RECOMENDAÇÃO TÉCNICA 01/21

STARTTLS E DANE

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

PÚBLICO-ALVO

TEMPO DE LEITURA

DIFICULDADE

Este documento descreve a importância e recomenda a utilização dos padrões STARTTLS e DANE para uma maior segurança ao nível da transferência de correio eletrónico (SMTP) entre organizações.

Classificação	Data	Versão do Documento
TLP: WHITE	30/12/2021	1.0

Título
Recomendação Técnica do Centro Nacional de Cibersegurança: STARTTLS e DANE

Histórico de Versões			
Versão	Data	Revisor	Comentários/Notas
1.0	30/12/2021	CNCS	Versão inicial do documento

ÍNDICE

Lista de abreviaturas

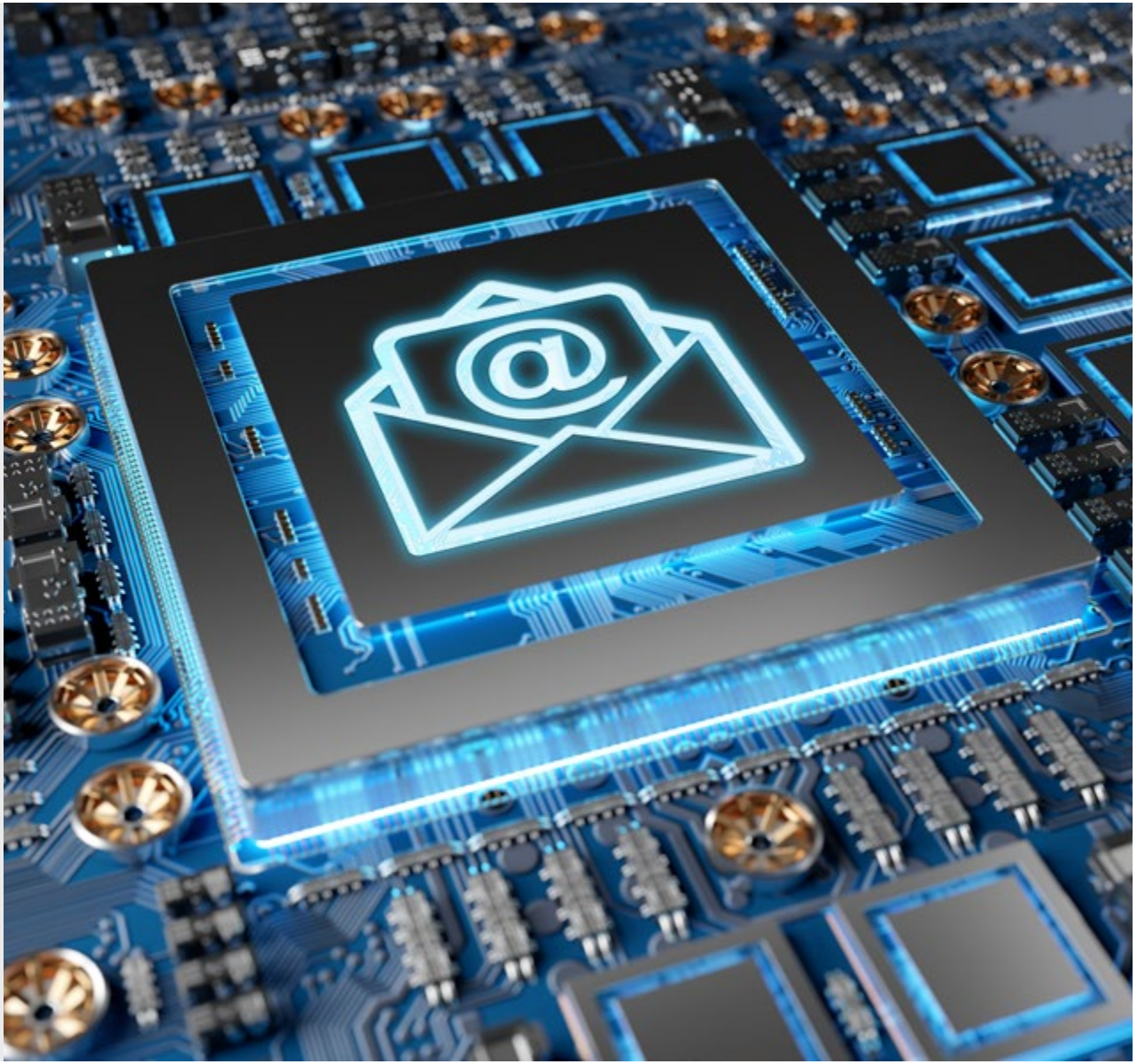
CA	*Certificate Authority*
CNCS	*Centro Nacional de Cibersegurança*
DANE	*DNS-Based Authentication of Named Entities*
DNS	*Domain Name System*
FQDN	*Fully Qualified Domain Name*
SMTP	*Simple Mail Transfer Protocol*
SAN	*Subject Alternate Name*
TLS	*Transport Layer Security*

Introdução

A segurança associada à **transmissão de mensagens de correio eletrónico** tem sido uma questão muitas vezes subvalorizada na configuração dos sistemas de *e-mail*. Por omissão, ou seja, sem uma configuração precisa e expressa, as mensagens de correio eletrónico são transmitidas através da Internet sob a forma de texto legível, permitindo a sua interceção ou a sua manipulação por parte de um atacante.

O Centro Nacional de Cibersegurança (CNCS) tem vindo a promover e incentivar a utilização de um conjunto de padrões, protocolos e boas práticas com o objetivo de reforçar os níveis de segurança associados ao correio eletrónico das organizações, quer através da disponibilização da ferramenta **Webcheck.PT** (que permite realizar uma avaliação da conformidade com estas boas práticas), como pela disponibilização de guias e recomendações técnicas para a implementação de alguns desses padrões, tais como o SPF, DKIM ou o DMARC.

Neste sentido, o CNCS recomenda a utilização de STARTTLS e DANE (preferencialmente em conjunto), como forma de dificultar a interceção ou manipulação de tráfego de correio eletrónico. O presente documento descreve a importância destes instrumentos no incremento da segurança na transmissão de correio eletrónico.



A importância da utilização de STARTTLS e DANE

STARTTLS consiste numa extensão para o protocolo SMTP (*Simple Mail Transfer Protocol*) que permite que dois servidores de correio eletrónico possam utilizar o protocolo TLS (*Transport Layer Security*) para a troca de uma mensagem através de uma comunicação privada e autenticada pela Internet. Um servidor de destino pode assim indicar que oferece suporte TLS e, de seguida, o servidor de envio utiliza o comando STARTTLS para assinalar que deseja utilizar essa opção.

Ao contrário dos navegadores de internet (*browsers*), os servidores de correio eletrónico comunicam entre si sem envolvimento humano e, em contraste com a utilização de HTTPS, o uso de TLS permanece opcional. Um servidor pode solicitar uma atualização (*upgrade*) para a utilização de TLS, mas a cifra da ligação só ocorre se ambos os servidores oferecerem suporte ao protocolo.

A utilização de STARTTLS por servidores de correio eletrónico oferece um grau de proteção limitado uma vez que se torna eficaz contra os denominados atacantes passivos (que conseguem intercetar o conteúdo da comunicação mas não modificá-lo) mas não contra um atacante ativo, que consiga modificar o tráfego e desabilitar a utilização de STARTTLS. Caso um atacante ativo tenha a capacidade de conduzir um ataque *man in the middle*, este pode bloquear o sinal de atualização (*upgrade*) que os servidores utilizam para indicar o suporte para STARTTLS e, se o sinal não for recebido, a troca de e-mail ocorrerá sem a utilização de cifra, sendo esta interferência denominada de um ataque de *downgrade* ou STRIPTLS (que resulta no envio da mensagem utilizando o protocolo original, ou seja, em formato legível). Um ataque *man in the middle* também pode consistir na interceção de mensagens de correio eletrónico através de um certificado TLS falso.

É nesse sentido que surge a importância da **utilização em conjunto de STARTTLS e DANE**.

O protocolo DANE permite a indicação, de forma verificável, que o(s) servidor(es) de correio eletrónico[1] da sua organização disponibilizam e têm preferência pelo estabelecimento de uma ligação segura (cifrada através de STARTTLS) com qualquer outro servidor de correio eletrónico que também o suporte. Esta indicação é efetuada através da publicação de informações sobre os certificados de servidor de correio eletrónico num registo de DNS especial, denominado TLSA. Adicionalmente, e também por intermédio deste registo, os servidores de envio podem verificar a autenticidade do(s) certificado(s) associado(s) ao(s) servidor(es) de destino, para além da utilização de uma autoridade de certificação (CA).

A utilização de DANE por parte de um servidor de envio e de destino previne, deste modo, a execução de um ataque de *downgrade* ou STRIPTLS, uma vez que o atacante teria de comprovar a autenticidade do seu certificado para desabilitar a utilização de STARTTLS

1 A utilização de DANE não se restringe ao âmbito do correio eletrónico, podendo aplicar-se também, com sucesso, às ligações a páginas de internet (HTTPS) e protocolos de comunicação por instant messaging (XMPP, por exemplo).

Recomendações Gerais

1. O CNCS recomenda a ativação/configuração de STARTTLS e DANE para todo o tráfego de entrada de correio eletrónico na sua organização. Deste modo, qualquer organização pode comunicar de uma forma mais segura com os seus servidores de correio eletrónico.
2. O CNCS recomenda ainda habilitar STARTTLS e DANE para todo o tráfego de correio eletrónico dirigido ao exterior da sua organização.
3. A segurança assegurada pelo DNSSEC é um dos pilares para uma eficaz implementação de DANE. Por esse motivo, deve garantir que o seu domínio primário e domínio dos servidores de correio eletrónico suportam DNSSEC, antes de implementar DANE.
4. A correta implementação dos padrões mencionados nesta recomendação técnica, bem como de um conjunto de outros standards, configurações e boas práticas, pode ser avaliada, em tempo real, através da ferramenta **Webcheck.PT**.
5. Em **Webcheck.PT** poderá também encontrar guias de apoio à implementação de alguns padrões como, por exemplo, o DNSSEC.

STARTTLS e DANE na entrada de correio eletrónico

Dada a multiplicidade das soluções técnológicas existentes e envolvidas na implementação (plataformas de correio eletrónico, sistemas operativos, servidores de resolução de nomes, etc.) indicam-se de seguida alguns requisitos genéricos para a implementação de STARTTLS e DANE ao nível do tráfego de **entrada** de correio eletrónico. Para detalhes técnicos mais específicos sobre a implementação poderá consultar os guias referidos na secção "Referênciais e guias de implementação".

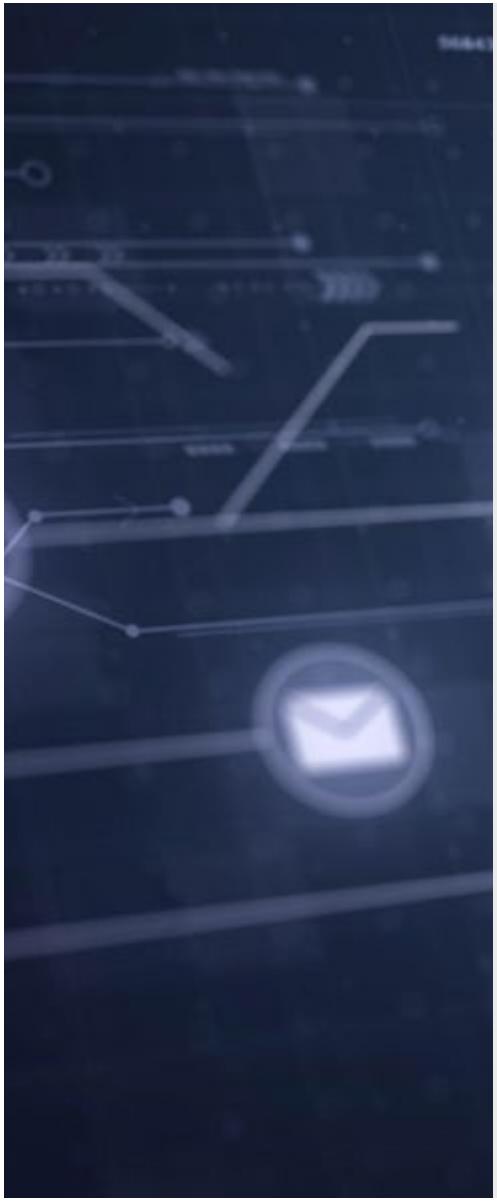
- Comece por realizar um levantamento exaustivo dos servidores de correio eletrónico através dos quais a sua organização **recebe *e-mail*.** Inclua nesse levantamento todos os servidores que possam receber *e-mail* a partir de outros servidores externos (estes podem incluir servidores que não se encontram sob seu controlo como, por exemplo, servidores de um serviço de filtragem antispam). Deve incluir todos os servidores que se encontram definidos ao nível do(s) registo(s) MX do(s) domínios da sua organização;
- Considere a configuração de STARTTLS com base numa autoridade de certificação (CA) pública ou por intermédio de uma autoridade de certificação própria. Apenas opte pela utilização da sua própria CA caso possua o conhecimento e os meios técnicos necessários para configurá-la e mantê-la;
- Certifique-se de que é gerado um **certificado para cada servidor de correio eletrónico**, e que este inclui o *Fully Qualified Domain Name* (FQDN) do servidor no campo *Subject Alternative Name* (SAN);
- **Ative o STARTTLS em todos os servidores de correio eletrónico** da sua lista e configure-o de acordo com as melhores práticas de segurança (evite, por exemplo, a utilização de versões de TLS inseguras e cifras obsoletas);
- Utilize o certificado criado para o servidor de correio eletrónico e configure-o de forma a que seja enviada toda a cadeia de certificados, até e incluindo a CA;
- **Verifique se o servidor se encontra acessível via STARTTLS**. Para tal pode, por exemplo, utilizar uma ferramenta de verificação de conformidade como o **Webcheck.PT**. Caso não obtenha acesso, verifique por eventuais bloqueios ou parametrizações para a remoção de STARTTLS de todo o tráfego de *e-mail* de entrada, ao nível dos dispositivos de proteção perímetral (*firewall*);
- Para cada servidor de correio eletrónico, publique informações sobre o certificado e a CA nos **registos TLSA da zona de DNS do servidor**. Por exemplo, se o servidor de correio eletrónico *mail.teste.pt* é responsável pelo *e-mail* do domínio *teste.org*, deve definir os registos TLSA ao nível da zona de DNS *teste.pt*;
- Certifique-se de que a zona de DNS do domínio de correio eletrónico bem como a que contém o registo TLSA se encontram configuradas com DNSSEC. Este protocolo garante que os servidores de envio de correio eletrónico serão capazes de verificar a autenticidade das informações definidas ao nível dos registos TLSA;
- Verifique regularmente se as respetivas configurações de DNSSEC, STARTTLS e DANE se encontram corretas e funcionais, recorrendo, por exemplo, à ferramenta **Webcheck.PT**;
- STARTTLS e DANE podem também ser utilizados para conferir maior segurança aos fluxos internos de correio eletrónico da organização.

STARTTLS e DANE na saída de correio eletrónico

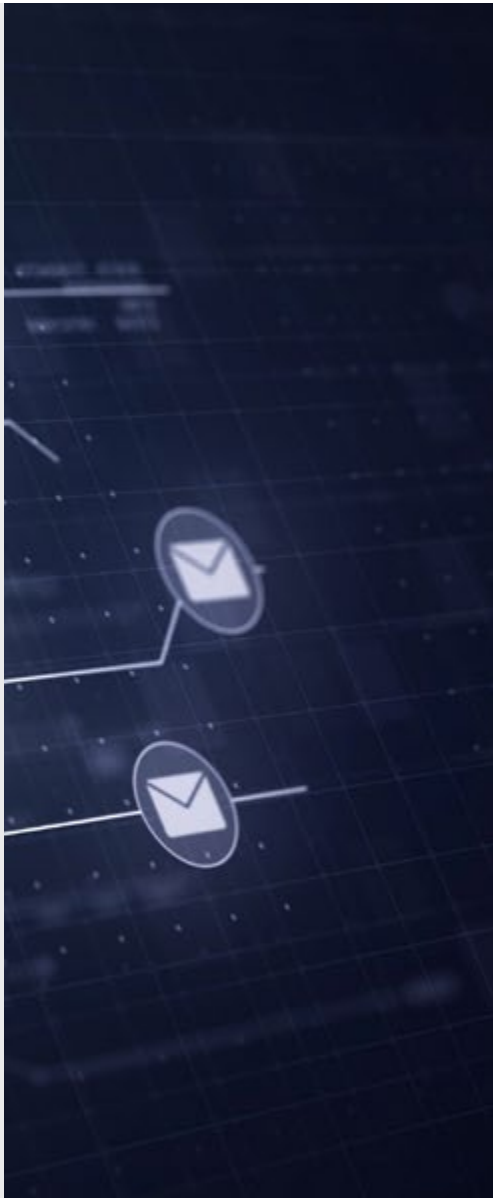
Referem-se também de seguida alguns requisitos genéricos para a implementação de STARTTLS e DANE ao nível do tráfego de saída de correio eletrónico. Para detalhes técnicos mais específicos sobre a implementação poderá consultar os guias referidos na secção “Referênciais e guias de implementação”:

- Comece por realizar um levantamento dos servidores de correio eletrónico através dos quais a sua organização **envia *e-mail*.** Inclua nesse levantamento todos os servidores que possam enviar *e-mail* para outros servidores externos;
- Para cada servidor que conste da lista, determine se a respetiva solução (*software*) de correio eletrónico suporta DANE e STARTTLS para a saída de *e-email*. Consulte a documentação do seu servidor de correio eletrónico ou peça mais informações ao fornecedor da solução ou eventual parceiro responsável pela implementação;
- Se um servidor de correio eletrónico suportar DANE e STARTTLS, habilite-os;
- Caso disponível, utilize a opção de realizar apenas a validação DANE quando os registos TLSA se encontram configurados. Esta opção é normalmente denominada de *oportunistic DANE validation*;
- Certifique-se de que o servidor de correio eletrónico se encontra configurado para utilizar um servidor de DNS recursivo para a validação de DNSSEC;
- Se um servidor de correio eletrónico suportar STARTTLS mas não suportar DANE, este servidor não pode proteger automaticamente as ligações com servidores de *e-mail* externos. Comece por questionar o fornecedor da solução de correio eletrónico sobre quando será adicionado o suporte para DANE. Como solução temporária, poderá configurar um novo servidor de correio eletrónico que funcionará como um *relay* para este servidor. Neste *relay*, utilize uma solução que suporte STARTTLS e DANE;

Em resumo



- A proteção do tráfego de correio eletrónico recorrendo a DANE e STARTTLS deve ser efetuada tanto ao nível do *e-mail* de entrada como de saída. No entanto, tal não precisa de ser implementado ao mesmo tempo, privilegiando-se, por exemplo, a proteção de todo o tráfego de entrada com DANE e STARTTLS, e adiando a configuração ao nível do tráfego de saída para um momento posterior. Desta forma, garante desde logo a todos os seus contatos (que se encontrem também tecnicamente habilitados para tal) a existência de um mecanismo seguro para o envio de correio eletrónico para a sua organização;
- Só é útil proteger o tráfego de e-mail recebido para um domínio de correio eletrónico com DANE e STARTTLS se todos os servidores de e-mail de entrada desse domínio forem abrangidos. Caso contrário, um atacante ativo pode bloquear o acesso aos servidores de e-mail protegidos e, desse modo, forçar uma ligação não cifrada. Por outro lado, tal não se aplica da mesma forma para o tráfego de saída, uma vez que cada servidor de envio de correio eletrónico que se encontra protegido com DANE e STARTTLS consiste numa melhoria;
- De qualquer modo, habilite o STARTTLS para todo o seu tráfego de entrada e saída de correio eletrónico, mesmo que isso signifique um adiamento da implementação de DANE. Conforme referido, o STARTTLS é uma medida eficaz contra atacantes passivos;
- Monitorize a validade dos certificados de seus servidores de correio eletrónico e a exatidão dos registos TLSA (existem dois registos TLSA para cada servidor de correio eletrónico). A qualquer momento, um desses dois registos tem que ser válido para que o seu servidor de *e-mail* seja acessível, pelo que deve assegurar que consegue detetar antecipadamente eventuais problemas antes que ambos os registos TLSA deixem de ser válidos.



Referênciais e guias de implementação

DANE for SMTP how-to (Internet.NL)

DANE for SMTP Implementation resources

RFC 3207: SMTP Service Extension for Secure SMTP over Transport Layer Security [STARTTLS]

RFC 7672: SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)

RFC 7671: The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance