RT01/19

Recomendação Técnica 01/19

SPF, DKIM e DMARC

Este documento descreve a importância e recomenda a utlização dos standards SPF, DKIM e DMARC para reforço da segurança do correio eletrónico das organizações

CNCS

Classificação	Data	Versão do documento
TLP: WHITE	14/06/2019	1.0

Título
Recomendação Técnica do Centro Nacional de Cibersegurança: SPF, DKIM e DMARC

Histórico de Versões			
Versão	**Data**	**Revisor**	**Comentários/Notas**
1.0	14/06/2019	CNCS	Versão inicial do documento

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Índice

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Lista de abreviaturas

AFRF	*Authentication Failure Reporting Format*
DKIM	*DomainKeys Identified Mail*
DMARC	*Domain-based Message Authentication, Reporting and Conformance*
DNS	*Domain name system* – Sistema de nomes de domínio
IETF	*Internet Engineering Task Force*
MTA	*Mail Transfer Agent* – Agente de transporte de correio eletrónico
SPAM	Correio eletrónico não-solicitado
SPF	*Sender Policy Framework*

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Introdução

O serviço de correio eletrónico continua a ser um dos serviços internet mais utilizados nos contextos de uso pessoal, institucional e empresarial. No entanto, o mesmo foi concebido numa lógica de garantia da entrega das mensagens (disponibilidade), mas sem as preocupações de segurança quer com a integridade do conteúdo, quer com a autenticidade do envelope (autenticidade do remetente).

De facto, o serviço de correio eletrónico é utilizado de forma abusiva diariamente, seja para envio massivo de mensagens não solicitadas, vulgo SPAM, seja para envio de mensagens com remetente forjado. Se a primeira técnica se caracteriza por uma elevada intensidade e baixo impacto, a segunda é comummente utilizada em esquemas de furto de identidade, burla informática e ciberespionagem.

Para fazer face a estes e outros problemas, a indústria, através do *Internet Engineering Task Force* (IETF), tem vindo a promover a adoção de um conjunto de instrumentos com vista a melhorar a segurança do popular serviço de correio eletrónico, de entre os quais se destacam o ***Sender Policy Framework*** **(SPF)**, o ***DomaimKeys Identified Mail*** **(DKIM)** e o ***Domain-based Message Authentication, Reporting and Conformance*** **(DMARC)**.

Tendo em conta a arquitetura distribuída da internet, o sucesso destas iniciativas não depende apenas do Utilizador, mas das respetivas taxas de adoção e do exemplo fornecido quer pela indústria, quer pelos estados. Neste contexto interessa relevar que de entre os domínios internet mais importantes, a taxa de adoção destas técnicas é superior a 70%, onde se incluem os gigantes Google, Microsoft ou a Yahoo. Em Portugal, o SPF em particular foi operacionalizado no final da década passada quer na rede académica, quer na rede escolar.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Desta feita, o Centro Nacional de Cibersegurança (CNCS) recomenda a adoção dos standards SPF, DKIM e DMARC a todas as organizações públicas e privadas com presença na internet.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Sender Policy Framework (SPF)

O ***Sender Policy Framework* (SPF)** foi adotado pelo IETF pela primeira vez em Abril de 2006[1], apresentando hoje em dia uma taxa de adoção de cerca de 70%, entre os domínios mais visitados[2].

SPF designa uma *framework* de validação do canal de envio de correio eletrónico, baseada na utilização do serviço de nomes de domínio (DNS) para publicação dos endereços IP dos servidores autorizados a enviar correio eletrónico para o respetivo domínio. O seguinte registo de DNS representa, a título exemplificativo, a autorização específica ao *Mail Transfer Agent* (MTA) com o endereço *mail.example.com* para envio de mensagens oriundas do domínio example.com:

```
example.com.  TXT  "v=spf1 a:mail.example.com -all"
```

Cada registo SPF consiste num registo de DNS do tipo "TXT" na raiz de um domínio ou subdomínio que começa com "v=spf1". A partir daqui, são utilizados parâmetros para descrever os servidores de correio eletrónico autorizados (ou não autorizados) a enviar correio eletrónico em nome desse domínio ou subdomínio. Um domínio ou subdomínio pode possuir apenas um registo SPF, mas cada subdomínio pode ter o seu próprio registo SPF.

