O que é um registro de DNS DMARC?

O DMARC é uma parte importante da segurança de e-mails. As políticas DMARC são armazenadas nos registros de DNS TXT.

Registros DNS

Copiar o link do artigo

O que é DMARC?

O Domain-based Message Authentication Reporting and Conformance (DMARC) é um método de autenticação de mensagens de e-mail. Uma política DMARC diz a um servidor receptor de e-mails o que fazer depois de verificar a Sender Policy Framework (SPF)de um domínio e os registros DomainKeys Identified Mail (DKIM), que são métodos adicionais de autenticação de e-mails.

O DMARC e outros métodos de autenticação de e-mail são necessários para evitar a falsificação de e-mails. Cada endereço de e-mail possui um domínio, que é a parte do endereço que vem depois do símbolo "@". As partes maliciosas e os spammers às vezes tentam enviar e-mails de um domínio que eles não estão autorizados a usar, como alguém que escreve o endereço do remetente errado em uma carta. Eles podem fazer isso para tentar enganar os usuários (como em um ataque de phishing), entre outras razões.

Juntos, DMARC, DKIM e SPF funcionam como uma verificação de antecedentes dos remetentes de e-mail, para ter certeza de que eles realmente são quem dizem ser.

Por exemplo, imagine que um spammer envia um e-mail com o endereço "trustworthy@example.com", apesar de não estar autorizado a enviar um e-mail usando o domínio "example.com". O spammer faria isso substituindo o cabeçalho "De" do e-mail por "trustworthy@example.com". Eles não enviariam um e-mail do verdadeiro servidor de e-mail example.com. Os servidores de e-mail que recebem esse e-mail podem usar DMARC, SPF e DKIM para descobrir se é um e-mail não autorizado e podem marcar a mensagem de e-mail como spam ou se recusar a enviá-la.

O que é uma política DMARC?

Uma política DMARC determina o que acontece com um e-mail depois que ele é verificado com relação aos registros SPF e DKIM. Um e-mail tanto pode ser aprovado como reprovado pelo SPF e pelo DKIM. A política DMARC determina se a reprovação faz com que um e-mail seja marcado como spam, seja bloqueado ou seja entregue ao seu devido destinatário. (Os servidores de e-mail ainda podem marcar os e-mails como spam se não houver registro DMARC, mas o DMARC fornece instruções mais claras sobre quando fazer isso).

A política de domínio do site example.com poderia ser:

"Se um e-mail não for aprovado nos testes DKIM e SPF, marque-o como spam".

Essas políticas não são registradas como frases legíveis por seres humanos, mas sim como comandos legíveis por máquinas para que os serviços de e-mail possam interpretá-las automaticamente. Essa política DMARC na verdade seria mais ou menos assim:

```
v=DMARC1; p=quarentena; adkim=s; aspf=s;
```

O que isso significa?

- `v=DMARC1` indica que esse registro TXT contém uma política DMARC e deve ser interpretado como tal pelos servidores de e-mail.

- `p=quarentena` indica que os servidores de e-mail devem colocar os e-mails que não forem aprovados pelo DKIM e pelo SPF em "quarentena", considerando-os como provável spam. Outras configurações possíveis para isso incluem `p=nenhuma`, que permite que os e-mails reprovados ainda assim sejam aprovados, e `p=rejeitar`, que instrui os servidores de e-mail a bloquearem os e-mails reprovados.

- `adkim=s` significa que as verificações de DKIM são "rigorosas". Isso também pode ser ajustado para "relaxado" mudando o `s` para um `r`, como `adkim=r`.

- `aspf=s` é o mesmo que `adkim=s`, mas para o SPF.

- Note que `aspf` e `adkim` são configurações opcionais. O atributo `p=` é o que indica o que os servidores de e-mail devem fazer com e-mails que são reprovados pelo SPF e pelo DKIM.

Se o administrador do example.com quisesse tornar esta política ainda mais estrita e sinalizar mais fortemente aos servidores de e-mail para que considerem mensagens não autorizadas como spam, eles ajustariam o atributo "p=" da seguinte forma:

```
v=DMARC1; p=rejeitar; adkim=s; aspf=s;
```

Basicamente, isso diz: "Se um e-mail for reprovado nos testes DKIM e SPF, não o envie".

O que é um relatório DMARC?

As políticas DMARC podem conter instruções para enviar relatórios sobre e-mails que são aprovados ou reprovados pelo DKIM ou pelo SPF. Normalmente, os administradores definem relatórios a serem enviados a um serviço de terceiros que os reduz a uma forma mais digerível, para que os administradores não fiquem sobrecarregados com informações. Os relatórios DMARC são extremamente importantes porque eles dão aos administradores as informações necessárias para decidir como ajustar suas políticas DMARC, como por exemplo, se seus e-mails legítimos estão sendo reprovados pelo SPF e pelo DKIM ou se um spammer está tentando enviar e-mails ilegítimos.

O administrador do example.com acrescentaria a parte `rua` dessa política para enviar seus relatórios DMARC a um serviço de terceiros (com um endereço de e-mail "example@third-party-example.com"):

```
v=DMARC1; p=rejeitar; adkim=s; aspf=s; rua=mailto:example@third-party-example.co
```

O que é um registro DMARC?

Um registro DMARC armazena a política DMARC de um domínio. Os registros DMARC são armazenados no Domain Name System (DNS) como registros de DNS TXT. Um registro de DNS TXT pode conter quase qualquer texto que um administrador de domínio queira associar ao seu domínio. Uma das maneiras pelas quais os registros de DNS TXT são usados é para armazenar as políticas DMARC.

(Note que um registro DMARC é um registro de DNS TXT que contém uma política DMARC, não um tipo especializado de registro de DNS .)

A política DMARC do site example.com pode ficar assim:

Nome	Tipo	Conteúdo	TTL
`exemplo.com`	TXT	`v=DMARC1; p=quarentena; adkim=r; aspf=r; rua=mailto:example@third-party-example.com;`	32600

Nesse registro TXT, a política DMARC está contida no campo "Conteúdo".

E os domínios que não enviam e-mails?

Os domínios que não enviam e-mails ainda assim devem ter um registro DMARC a fim de

evitar que os spammers utilizem esse domínio. O registro DMARC deve ter uma política DMARC que rejeite todos os e-mails reprovados pelo SPF e pelo DKIM, que devem ser todos os e-mails enviados por aquele domínio.

Em outras palavras, se o site example.com não estivesse configurado para enviar e-mails, todos os e-mails seriam reprovados pelo SPF e pelo DKIM e seriam rejeitados.

O Assistente de Segurança de DNS para Email da Cloudflare simplifica a configuração dos registros de DNS TXT corretos e bloqueia a utilização de um domínio pelos spammers. Leia sobre isso aqui.

Saiba mais sobre registros DNS para e-mail:

- Registro DNS SPF
- Registro DNS DKIM
- Registro DNS MX
- Registro DNS TXT

O DMARC é descrito mais detalhadamente em RFC 7489.

CONTEÚDO RELACIONADO

Registro DNS DKIM

Registro DNS SPF

Registro DNS TXT

Registro DNS MX

Registros DNS