O que é um registro de DNS DKIM?

Um registro DKIM é um registro de DNS TXT especializado que armazena a chave pública usada para verificar a autenticidade de um e-mail.

Registros DNS

Copiar o link do artigo

O que é DKIM?

DomainKeys Identified Mail (DKIM) é um método de autenticação de e-mail que ajuda a evitar que spammers e outras partes maliciosas se façam passar por um domínio legítimo.

Todos os endereços de e-mail têm um domínio, a parte do endereço depois do símbolo "@". Spammers e invasores podem tentar imitar um domínio ao enviar e-mails para realizar ataques de phishing ou outros golpes.

Suponha que Chuck queira enganar Alice, que trabalha no site example.com, para que lhe envie informações confidenciais da empresa. Ele poderia enviar a ela um e-mail que parece ter sido enviado por "bob@example.com" para fazê-la pensar que ele também trabalha para o site example.com.

O DKIM, juntamente com o Sender Policy Framework (SPF) e o Domain-based Message Authentication Reporting and Conformance (DMARC), tornam muito mais difícil para os invasores se fazerem passar pelos domínios dessa forma. Os e-mails que não forem aprovados pelo DKIM e pelo SPF são marcados como "spam" ou não são entregues pelos servidores de e-mail. Se o site example.com possui DKIM, SPF e DMARC configurados para seu domínio, então provavelmente Alice nunca verá o e-mail malicioso de Chuck porque ele irá para sua pasta de spam ou será totalmente rejeitado pelo servidor de e-mail.

Como funciona o DKIM?

O DKIM é composto por dois elementos principais: o registro DKIM, que é armazenado nos registros do Domain Name System (DNS) para o domínio, e o cabeçalho DKIM, que é anexado a todos os e-mails do domínio.

O DKIM usa esquemas de assinatura digital baseados em criptografia de chave pública para autenticar a origem de um e-mail e confirmar que este realmente é de de um servidor que envia e-mails daquele domínio. Para isso, utiliza-se um par de chaves criptográficas: uma chave privada para o remetente assinar as mensagens e uma chave pública para o receptor verificar as assinaturas. Um receptor não pode usar a chave pública para assinar mensagens, e vice-versa.

O provedor de e-mail gera a chave pública e a chave privada. Eles dão a chave pública ao proprietário do domínio, que armazena a chave pública em um registro de DNS disponível publicamente: o registro DKIM.

Todos os e-mails enviados desse domínio incluem um cabeçalho DKIM, que contém uma seção de dados assinada com a chave privada: a isso dá-se o nome de "assinatura digital". Um servidor de e-mail pode verificar o registro de DNS DKIM, obter a chave pública e usá-la para verificar a assinatura digital.

Esse processo também garante que o e-mail não foi alterado durante o trânsito. A assinatura digital não será verificada se os cabeçalhos dos e-mails ou o corpo do e-mail forem alterados: é como um selo à prova de adulteração em um recipiente de medicamentos.

O que é um registro DKIM?

Um registro DKIM armazena a chave pública DKIM que é uma string de caracteres aleatória usada para verificar qualquer coisa assinada com a chave privada. Os servidores de e-mail consultam os registros de DNS do domínio para ver o registro DKIM e visualizar a chave pública.

Um registro DKIM é na verdade um registro de DNS TXT ("texto") . Os registros TXT podem ser usados para armazenar qualquer texto que um administrador de domínio deseje associar ao seu domínio. O DKIM é um dos muitos usos desse tipo de registro de DNS.

Aqui está um exemplo de um registro de DNS TXT DKIM:

Nome	Tipo	Conteúdo	TTL
`big-email._domainkey.example.com`	`TXT`	`v=DKIM1; p=76E629F05F70 9EF665853333 EEC3F5ADE69A 2362BECE4065`	`6000`

		8267AB2FC3CB 6CBE	

Nome

Ao contrário da maioria dos registros de DNS TXT, os registros DKIM são armazenados com um nome especializado, não apenas com o nome do domínio. Os nomes dos registros DKIM seguem este formato:

`[seletor]._domainkey.[domínio]`

O `seletor` é um valor especializado emitido pelo provedor de serviços de e-mail utilizado pelo domínio. Ele está incluído no cabeçalho DKIM para permitir que um servidor de e-mail realize a pesquisa de DKIM necessária no DNS. O `domínio` é o nome do domínio de e-mail. `._domainkey.` está incluído em todos os nomes de registro DKIM.

Para pesquisar o registro DKIM, os servidores de e-mail utilizam o seletor DKIM fornecido pelo provedor de serviços de e-mail e não apenas o nome do domínio. Suponha que o site

example.com utilize o Big Email como seu provedor de serviços de e-mail, e suponha que o Big Email utilize o seletor DKIM `big-email`. A maioria dos registros de DNS do site example.com seria nomeada `example.com`, mas seu registro de DNS DKIM estaria com o nome `big-email._domainkey.example.com`, que está listado no exemplo acima.

Conteúdo

Essa é a parte do registro de DNS DKIM que lista a chave pública. No exemplo acima, `v=DKIM1` indica que esse registro TXT deve ser interpretado como DKIM, e a chave pública é tudo que vem depois de `p=`.

Tipo de registro e TTL

Trata-se de campos padrão dos registros de DNS. `TXT` indica que este é um registro de DNS TXT. "TTL" significa "tempo até entrar no ar" (medido em segundos), e indica quanto tempo este registro deve ser considerado válido antes de precisar ser atualizado. Os registros DKIM geralmente têm uma TTL de vários minutos.

O que é um cabeçalho DKIM? Como funciona uma assinatura DKIM?

O servidor de envio de e-mails cria sua assinatura digital usando cabeçalhos de e-mail, o corpo do e-mail (na verdade um hash do corpo do e-mail: leia mais abaixo), e sua chave privada. Essa assinatura digital é anexada ao e-mail como parte do cabeçalho DKIM.

O cabeçalho DKIM é um dos muitos cabeçalhos anexados a um e-mail. A maioria dos aplicativos de e-mail não mostra o cabeçalho ao exibir um e-mail, a menos que o usuário selecione determinadas opções. No Gmail, por exemplo, os usuários podem visualizar o cabeçalho de um e-mail clicando nos três pontos verticais no canto superior direito do e-mail, e depois clicando em "Mostrar original."

Aqui está um exemplo de um cabeçalho DKIM:

```
v=1; a=rsa-sha256;
        d=example.com; s=big-email;
        h=from:to:subject;
      bh=uMixy0BsCqhbru4fqPZQdeZY5Pq865sNAnOAxNgUS0s=;
  b=LiIvJeRyqMo0gngiCygwpiKphJjYezb5kXBKCNj8DqRVcCk7obK6OUg4o+EufEbB
tRYQfQhgIkx5m70IqA6dP+DBZUcsJyS9C+vm2xRK7qyHi2hUFpYS5pkeiNVoQk/Wk4w
ZG4tu/g+OA49mS7VX+64FXr79MPwOMRRmJ3lNwJU=
```

- v= mostra qual versão do DKIM está sendo usada.

- d= é o nome de domínio do remetente.

- s= é o seletor que o servidor receptor deve usar para consultar o registro de DNS.

- h= lista os campos de cabeçalho usados para criar a assinatura digital, ou b. Nesse caso, são usados os cabeçalhos "de", "para" e "assunto". Se Bob enviou um e-mail para Alice usando o domínio example.com e a linha de assunto era "Receita de cheesecake", o conteúdo usado aqui seria "bob@example.com" + "alice@example.com" + "Receita de cheesecake". (Esse conteúdo também seria "canonizado", isto é, colocado em um formato padronizado).

- bh= é o hash do corpo do e-mail. Um hash é o resultado de uma função matemática especializada chamada função hash. Essa informação é incluída para que o servidor de e-mail receptor possa calcular a assinatura antes que todo o corpo do e-mail seja carregado, já que os corpos dos e-mails podem ter qualquer comprimento e o carregamento, em alguns casos, pode demorar muito tempo.

- a= é o algoritmo usado para calcular a assinatura digital, ou b, bem como gerar o hash do corpo do e-mail, ou bh. Nesse exemplo, está sendo utilizado o RSA-SHA-256 (RSA usando

SHA-256 como a função hash para a assinatura digital, e SHA-256 para o hash do corpo).

- b= é a **assinatura digital**, gerada a partir de h e de bh e assinada com a chave privada.

A assinatura digital (b=) permite ao servidor receptor 1. autenticar o servidor remetente e 2. assegurar a integridade, ou seja, que o e-mail não foi adulterado.

O servidor receptor faz isso usando o mesmo conteúdo listado em h= mais o hash do corpo (bh=) e usando a chave pública do registro DKIM para verificar se a assinatura digital é válida. Caso a chave privada correta tenha sido utilizada e caso o conteúdo (cabeçalhos e corpo) não tenha sido alterado, o e-mail é aprovado na verificação do DKIM.

Qual a relação entre o DKIM e o DMARC?

DMARC é um método de autenticação de e-mail baseado no DKIM e no SPF. O DMARC descreve o que fazer com um e-mail reprovado pelo SPF e pelo DKIM. Juntos, SPF, DKIM e DMARC ajudam a evitar spams e falsificação de e-mails. Da mesma forma que nos registros DKIM, as políticas DMARC são armazenadas como registros de DNS TXT.

A Cloudflare oferece um Assistente de Segurança de DNS para E-mail que permite que os usuários configurem rapidamente os registros de DNS TXT de autenticação de e-mails, ajudando os administradores de domínios a impedir que partes maliciosas se façam passar por seus domínios.

Saiba mais sobre registros DNS para e-mail:

- Registro DNS SPF
- Registro DNS DMARC
- Registro DNS MX
- Registro DNS TXT

Para saber mais sobre o DKIM, veja RFC 6376.

CONTEÚDO RELACIONADO

Registro DNS DMARC

Registro DNS SPF

Registro DNS TXT

Registro DNS MX

O que é DNS?

Vendas

Vendas para empresas

Seja um parceiro

Contato de vendas:

+55 (11) 3230 4523

Sobre o DNS

Servidores de DNS

Registros DNS

Glossário de DNS

Navegação no Centro de Aprendizagem