O servidor de destino (também conhecido por *Mail Transfer Agent* – MTA – de destino) valida a origem da mensagem recebida, mais precisamente o respetivo campo "*return-path*", com a informação publicada no DNS e aplica uma política de tratamento de mensagens que resulta na aceitação, rejeição ou colocação em quarentena dessa mensagem.

[1] Ver RFC 7708 Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, disponível em https://tools.ietf.org/html/rfc7208, consultado em Junho de 2019.
[2] Ver *SPF Usage Statistics*, disponível em https://trends.builtwith.com/mx/SPF, consultado em Junho de 2019.

Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Porque o SPF verifica o campo "*return-path*" e não o campo "*from*", um remetente mal-intencionado consegue, ainda assim, manipular o envelope da mensagem e iludir o destinatário da mensagem. Note-se que o utilizador comum observa o campo "*from*" e não o "*return-path*". Esta falha é colmatada com utilização de DMARC, em complemento ao SPF.

Componentes de um registo SPF

Um registo SPF consiste no número de versão seguido de um conjunto de parâmetros, denominados de (i) mecanismos e (ii) qualificadores. Os processos de validação ignoram registos que não começam pela indicação da versão "v=spf1 …".

Os registos SPF podem definir zero ou mais mecanismos, que são utilizados para descrever o conjunto de servidores autorizados para o envio de correio eletrónico em nome desse domínio. De seguida indicam-se os mecanismos mais comummente utilizados num registo SPF:

```
all | ip4 | ip6 | a | mx | ptr | exists | include
```

Todos os mecanismos, ou cada um individualmente, podem ser combinados com um de quatro qualificadores. Os qualificadores determinam como os MTA devem lidar com a respetiva correspondência.

Qualificador	Descrição
+	***Pass*** = O endereço passou o teste; Aceitar a mensagem. Exemplo: "v=spf1 +all"
-	***(Hard) Fail*** = O endereço falhou o teste; Recusar qualquer mensagem que não cumpra esta validação. Exemplo: "v=spf1 -all"

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

~	***Soft Fail*** = O endereço falhou o teste, mas o resultado não é definitivo; Aceitar e marcar qualquer mensagem que não se encontre em conformidade. Exemplo: "v=spf1 ~all"
?	***Neutral*** = O endereço não passou nem falhou o teste; Deixa à decisão do destinatário o que fazer com a mensagem (provavelmente aceitar). Exemplo: "v=spf1 ?all"

Se o registo SPF não incluir um qualificador, assume-se o seguinte: "+".

SPF - Recomendações CNCS

1. Todas as organizações com presença na internet devem adotar o standard SPF ao nível da configuração do seu domínio de correio eletrónico;

2. Ao realizar as configurações iniciais do SPF, pode optar por um qualificador neutro ("?all") de modo a avaliar a aplicação da respetiva política;

3. Após saber com exatidão quais os endereços IP dos servidores de correio eletrónico que enviam legitimamente em nome do seu domínio, atualize o registo SPF de acordo com essa informação e assuma um qualificador mais restritivo ("-all");

4. Caso seja responsável pela gestão de domínios a partir dos quais não é enviado correio eletrónico, recomenda-se a configuração do seguinte registo SPF (que indica explicitamente que nenhum MTA se encontra autorizado a enviar correio eletrónico em nome desse domínio) em cada um deles:

v=spf1 -all

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

DomainKeys Identified Mail (DKIM)

O ***DomainKeys Identified Mail*** **(DKIM)** foi promovido pela Yahoo, junto do IETF, pela primeira vez em 2007[3], contando hoje com a participação dos principais prestadores de serviços de correio eletrónico.

