

- **Inteligência de falsificação**
- Falsificação

  Quando algo ou alguém finge ser outra coisa na tentativa de ganhar nossa confiança, ter acesso a nossos sistemas, roubar dados ou dinheiro ou espalhar malware, chamamos isso de falsificação.

  Falsificação de domínio primo (domínio semelhante) e falsificação do nome de exibição são outras metodologias usadas por ferramentas de phishing para fazer parecer que uma mensagem veio de uma fonte confiável.

- **Verificação de vírus e malware**

O mecanismo de spam utiliza múltiplas camadas para verificação de vírus e descompacta arquivos automaticamente para uma proteção abrangente. A verificação de vírus precede qualquer outra técnica de verificação disponível e é aplicada mesmo se o e-mail passar por qualquer outra camada de conexão. Isso significa que, mesmo se um e-mail vier de endereços IP ou domínios “permitidos” ou “confiáveis”, os e-mails ainda serão verificados e bloqueados caso sejam detectados vírus.

- **Graylist**

Caso o sistema receba e-mails de spam de IPs com uma reputação muito ruim, ele automaticamente colocará o endereço IP na graylist, reduzindo a quantidade de spams recebidos.

C. Aplicação de políticas

- **Com base em IPs**

Com o mecanismo de spam do Zoho Mail, os administradores podem definir uma lista de servidores de e-mail confiáveis pelo endereço IP e, assim, evitar a verificação de spam de e-mails legítimos. Da mesma forma, eles também podem segregar e organizar uma lista de remetentes de e-mails fraudulentos para bloqueá-los. Em alguns casos, os administradores podem preferir utilizar o intervalo de bloqueios de IP para limitar servidores de e-mail específicos por uma questão de política, e não por uma questão de proteção contra spam.

- **Com base em domínios, TLDs e e-mails**

- Lista de Bloqueio
  Ela permite filtrar endereços e domínios de remetentes de quem você não quer receber e-mails.

- Lista de Permissões
  Ao aprovar os remetentes, você permite automaticamente mensagens de servidores ou endereços de e-mail confiáveis. Mensagens de remetentes ou domínios aprovados não passam pela verificação de spam ou reputação da fonte. No entanto, as mensagens desta lista ainda passam pela verificação de vírus.

- Listas confiáveis
  E-mails de endereços adicionados à lista de e-mails confiáveis são entregues na caixa de e-mail sem verificação de spam. Esses e-mails não serão validados com as verificações da lista de bloqueio/SPF/DKIM.

- **Com base na localização e no idioma**

Algumas organizações esperam nunca se comunicar com países ou idiomas específicos dos quais recebem muito spam. Portanto, usam filtros baseados no país ou no idioma (ou os dois), uma técnica que bloqueia e-mails de determinados países ou idiomas. Dessa forma, você pode identificar e bloquear e-mails de spam de acordo com o país de origem.

D. Proteção avançada contra ameaças

- **Detecção de URL com phishing**

Este módulo de detecção verifica se e-mails recebidos possuem hyperlinks mal-intencionados. Ele possibilita a verificação em tempo real de links, incluindo links para baixar conteúdo.

- **Colheita de credenciais**

Campanhas de e-mail maliciosas usam credenciais recolhidas (combinação de nome de usuário e senha) para explorar a conta de e-mail do usuário ou outras contas para outros fins mal-intencionados.

- **Política de segurança de anexos**

A Política de segurança de anexos foi criada para proteger os usuários contra arquivos e anexos mal-intencionados. Alguns anexos que contêm arquivos de programas/executáveis podem ter programas destrutivos ou funções maliciosas que realizam phishing, spam ou outras atividades mal-intencionadas no sistema do usuário. Para evitar essas ameaças à segurança, e-mails com determinados tipos de arquivo anexos são bloqueados no Zoho Mail.

E. Análise de impressão digital de spam

- **Identificação de spam**
- **Análise de intenção**
  Todo e-mail de spam é enviado com a “intenção” de receber uma resposta, uma chamada ou um acesso ao site. Com a análise de intenção, identificamos as intenções por trás da sequência de e-mails recebidos e detectamos se tratarem de spam. Geralmente, a análise de intenção age como uma camada de defesa que captura ataques de phishing.

- **Análise de conteúdo**
  O mecanismo de spam do Zoho Mail permite que os administradores definam filtros de conteúdo personalizados com base na linha de assunto, cabeçalhos e corpos das mensagens e conteúdo do arquivo anexo. Em geral, os administradores não precisam definir seus próprios filtros para bloquear spam, já que mecanismos de análise abrangentes são pré-configurados e constantemente atualizados no mecanismo de spam do Zoho Mail para enfrentar situações de

spam de forma inteligente. Isso permite que o DLP mantenha visibilidade e controle completos, principalmente no caso de e-mails enviados.

- **Outra análise**

  Baseada em tag HTML: E-mails com formulário, incorporação, iframe ou tag de objeto potencialmente prejudicial também podem cair na categoria de spam, se marcados.

  Filtros de anexo: O recurso de filtro de anexo pode rejeitar ou colocar em quarentena e-mails com base na extensão do arquivo anexado. Se algum deles corresponder, o e-mail será diretamente rejeitado ou marcado como spam.

  Bloquear anexos com macros: Determinados macros maliciosos em anexos podem ser executados quando são abertos. Você pode escolher bloquear anexos com macros.

- **Proteção contra Backscatter**

Backscatter ocorre quando um spammer envia e-mails com spam ou vírus usando um endereço de e-mail falso na linha “De:” ou como caminho de retorno de suas mensagens. Isso a leva a milhares de notificações de e-mails com erro de entrega ou autoresponders na sua caixa de e-mail. Para combater o backscatter, a Zoho garante que somente notificações de status de entrega e autoresponders legítimos cheguem às suas contas.

- **Aplicação de padrões de RFC**

Muitos spammers usam softwares mal escritos ou não conseguem atender aos padrões porque não têm controle legítimo do computador que estão usando para enviar spam. Ao definir limites rígidos ao desvio dos padrões de RFC, a Zoho possibilita que você reduza significativamente a quantidade de spams recebidos.

- **Pontuação de spam**

Depois que uma mensagem recebida passar pelos filtros iniciais de aceite/bloqueio do mecanismo de spam do Zoho Mail, ela receberá uma pontuação indicando a probabilidade de que tenha spams. De acordo com essa pontuação, o mecanismo de spam do Zoho Mail pode tomar uma das seguintes medidas:

- Bloquear
- Quarentena

- Permitir (somente e-mail recebido)

- **Quarentena**

O mecanismo de spam coloca e-mails com spam em quarentena automaticamente, garantindo que sua caixa de entrada esteja livre de qualquer tipo de ameaça. Esses e-mails em quarentena são retidos por 60 dias e depois eliminados. Os administradores podem visualizar o cabeçalho do e-mail para verificar e recuperar e-mails legítimos colocados em quarentena.

F. Proteção a e-mails enviados

- **Proteção no nível do usuário**
- **Autenticação do usuário**
  Para eliminar o risco de logins suspeitos ou falsificação, o mecanismo de spam do Zoho Mail pode ser configurado para realizar autenticação SMTP, gerando confiança na troca de e-mails do cliente com ele mesmo. Isso evita que spammers enviem e-mails como se fossem um usuário.

- **Verificações de reputação e lista de bloqueio**
  Embora a reputação do IP seja importante, as reputações do domínio e remetente do e-mail são fatores significativos quando se trata de capacidade de entrega. Quanto maior a pontuação, maior a probabilidade de um provedor de serviços de e-mail (ESP) entregar e-mails às caixas de entrada de destinatários em sua rede. Se a pontuação ficar abaixo de determinado limite, o ESP pode enviar as mensagens às pastas de spam dos destinatários ou até mesmo rejeitá-las de imediato. Portanto, são incorporados vários mecanismos para validar a reputação do remetente.

- **Limitação de taxa**
  Para evitar que cheguem e-mails de spam em massa, a limitação inteligente de taxas é aplicada nos e-mails enviados. Por exemplo, se um usuário atingir o limite de envio em um período, ele será automaticamente impedido de enviar mais e-mails até que a contagem volte a estar abaixo do limite.

- **Proteção de conteúdo**

- **Análise de intenção e conteúdo**
  A filtragem de conteúdo personalizado com base no assunto, nos cabeçalhos, no corpo do e-mail e no tipo de arquivo anexo pode ser aplicada a e-mails enviados da mesma forma que para e-mails recebidos. Isso também inclui validação de URL, verificação de vírus e de phishing, detecção de e-mails de spam e e-mails solicitando informações confidenciais e correspondência de padrão, entre outros, para evitar vazamento de dados e garantir a conformidade.

- **Pontuação de spam**
  Da mesma forma que acontece com os e-mails recebidos, também são atribuídas pontuações aos e-mails enviados para definir se eles serão enviados ou bloqueados.

- **Quarentena de envios**
  Colocar e-mails enviados em quarentena significa que existe a suspeita de que a mensagem seja um spam ou que viole a política, e será armazenada para o administrador analisar e tomar medidas.

- **Capacidade de entrega**
- **Maior capacidade de entrega** (com base na reputação do IP do remetente)
  A entrega do e-mail está diretamente relacionada à reputação do IP do remetente. Se você tiver vários endereços IP dedicados ou enviar vários tipos de e-mails, é recomendável separar seus IPs em grupos para gerenciar melhor sua reputação de envio. Volume consistente de e-mails, menos rejeições e reclamações, prevenção de armadilhas de spam, interações do usuário e taxas de assinatura são alguns outros fatores que influenciam positivamente a reputação e a capacidade de entrega.

- **Limitação e restrição de taxas**
  Embora a limitação de taxas seja aplicada para garantir que seus servidores de e-mail não sejam usados indevidamente para spams, a restrição armazena e-mails de forma inteligente com base na capacidade de entrega do servidor de e-mail do destinatário, garantindo capacidade de entrega ideal.

G. Alertas do momento de clique

Os alertas do momento de clique são uma notificação por e-mail automática enviada com base em determinada categoria de remetentes, como os não autenticados ou fora da lista de contatos e remetentes externos à organização, conforme definido pelo administrador. Eles também alertam os usuários de malware baseado em link e ataques de phishing, analisando a reputação de um URL no momento do clique dos usuários em seus endpoints.

H. Filtragem após a entrega

Enquanto a maioria dos provedores de gateway de e-mail seguros tendem a se concentrar em impedir que phishing, spear phishing e malware cheguem aos usuários finais, o mecanismo de spam do Zoho Mail oferece proteção após a entrega também, estendendo a defesa até mesmo para o momento do clique e depois.

CONCLUSÃO

A extensa proteção contra spam do Zoho Mail é sua melhor defesa contra ameaças de e-mail. Junto com seus sofisticados clientes de e-mail nativos e da web, oferece a melhor experiência de e-mail na nuvem do mercado, com proteção ao e-mail a nível empresarial.

Nosso software é extraordinariamente simples de configurar e gerenciar e conta com muitos recursos, incluindo 99,97% de detecção de spam, bloqueio de vírus e malware, controle de autenticidade, verificação de envios e estruturas sólidas de geração de relatórios.