RECOMENDAÇÃO TÉCNICA 01/20

PROTEÇÃO DE DOMÍNIOS “ESTACIONADOS”/PARKED DOMAINS

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÚBLICO-ALVO

TEMPO DE LEITURA

DIFICULDADE

Este documento descreve um conjunto de boas práticas que devem ser adotadas com os domínios (e subdomínios) "estacionados" (também conhecidos como *parked domains*), e que não são utilizados para o envio de correio eletrónico.

Classificação	Data	Versão do Documento
TLP: WHITE	01/12/2020	1.0

Título
Recomendação Técnica do Centro Nacional de Cibersegurança: Proteção de Domínios "Estacionados" / *Parked Domains*

Histórico de Versões			
Versão	Data	Revisor	Comentários/Notas
1.0	01/12/2020	CNCS	Versão inicial do documento

ÍNDICE

Lista de abreviaturas 4

Introdução 5

Recomendações Gerais CNCS 6

Ações a tomar com os domínios “estacionados” 7

Registo SPF 7

Registo DMARC 7

Registo MX “Nulo” (NULL MX Record) 8

Registo DKIM Wildcard 8

LISTA DE ABREVIATURAS

DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain name system – Sistema de nomes de domínio
SPF	Sender Policy Framework

INTRODUÇÃO

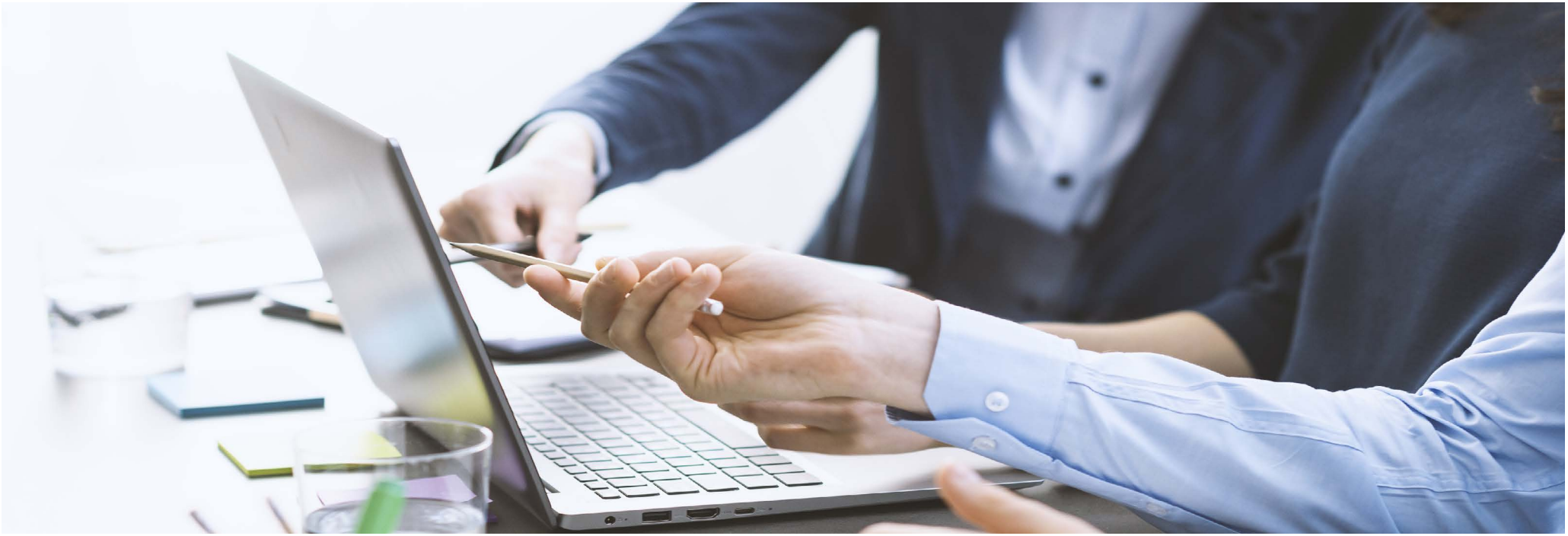
Um **domínio "estacionado"** (também conhecido como ***parked domain)*** consiste num **domínio que não se encontra associado ao envio de correio**. Podem também ser designados deste modo os domínios de internet unicamente utilizados no redireccionamento para um domínio principal / sítio de internet.

Muitas organizações e indivíduos registam domínios de internet sem intenção imediata de utilizá-los ou apenas com o objetivo de serem utilizados num contexto limitado, sem que aos mesmos seja associado o envio e receção de correio eletrónico. Por exemplo, um domínio pode ser registado para impedir que um agente malicioso adquira e abuse da utilização do mesmo (também conhecido como registo defensivo), no entanto, um mero registo de domínio com objetivos defensivos não significa que o mesmo se encontre protegido, podendo até ter o efeito indesejado de convencer as entidades com quem se relaciona de que uma mensagem de correio eletrónico enviada a partir desse domínio é genuína.

Nesse sentido, e **sem as devidas medidas de segurança**, os domínios "estacionados" **podem ser utilizados com relativa facilidade para forjar endereços de correio eletrónico** (*email spoofing*) **e no envio de mensagens de *phishing***, prejudicando a confiança na organização à qual se encontram associados.

Atualmente, os fornecedores de serviço de correio eletrónico *(email providers*) utilizam técnicas cada vez mais eficientes (onde se inclui a adoção e validação dos standards referidos na Recomendação Técnica 01/19) para autenticar as mensagens que lhes são destinadas. No entanto, e para que tais técnicas produzam os efeitos desejados, esses domínios devem ter a si associados um conjunto de identificadores.

Este documento visa descrever que identificadores devem ser utilizados para assinalar que um domínio ou subdomínio não se destina a enviar ou receber mensagens de correio eletrónico, contribuindo, deste modo, para prevenir a sua utilização abusiva.



RECOMENDAÇÕES GERAIS CNCS

Deve proteger os seus domínios “estacionados“ ao mesmo tempo que aplica proteções aos que enviam correio eletrónico (ver Recomendação Técnica 01/19), no entanto, recomenda-se que comece a aplicação de medidas com os domínios “estacionados”, uma vez que estes são mais fáceis de proteger e assim que se encontrem corretamente configurados não requerem manutenção adicional.

É recomendada a implementação das quatro ações que a seguir se indicam, no entanto, limitações inerentes a algumas interfaces de gestão ou sistemas podem não permitir que isso aconteça na totalidade. Deste modo, deverá ser aplicado o máximo de configurações possível.

AÇÕES A TOMAR COM DOMÍNIOS "ESTACIONADOS"

As seguintes quatro ações, baseadas na publicação de registos de nomes de domínio (DNS) específicos* - SPF, DKIM, DMARC e MX, informarão os destinatários que nenhuma mensagem de correio eletrónico deve ser originária do seu domínio "estacionado" e que, caso exista alguma, ela deve ser descartada. **As medidas apresentadas devem ser implementadas pela ordem referida.**

***Para melhor compreensão dos registos referidos deve ser consultada a Recomendação Técnica 01/19**

Registo SPF

Caso um domínio não seja utilizado para o envio de correio eletrónico deve ter associado um **registo de DNS** do **tipo SPF TXT**, conhecido como "naked" -all. Um exemplo desse registo é o seguinte:

exemplo.pt TXT "v=spf1 -all"

Este registo indica que nenhum endereço/servidor se encontra autorizado a enviar correio eletrónico em nome do domínio "exemplo.pt".

No caso dos subdomínios, a proteção destes poderá ser um pouco mais demorada uma vez que terá de ser criado um registo de DNS para cada potencial subdomínio que não necessite de enviar correio eletrónico.

Registo DMARC

Caso um domínio não seja utilizado para o envio de correio eletrónico deve ter associado um **registo de DNS** do **tipo DMARC TXT, que especifique "p=reject**", configurado da seguinte forma:

_dmarc.exemplo.pt TXT "v=DMARC1; p=reject; rua=mailto:rua@dominioativo.pt; ruf=mailto:ruf@dominioativo.pt"

A inclusão da *tag* "**rua**" é importante, pois permite que o proprietário do domínio receba relatórios agregados de possíveis abusos. A presença de uma tag "**ruf**" é opcional, mas recomendada. Como o domínio "exemplo.pt" não se encontra configurado para a receção de correio, as tags "rua" e "ruf" devem especificar um endereço pertencente a um domínio ativo de correio eletrónico.

Registo MX “Nulo” (*NULL MX Record*)

Caso possua um registo de DNS do tipo A e/ou AAAA (A/AAAA *record*) **associado ao seu domínio “estacionado” deverá criar um registo MX “Nulo”**. Caso este registo não se encontre definido, um servidor de envio poderá tentar enviar uma mensagem de correio eletrónico para o endereço IP especificado no registo A e/ou AAAA.

Deste modo, deverá ser criado um registo de DNS do tipo MX com uma prioridade de 0 (maior prioridade) e um *hostname* de “.”:

exemplo.pt MX 0 .

Registo DKIM Wildcard

A definição de um registo DKIM nulo ou vazio não é absolutamente necessária uma vez que a mensagem de correio eletrónico seria provavelmente tratada da mesma forma caso não existisse nenhum registo.

No entanto, a definição desse registo pode revelar-se útil uma vez que alguns destinatários irão tratar um registo DKIM nulo com cuidado redobrado, sendo que este revoga explicitamente todas as chaves que possam estar armazenadas em cache.

O registo abaixo indicado assinala que nenhuma mensagem de correio eletrónico poderá ser assinada para o seu domínio estacionado:

***._domainkey.exemplo.pt TXT “v=DKIM1; p=”**