O DKIM disponibiliza um método para validação de uma identidade digital associada a uma mensagem (tipicamente o domínio do remetente). O objetivo é o não repúdio da atribuição da mensagem, conseguido através da aposição de uma assinatura criptográfica a cada mensagem enviada. Ou seja, o DKIM apenas atribui a responsabilidade do envio de uma mensagem a uma identidade digital.

Uma assinatura DKIM por si só não aumenta ou diminui a reputação de uma mensagem. No entanto a assinatura aposta à mensagem é um dado importante para os sistemas de avaliação de reputação e para a tomada de decisão sobre uma mensagem em particular.

Assim, numa perspetiva prática, é tão importante operacionalizar a assinatura DKIM das mensagens enviadas, como adaptar os mecanismos de receção de correio eletrónico com a integração da validação DKIM na aferição da reputação das mensagens recebidas.

Operacionalização do DKIM

O DKIM utiliza criptografia de chave pública, o que significa que existe uma chave privada que apenas o assinante da mensagem conhece, e uma chave pública que

[3] Ver RFC 6376 DomainKeys Identified Mail (DKIM) Signatures, disponível em https://www.ietf.org/rfc/rfc6376.txt, consultado em Junho de 2019. Para uma melhor informação sobre a arquitetura do DKIM, ver RFC 5585 DKIM Service overview, disponível em http://dkim.org/specs/rfc5585.html, consultado em Junho de 2019.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

todos conhecem e pode ser utilizada para verificar a mensagem. O assinante da mensagem de correio eletrónico (que pode ser diferente do remetente) cria o *hash* e o destinatário da mensagem pode verificar esse mesmo *hash* utilizado a chave pública, que deve ser publicada no serviço DNS do respetivo domínio (identidade digital).

Através do sítio na internet dkim.org poderá encontrar informação mais detalhada sobre a implementação deste *standard*, que pode variar consoante o MTA e/ou sistema operativo utilizado.

DKIM - Recomendações CNCS

1. Todas as organizações com presença na internet devem adotar o standard DKIM ao nível da configuração do seu domínio de correio eletrónico;

2. A segurança e confidencialidade da chave privada é essencial. Assim sendo, esta deve ser protegida utilizando os métodos padrão (limitações de acesso através do sistema operativo, cifra de discos, etc.);

3. Recomenda-se a utilização de uma chave com um mínimo de 2048 bits. Note-se, no entanto, que as chaves de grande dimensão (normalmente acima de 4096 bits) podem, potencialmente, causar problemas ao nível de DNS.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Domain-based Message Authentication, Reporting and Conformance (DMARC)

O ***Domain-based Message Authentication, Reporting and Conformance*** **(DMARC)**, adotado pelo IETF em Março de 2015[4], veio complementar o SPF e o DKIM, acrescentando-lhe uma camada de controlo que permite a cooperação e partilha de informação entre remetentes e destinatários com vista a melhorar a validação da autenticidade de mensagens de correio eletrónico.

O DMARC habilita o remetente a declarar ao destinatário a utilização de SPF e/ou DKIM, bem como o que este deve fazer com uma mensagem que falha a validação de qualquer um dos métodos declarados. Por outro lado, verifica o "alinhamento" entre o endereço apresentado no campo "*from"* e o MTA verificado através do SPF.

Esta funcionalidade permite ao destinatário da mensagem a aplicação da política de tratamento das mensagens recebidas em conformidade com a declaração feita pelo remetente.

