SMTP Reforçado
Mitigando Ataques Ativos e Passivos

nic.br cgi.br | registro.br

GTER 39
Rio de Janeiro, RJ | 29/05/15

Engenharia/Sistemas - Registro.br

Melhores práticas

Postgrey/Greylisting - recusa temporariamente a entrega caso o triplex IP de origem, “de” e “para” não sejam conhecidos. Elimina o ainda presente envio direto de e-mail (DirectDelivery).

Spamassassin + Amavis – plataforma anti-spam, utiliza análise heurística e estatística para classificar e bloquear e-mails. Amavis é um scanner de vírus.

DMARC - valida usando SPF e DKIM, além de propor um padrão para permitir com que haja cooperação e compartilhamento de informações (relatórios) entre os operadores dos serviços de e-mail. A política também é publicada no DNS.

> **SPF** - verifica se o host de origem está autorizado a enviar a mensagem, política publicada no DNS.
>
> **DKIM** - assina as mensagens, a chave pública é disponibilizada via DNS.

Opportunistic TLS encryption

Opportunistic SSL/TLS encryption

“Atualização” de um canal não seguro com uso de criptografia.

> Ex. STARTTLS, upgrade de uma conexão SMTP plain-text para TLS (na mesma porta).

Defesa contra ataques passivos (alguém interceptando/escutando o tráfego no meio do caminho).

O STARTTLS é vulnerável à ataques ativos, pois não é verificado nada do certificado, nem a cadeia e nem mesmo o CN.

Mitigação a ataques ativos possível em SMTP via *Opportunistic DANE TLS*, definido num draft em revisão final pelo IESG: draft-ietf-dane-smtp-with-dane

DANE

DNS-Based Authentication of Named Entities

Definido na RFC 6698, tem como premissas:
- Ser um contraponto ao modelo de CAs atual, enfatizando o “princípio do menor privilégio”
- Uso mandatório de DNSSEC para armazenar e assinar chaves e certificados TLS

DANE define um novo RR TLSA usado para associar um certificado TLS ou uma chave pública ao nome de domínio onde o resource record está armazenado

Benefícios:
- segurança contra certificados TLS/SSL falsos ou forjados,
- conexão criptografada **e autenticada** entre servidores,
- não é necessário revogar certificados (basta substituir o record TLSA),
- previne ataques do tipo man-in-the-middle,
- proteção contra ataques de downgrade STARTTLS e
- controle passa para o operador do DNS, não é necessário um CA como intermediário.

DANE x Modelo de CAs

Modelo atual de CAs:

- Muitos “trust anchors” nem tão conhecidos e confiáveis
- Qualquer CA podem emitir certificados para qualquer nome de domínio

DANE:

- Chaves são associadas a nomes no DNS ao invés de strings arbitrárias
- Chaves são distribuídas pelo próprio DNS
- Uma chave só pode ser assinada pelo parent domain

DANE ainda permite que sejam indicadas quais CAs são utilizadas para um nome de domínio

DANE – RR TLSA

Exemplo de record TLSA (ISC Bind – TLSA >= 9.9.1-P3):

```
_25._tcp.eng.registro.br. 171455 IN TLSA 3 1 1 (

19FD6F0C6663789D83A4289AC2432C882CCCCBEDFE4A
                        69839CCB15C6906F5F2B )
```

```
$ printf '_25._tcp.%s. IN TLSA 3 1 1 %s\n' $(uname -n) \
  $(openssl x509 -in eng.registro.br.crt -noout -pubkey | \
  openssl pkey -pubin -outform DER | openssl dgst -sha256 -binary
| \
  hexdump -ve '/1 "%02x"')
```

DANE – RR TLSA

O TLSA possui as seguintes informações:

Usage: especifica qual o tipo de certificado será usado na comparação:

0 - usado para especificar que o TLSA armazena um certificado (ou chave pública) de uma CA

1 - usado para especificar que o TLSA armazena um certificado (ou chave pública) de uma entidade final

2 - usado para especificar que o TLSA armazena um certificado (ou chave pública) que deve ser usado como "trust anchor"

3 - usado para certificados "self-signed" (também conhecidos como "domain-issued certificate"). A diferença entre o usage 1 e 3 é que o 1 depende [de] que o certificado passe por toda [a] validação da cadeia, enquanto [que] no usage 3 esta validação não é feita.

DANE – RR TLSA

Selector: especifica qual parte do certificado TLS apresentado pelo servidor será usada para validação com o TLSA:

0 - Certificado completo
1 - Somente a chave pública

Matching Type: especifica como deverá ser feita a validação do certificado apresentado no handshake TLS com o conteúdo do TLSA

0 - comparação exata
1 - hash criptográfico SHA-256
2 - hash criptográfico SHA-512

Dados do certificado: pode conter o certificado completo ou somente a chave pública (depende do que está definido no campo 'selector'), ou o hash destas informações (depende do que está definido no matching type)

DANE e SMTP

O que é necessário?

- um servidor DNS recursivo com validação DNSSEC habilitado,
- zonas assinadas com DNSSEC,
- certificado TLS/SSL (pode ser auto-assinado) e
- MTA com suporte ao DANE

DANE e SMTP

Bind + DNSSEC validation (named.conf):

```
options {
 dnssec-validation auto;
 dnssec-lookaside auto;
};
```

O recursivo deve ser confiável, de preferência instalado no mesmo servidor do MTA.

DANE e SMTP

Postfix (>= 2.11.0) + DANE (main.cf):

```
smtpd_use_tls = yes
smtp_dns_support_level = dnssec
smtp_tls_security_level = dane
```

DANE e SMTP

```
% dig +m +dnssec tlsa _25._tcp.eng.registro.br

[...]
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17119
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 12
[...]
;; ANSWER SECTION:
_25._tcp.eng.registro.br. 171455 IN TLSA 3 1 1 (
                        19FD6F0C6663789D83A4289AC2432C882CCCCBEDFE4A
                        69839CCB15C6906F5F2B )
_25._tcp.eng.registro.br. 171455 IN RRSIG TLSA 5 5 172800 (
                        20150803104337 20150525104337 54964 registro.br.
                        u7HXmVXkgH/q11bxSkPLmf0yHlMNhMG1ReUPrVetUIUm
                        oZvhVn7d+86lCZgCnqAmutVIP5t1Kpek756pbjc6Ihbz
                        Uf2F/p3rc7cp+gTUtziiRk1WvYuwaS/awioIxwMMyAUp
                        ngf79c5QUuyI2yIlt75fJ4SgX9Ix6O8nBdH/nXkFUL3z
                        EsBdLM+5pwjQ8QOF )
```

DANE e SMTP

TLS connection - Opportunistic :

May 24 16:04:28 eng postfix/smtp[18343]: Untrusted TLS connection established to aspmx.l.google.com[64.233.186.27]:25: TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits)

TLS connection + DANE, ex 1:

May 24 16:04:46 eng postfix/smtp[18359]: Verified TLS connection established to mail.nic.br[200.160.4.5]:25: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)

TLS connection + DANE, ex 2:

May 29 14:28:33 mail postfix/smtp[9107]: Untrusted TLS connection established to fake-mta[192.0.2.1]:25: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)

May 29 14:28:33 mail postfix/smtp[9107]: F3CCB806DF: to=<test@fake-mta>,relay=fake-mta[192.0.2.1]:25, delay=0.08, delays=0.02/0.01/0.05/0, dsn=4.7.5,**status=deferred (Server certificate not trusted)**

Validando o record TLSA publicado e testando o MTA: **https://dane.sys4.de**

DANE e TLSA no Registro.br

Configuração utilizando os servidores DNS do Registro.br

A inserção de resource records TLSA é feita por meio da tela de edição de zona DNS.

Lá é possível inserir um record TLSA manualmente ou deixar que o próprio sistema insira automaticamente os records baseado na configuração de sua zona.

Opções disponíveis:

- manual
- automática

DANE e TLSA no Registro.br

Configuração automática

• estará disponível sempre que existirem records do tipo A, AAAA e MX;

• cada record MX encontrado iniciará uma busca por um certificado via SMTP no servidor informado no record;

• cada record A ou AAAA iniciará uma busca por um certificado via HTTPS no domínio informado no record;

• cada record A ou AAAA no APEX da zona iniciará uma busca por um certificado tanto via HTTPS quanto via SMTP, ainda que não haja nenhum record MX para o APEX;

• para cada certificado encontrado, será inserido automaticamente um record TLSA na configuração da zona como um record novo.

Obrigado

registro.br

dev@registro.br sistemas@registro.br

29 de Maio de 2015

nic.br cgi.br

www.nic.br | www.cgi.br