1.Segurança de e-mails

Se você verificar sua pasta de spam agora, provavelmente encontrará algumas mensagens que parecem ter sido enviadas por um amigo ou membro da família, mas que claramente não vieram dessas pessoas. Isso acontece porque os protocolos que usamos para enviar e receber e-mails não possuem muitas verificações de segurança embutidas. Para compensar essa falta de segurança nos protocolos originais, foram adicionadas camadas extras de proteção para garantir alguma forma de autenticação e verificação dos e-mails.

É surpreendente quantos e-mails na pasta de spam são **spoofed**, ou seja, o nome do remetente mostrado na mensagem não é a pessoa real que enviou o e-mail. Esse é um problema sério não apenas para indivíduos, mas também para empresas e outras organizações, que precisam garantir que as mensagens que recebem são realmente legítimas e vieram da fonte correta.

Por exemplo, você pode receber um e-mail que parece ter sido enviado por mim, com o endereço **james@professormesser.com**, mas como saber se essa mensagem realmente veio do meu servidor de e-mail? Felizmente, existem verificações de segurança que podemos adicionar aos **servidores DNS** para confirmar se um e-mail foi enviado por um servidor legítimo.

O primeiro elemento necessário para validar um e-mail é um **gateway de e-mail**, que funciona como um filtro para todas as mensagens recebidas pela organização. Esse gateway verifica cada mensagem antes que ela seja entregue à caixa de entrada do usuário. Se o e-mail for legítimo, ele será encaminhado para o destinatário. Se não for, ele pode ser descartado ou enviado para a pasta de spam. Algumas empresas usam gateways de e-mail internos, configurando-os dentro de uma sub-rede protegida, enquanto outras preferem utilizar serviços baseados na nuvem que oferecem essa filtragem.

Se você é responsável pelo gerenciamento de e-mails dentro de um domínio, precisa configurar um registro chamado **Sender Policy Framework (SPF)** no seu servidor DNS. **O SPF é um protocolo que define quais servidores de e-mail estão autorizados a enviar mensagens em nome do seu domínio**. Esse registro é adicionado ao DNS como um **TXT record** e pode ser consultado publicamente.

Quando um servidor de e-mail recebe uma mensagem enviada do meu endereço, ele consulta meu servidor DNS para verificar a lista de servidores autorizados a enviar e-mails em nome de **professormesser.com**. Se o servidor que enviou a mensagem estiver na lista de permissões, o e-mail será aceito. Caso contrário, ele poderá ser marcado como suspeito ou rejeitado.

Por exemplo, no meu **registro SPF**, o servidor **mailgun.org** está autorizado a enviar e-mails em nome do meu domínio. Se um servidor de terceiros verificar o

cabeçalho da mensagem e identificar que ela foi enviada pelo **mailgun.org**, ele pode confiar que o e-mail é legítimo. Se a mensagem tiver sido enviada por um servidor diferente, ela pode ser sinalizada como suspeita.

A adição desse registro é bastante simples em um painel de controle de DNS. Basta criar um novo **TXT record**, inserir o conteúdo correspondente e salvar a alteração. No meu caso, eu especifico que **mailgun.org** pode enviar e-mails para o domínio **professormesser.com**.

Além do SPF, é possível adicionar uma camada extra de verificação usando **assinaturas digitais** com o protocolo **DKIM (Domain Keys Identified Mail)**. **O DKIM permite que o servidor de e-mail assine digitalmente todas as mensagens enviadas, garantindo sua autenticidade**.

Essa assinatura digital não é visível no corpo do e-mail; ela faz parte dos cabeçalhos do protocolo de transporte entre os servidores de e-mail. O servidor que recebe a mensagem pode verificar essa assinatura consultando o **registro DKIM** armazenado no DNS do remetente. Esse registro contém a **chave pública** usada para validar a assinatura.

Se um servidor recebe um e-mail supostamente vindo de mim, ele pode consultar meu servidor DNS, obter a chave pública e utilizá-la para verificar a assinatura digital no cabeçalho do e-mail. Se a assinatura for válida, a mensagem pode ser considerada confiável. Caso contrário, pode ser um e-mail forjado.

O registro DKIM é adicionado ao DNS da mesma maneira que o SPF, como um **TXT record** contendo a chave pública do domínio. Ao salvar essa informação no DNS, qualquer servidor que receba um e-mail meu pode validar se ele foi realmente enviado a partir de um servidor autorizado.

Após configurar SPF e DKIM, ainda há uma questão pendente: o que fazer com os e-mails que falham nesses testes de autenticação? Para definir essa política, adicionamos um terceiro registro no DNS chamado **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**.

O DMARC expande as funcionalidades do SPF e do DKIM, permitindo especificar regras sobre como os e-mails não autenticados devem ser tratados. Esse registro informa ao servidor destinatário se ele deve **aceitar, enviar para a pasta de spam ou rejeitar** mensagens que não passam na verificação.

As opções dentro do DMARC incluem:

- **Aceitar todos os e-mails**, independentemente da validação.
- **Enviar e-mails não autenticados para a pasta de spam**.
- **Rejeitar automaticamente e-mails que falhem na autenticação**.

Se um servidor recebe uma mensagem e não consegue validá-la por SPF ou DKIM, ele pode consultar o registro DMARC para decidir o que fazer com o e-mail.

Outro benefício do DMARC é a capacidade de gerar **relatórios de conformidade**, que ajudam os administradores a monitorar a autenticidade dos e-mails enviados pelo domínio. Esses relatórios fornecem estatísticas detalhadas sobre quantos e-mails foram recebidos corretamente e quantos falharam na validação.

Com um serviço de relatórios DMARC configurado, o proprietário do domínio pode analisar quantos e-mails legítimos estão sendo entregues corretamente e quantos estão sendo rejeitados por falhas na autenticação. Esse monitoramento ajuda a identificar possíveis ataques de spoofing e melhora a proteção contra fraudes por e-mail.

Assim, ao configurar corretamente **SPF, DKIM e DMARC**, é possível garantir que apenas servidores autorizados possam enviar e-mails em nome do seu domínio, reduzindo significativamente o risco de **phishing, spoofing e outras ameaças cibernéticas relacionadas a e-mails falsificados**.