Como funciona o DMARC

Em termos gerais, o processo de validação do DMARC funciona da seguinte forma:

1. Um administrador de domínio publica a política que define as suas práticas de autenticação de correio eletrónico e de que forma é que o recetor da mensagem deve lidar com mensagens que violem essa política. Esta política de DMARC é definida através de um registo no serviço de DNS do domínio do remetente;

[4] Ver RFC 7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC), disponível em https://tools.ietf.org/html/rfc7489, consultado em Junho de 2019.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

2. Quando um servidor MTA recebe uma mensagem de correio eletrónico utiliza o DNS para pesquisar a política DMARC do domínio contido no cabeçalho "*From*" (RFC 5322) da mensagem. O MTA verifica então a mensagem através de três fatores principais:
    - A assinatura DKIM da mensagem é válida?
    - A mensagem veio de endereços IP permitidos pelos registos SPF do domínio de envio?
    - Os cabeçalhos da mensagem mostram o "alinhamento de domínio" adequado?
3. Através dessas informações, o MTA está pronto para aplicar a política DMARC do domínio de envio e decidir se aceita, rejeita ou, de outro modo, sinaliza a mensagem de correio eletrónico;
4. Depois de utilizar a política DMARC para determinar a disposição adequada da mensagem, o MTA poderá relatar o resultado ao responsável do domínio de envio.

Exemplo de um registo DMARC

Um registo DMARC deve ser definido ao nível do serviço de DNS da própria organização. Trata-se de uma versão particularmente formatada de um registo de DNS do tipo "TXT", com um nome de registo específico, nomeadamente "_dmarc.example.com" (de notar o prefixo "_"):

```
_dmarc.example.com. IN TXT "v=DMARC1\; p=none\;
rua=mailto:dmarc-aggregate@example.com\;
ruf=mailto:dmarc-afrf@example.com\; pct=100"
```

Analisando este exemplo específico, da esquerda para a direita:

- "v=DMARC1" define a versão de DMARC;

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

- "p=none" especifica o tratamento preferencial, ou a política de DMARC a aplicar;
- "rua=mailto:dmarc-aggregate@example.com" define a caixa de correio para onde os relatórios agregados devem ser enviados;
- "ruf=mailto:dmarc-afrf@example.com" define a caixa de correio para onde os relatórios forenses devem ser enviados;
- "pct=100" representa a percentagem de mensagens de correio eletrónico para a qual o responsável do domínio pretende ver a sua política aplicada.

As opções acima apresentadas representam o conjunto de parâmetros mais utilizados ao nível da definição da política de DMARC, no entanto encontram-se disponíveis mais opções de configuração.

Alinhamento do domínio através do DMARC

"Alinhamento do domínio" através do DMARC é um conceito que expande a avaliação de domínio efetuada intrinsecamente pelo SPF e DKIM. Desta forma, o DMARC compara o domínio de "*from*" de uma mensagem com informação relevante destes outros *standards*:

- No caso do SPF, o domínio definido no "*from*" da mensagem e o domínio presente no seu "*return-path*" devem corresponder (a manipulação do "*return-path*" é uma técnica muito utilizada ao nível das mensagens de phishing, de modo a forjar o remetente que é apresentado pelo cliente de correio eletrónico);
- No caso do DKIM, o domínio presente no "*from*" da mensagem e o domínio definido no campo "d= domain" da assinatura DKIM devem corresponder.

O alinhamento pode ser "*relaxed*" (correspondência entre domínio-base, mas permitindo diferentes subdomínios) ou "*strict*" (correspondência exata de todo o

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

domínio). Esta escolha é definida ao nível da política de DMARC estabelecida para o domínio originador da mensagem.

Refira-se ainda que o alinhamento com o DKIM é mais importante do que com o SPF porque só o DKIM permanece alinhado quando a mensagem é encaminhada (por exemplo, através de uma regra definida na caixa de correio do utilizador).

Políticas de DMARC

Ao nível da especificação do DMARC, são fornecidas três opções para os responsáveis por cada domínio definirem o tratamento preferencial a dar a uma mensagem de correio eletrónico que falhe nas verificações de validação do DMARC. Estas políticas ("*p=<policy>*") são:

- ***none***: tratar a mensagem da mesma forma que ocorreria sem qualquer validação do DMARC;
- ***quarantine***: aceitar a mensagem, mas colocá-la em outro lugar que não seja a caixa de entrada do destinatário (geralmente, a pasta de spam);
- ***reject***: rejeitar a mensagem imediatamente.

De notar que o responsável pelo domínio só pode solicitar, não forçar, a aplicação de seu registo DMARC. Cabe ao(s) MTA(s) de destino decidir se deve(m) ou não respeitar a política solicitada.

Relatórios DMARC

Os relatórios DMARC são gerados pelo(s) MTA(s) de entrada como parte do processo de validação do DMARC. Existem dois formatos de relatórios DMARC:

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

- **Agregado (*Aggregate report*)**, consistem em documentos XML que mostram dados estatísticos sobre as mensagens recebidas que reivindicam ser de um domínio específico. A informação inclui resultados de autenticação e disposição de mensagens. Os relatórios agregados foram projetados para serem legíveis por máquina;
- **Forense (*Forensic report*)**, são cópias individuais de mensagens que falharam a autenticação, cada uma incluída numa mensagem completa utilizando um formato especial denominado de AFRF. O relatório forense pode ser útil para solucionar problemas de autenticação de um domínio e para identificar domínios e sítios de internet mal-intencionados.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

DMARC - Recomendações CNCS

1. Todas as organizações com presença na internet devem adotar o *standard* DMARC ao nível da configuração do seu domínio de correio eletrónico;

2. Sendo os relatórios DMARC de difícil leitura, poderão ser utilizadas ferramentas (fornecidas por terceiras partes) agregadoras desses mesmos relatórios de modo a se conseguir obter uma leitura e análise mais eficaz dos resultados. Chama-se, no entanto, a atenção para o facto de essa operação implicar a partilha da informação constante nesses relatórios com a entidade fornecedora do serviço pelo que caberá a cada organização a respetiva avaliação das vantagens e inconvenientes dessa operação;

3. Existem variadas ferramentas web disponíveis que poderão auxiliar no processo de configuração de um registo DMARC. No entanto, e como medida de salvaguarda, sugere-se a utilização de valores não reais em substituição dos dados mais sensíveis (domínio, endereços de correio eletrónico, etc.);

4. Numa fase inicial de configuração do DMARC ao nível de um domínio, sugere-se a adoção de uma política "*p=none*". Na sequência disso, e após análise dos relatórios agregados entretanto recebidos bem como de eventuais afinações efetuadas ao nível da configuração de DKIM e SPF, deverá efetuar-se uma transição progressiva para uma política mais restritiva ("*p=quarantine*" e "*p=reject*").

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

Resumo

DKIM, SPF e DMARC são *standards* que endereçam questões complementares associadas à segurança e autenticação do correio eletrónico.

O SPF permite aos remetentes definirem que endereços IP se encontram autorizados a enviar correio eletrónico a partir de um determinado domínio.

O DKIM fornece uma chave de cifra e uma assinatura digital que permite verificar se uma mensagem de correio eletrónico não foi falsificada ou alterada.

O DMARC unifica os mecanismos de autenticação do SPF e do DKIM numa *framework* comum e permite aos responsáveis de cada domínio definirem de que forma é que uma mensagem de correio eletrónico desse domínio deve ser tratada caso falhe um teste de autorização.

Finalmente, sugere-se a seguinte sequência de passos para a implementação destes três *standards*:

1. Configurar MTA(s) de modo a garantir que estes validam corretamente os registos DMARC;
2. Configurar MTA(s) de modo a que estes consigam enviar relatórios agregados de DMARC;
3. Inventariar domínios;
4. Implementar SPF;
5. Implementar DKIM;
6. Configurar caixa(s) de correio para a receção dos relatórios DMARC;
7. Configurar o(s) registo(s) de DNS DMARC;
8. Analisar os relatórios DMARC recebidos;

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

9. Ajustar registo(s) SPF, assinatura(s) DKIM e política(s) de DMARC conforme necessário.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt