Diagnóstico do Estado da Adopção de Normas de Segurança na Internet Portuguesa

Capítulo Português
da
Internet Society

secretariado@isoc.pt

30/04/2021
Versão 1.0

Internet Society
Portugal Chapter

Internet Society
Foundation

Sumário Executivo

Este documento apresenta um relatório preliminar do Projecto OSSE - uma iniciativa do Capítulo Português da Internet Society (ISOC.PT) que tem como objectivo observar o estado de adopção de normas de segurança do ponto de vista da presença na Internet de diferentes instituições e empresas portuguesas. Neste contexto, a observação é focada: (1) na análise da implementação de normas de segurança pelos servidores web (servidores *Hyper Text Transfer Protocol* (HTTP)); (2) na análise do grau de penetração de normas de segurança nos servidores de correio electrónico (servidores *Simple Mail Transfer Protocol* (SMTP)) das instituições observadas; (3) na análise da contribuição para a segurança da Internet portuguesa de algumas empresas relevantes que actuam em Portugal como fornecedores de serviços de *web hosting*; e (4) na análise da contribuição dos *Internet Service Providers* (ISPs) portugueses para a disponibilização de suporte *Internet Protocol Version 6* (IPv6), das normas *Domain Name System Security Extensions* (DNSSEC) e das normas associadas às boas práticas de encaminhamento seguro, nomeadamente, o progresso da adesão às normas baseadas na *Resource Public Key Infrastructure* (RPKI).

O Referencial de observação OSSE O projecto OSSE utiliza para o seu referencial de observação uma metodologia que propicia não apenas uma observação de diagnóstico, mas também a ligação da mesma à identificação de acções concretas que visam a melhoria do estado da segurança da utilização da Internet em Portugal. O observatório OSSE diferencia-se de outros existentes nas seguintes características principais:

- **Independência, neutralidade e privilegiando os utilizadores** Constitui um referencial de observação independente e neutral, transparente e privilegiando a visão que os utilizadores têm da Internet (como cidadãos ou consumidores) e não a visão interna ou do ponto de vista dos fornecedores dos serviços.

- **Baseado em ferramentas auditáveis** A observação é baseada em ferramen-

tas auditáveis e escrutinadas, em parte de código aberto e de domínio público.

- **Gestão flexível de listas de pontos de presença a observar** A Plataforma de observação OSSE suporta uma metodologia de observação que permite a gestão de listas de *endpoints* (i.é. domínios de *sites web* e de correio electrónico), de agregação de entidades por sectores ou áreas de actividade, que permite retirar indicadores qualitativos e quantitativos com rigor, detalhe e ligação dos mesmos a acções de melhoria para futuras classificações obtidas.

- **Plataforma com carácter mobilizador** Na plataforma OSSE as ferramentas utilizadas foram concebidas de modo a serem potenciadas em projectos mobilizadores, permitindo a possível reutilização e evolução futura em diferentes quadros de colaboração envolvendo diferentes entidades, em particular na esfera de colaboração entre entidades de representação de utilizadores ou consumidores ou, por exemplo, no âmbito da promoção de políticas públicas que visem a melhoria da qualidade e segurança da utilização de recursos na Internet em Portugal.

- **Observação com métricas quantitativas e factores de comparabilidade** As observações OSSE baseiam-se na aferição de métricas quantitativas e qualitativas comparáveis, permitindo correlacionar critérios de diferentes instituições, sectores ou entidades representativas de diferentes áreas, bem como a possibilidade de suportar métricas de comparabilidade com outras plataformas e ferramentas que permitem obter métricas de classificação qualitativas e quantitativas.

- **Alinhamento com o estado da arte no que diz respeito a normas** Os critérios de observação OSSE são fundados num referencial de normas e práticas de segurança estabelecidos e bem alinhados com as normas IETF, com os resultados relacionados da investigação nas áreas da Segurança da Internet e que também acompanham as preocupações de entidades que têm promovido recomendações relevantes na área, incluindo a ISOC.ORG, iniciativas colaborativas congéneres na Europa ou recomendações relacionadas por parte de agências supranacionais, nomeadamente a ENISA.

Domínios de observação Os resultados do relatório (que se consideram como resultados preliminares) foram obtidos a partir de vários domínios de observação, que incluem dois grupos de fornecedores de serviços: empresas de serviços de *web hosting* e ISPs, e ainda duas listas de domínios DNS:

- **Lista Portugal 1000** - constituída por um conjunto de cerca de mil entidades observadas a partir da sua agregação por sectores, representando, na actual configuração, os seguintes sectores: **(1)** Presidência da República e órgãos do Governo; **(2)** serviços tutelados pelo Governo ou organismos governamentais que disponibilizam sistemas e serviços para interacção com os cidadãos; **(3)** órgãos e instituições da área da Justiça; Parlamento; **(4)** partidos políticos; **(5)** imprensa; **(6)** banca e serviços financeiros; **(7)** empresas ou organizações associadas a *utilities*; **(9)** organizações, instituições ou *sites* de confissões religiosas; **(10)** organizações de representativas da sociedade civil; **(11)** bibliotecas; **(12)** editoras; **(13)** empresas com actividade relevante na área do comércio electrónico e de fornecimento de serviços online e **(14)** instituições do sistema nacional de investigação e ensino superior.

- **Lista Alexa Top 100** - constituída pelos 100 *sites web* com maior volume de tráfego online em Portugal (de acordo com as estatísticas da empresa Alexa Inc.) e que inclui entidades nacionais e internacionais entre as mais acedidas pelos utilizadores portugueses.

O relatório apresenta não apenas os resultados das observações dos domínios acima indicados, mas também recomendações que visam a melhoria das métricas e práticas de segurança que foram observadas. Os resultados são apresentados de forma agregada, considerando-se como resultados preliminares na actual versão do relatório. Não obstante, as observações realizadas permitiram já a obtenção sistemática de observações sectoriais com métricas quantitativas e qualitativas comparativas entre diferentes sectores (não publicadas por agora).

Conclusões da Observação e Acções de Melhoria As conclusões gerais da actual observação *Open Security Standards Everywhere* (OSSE) (que decorrem dos resultados de detalhe apresentados no relatório completo) mostram, como a seguir se detalha, que existem inúmeros aspectos e oportunidades de melhoria. Os mesmos são a seguir evidenciados.

Sobre a escassez da adopção de DNSSEC A adopção das normas DNSSEC é residual na Internet portuguesa. Existe uma clara necessidade de combater a visão de que com a adopção de *Transport Layer Security* (TLS), o DNSSEC não é necessário. Antes pelo contrário, dada a a tendência actual de usar o *Domain Name Service* (DNS) para publicar informações de segurança para os servidores HTTP e SMTP, através das entradas *DNS-Based Authentication of Named Entities* (DANE),

Sender Policy Framework (SPF), *DomainKeys Identified Mail* (DKIM) e *Domain-based Message Authentication, Reporting and Conformance* (DMARC), a adopção de DNSSEC está a tornar-se cada vez mais importante.

As empresas de *web hosting* e os *registrars* têm aqui um papel decisivo e, tal como o relatório mostra, uma parte destas já está a tomar esta tarefa em mãos.

Sobre o grau de implementação de normas de segurança pelos servidores web É possível e necessário melhorar o nível de segurança da utilização da Internet evitando que organizações portuguesas tenham "uma presença deficiente ou mesmo de facto vulnerável". De facto, o suporte de *Hyper Text Transfer Protocol Secure* (HTTPS) é generalizado mas apenas 32% dos servidores da lista Alexa Top 100 apenas usam versões de TLS adequadas, enquanto que na lista Portugal 1000 48% só usam versões TLS *deprecated*.

É necessário:**(1)** adoptarem-se as práticas recomendadas no suporte pelos servidores HTTP de TLS; **(2)** introduzir uma gestão"mais rigorosa" da configuração dos parâmetros de segurança TLS e da criptografia fim-a-fim subjacente; **(3)** reforçar e rever os cabeçalhos HTTP relacionados com segurança, e **(4)** melhorar o suporte de DANE (a articular com adopção de DNSSEC), e ainda uma atenção particular para a protecção com recurso a *Online Certificate Status Protocol* (OCSP) e HTTP Strict Transport Security (HSTS).

Dada a situação actualmente observada, as acções indicadas permitiriam avançar para uma base mais sólida de defesa e mitigação de vulnerabilidades que podem ser articuladas com outros vectores de ataques à Web portuguesa, quer no plano de vulnerabilidades de serviços e aplicações Web, quer na correcção a curto prazo de deficiências muito gritantes que se verificam em alguns sectores e instituições observadas.

Diagnóstico da adopção de normas de segurança pelos servidores de correio electrónico A observação do estado da segurança do eco-sistema de correio electrónico em Portugal revela deficiências gritantes que urge melhorar significativamente. Por exemplo, na lista Alexa Top 100, 76% dos servidores suportam *SMTP will be executed over TLS/SSL* (START/TLS) mas na lista PT 1000 este número desce para 26%. O número de servidores que só suportam versões TLS adequadas nessas listas é, respectivamente, 16% e 5%.

As outras principais deficiências prendem-se com a baixa penetração do DNSSEC e a não conformidade com as normas DKIM, DMARC e SPF. Estando o eco-sistema de correio electrónico particularmente associado a vectores de ataque com relevância em muitos incidentes de segurança mais recentes, o reforço das anteriores práticas

de segurança e a adopção das respectivas normas, não sendo só por si a panaceia para a globalidade desses problemas, poderia no entanto constituir uma importante base comum de incremento de garantias de segurança, a associar a outras medidas de defesa.

De forma geral, a necessidade de melhoria nos servidores de correio electrónico revela-se ainda mais urgente que no eco-sistema web mais tradicional.

Sobre a contribuição das empresas de Web *hosting* Esta empresas, entre os quais algumas das com maior expressão no mercado foram observadas, têm um impacto directo na segurança dos seus clientes, que são muito numerosos entre o tecido das pequenas e médias empresas. As suas práticas têm, portanto, um impacto directo na segurança dos clientes dos seus clientes.

O observatório fornece uma visão detalhada sobre a adopção de normas de segurança por 6 destes fornecedores. De forma geral o serviço prestado está em linha com o diagnóstico acima apresentado no que diz respeito à segurança dos servidores HTTP e SMTP do eco-sistema da Internet portuguesa. No entanto, não podemos deixar de realçar que existe um subconjunto destas empresas que já estão a fazer um esforço muito meritório para incremento do nível de segurança oferecido, o que se traduz na oferta de DNSSEC e serviços de suporte a HTTP através de servidores já com um nível de segurança bastante próximo do adequado. Já no que diz respeito ao serviço de correio electrónico, não nos é possível dar um retrato tão optimista.

Sobre a contribuição dos ISPs portugueses Os ISPs podem dar uma uma contribuição decisiva na melhoria da situação actual nos seus campos de actuação específicos. Tal resulta do seu importante papel: **(1)** no alargamento da utilização do IPv6; **(2)** no incremento do suporte a uma visão pelos clientes de DNS conforme com o uso de DNSSEC e **(3)** na adopção de normas e boas práticas de operação na gestão do encaminhamento do tráfego na Internet em Portugal, em particular combatendo os ataques com o objectivo da captação ilegal de tráfego.

As nossas observações permitem concluir que a disponibilização de endereços e o acesso a serviços só endereçáveis por IPv6 ainda é muito deficiente na Internet portuguesa, apesar de existirem algumas honrosas excepções entre os ISP portugueses. Como os próximos biliões de novos utilizadores da Internet mundial só terão acesso a e por IPv6, a sua adopção em Portugal contribuirá para um maior entrosamento de toda a futura Internet.

No que diz respeito a proporcionar aos seus utilizadores *resolvers* DNS com suporte da verificação das assinaturas DNSSEC, verifica-se que uma fracção significativa dos ISPs fornecem um nível de serviço adequado.

Finalmente, verifica-se que começa a ser popular entre os ISPs portugueses a adopção das normas RPKI, no entanto a sua utilização a fundo para filtrar rotas não autenticadas ou com falsa autenticação ainda é uma tarefa a necessitar de maior progresso.

É necessário um maior compromisso com a segurança em toda a Internet portuguesa Para tal é necessário promover uma maior visibilidade dos esforços que as empresas de serviços de *Web hosting*, os *registrars* e os ISPs fazem, ou não, para promover a segurança dos seus clientes. O mercado tem de amadurecer e premiar quem investe na segurança, descartando os que a menosprezam.

É lamentável a quase total ausência de referência a normas de segurança, ou a adesão a iniciativas como a *Mutually Agreed Norms for Routing Security* (MANRS), quando se consultam as ofertas de serviços destas empresas.

Interessa que os seus esforços de incremento da base de segurança anteriormente referida sejam identificados e valorizados pelos consumidores (desde logo por parte das Entidades de Regulação e utilizadores representando o sector público e serviços do Estado).

Tal poderia permitir que se caminhasse para a criação de condições de valorização da"economia da segurança" e, consequentemente, de uma maior exigência por parte dos consumidores. A divulgação de métricas de compromisso por parte de entidades prestadoras de serviços para a melhoria da situação actual, poderia desempenhar um papel relevante para permitir o reconhecimento da diferenciação da qualidade da oferta de serviços por parte dos *players* envolvidos, o estabelecimento de quadros de colaboração e parceria *"multi-stakeholder"* para o reforço das práticas de segurança e o aumento progressivo da exigência dos cidadãos e consumidores.

Conteúdo

.

1 Introdução

Um diagnóstico do progresso da adopção de normas de segurança do ponto de vista da presença na Internet das instituições e empresas portuguesas mais relevantes, tem o interesse de permitir fazer uma análise do grau de penetração das mais modernas práticas de segurança na Internet portuguesa. Tal reveste-se da maior importância para a defesa da segurança das instituições com presença online e do público em geral que lhes acede. Esta análise facilita igualmente elencar as acções capazes de ajudar à correcção das deficiências existentes.

O projecto OSSE, do Capítulo Português da *Internet Society* (ISOC PT), tem por objectivo fazer este diagnóstico e apontar pistas para a melhoraria da presença na web de instituições que, ou porque atraem muito tráfego, ou porque têm grande importância para os cidadãos portugueses, importa que façam parte deste diagnóstico. O mesmo princípio aplica-se igualmente aos servidores de correio electrónico que utilizam.

O ISOC PT está numa posição privilegiada para realizar este diagnóstico. Em primeiro lugar porque o mesmo se inscreve na sua missão. Em segundo lugar porque o ISOC PT faz ponto de honra da sua independência de forças políticas, empresariais ou quaisquer outras, que tenham motivações que de alguma forma pudessem contribuir para algum enviesamento dos objectivos desta análise. Finalmente, e em terceiro lugar, porque o ISOC PT dispõe de competência para realizar este diagnóstico e faz parte da comunidade Internet mais vasta que tem preocupações com a segurança,

abertura e impacto social da Internet.

Este projecto inscreve-se nos objectivos da *Internet Society* (ISOC), na qual o ISOC PT é filiado. Esses objectivos consistem na promoção e defesa de uma Internet para todos, aberta, segura e confiável. Em particular, o projecto inscreve-se nas linhas de acção da Internet Society: *Open Standards Everywhere* (OSE), MANRS e Support of Encryption e foi parcialmente financiado pela Internet Society Foundation.

A análise realizada incide sobre diversas facetas da Internet portuguesa, entre as quais:

- O grau de implementação de normas de segurança pelos servidores web (servidores HTTP[1, 2]).

- O grau de implementação de normas de segurança pelos servidores de correio electrónico (servidores SMTP[3, 4]) das instituições.

- Qual a contribuição para a segurança da Internet portuguesa de algumas empresas relevantes no fornecimento de serviços de suporte à presença na web através de serviços na Cloud, especialmente destinados a instituições portuguesas de pequena ou média dimensão, também designados por serviços de *Web hosting*.

- Qual a contribuição dos ISP portugueses para a utilização do IPv6 [5], de DNSSEC [6, 7] e de normas de encaminhamento seguro, nomeadamente, o grau de progresso da sua adesão às normas baseadas na RPKI [8].

Este relatório apresenta os resultados do diagnóstico, antecedidos por um conjunto de secções que apresentam a forma como o mesmo foi realizado, e complementados com recomendações e conclusões. Assim:

O Capítulo 2 apresenta os mecanismos usados para realizar as observações e quais os parâmetros de observação mais relevantes.

O Capítulo 3 discute as diversas listas de domínios usadas para analisar a penetração de normas de segurança nos servidores HTTP e de correio electrónico.

Os Capítulos 4, 5 e 6 apresentam os resultados da análise com base nas listas anteriores.

O Capítulo 7 introduz os resultados da análise da contribuição dos ISPs portugueses para a segurança da Internet portuguesa.

Os Capítulos 8, 9 terminam este relatório com um diagnóstico global e conclusões, assim como com um conjunto de indicações de como a situação pode ser melhorada.

O Capítulo 9.5 lista um conjunto de referências úteis.

Este relatório foi elaborado e é da responsabilidade da direcção do Capítulo Português da Internet, constituída por José Legatheaux Martins, Henrique João Domingos e Rogério Ventura Reis.

O ISOC PT agradece o apoio recebido da Internet Society Foundation assim como a colaboração técnica na execução dos testes prestada pelos estudantes de mestrado Filipe Luna e Sara Ferreira.

Ortografia. Este relatório utiliza a ortografia portuguesa anterior ao último acordo ortográfico.

2
Instrumentação

A realização de medidas sobre diversas facetas do funcionamento da Internet é alvo de actividade intensa de diversos organismos académicos e científicos, *Internet Regional Registries* (IRRs), iniciativas empresariais, plataformas especializadas e de conferências dedicadas ao tema, não cabendo neste relatório a sua enunciação.

Para a realização deste diagnóstico recorreu-se a vários observatórios cujos objectivos se aproximam dos nossos e montou-se igualmente uma instância de um deles. Neste capítulo apresentam-se brevemente alguns observatórios existentes, justifica-se qual o subconjunto a que recorremos, e apresentam-se os instrumentos usados. Finalmente, discutem-se os principais parâmetros relevantes para a análise que o relatório apresenta.

2.1 Observatórios

Existem presentemente na Internet vários conjuntos de instrumentos que permitem a observação, medição e análise da forma como esta está a funcionar internamente. Esses observatórios permitem testar serviços e redes, assim como obter agregados dos resultados desses testes (e.g. por exemplo por país ou por região). A seguir apresentamos alguns dos que recenseámos, parte dos quais foram utilizados nesta análise. Como é natural, existem muito mais observatórios, mas os apresentados a seguir caracterizam-se por adoptarem, no essencial, objectivos e pontos de vista que

contribuem para a nossa análise.

Internet.nl (https://internet.nl)

Este observatório foi montado por iniciativa de diversas fundações e outras organizações ligadas à Internet e também é suportado pelo governo dos Países Baixos e pela Internet Society. Os participantes no projecto desenvolveram um sistema de teste da adopção por um *site web*, identificado por um domínio, de várias normas de segurança, assim como da sua acessibilidade através de endereçamento IPv6. Realiza também testes semelhantes aos servidores de correio electrónico que servem um domínio dado.

O *site web* principal do projecto (`https://internet.nl`) permite a execução destes testes interactivamente. O software desenvolvido para suporte dos testes está disponível em:

`https://github.com/internetstandards`

e, tanto quanto nos foi dado perceber, é dos poucos observatórios da sua classe que disponibiliza integralmente o código fonte que utiliza o que permite validar o seu funcionamento. Para além dos resultados parciais dos testes, é mostrada uma classificação final, para o domínio observado, usando uma escala de 0 a 100. Para cada um dos testes realizados é disponibilizada uma extensa documentação explicativa que faz referência às recomendações do centro de ciber segurança dos Países Baixos e às normas e recomendações da *Internet Engineering Task Force* (IETF) (`https://ietf.org` e `https://www.isoc.org/about-the-ietf/`).

Webcheck.pt (https://webcheck.pt)

É um site semelhante ao Internet.nl mantido pelo Centro Nacional de Ciber Segurança de Portugal (CNCS) (`https://cncs.gov.pt`), assim como pela associação DNS.PT (`https://dns.pt`). Dado um nome de domínio, o *site* permite realizar testes interactivos aos servidores HTTP e do serviço de correio electrónico associados ao mesmo. Não são realizados testes à acessibilidade através de IPv6. O resultado dos testes é apresentado sinteticamente e os resultados são fáceis de seguir. O site

contém igualmente apontadores para algumas recomendações do CNCS sobre as normas envolvidas nos testes. Para cada faceta testada é dado um veredicto: satisfaz, satisfaz parcialmente, não satisfaz e não testado.

Mozilla observatory (https://observatory.mozilla.org)

Permite fazer testes interactivos a um *site web*, como os observatórios anteriores, mas não faz testes aos servidores de correio electrónico. No que diz respeito aos testes ao servidor HTTP, centra-se em realizar testes alargados da implementação de TLS e aos cabeçalhos de segurança enviados pelo servidor do domínio testado. Fornece documentação sobre como corrigir as deficiências reportadas. Dá uma classificação qualitativa global ao *site web* de um domínio baseado nos testes que realiza.

SSL Labs da Qualys (https://www.ssllabs.com/ssltest/analyze.html)

Este observatório é mantido pela empresa Qualys e permite fazer a análise muito detalhada do suporte de TLS por um *site web*. Dá uma classificação qualitativa global, estritamente desse ponto de vista, ao *site web* de um domínio. Apresenta um diagnóstico profundo do certificado e de todas as informações de segurança associadas ao mesmo, das versões e *cypher suites* TLS suportadas, incluindo uma análise detalhada de como os diferentes *browsers* realizariam o *handshake* TLS. Finalmente analisa como o *site web* se comportaria face a uma lista de ataques conhecidos.

Censys (https://support.censys.io)

A empresa Censys teve origem num projecto académico da Michigan University. Disponibiliza os resultados de um *scanning* sistemático do espaço de endereçamento, fazendo análise, para cada endereço *Internet Protocol Version 4* (IPv4), de quais os protocolos acessíveis na Internet (testa cerca de 2000 portas diferentes). Disponibiliza os resultados obtidos com fins científicos e comerciais.

Observatórios APNIC (https://labs.apnic.net)

O *Asia Pacific Network Information Centre* (APNIC), Regional Internet Registry para a Ásia e Oceania, disponibiliza através do seu laboratório, dirigido por Geof Houston, vários observatórios: sobre a penetração do IPv6, sobre a execução pelos *resolvers* DNS de verificações com base na norma DNSSEC, quando esta está implementada por um domínio. Disponibiliza também um observatório, ainda em desenvolvimento, que permite analisar facetas da adopção das normas RPKI, nomeadamente a filtragem de rotas com base nos certificados *BGP Route Origination Authorizations* (ROAs)[9]. O capítulo 7 apresenta esta faceta de análise mais em detalhe. Como veremos nesse capítulo, este observatório publica resultados agregados por países que estão na base de uma parte significativa dos resultados sobre Portugal aí reportados.

2.2 Observatórios seleccionados

As análises apresentadas neste relatório estão essencialmente sustentadas em observações realizadas com base numa implementação de um motor de análise montado usando o software disponibilizado pelo projecto Internet.nl, assim como com base nos resultados recolhidos pelos observatórios dos APNIC Labs. Dada a necessidade de realizar periodicamente, e no mais breve espaço de tempo possível, a análise de mais de 1000 domínios, tornou-se evidente a necessidade de montar um motor de testes próprio. Assim, porque a Internet.nl disponibiliza o código fonte e pela sua abrangência e equilíbrio, seleccionámos aquele observatório como ponto de partida.

Os testes por ele realizados são se âmbito muito largo integrando testes de IPv6, DNSSEC, TLS e certificados `X.509`[10], normas do correio electrónico, etc. Adicionalmente, dos observatórios da sua classe acima referidos, é o único software que testa a acessibilidade por IPv6. Esta faceta, e a sua razão de ser, é clarificada na secção 2.3.

A análise realizada pela plataforma à implementação de DNSSEC é completa e semelhante à realizada pelo observatório Webcheck. No que respeita à análise da implementação do TLS e da certificação `X.509`, a mesma é completa e de acordo com as recomendações do Centro Nacional de Ciber Segurança dos Países Baixos, acessível em `https://english.ncsc.nl/publications`. Sob este aspecto, é apenas ultrapassada pela profundidade da análise realizada pelo observatório SSL labs. O detalhe da análise realizada aos cabeçalhos HTTP de segurança é inferior ao da

implementação feita pelos observatórios Mozilla e SSL Labs. Esses fazem uma análise com uma grande ênfase na segurança aplicacional do serviço HTTP, o que ultrapassa o fito de observação a que nos propusemos.

Dados sobre a penetração do IPv6 estão disponíveis em inúmeros observatórios. Os do APNIC labs fornecem dados sobre a adopção de IPv6 mas também dados sobre como funcionam os *resolvers* de DNS usados pelos utilizadores e sobre a implementação da filtragem de rotas com base nas normas RPKI. Estes observatórios distinguem-se de outros observatórios semelhantes por adoptarem uma técnica muito original de realização das medidas. A mesma repousa na distribuição de código executável em *browsers* de utilizadores espalhados por toda a Internet, o que permite implementar uma infraestrutura de testes massivamente distribuída. Desta forma, as medidas que realizam dão uma visão próximo do impacto real da forma de implementação das normas nos utilizadores finais. Esta característica torna os resultados produzidos bastante singulares.

2.3 Parâmetros relevantes para a análise

Pelas razões expostas acima, para a realização desta análise foi utilizado o código disponibilizado pelo observatório Internet.nl. Com essa base, foi montado um servidor que realiza periodicamente e de forma automática o teste de uma lista de domínios. Os resultados são depois guardados numa base de dados.

Dada a grande diversidade dos parâmetros testados, na apresentação de resultados utilizam-se subconjuntos constituídos pelos que são mais relevantes. Diversos outros parâmetros são também agregados em indicadores qualitativos, sobretudo os que dizem respeito à análise do suporte de TLS/SSL.

Para a selecção dos parâmetros mais relevantes seguimos a organização proposta pela Internet.nl, a qual, como já foi referido, está alinhada com as melhores práticas e pode ser consultada em detalhe em

`https://internet.nl/faqs/report`.

Aí poderá o leitor encontrar referência a um documento do Centro de Cybersegurança dos Países Baixos, com uma discussão detalhada dos testes e recomendações embutidas no software de teste que usámos. Por exemplo, no que diz respeito ao teste das versões de TLS, o mesmo é compatível com as últimas recomendações do IETF, ver [11].

A nossa base de dados contém todos os parâmetros individuais medidos. No entanto, num esforço de síntese, a caracterização dos servidores, do ponto de vista segurança, é apresentada de forma agregada como é explicado a seguir.

Para a análise do contributo dos operadores de rede a actuarem em Portugal para a segurança da Internet do país, utilizámos exclusivamente os dados fornecidos pelo observatório dos APNIC Labs. Estes permitiram analisar o grau de adesão dos operadores ao IPv6, o nível provável de suporte fornecido pelos seus *resolvers* ao DNSSEC, e ainda o seu grau de adesão às normas e práticas baseadas na RPKI. No capítulo 7 são fornecidas explicações mais detalhadas sobre este conjunto de normas.

O diagnóstico sobre a disponibilização de IPv6 merece algumas observações suplementares. O IPv6 é uma versão do protocolo IP cuja principal diferença face à versão IPv4 é a disponibilidade de um espaço de endereçamento mais alargado. O IPv6 não é uma norma de segurança, apesar de nas suas versões iniciais incluir a obrigatoriedade de suporte de IPSec, opção que foi posteriormente abandonada.

Ainda que a acessibilidade por IPv6 não seja um indicador de segurança de um *site web*, a mesma vai sendo cada vez mais importante à medida que os novos operadores que vão surgindo já não têm possibilidade de fornecer conectividade IPv4 nativa aos seus clientes. Isso será cada vez mais uma realidade para os novos subscritores de acessos móveis G4 e G5 pelo que disponibilizar acesso por IPv6 é uma garantia de acessibilidade futura dos *sites web*.

Com efeito, dado que nos dias de hoje as IRRs já praticamente não dispõem de espaço de endereçamento IPv4 para afectar, muitos novos operadores só disponibilizam de forma nativa endereçamento IPv6, ficando geralmente o IPv4 apenas suportado por *gateways* de tradução. A implementação generalizada de IPv6 contribui portanto para facilitar a intercomunicação de todos as redes ligadas à Internet.

No entanto, não cabe aqui discutir se esta implementação é ou não imprescindível para manter essa universalidade das comunicações, nem se a adopção de IPv6 dificulta ou enfraquece a segurança dos utilizadores.

Parâmetros dos servidores de *sites web*

A Tabela 2.1 introduz os parâmetros usados nas tabelas de apresentação de resultados da análise de um domínio, do ponto de vista da segurança do serviço web fornecido (servidor ou servidores HTTP). Para cada um deles é introduzida a nomenclatura com que figura nas tabelas de resultados, assim como uma breve descrição. A forma mais expedita de conhecer o significado completo de cada agregação é executar interactivamente o teste de um *site web* via o Internet.nl, usando por exemplo `isoc.pt` como referência, e consultar as explicações fornecidas no diagnóstico.

Tabela 2.1: Nomenclatura e significado dos parâmetros da análise de um *site web* através da análise do ou dos servidores HTTP associados ao seu domínio

Parâmetro	**Descrição**
Classificação	Valor da classificação (0 a 100) atribuída na sequência do teste Internet.nl.
Tem IPv6	Os servidores DNS e os servidores HTTP do domínio são acessíveis por IPv6.
Tem DNSSEC	Os RRs correspondentes aos nomes dos servidores estão assinados de forma verificável por DNSSEC.
Tem HTTPS	Os servidores do domínio suportam HTTPS.
Tem HTTPS red.	Os pedidos HTTP são *redirected* para HTTPS.
Tem HSTS	Os servidores apresentam um cabeçalho HSTS com validade de pelo menos 1 ano.
Só tem versões TLS ok	O servidor só usa versões TLS/SSL recomendadas.
Inclui versões TLS não recomendadas	O servidor usa versões TLS/SSL recomendadas e outras *phasedout*.
Só tem versões TLS *phasedout*.	O servidor só usa versões TLS/SSL NÃO recomendadas ou não usa TLS/SSL.
Só tem *cypher suites* ok	O servidor só usa suites criptográficas adequadas.
Inclui *cypher suites* não recomendadas	O servidor usa suites criptográficas adequadas e outras *phasedout*.
Só tem *cypher suites phasedout*.	O servidor só usa suites criptográficas *phasedout* ou não usa TLS/SSL.
Certificado	Os servidores apresentam um certificado `X.509` válido cobrindo o domínio e a sua *trust certificate chain* também foi validada.
OCSP stapling	O servidor suporta OCSP Stapling.
Tem DANE	Existem entradas DANE válidas no domínio.
HTTP headers	Os servidores respondem com o conjunto completo de cabeçalhos HTTP de segurança requeridos.

Parâmetros dos servidores de correio electrónico

A Tabela 2.2 introduz os parâmetros usados nos testes dos servidores de correio electrónico (servidores SMTP). Sugere-se igualmente a execução do teste interactivo do domínio de correio `isoc.pt` para consultar as explicações fornecidas pelo diagnóstico.

Tabela 2.2: Nomenclatura e significado dos parâmetros da análise do serviço de correio electrónico de um domínio através da análise do ou dos servidores SMTP do domínio

Parâmetro	**Descrição**
Classificação	Valor da classificação (0 a 100) atribuída na sequência do teste Internet.nl.
Tem IPv6	Os servidores DNS e os servidores SMTP do domínio são acessíveis por IPv6.
Tem DNSSEC	Os RRs correspondentes aos nomes dos servidores estão assinados de forma verificável por DNSSEC.
Tem DMARK	Existe uma entrada DMARC válida no domínio.
Tem DKIM	Existe uma entrada DKIM válida no domínio.
Tem SPF	Existe uma entrada SPF válida no domínio.
Tem START/TLS	Os servidores do domínio oferecem STARTTLS.
Só tem versões TLS ok	O servidor só usa versões TLS/SSL recomendadas.
Inclui versões TLS não recomendadas	O servidor usa versões TLS/SSL recomendadas e outras *phasedout*.
Só versões TLS *phasedout*	O servidor só usa versões TLS/SSL *phasedout* ou não usa TLS/SSL.
Só tem *cypher suites* ok	O servidor só usa suites criptográficas adequadas.
Inclui *cypher suites* não recomendadas	O servidor usa suites criptográficas adequadas e outras *phasedout*
Só *cypher suites phasedout*	O serv. só usa suites criptográficas NÃO adequadas ou não usa TLS/SSL.
Certificado	Os servidores apresentam um certificado `X.509` válido cobrindo o domínio e a sua *trust certificate chain* também foi validada.

Tabela 2.2: Continuação da Tabela 2.2

Parâmetro	**Descrição**
Tem DANE	Existem entradas DANE válidas no domínio.

3
Listas de domínios analisados

Em muitos estudos é comum usarem-se diversos tipos de listas públicas de domínios para obter radiografias da adopção de normas de segurança. Por exemplo, podem usar-se listas de domínios considerados mais relevantes, listas de domínios ordenadas pelo critério do nível de utilização ou popularidade (elaboradas através de painéis de utilizadores, código de rastreio colocado nos *sites web* ou análise de diversos tipos de tráfego), listas organizadas por sectores de actividade, ou ainda listas tendencialmente exaustivas. Naturalmente, listas exaustivas são muito difíceis de organizar e incluem certamente uma longa lista de domínios irrelevantes.

O artigo de Victor Le Pochat et al [12] para além de propor uma nova lista de grande dimensão (consultar `https://tranco-list.eu`), apresenta igualmente uma panorâmica das listas disponíveis e de como estas são organizadas. Duas dessas listas de acesso público merecem algum realce:

- Alexa
  (`https://aws.amazon.com/alexa-top-sites/`), ver a seguir.

- Cisco Umbrella
  (`http://s3-us-west-1.amazonaws.com/umbrella-static/index.html`)
  Lista baseada na análise das *queries* DNS feitas pelos utilizadores do serviço OpenDNS e outras fontes acessíveis às diferentes companhias da Cisco.

Neste trabalho resolvemos adoptar as seguintes três diferentes listas especialmente adaptadas a Portugal.

3.1 Lista *web hosters*

A primeira lista usada neste estudo é a de um subconjunto de serviços de apoio à montagem de presença na web para entidades e pessoas individuais, mais conhecidos por serviços de *hosting*. No calão internacional do meio, estas empresas são designadas por *cloud web hosters*. Como muitas entidades de pequena e média dimensão recorrem aos serviços dos *cloud web hosters*, as características do serviço disponibilizado têm um grande impacto sobre a presença na web de inúmeras entidades. Esta lista e a sua análise são objecto do capítulo 4.

3.2 Lista Alexa Top 100 — Portugal

Alexa Internet Inc. (`https://alexa.com`) é uma empresa do grupo Amazon que faz estudos de popularidade dos *sites web* com base em diversos tipos de estatísticas, nomeadamente a percentagem do tempo que os utilizadores visualizam páginas de cada domínio Internet. As estatísticas são coligidas através de *plugins* para os *browsers*, código inserido em páginas e utilizadores pagos cuja navegação é rastreada. A empresa disponibiliza diversas listas, nomeadamente listas de popularidade globais, por país e por sector de actividade. O conteúdo das listas é dinâmico.

A lista Alexa Top 100 — Portugal corresponde aos 100 mais populares *sites web* em Portugal e foi compilada pela Alexa no meio do mês de Março de 2021. Naturalmente, a mesma lista obtida noutra data conteria um conjunto distinto de *sites web*.

Mais de 50% dos *sites web* que integram esta lista têm nomes de domínio não terminado em .PT, sendo a terminação .COM dominante. Também, é provável que mais de 50% destes *sites web* pertençam a empresas estrangeiras com a sua presença web gerida fora de Portugal. Assim, as características de segurança recenseadas com esta lista são significativas do ponto de vista da segurança com que os portugueses acedem à Internet, mas, possivelmente, menos significativas para a caracterização da cultura de segurança prevalecente na comunidade técnica portugueses.

Na capítulo 5 são apresentados os resultados da análise usando esta lista.

3.3 Lista Portugal 1000

A lista Portugal 1000 é uma lista constituída por cerca de 1000 *sites web* portugueses. Estes *sites web* foram seleccionados manualmente e contém grupos, de pelo menos 10 *sites web* (mas geralmente bastante mais), distribuídos por diferentes áreas, nomeadamente:

- Todos os órgãos de soberania. Serviços oficiais ou equiparados de apoio ao cidadão.
- Partidos políticos e correspondentes grupos parlamentares.
- Autoridades policiais e de segurança nacional. Autoridades e infraestruturas de navegação aérea e marítima. Entidades de regulação e supervisão. Entidades de certificação.
- *Utilities* públicas e privadas, incluindo as de distribuição de combustíveis.
- Serviços oficiais ou equiparados da área da cultura. Bibliotecas e Arquivos documentais. Editoras.
- Serviços públicos e privados de saúde.
- Universidades e sistema científico nacional público e privado.
- Banca, serviços financeiros e seguradoras. Empresas do PSI20. Empresas de consultoria e engenharia e de serviços nas várias áreas de actividade.
- Transportes públicos e privados de camionagem, marítimos, ferroviários e aéreos.
- Comunicação social incluindo jornais, rádios, televisão, redes sociais, serviços de *streaming* operando em Portugal e portais de notícias e afins.
- Associações empresariais e profissionais, incluindo ordens profissionais e sindicatos.
- Empresas de distribuição e de comércio electrónico dos vários tipos de artigos acessíveis ao público. Lojas online de aplicações, software e jogos.
- Instituições religiosas.
- Clubes desportivos, *sites web* de jogos online e equiparados.

Esta lista constituí uma primeira tentativa de cobrir diferentes tipos de *sites web* e áreas de actividade, independentemente da sua popularidade, mas tendo em consideração o seu impacto horizontal na vida dos cidadãos. É também uma primeira tentativa de diferenciar as culturas sobre a segurança dos diferentes tipos de presença na web. A análise com base nesta lista é apresentada no capítulo 6.

4

Resultados: lista *web hosters*

Os resultados reportados nesta secção foram obtidos montando um *site web* tipo em 6 fornecedores de serviços de *hosting* em Portugal. Os 6 fornecedores escolhidos foram-no entre os 10 com maior número de registos de domínios terminados em .PT[1]. Não foram seleccionados mais fornecedores por limitações orçamentais deste projecto.

Os *sites web* montados nos fornecedores testados são, por ordem alfabética do nome da empresa fornecedora dos serviços, os seguintes:

Ptisp - AlmourolTec - Servicos de Informatica e Internet Lda
`https://teste-osse-isoc-ptisp.pt`

Amen - Amenworld Serviços Internet - Sociedade Unipessoal Lda
`https://teste-osse-isoc-amen.pt`

Dominios - Domínios, S.A. - `https://teste-osse-isoc-dominios.pt`

Ovh - Société par Actions Simplifiée - `https://teste-osse-isoc-ovh.pt`

Sampling - Sampling Line - Serviços e Internet, Lda
`https://test-osse-isoc-ptservidor.pt`

WebSP - Comércio e Prestação de Serviços Informáticos Lda
`https://teste-osse-isoc-wh.pt`

[1]Dados obtidos em Fevereiro de 2021, podendo no entretanto ter evoluído.

De acordo com o relatório de execução e contas de 2020 da associação DNS.PT, que gere o domínio .PT, 4 destes 6 fornecedores seleccionados geriam em 2020 cerca de 200.000 domínios. Por essa razão, é natural que estes 6 fornecedores forneçam suporte a vários dezenas de milhar de páginas web acessíveis através de domínios terminados em .PT. As características do serviço fornecido representam portanto uma fracção não negligenciável do panorama do suporte das normas de segurança na web Portuguesa visto que um pouco mais dos 30% de *sites web* activos em Portugal têm nomes de domínio terminados em .PT. Para a obtenção de uma amostra mais significativa, seria necessário alargar muito o leque de empresas testadas.

Para a realização dos testes, de forma anónima, o Capítulo Português da Internet Society contratou (via um utilizador anónimo) os serviços de cada fornecedor, chamemos-lhe fornecedor (r), e executou as seguintes acções:

- Contratou a r o registo e gestão do domínio"teste-osse-isoc-r.pt".
- Solicitou a adopção do serviço DNSSEC para esse domínio.
- Contratou a r um serviço de hosting da página web associada ao domínio "teste-osse-isoc-r.pt".
- Solicitou a adopção de um certificado LetsEncrypt associado ao site desse domínio.
- Contratou igualmente o serviço de correio electrónico para o domínio.
- Criou a mailbox "test@teste-osse-isoc-r.pt".
- Criou uma página web com um conteúdo que apenas usa HTML e CSS.
- Fez alguns ajustes na página ao nível do ficheiro: ".htaccess"para forçar a redirecção para HTTPS.

A Tabela 4.1 apresenta a caracterização do serviço web providenciado aos clientes das empresas de *hosting* seleccionadas. Analisando a tabela verifica-se que apenas uma delas suporta IPv6 o que mostra o atraso na adopção desta versão do protocolo IP em Portugal. Como esta adopção vale cerca de 20 pontos na classificação Internet.nl, sem a mesma, a OVH teria uma pontuação da mesma ordem de grandeza que a pontuação da Domínios.

Assim, as 3 empresas que disponibilizam DNSSEC, 50% do universo, coincidem com as empresas que maior cuidado revelam na adopção de normas de segurança e constituem o pelotão da frente da segurança no serviço web. Apesar disso, verifica-se

Tabela 4.1: Caracterização da segurança do serviço de gestão de domínios e de disponibilização de *sites web* providenciado - dados obtidos no início de Abril de 2021. Significado da primeira coluna explicado na Tabela 2.1.

Fornecedor	Ptisp	Amen	Domínios	Ovh	Sampling	Websp
Classificação (0 a 100)	34	32	76	94	66	32
Tem IPv6	-	-	-	sim	-	-
Tem DNSSEC	-	-	sim	sim	sim	-
Tem HTTPS	sim	sim	sim	sim	sim	sim
Tem HTTPS *redirect*	-	sim	sim	sim	sim	sim
Tem HSTS	-	-	-	-	-	-
Só tem versões TLS ok	-	sim	sim	-	sim	sim
Inclui versões TLS não recomendadas	sim	-	-	sim	-	-
Só tem *cypher suites* ok	sim		sim		sim	sim
Inclui *cypher suites* não recomendadas	-	sim	-	sim	-	-
Certificado	sim	sim	sim	sim	sim	sim
Tem OCSP stapling	-	-	sim	-	sim	sim
Tem DANE	-	-	-	-	-	-
HTTP headers	-	-	-	-	-	-

que todas as empresas analisadas não adoptam HSTS. Apesar de todas as empresas fornecerem certificados LetsEncrypt correctos, poucas adoptam OCSP e nenhuma adopta DANE.

No que diz respeito às versões de TLS suportadas, apenas 66% suportam versões aconselhadas tendo descontinuado as desaconselhadas. Também apenas 66% suportam apenas *cypher suites* recomendadas.

Estes números mostram que o mercado não valoriza a disponibilização de IPv6 e que a exigência de um nível de segurança adequado e ao nível das melhores práticas recomendadas para os servidores web não está enraizado no mercado.

As características do suporte de normas de segurança pelos servidores de correio electrónico oferecidos aos clientes desses fornecedores são apresentados na Tabela 4.2. Os resultados indicam que, de forma geral, o investimento na segurança dos serviços

Tabela 4.2: Caracterização da segurança do serviço de correio electrónico providenciado - dados obtidos no início de Abril de 2021. Significado da primeira coluna explicado na Tabela 2.2.

Fornecedor	Ptsip	Amen	Dominios	Ovh	Sampling	Websp
Classificação (0 a 100)	44	35	65	47	64	42
Tem IPv6	-	-	-	-	-	-
Tem DNSSEC	-	-	sim	-	sim	-
Tem DMARC	-	-	-	-	-	-
Tem DKIM	sim	-	-	-	sim	sim
Tem SPF	sim	sim	sim	sim	sim	sim
Tem START/TLS	sim	sim	sim	sim	sim	sim
Inclui versões TLS não recomendadas	sim	-	-	-	-	sim
Só tem versões TLS *phasedout*	-	sim	sim	sim	sim	-
Inclui *cypher suites* não recomendadas	sim	-	-	-	-	sim
Só tem *cypher suites* não recomendadas	-	sim	sim	sim	sim	-
Certificado	-	sim	-	sim	-	sim
Tem DANE	-	-	-	-	-	-

de correio electrónico providenciados é bastante inferior ao realizado nos serviços de *hosting* de páginas web e gestão dos domínios. Tudo indica que se trata de um serviço que as empresas, e naturalmente também os seus clientes, tratam de forma menos rigorosa do ponto de vista da segurança.

Como neste serviço a empresa OVH deixou de suportar IPv6 e DNSSEC (o que faz no serviço web), junta-se agora ao pelotão de retaguarda. O pelotão mais avançado é apenas composto pelas empresas Domínios e Sampling que suportam ambas DNSSEC. No entanto, os seus servidores não são capazes de apresentar certificados do domínio adequados, característica apenas satisfeita por 3 das 4 empresas do pelotão da retaguarda.

De forma geral todas as empresas providenciam servidores que suportam START / TLS e têm um registo SPF correcto. Poucas adoptam DKIM e nenhuma DMARC. Todas suportam versões de TLS e *cypher suites* desaconselhadas, sendo que apenas

duas delas apresentam, para além dessas, também versões recomendadas. Várias só têm versões desaconselhadas. Finalmente, tal como para o serviço web, nenhuma adopta DANE.

Em resumo, ambos os serviços mostram que existe desprezo pelo IPv6 e uma valorização mediana das normas de segurança a nível do serviço web e ainda menor a nível do serviço de correio electrónico. Tal é lamentável dada a cada vez maior criticidade da segurança do serviço de correio electrónico em ataques do tipo *phishing* com base em mensagens de correio forjadas.

É possível que uma significativa parte dos clientes destas empresas contratem o serviço de alojamento de *sites web* com as mesmas, mas usem outros fornecedores para o seu serviço de correio electrónico, o que poderia explicar a menor atenção prestado ao mesmo.

5

Resultados - lista Alexa Top 100 — Portugal

Neste capítulo apresentam-se e analisam-se os resultados obtidos com a lista Alexa Top — 100 Portugal. A Tabela 5.1 permite caracterizar sinteticamente os 100 *sites web* mais populares em Portugal do ponto de vista da segurança.

Desde logo importa realçar que a penetração de IPv6 é bem superior entre estes *sites web* apesar de continuar a ser minoritária. No entanto, é um facto que todas as plataformas mais conhecidas já fornecem acesso via IPv6. Em contrapartida, a oferta de DNSSEC é muito escassa mesmo entre *sites web* com grande visibilidade pois apenas 9% deles suportam essa norma de segurança.

Em contrapartida, a quase totalidade suporta acesso por HTTPS, sendo o número das que implementam redirecção para HTTPS quase 60%, ainda muito longe da totalidade. Em contrapartida apenas 32% suportam HSTS pelo que ainda existe neste campo um grande caminho de melhoria possível. Também, no que respeita às versões de TLS e às *cypher suites* suportadas existe necessidade de melhoria ao mesmo nível da melhoria necessária no HSTS. O mesmo se aplica à utilização de cabeçalhos HTTP de segurança pois nenhum dos *sites web* da lista os apresenta de forma completa.

Finalmente, verifica-se bastante cuidado com os certificados `X.509` pois 94% dos *sites web* têm um bom certificado e uma correcta cadeia de certificação e quase 50%

já suportam OCSP stapling.

Importa realçar que a classificação média é aproximadamente 50%, provavelmente muito influenciada pela penalização devido à quase ausência de suporte de DNSSEC (20 pontos de penalização) e à ainda baixa penetração de IPv6 (também 20 pontos de penalização). O desvio em relação à média das classificações é muito elevado (14%), provavelmente bastante influenciado por este dois factores.

Se fossem descontadas as penalizações devido à generalizada ausência de suporte de DNSSEC, e também de IPv6, verificar-se-ia que a pontuação média subiria provavelmente para perto de 80%. Tal revela que, descontando os 7 *sites web* com uma pontuação inferior a 30, existe uma preocupação razoável com a segurança[1] no conjunto desta lista, mas não deixa de existir uma quantidade elevada de aspectos que podem ser melhorados.

No que diz respeito à análise do suporte de segurança pelo serviço de correio electrónico dos domínios que fazem parte desta lista, os resultados mostram que o suporte de DNSSEC tem uma incidência ainda mais baixa que no serviço web dos mesmos domínios, que o número de servidores que suportam START/TLS é 76%, mas que apenas 16% só suportam as versões de TLS recomendadas e apenas 17% só suportam *cypher suites* recomendadas (ou seja, já abandonaram todas as não recomendadas). Infelizmente, pelo menos 35% dos servidores só suportam versões de TLS e *cypher suites* não recomendadas. Considerando estes números em conjunto com o facto de que 24% dos domínios nem sequer suportam START/TLS, pode concluir-se que quase metade dos domínios suportam formas muito deficientes de segurança, o que é compatível com o facto de que o número de servidores que exibem certificados correctos é à volta de 60%.

A percentagem de domínios que começam a incluir os registos DNS para combate de *phishing* é superior a 70% mas o registo DMARC é muito pouco popular (só 15% dos domínios o exibem). Não se pode deixar de observar que sem suporte de DNSSEC, estes domínios continuam susceptíveis de ataques de *phishing* por oponentes muito sofisticados. Finalmente o suporte de DANE é praticamente nulo.

O suporte de IPv6 pelos servidores SMTP desta lista é da mesma ordem de grandeza que os servidores HTTP.

[1] À excepção do suporte de DNSSEC e DANE dele dependente.

Tabela 5.1: Caracterização agregada da segurança do serviço dos *sites web* que integram a lista Alexa 100 - dados obtidos no início de Abril de 2021. Significado da primeira coluna explicado na Tabela 2.1.

Classificação (0 a 100)	Média 47	Melhor 97	Pior 19	Desvio 14
Tem IPv6	32%	sim	—	
Tem DNSSEC	9%	sim	—	
Tem HTTPS	98%	sim	—	
Tem HTTPS red.	58%	sim	—	
Tem HSTS	28%	sim	—	
Só tem versões TLS recomendadas	32%	—	—	
Inclui versões TLS não recomendadas	65%	sim	—	
Só tem versões TLS não recomendadas	3%	—	—	
Só tem cypher suites recomendadas	16%	—	—	
Inclui cypher suites não recomendadas	77%	sim	—	
Só tem cypher suites não recomendadas	7%	—	—	
Certificado	94%	sim	—	
Tem OCSP stapling	49%	sim	—	
Tem DANE	0%	—	—	
HTTP headers	0%	—	—	

Tabela 5.2: Caracterização agregada da segurança do serviço de correio electrónico dos domínios que integram a lista Alexa Top 100 - dados obtidos no início de Abril de 2021. Significado da primeira coluna explicado na Tabela 2.2.

Classificação (0 a 100)	Média 54	Melhor 75	Pior 6	Desvio 13
Tem IPv6	34%	sim	-	
Tem DNSSEC	1%	-	-	
Tem DMARC	15%	-	-	
Tem DKIM	72%	sim	-	
Tem SPF	72%	sim	-	
Tem START/TLS	76%	sim	-	
Só tem versões TLS recomendadas	16%	-	-	
Inclui versões TLS não recomendadas	42%	sim	-	
Só tem versões TLS não recomendadas	42%	-	-	
Só tem *cypher suites* recomendadas	17%	-	-	
Inclui *cypher suites* não recomendadas	48%	sim	-	
Só tem *cypher suites* não recomendadas	35%	-	-	
Certificado	67%	sim	-	
Tem DANE	1%	-	-	

6

Resultados - lista Portugal 1000

Neste capíitulo apresentam-se e analisam-se os resultados obtidos com a lista Portugal 1000. A Tabela 6.1 permite caracterizar sinteticamente do ponto de vista da segurança os *sites web* da lista PT 1000. A segunda coluna apresenta, para comparação, os resultados médios da lista Alexa Top 100 para o serviço HTTP. Algumas entidades da lista Portugal 1000 partilham o mesmo domínio e servidores, sendo os seus resultados contabilizadas mais do que uma vez. Por um lado, isso não desvirtua o ponto de vista dos utilizadores pois são esses os serviços a que realmente acedem. Por outro lado, dado que o número de ocorrências desse facto é baixo, sendo apenas comum em alguns *sites web* do Governo de Portugal, a sua influência nos resultados agregados não é significativa.

Ao analisarmos a tabela constata-se de novo que o IPv6 e o DNSSEC são igualmente desprezados nesta lista. Só que desta vez o menosprezo do IPv6 é bastante maior do que na lista Alexa Top 100, provavelmente porque a exposição internacional dos membros desta lista é menor do que os daquela. Em contrapartida, o suporte de DNSSEC é aqui superior ao da lista Alexa Top 100 - Portugal. Provavelmente isso pode ser explicado pelo facto de que mais *sites web* desta lista recorrem a serviços de *hosting* do que os da lista Alexa Top 100 - Portugal. Quanto mais empresas de *hosting* suportarem DNSSEC, maior será a sua penetração na web portuguesa.

No que diz respeito ao suporte de HTTPS e HSTS, os números medidos são da mesma ordem de grandeza mas inferiores do que os da lista Alexa Top 100 - Portugal

e por isso também há nesta faceta uma margem de progresso importante.

No que diz respeito ao suporte do TLS existem cerca de 42% de *sites web* que apenas suportam as versões recomendadas de TLS e 10% que utilizam as versões recomendadas mas também versões não recomendadas. Infelizmente, uma grande quantidade de servidores apenas usam versões não recomendadas ($48\% = 100\% - 42\% - 10\%$). Este último valor é dramaticamente elevado e inclui igualmente os 6% de servidores que não suportam HTTPS. No caso da lista Alexa, o mesmo número baixa de 48% para 3%.

Também as *cypher suites* suportadas apresentam uma panorâmica a necessitar sem dúvida de melhoria: apenas 25% suportam exclusivamente *cypher suites* recomendadas e mais 18% suportam estas e mais alguma não recomendada. O número de servidores que não suportam *cypher suites* ou apenas suportam as não recomendadas é muito elevado ($57\% = 100\% - 25\% - 18\%$). No caso da lista Alexa este número é apenas de 7%. O número de certificados deficientes é também superior ao da lista Alexa Top 100 - Portugal (o número reportado inclui os 6% de servidores que não suportam HTTPS). O suporte de DANE e do conjunto completo de cabeçalhos de segurança HTTP é também nulo tal como na lista Alexa.

O suporte de normas de segurança no conjunto dos servidores que servem os domínios da lista Portugal 1000 é de facto muito deficiente. Dos cerca de 1000 domínios analisados, mais de 50% têm classificação inferior a 40%, e necessitam portanto de uma grande melhoria. Cerca de 75% têm classificação inferior a 60% e apenas 19 têm classificação maior ou igual a 80%. Existe portanto uma muito elevada margem de melhorias a serem introduzidas.

A lista Portugal-1000 permite tirar algumas conclusões sectoriais. Por exemplo, existem 31 domínios servidos por servidores web com classificação igual a 6, a classificação mínima. Esses domínios não são acessíveis por HTTPS e falham em praticamente todos os critérios. Entre estes encontram-se os domínios de numerosas instituições da área da cultura, como museus e escola de artes, arquivos bibliográficos, diversas escolas superiores entre as quais bastante privadas, vários serviços públicos, mas também duas empresas do PSI20 e até um banco. Desses 31 domínios, 20 estão ligados a organismos públicos.

Voltemos agora a nossa atenção para os resultados da análise do serviço de correio electrónico da lista Portugal 1000. A Tabela 6.2 permite caracterizar sinteticamente do ponto de vista da segurança os domínios da lista PT 1000.

A comparação dos resultados da lista Portugal 1000 com os da lista Alexa Top 100 Portugal mostra uma descida acentuada de todos os parâmetros de segurança. Tal revela que de forma geral o serviço de correio electrónico associado aos domínios da lista é de bastante baixa qualidade do ponto de vista de segurança. Por exemplo,

apenas 26% dos domínios têm servidores que suportam START/TLS. Esta situação reveste-se de algum alarme dado que o serviço de correio electrónico se está a revelar um dos vectores de ataque mais significativos na actualidade. A acessibilidade por IPv6 só se verifica em 6% dos sites e o suporte de DNSSEC é novamente negligenciável.

É importante referir que os *sites web* de alguns deste domínios, em particular aqueles ligados a muitos organismos oficiais, não referem o correio electrónico como um meio de contacto com os serviços. De facto, o número de domínios desta lista para os quais se não encontra um servidor SMTP é significativo (cerca de 1/4). No entanto, para os restantes existe servidor SMTP e este serviço pode ser abusado.

Tabela 6.1: Caracterização agregada da segurança do serviço dos *sites web* que integram a lista Portugal 1000 - dados obtidos no início de Abril de 2021. A coluna da direita contém os resultados médios da lista Alexa Top 100. Significado da primeira coluna explicado na Tabela 2.1.

Lista	PT 1000	Alexa
Classificação (0 a 100)	44	47
Tem IPv6	14%	32%
Tem DNSSEC	12%	9%
Tem HTTPS	94%	98%
Tem HSTS	25%	28%
Só tem versões TLS recomendadas	42%	32%
Inclui versões TLS não recomendadas	10%	65%
Só tem versões TLS não recomendadas ou não suporta TLS	48%	3%
Só tem *cypher suites* recomendadas	25%	16%
Inclui *cypher suites* não recomendadas	18%	77%
Só tem *cypher suites* não recomendadas	57%	7%
Certificado	88%	94%
Tem OCSP stapling	34%	49%
Tem DANE	0%	0%
HTTP headers	0%	0%

Tabela 6.2: Caracterização agregada da segurança do serviço de correio electrónico dos domínios que integram a lista Portugal 1000 - dados obtidos no início de Abril de 2021. A coluna da direita contém os valores médios para o mesmo serviço da lista Alexa Top 100. Significado da primeira coluna explicado na Tabela 2.2.

Lista	PT 1000	Alexa
Classificação (0 a 100)	33	54
Tem IPv6	6%	34%
Tem DNSSEC	1%	1%
Tem DMARC	10%	15%
Tem DKIM	23%	72%
Tem SPF	29%	72%
Tem START/TLS	26%	76%
Só tem versões TLS recomendadas	5%	16%
Inclui versões TLS não recomendadas	23%	42%
Só tem versões TLS não recomendadas	72%	42%
Só tem *cypher suites* recomendadas	5%	17%
Inclui *cypher suites* não recomendadas	24%	48%
Só tem *cypher suites* não recomendadas	71%	35%
Certificado	19%	67%
Tem DANE	0%	1%

7
Contribuição dos ISP

Nesta secção analisamos a popularidade do fornecimento e utilização de conectividade IPv6, assim como o grau de apoio e adesão dos fornecedores de conectividade Internet portugueses a um conjunto de normas de segurança de natureza infra-estrutural, nomeadamente *Domain Name System Security Extensions* (DNSSEC) e *Resource Public Key Infrastructure* (RPKI).

Os dados que se seguem foram obtidos através dos observatórios dos APNIC Labs (`https://labs.apnic.net`) no início do mês de Abril de 2021. Para consultar a metodologia usada para realizar as medidas, o leitor deve consultar a documentação explicativa fornecida pelos APNIC Labs no seu *blog*, com especial realce para os *posts* de Geoff Houston, o seu director.

Muitos dos dados apresentados nesta secção estão organizados por Sistemas Autónomos ou *Autonomous Systems* (ASs). Um AS é uma rede visível pelo *Border Gateway Protocol* (BGP), o protocolo de encaminhamento no *core* da Internet (ver os RFC 2283 [13] de 1998 e RFC 4271 [14] de 2006). Grosso modo, um AS é uma rede constituinte da Internet, com capacidade de participar em decisões de encaminhamento global e com gestão autónoma. Cada ISP tem pelo menos um sistema autónomo próprio. A Tabela 7.1 dá uma estimativa da dimensão relativa dos diferentes ASs de Portugal de acordo com o método de medida usado pelos APNIC Labs. Como já referimos essa visão é uma tentativa de análise do tipo "caixa preta" com base num visão a partir da periferia dos diferentes ASs. A informação permite

relativizar alguns dos quadros que serão a seguir apresentados.

É, no entanto, importante tomar em consideração que o método de observação usado pelos APNIC Labs mostra sempre uma "fotografia" tirada da periferia dos ASs, isto é, a partir de computadores ligados directamente à rede do AS ou às redes dos seus clientes. Assim, um AS sem clientes individuais residenciais pode ser representado nas medidas de forma enviesada. Por esta razão são sempre listadas o número de amostras recolhidas para obter um indicador.

A Tabela 7.2 apresenta uma estimativa do grau de penetração entre os utilizadores dos diferentes ASs portugueses da disponibilidade / utilização de endereços IPv6 para envio e recepção de pacotes IP e para estabelecer conectividade com sistemas apenas endereçáveis em IPv6. Verifica-se claramente que essa disponibilidade apenas é relevante entre os utilizadores de 2 dos vários operadores de telecomunicações portugueses. Assim, a utilização de IPv6 entre os operadores é semelhante à das outras entidades do país. No entanto, é necessário ter presente que no caso de operadores sem utilizadores individuais, é possível que estes suportem IPv6 mas os seus clientes não. Este é, por exemplo, o caso do AS RCCN FCT, I.P.

7.1 Penetração do suporte de DNSSEC em Portugal

Não é fácil medir qual a percentagem exacta dos domínios associados a entidades com sede em Portugal que suportam DNSSEC. De acordo com o *country code Top-Level Domain* (ccTLD) de Portugal (`https://dns.pt/pt/estatisticas`) no fim de Março de 2021 existiam cerca de 400.000 domínios terminados em .PT activos. No entanto, na mesma altura, o número de domínios terminados em .PT com DNSSEC activo eram à volta de 11.000. Portanto, essa percentagem parece não ser superior a 2.75% se considerarmos o conjunto dos domínios terminados em .PT activos. Repare-se ainda que nem todas as entidades portuguesas utilizam domínios terminados em .PT, sendo a opção por .COM provavelmente dominante.

No que diz respeito à verificação de que a informação obtida do DNS é certificada quando o domínio na qual a mesma tem origem utiliza DNSSEC, os números são diferentes. Dado que os utilitários e as aplicações que são usados para aceder à Internet (*browsers* por exemplo), não verificam directamente a validade da informação com origem em domínios com suporte de DNSSEC, essa verificação está a cargo dos servidores *resolvers*[6] (ou *proxies* de DNS) que utilizam, isto é, geralmente o fornecido pelo seu fornecedor de conectividade (ISP), ou, mais raramente, algum dos serviços públicos de DNS actualmente disponíveis como por exemplo Google DNS,

Tabela 7.1: Dimensão relativa de diferentes ASs com sede em Portugal - dados do observatório APNIC Labs, obtidos no início de Abril de 2021

Rank	ASN	AS Name	Users (est.)	% of country	Samples
1	AS2860	NOS-Comunicações	2.810.887	34.98	860.600
2	AS3243	MEO-RESIDENCIAL	2.507.314	31.20	767.656
3	AS12353	Vodafone Portugal	1.867.531	23.24	571.776
4	AS42863	MEO-MOVEL	339.821	4.23	104.042
5	AS13156	AS13156 Palmela	217.185	2.70	66.495
6	AS15457	NOS_MADEIRA	129.694	1.61	39.708
7	AS15525	MEO-EMPRESAS	57.514	0.72	17.609
8	AS42580	CABOTVA	55.878	0.70	17.108
9	AS203020	HOSTROYALE	10.654	0.13	3.262
10	AS1930	RCCN FCT, I.P.	6.643	0.08	2.034
11	AS9186	ONI Lisbon, Portugal.	3.906	0.05	1.196
12	AS199155	REDE-MEC	3.498	0.04	1.071
13	AS204094	I4W	3.04	0.04	931
14	AS47202	LAZER	2.194	0.03	672
15	AS24768	ALMOUROLTEC	2.087	0.03	639
16	AS13335	CLOUDFLARENET	1.753	0.02	537
17	AS5626	ONI ISP	1.42	0.02	435
18	AS202170	BLU-AS	1.205	0.01	369
19	AS197802	UTIS-AS	1.146	0.01	351
20	AS29615	PORTODIGITAL-AS	1.103	0.01	338
21	AS8220	COLT	1.028	0.01	315
22	AS43887	MJ-PT-AS	1.012	0.01	310
23	AS49260	UNITELDATA	947	0.01	290
24	AS47674	NETSOLUTIONS	921	0.01	282
25	AS12926	AR TELECOMPT	738	0.01	226
26	AS29286	SKYLOGIC-AS	663	0.01	203
27	AS43643	TAP-AS TAP Air PT	561	0.01	172
28	AS201523	EDP-AS	519	0.01	159
29	AS29003	REFERTELECOM-AS	516	0.01	158
30	AS204287	HOSTROYALE_TECH.	434	0.01	133

Tabela 7.2: Utilização de IPv6 em Portugal - dados do observatório APNIC Labs, obtidos no início de Abril 2021

ASN	AS Name	IPv6 Capable	IPv6 Preferred	Samples
AS2860	NOS-Comunicações	0.06%	0.06%	5,395
AS12353	Vodafone-Portugal	13.98%	13.70%	1,817
AS3243	MEO-RESIDENCIAL	44.01%	42.79%	1,470
AS42863	MEO-MOVEL	0.80%	0.40%	748
AS13156	AS13156 Palmela	0%	0%	399
AS15457	NOS_MADEIRA	0%	0%	228
AS42580	CABOTVA	0%	0%	137
AS15525	MEO-EMPRESAS	0%	0%	62
AS204094	I4W	0%	0%	27
AS203020	HOSTROYALE	0%	0%	26
AS1930	RCCN FCT, I.P.	0%	0%	10
AS14618	AMAZON-AES	0%	0%	9
AS197802	UTIS-AS	0%	0%	6
AS9186	ONI Lisbon, Portugal.	0%	0%	5
AS47202	LAZER	0%	0%	4
AS47674	NETSOLUTIONS	0%	0%	3
AS201523	EDP-AS	0%	0%	3
AS201341	TESONET	0%	0%	2
AS8220	COLT	0%	0%	2
AS203724	MCAFEE-ENG-PDB	0%	0%	2

Tabela 7.3: Estimativa da verificação de *queries* DNS com DNSSEC - dados do observatório APNIC Labs, obtidos no início de Abril 2021

ASN	AS Name	DNSSEC Validates	Partial Validation	Samples
AS3243	MEO-RESIDENCIAL	98.21%	1.57%	9.092
AS15457	NOS_MADEIRA	94.50%	5.50%	564
AS203020	HOSTROYALE	90.00%	0.00%	50
AS15525	MEO-EMPRESAS	32.17%	12.17%	115
AS2860	NOS-Comunicações	7.70%	58.40%	11.403
AS13156	AS13156 Palmela	5.76%	11.53%	885
AS42580	CABOTVA	5.34%	92.88%	281
AS12353	Vodafone Portugal	2.69%	1.48%	6.843
AS42863	MEO-MOVEL	0.56%	0.70%	1.425
AS1930	RCCN FCT, I.P.	0	0	15
AS5626	ONI ISP	0	0	7
AS9186	ONI Lisbon	0	0	19
AS13335	CLOUDFLARENET	0	0	3
AS14618	AMAZON-AES	0	0	9
AS16276	OVH	0	0	1
AS24768	ALMOUROLTEC	0	0	7
AS29003	REFERTELECOM-AS	0	0	1

Cloudflare DNS, OneDNS, OpenDNS da Cisco, ...

Os APNIC Labs disponibilizam os resultados do seu observatório de DNSSEC que reportam a percentagem de consultas feitas a partir computadores ligados aos ASs de Portugal que, nos casos em que o domínio consultado suporta DNSSEC, o resultado da consulta foi validado pelo *resolver* utilizado. Como cerca de 90% (consultar os dados dos APNIC Labs) das consultas ao DNS realizadas em Portugal se dirigem a um *resolver* situado no mesmo AS que a origem da consulta, os dados apresentados na Tabela 7.3 são uma indicação indirecta da implementação da verificação das assinaturas de dados DNS no caso em que o domínio consultado suporta DNSSEC. Isto é, são uma indicação de que o ISP em questão fornece um serviço de *resolving* aos seus clientes que suporta a verificação dos certificados DNSSEC.

Na análise dos dados apresentados é necessário ter em atenção que nem sempre são os *resolvers* do fornecedor que são utilizados pelos utilizadores finais ligados ao mesmo AS. Nos fornecedores com clientes que são predominantemente empresas

ou universidades, estas implementam directamente os seus *resolvers* e o facto de a percentagem ser baixa, pode ser explicado porque os clientes do fornecedor têm *resolvers* que não fazem a verificação. Por exemplo, o AS MEO EMPRESAS tem uma percentagem bastante inferior ao AS MEO RESIDENCIAL, mas é provável que ambos usem *resolvers* parametrizados de forma semelhante, no entanto, é mais provável que os clientes do AS MEO EMPRESAS utilizem os seus próprios *resolvers*. Razões do mesmo tipo explicam provavelmente os números obtidos para o AS RCCN FCT, I.P, fornecedor de conectividade às entidades do sistema de ensino superior e de investigação.

7.2 Estimativa da adesão dos operadores portugueses às normas RPKI

O protocolo BGP não comporta na sua definição mecanismos de segurança contra a introdução de anúncios e rotas falsas. Um mecanismo, complementar ao BGP, mas externo a este, que foi posteriormente introduzido para ajudar a prevenir alguns dos mais comuns ataques deste tipo é designado RPKI, ver o RFC 6840 [15] e seguintes de 2013.

A infraestrutura RPKI propaga certificados de origem das rotas chamados ROAs (RFC 6811 - BGP Prefix Origin Validation [16]). Estes certificados permitem a um AS verificar que outro AS pode ser o AS origem de uma rota que conduz a um dado conjunto de endereços IP. A RPKI permite emitir, obter e validar estes certificados.

Através de ROAs é possível um AS analisar uma rota recebida de um *vizinho BGP*, e validar a origem da mesma, isto é, verificar que a rota tem início num AS que está certificado para poder ser origem e destino de pacotes com os endereços incluídos na rota. Este mecanismo permite uma primeira barreira contra a introdução de rotas falsas com o objectivo de capturar tráfego pertencente a outros (BGP *route hijacking*).

Apesar de o mecanismo ter sido definido há cerca de 7 anos, só desde os anos de 2019/2020 é que uma percentagem significativa de ASs começaram a emitir e publicar via a RPKI os seus ROAs. No entanto, a percentagem de ASs que os utiliza para bloquear rotas falsas ainda é relativamente baixa.

As Tabelas 7.4 e 7.5 mostram, respectivamente, a percentagem de rotas contendo falsos ROAs que não são aceites pelos ASs, respectivamente por continente e por AS em Portugal, no início de Abril de 2021 segundo os APNIC Labs. Na verdade, este quadro não significa que o AS em questão esteja já a implementar o bloqueio dinâmico de anúncios de rotas com ROA falso ou sem ROA. Esse bloqueio pode

estar a ser assegurado por um outro AS que já implementa o bloqueio e que actua como fornecedor de conectividade para os ASs listados.

Tabela 7.4: Estimativa preliminar por continente da % de filtragem pelos ASs de rotas para uma rede cujo ROA é falso ou inexistente - dados do observatório APNIC Labs, obtidos no início de Abril de 2021

Code	Region	I-RoV Filtering	Samples	Weight	Weighted Samples
XA	World	14.76%	47,653,316	1	47,653,316
XF	Oceania	28.65%	179.013	1.92	343.656
XB	Africa	23.53%	3,747,097	1.25	4,673,722
XC	Americas	18.40%	11,431,511	0.74	8,498,444
XD	Asia	12.48%	23,346,107	1.16	27,117,453
XE	Europe	12.09%	8,949,530	0.78	7,018,999
XG	Unclassified	3.45%	58	1	58

Com efeito, verifica-se que os pequenos ASs que dependem de um único outro AS para se ligarem à Internet, apresentam por vezes, nestas medidas, uma taxa de sucesso de 100% nas filtragens se o AS de quem dependem já implementa ele próprio a filtragem. Os números da figura podem, por esta razão, ser demasiado optimistas.

Em conversa com os técnicos de diversos dos ASs listados foi possível confirmar que apesar de estes apresentarem uma taxa de filtragem superior a 0%, o AS propriamente dito não implementa ainda nenhum bloqueio, apenas publica os seus ROAs.

Tabela 7.5: Estimativa preliminar da % de filtragem pelos ASs com sede em Portugal de rotas para uma rede cujo ROAs é falso ou inexistente - dados do observatório APNIC Labs, no início de Abril de 2021

ASN	AS Name	RPKI Validates	Samples
AS199155	REDE-MEC	100.00%	71
AS1930	RCCN FCT, I.P.	88.94%	199
AS2860	NOS_COMUNICACOES	25.01%	77.261

Continuação da Tabela 7.5

ASN	AS Name	RPKI Validates	Samples
AS15457	NOS_MADEIRA	19.07%	3.581
AS42580	CABOTVA	17.15%	1.685
AS204094	I4W	10.53%	152
AS24768	ALMOUROLTEC	9.09%	66
AS9186	ONI Lisbon, Portugal.	4.46%	112
AS203020	HOSTROYALE	4.27%	164
AS15525	MEO-EMPRESAS	3.56%	1.293
AS37645	ZAP-Angola	3.49%	86
AS3243	MEO-RESIDENCIAL	1.71%	70.347
AS13156	AS13156 Palmela	1.41%	5.808
AS42863	MEO-MOVEL	0.95%	8.497
AS12353	Vodafone Portugal	0.75%	48.923
AS47202	LAZER	0.00%	55
AS702	UUNET	0	3
AS5626	ONI ISP	0	31
AS8220	COLT	0	23
AS8426	CLARANET-AS	0	4
AS12926	ARTELECOMPT	0	18
AS13335	CLOUDFLARENET	0	11
AS14618	AMAZON-AES	0	8
AS15169	GOOGLE	0	3
AS16276	OVH	0	3
AS28998	MONTEPIO-GERAL Portugal	0	3
AS29003	REFERTELECOM-AS	0	19
AS29286	SKYLOGIC-AS	0	6
AS29615	PORTODIGITAL-AS	0	25
AS33876	FLESK-AS	0	3
AS34873	IGIF-AS	0	2
AS35822	CEGER-AS	0	3
AS42831	UKSERVERS-AS UK	0	5
AS43064	TEIXEIRAEDUARTE-AS	0	3
AS43643	TAP-AS TAP Air Portugal	0	10

Continuação da Tabela 7.5

ASN	AS Name	RPKI Validates	Samples
AS43887	MJ-PT-AS	0	19
AS44444	FORCEPOINT-CLOUD-AS	0	7
AS47674	NETSOLUTIONS	0	4
AS49260	UNITELDATA	0	13
AS49349	DOTSI	0	3
AS51171	VALICOM-AS	0	5
AS197802	UTIS-AS	0	23
AS201170	ANA-AS	0	8
AS201523	EDP-AS	0	8
AS202170	BLU-AS	0	25
AS203724	MCAFEE-ENG-PDB	0	8
AS204287	HOSTROYALE_TECH.	0	7

8 Como melhorar

Existem diversos guias que permitem aos gestores de serviço web e de correio electrónico introduzirem melhorias na forma como os seus servidores implementam as normas de segurança (e não só). O mesmo se aplica ao IPv6, ao DNSSEC e às normas RPKI.

Entre esses diversos guias disponíveis encontram-se os a seguir referidos.

8.1 Servidores HTTP

ISOC

O projecto OSE da ISOC mantém uma *knowledge base* no repositório GitHub:

`https://github.com/internetsociety/ose-documentation`

com informação sobre como parametrizar alguns dos servidores HTTP mais conhecidos de forma a obterem a classificação 100% nos testes Internet.nl.

Mozilla Foundation

Na página `https://ssl-config.mozilla.org` é disponibilizado um gerador de configurações do software de uma grande quantidade de servidores HTTP distintos, incluindo a geração de configurações com diversos níveis de segurança.

Internet.nl

Este projecto mantém uma *knowledge base* sobre HTTPS e outras facetas da segurança dos *sites web*, acessível em

`https://Internet.nl/faqs/https` e
`https://internet.nl/faqs/appsecpriv`

com bastante informação sobre as normas de segurança e de como as implementar.

8.2 Servidores e serviços de correio electrónico

Internet.nl

O repositório GitHub do projecto Internet.nl

`https://github.com/internetstandards/toolbox-wiki`

tem vários *howtos*, nomeadamente, sobre a parametrização de servidores de correio electrónico seguros e sobre como parametrizar o domínio do DNS para a introdução de registos DMARC, DKIM e SPF. A página `https://internet.nl/faqs/mailauth` tem muita informação complementar sobre estes registos.

Centro Nacional de Ciber Segurança de Portugal (CNCS)

O CNCS fornece as seguintes recomendações sobre o serviço de correio electrónico e os registos DMARC, DKIM e SPF que merecem igualmente referência:

`https://www.cncs.gov.pt/content/files/cncs_rt0119_spf_dkim_dmarc.pdf`
`https://www.cncs.gov.pt/content/files/recomendao_tcnica_0120.pdf`

8.3 Servidores DNS seguros — DNSSEC

Associação DNS.PT

A associação DNS.PT disponibiliza uma página com informação sobre DNSSEC

`https://www.dns.pt/pt/seguranca/dnssec`

na qual existem bastantes indicações e um apontador para um tutorial.

Internet.nl

A FAQ do *site web* Internet.nl sobre DNSSEC tem informação sobre este tema, com uma ênfase na importância da sua adopção e menos em indicações práticas.

`https://internet.nl/faqs/dnssec`

8.4 IPv6

ISOC

A introdução de IPv6 é sobretudo um esforço que depende dos operadores e das empresas de serviços e menos dos utilizadores. A página da ISOC dedicada ao IPv6 para operadores é um bom ponto de partida:

`https://www.internetsociety.org/deploy360/network-operators/ipv6`

Internet.nl

A FAQ do *site web* Internet.nl sobre IPv6 tem também imensa informação sobre este tema incluindo referência para diversos observatórios.

`https://internet.nl/faqs/ipv6`

8.5 Resource Public Key Infrastructure — RPKI

MANRS

Uma das principais fontes de informação e formação sobre segurança do encaminhamento BGP é o projecto MANRS apoiado pela Internet Society. Consultar

`https://www.manrs.org`

em particular a secção 4 das recomendações MANRS e as recomendações do IETF [17].

IRRs

Todas as IRR mantém informação detalhada de forma actualizada sobre a utilização da RPKI, tal também é o caso do RIPE NCC. Consultar

`https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/what-is-rpki`

9 Conclusões

Este documento apresenta um relatório preliminar do Projecto OSSE - uma iniciativa do Capítulo Português da Internet Society (ISOC.PT) que tem como objectivo observar o estado de adopção de normas de segurança do ponto de vista da presença na Internet de diferentes instituições e empresas portuguesas. Neste contexto, a observação é focada: (1) na análise da implementação de normas de segurança pelos servidores web (servidores HTTP); (2) na análise do grau de penetração de normas de segurança nos servidores de correio electrónico (servidores SMTP) das instituições observadas; (3) na análise da contribuição para a segurança da Internet portuguesa de algumas empresas relevantes que actuam em Portugal como fornecedores de serviços de *web hosting*; e (4) na análise da contribuição dos ISPs portugueses para a disponibilização de suporte IPv6, das normas DNSSEC e das normas associadas às boas práticas de encaminhamento seguro, nomeadamente, o progresso da adesão às normas baseadas na RPKI.

O diagnóstico resultante e o referencial suportado pela plataforma de software do observatório OSSE permite uma análise criteriosa com observações detalhadas do estado de segurança da adopção das normas e melhores práticas de segurança com vista a uma Internet mais segura e confiável para todos os utilizadores. A partir do diagnóstico e observações de detalhe, o observatório OSSE permite formular um conjunto de recomendações que teriam um impacto decisivo na melhoria das métricas e práticas de segurança observadas.

Os resultados e observações apresentadas no relatório privilegiam a apresentação de resultados agregados. Não obstante, as observações realizadas permitiriam obter observações agregadas por sector, permitindo análises comparativas entre os diferentes sectores. Isso poderia ajudar a progressos sectoriais, dado que permitiria destacar esforços sectoriais, que de outra forma ficariam diluídos no conjunto.

Segue-se a exposição das conclusões gerais resultantes da actual observação OSSE que decorrem dos resultados apresentados no relatório completo.

9.1 Servidores HTTPS e sua parametrização

É possível, e necessário, melhorar significativamente a base de segurança da utilização da Internet e da exposição web em Portugal. Isso evitaria que várias organizações exponham "uma imagem menos interessante" ou apresentem "uma presença deficiente e mais vulnerável".

Dificilmente se encontram entidades que consigam atingir classificações superiores a 80 na escala usada, que vai de 0 a 100. A maioria das entidades observadas ficam classificadas de forma intermédia (próximo de 50) nessa escala. Por outro lado verifica-se que existem algumas instituições e sectores com fragilidades muito acentuadas, seja porque exibem grande vulnerabilidade no suporte HTTPS, ou porque nem sequer adoptam HTTPS.

Nesta vertente, as seguintes acções parecem ser necessárias.

1. Promoção de uma gestão com um controlo mais fino e mais rigoroso dos parâmetros de segurança TLS e da criptografia "ponto-a-ponto" que lhe está subjacente. Em particular o abandono imediato das versões *deprecated* de TLS, ou seja, abandono de TLS1.0 e TLS1.1 [11] e transição de TLS1.2 para TLS1.3.

2. O reforço da utilização dos *headers* de segurança HTTP e do suporte DANE, em articulação com adopção de DNSSEC.

3. Particular atenção deve prestada à inclusão do suporte de HSTS e de OCSP *Stappling*.

Estas acções permitiriam obter uma base mais sólida para a segurança dos serviços e aplicações web, com melhores defesas e mitigação das vulnerabilidades passíveis de serem articuladas com outros vectores de ataques à web portuguesa, bem como corrigir, a curto prazo, as deficiências muito gritantes que se verificam em alguns sectores.

9.2 Servidores de correio electrónico e sua parametrização

A observação do estado da segurança do eco-sistema de correio electrónico em Portugal revela resultados bastante deficientes e necessidade de correcções significativas. Na maior parte das entidades observadas, as classificações, novamente numa escala de 0 a 100, são francamente insuficientes (em geral abaixo de 50 e em grande parte abaixo de 30).

Embora o trabalho futuro a ser desenvolvido no observatório deva abarcar uma análise progressivamente mais fina de todo este eco-sistema, algumas conclusões resultam imediatamente da observação realizada, nomeadamente:

1. A reduzida penetração DNSSEC nos domínios associados aos endereços do correio. Tal tem um impacto significativo na segurança da informação anti *phishing* registada nos domínios DNS relevantes.

2. A não conformidade ou a incompletude do suporte ao correio electrónico seguro, nomeadamente a introdução no DNS dos registos: DKIM, DMARC e SPF, e a necessidade da introdução de transporte seguro do correio através do suporte de START/TLS nos servidores SMTP.

Estando o eco-sistema de correio electrónico particularmente associado a vectores de ataque com grande relevância actual, o reforço das práticas de segurança listadas acima e a adopção das respectivas normas, não constituindo por si só a panaceia para a globalidade desses ataques, poderia, no entanto, constituir uma importante base comum de incremento de garantias de segurança, associadas a outras, necessárias, medidas complementares.

9.3 Empresas de web *hosting*

Os chamados *web hosters* podem contribuir de forma muito significativa para o aumento da segurança da Internet portuguesa dado o impacto que as normas que adoptam têm em todo o tecido dos seus clientes, constituído essencialmente por empresas de pequena ou média dimensão.

Estes prestadores de serviços devem consolidar uma rede de segurança capaz de evitar a adopção dos serviços que prestam a partir de operadores internacionais, o que pode ser um aspecto relevante na responsabilidade e base de jurisdição desse tipo de suporte, equilibrando a desintermediação no sector e as consequentes dificuldades

que por vezes daí decorrem. Este aspecto poderá ser particularmente relevante de acautelar na estratégia de *hosting* de serviços públicos ou de entidades do Estado, incluindo as questões que decorrem da certificação digital X509 não intermediada ou gerida em Portugal.

Dado o impacto destes prestadores de serviços na transição digital de muitas organizações, e na promoção de uma economia digital, este sector poderá justificar uma intervenção específica.

As observações realizadas mostram que alguns destes prestadores de serviços já fizeram um trabalho que se reflecte em propriedades de segurança mais elevadas da sua oferta de serviços. Outros, no entanto, apresentam limitações na sua oferta que deveriam ser ultrapassadas. É importante caminhar-se para um maior comprometimento e valorização dos fornecedores com uma oferta de soluções mais seguras, através das seguintes ações:

1. Abandono imediato de TLS 1.0 e TLS 1.1 e de *Secure Socket Layer* (SSL) e fomento da migração gradual de TLS 1.2 para TLS 1.3, logo que possível.

2. Reforço do suporte de HSTS e de OCSP *Stappling* e melhoria do suporte dos *headers* HTTP de segurança.

3. Imediata disponibilidade de DNSSEC e suporte de DANE e disponibilidade progressiva de IPv6.

4. Melhoria significativa do serviço de correio electrónico oferecido, nomeadamente através da introdução no DNS dos registos: DKIM, DMARC e SPF, e a necessidade da introdução de transporte seguro do correio através do suporte de START/TLS nos servidores SMTP.

9.4 ISPs portugueses

Os ISPs deverão continuar a reforçar a oferta de *resolvers* com suporte de DNSSEC e adoptarem de forma vigorosa o conjunto de boas práticas de encaminhamento recomendadas pela iniciativa MANRS (manrs.org). Neste campo a situação parece ser caracterizada por um progressivo alastramento do registo de ROAs, mas uma adopção tímida de filtragem com base na infraestrutura RPKI.

Infelizmente, ao que parece, ainda nenhum ISP comercial português adoptou a prática de exibir o selo de qualidade MANRS, dado o não comprometimento oficial com a iniciativa.

Finalmente, os esforços para disponibilizar endereçamento e conectividade IPv6 necessitam de uma adesão mais vigorosa dos ISPs que já o fazem, e de que os restantes se decidam a avançar com essa oferta.

9.5 Sobre a visibilidade, reconhecimento e compromisso com a segurança da Internet em Portugal

É necessário promover uma maior visibilidade e reconhecimento pelas empresas prestadoras de serviços de *web hosting* e pelos ISPs das características de segurança dos serviços que providenciam, e é também necessário levar a que os clientes valorizem esses esforços, descartando os fornecedores que os ignorem, de modo a que os esforços de incremento da base de segurança da Internet em Portugal sejam recompensados.

Esta frente, que tem sido acautelada em muitos países através da colaboração de diferentes entidades, com diferentes papéis, exige uma abordagem colaborativa. Este parece continuar a ser um terreno que precisa de ser percorrido com mais entusiasmo, envolvimento e compromisso, para lá das iniciativas localizadas, por vezes orientada para resultados mais limitados no alcance e na efectividade.

A nossa esperança e desejo é que o observatório OSSE contribua, ainda que modestamente, e mais pelo exemplo, para que se caminhe para a criação de condições de valorização de uma **"economia da segurança"** e, consequentemente, de uma maior exigência por parte dos consumidores. A divulgação de métricas de compromisso por parte de entidades prestadoras de serviços para a melhoria da situação actual, o reconhecimento da diferenciação da qualidade da oferta de serviços por parte dos *players* envolvidos, o estabelecimento de quadros de colaboração e parceria *"multi-stakeholder"* para o reforço das práticas de segurança e o aumento progressivo da exigência dos consumidores, são outras tantas vias para a promoção do nível de segurança da Internet portuguesa.

As entidades de regulação e o sector público podem desempenhar um importante papel através de uma intervenção, primeiro pedagógica, e depois de carácter regulatório. O usufruto das vantagens da transição digital só pode ter lugar num quadro de garantias de segurança a todos os níveis para os utilizadores e empresas. Caso contrário, não é expectável senão um incremento dos inevitáveis problemas que essa transição acarreta, e um decréscimo significativo das vantagens que potencia.

Bibliografia

[1] R. Fielding (Ed.) and J. Reschke (Ed.), "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing." RFC 7230 (Proposed Standard), June 2014. Updated by RFC 8615.

[2] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3." RFC 8446 (Proposed Standard), Aug. 2018.

[3] J. Klensin, "Simple Mail Transfer Protocol." RFC 5321 (Draft Standard), Oct. 2008. Updated by RFC 7504.

[4] D. Margolis, M. Risher, B. Ramakrishnan, A. Brotman, and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)." RFC 8461 (Proposed Standard), Sept. 2018.

[5] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification." RFC 8200 (Internet Standard), July 2017.

[6] P. Hoffman, A. Sullivan, and K. Fujiwara, "DNS Terminology." RFC 8499 (Best Current Practice), Jan. 2019.

[7] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements." RFC 4033 (Proposed Standard), Mar. 2005. Updated by RFCs 6014, 6840.

[8] G. Huston, G. Michaelson, C. Martinez, T. Bruijnzeels, A. Newton, and D. Shaw, "Resource Public Key Infrastructure (RPKI) Validation Reconsidered." RFC 8360 (Proposed Standard), Apr. 2018.

[9] R. Bush, R. Volk, and J. Heitz, "Resource Public Key Infrastructure (RPKI) Origin Validation for BGP Export." RFC 8893 (Proposed Standard), Sept. 2020.

[10] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280 (Proposed Standard), May 2008. Updated by RFCs 6818, 8398, 8399.

[11] K. Moriarty and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1." RFC 8996 (Best Current Practice), Mar. 2021.

[12] V. L. Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," *Proceedings 2019 Network and Distributed System Security Symposium*, 2019. arXiv: 1806.01156.

[13] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol Extensions for BGP-4." RFC 2283 (Proposed Standard), Feb. 1998. Obsoleted by RFC 2858.

[14] Y. Rekhter (Ed.), T. Li (Ed.), and S. Hares (Ed.), "A Border Gateway Protocol 4 (BGP-4)." RFC 4271 (Draft Standard), Jan. 2006. Updated by RFCs 6286, 6608, 6793, 7606, 7607, 7705, 8212, 8654.

[15] S. Weiler (Ed.) and D. Blacka (Ed.), "Clarifications and Implementation Notes for DNS Security (DNSSEC)." RFC 6840 (Proposed Standard), Feb. 2013. Updated by RFC 8749.

[16] P. Mohapatra, J. Scudder, D. Ward, R. Bush, and R. Austein, "BGP Prefix Origin Validation." RFC 6811 (Proposed Standard), Jan. 2013. Updated by RFCs 8481, 8893.

[17] R. Bush, "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)." RFC 7115 (Best Current Practice), Jan. 2014.

Lista de Tabelas

Siglas usadas

APNIC *Asia Pacific Network Information Centre*

AS *Automomous System*

BGP *Border Gateway Protocol*

ccTLD *country code Top-Level Domain*

CNCS Centro Nacional de Ciber Segurança de Portugal

DANE *DNS-Based Authentication of Named Entities*

DNS *Domain Name Service*

DNSSEC *Domain Name System Security Extensions*

DKIM *DomainKeys Identified Mail*

DMARC *Domain-based Message Authentication, Reporting and Conformance*

HSTS HTTP Strict Transport Security

HTTP *Hyper Text Transfer Protocol*

HTTPS *Hyper Text Transfer Protocol Secure*

IETF *Internet Engineering Task Force*

IPv4 *Internet Protocol Version 4*

IPv6 *Internet Protocol Version 6*

IRR *Internet Regional Registry*

ISOC *Internet Society*

ISOC PT Capítulo Português da *Internet Society*

ISP *Internet Service Provider*

MANRS *Mutually Agreed Norms for Routing Security*

OCSP *Online Certificate Status Protocol*

OSE *Open Standards Everywhere*

OSSE *Open Security Standards Everywhere*

ROA *BGP Route Origination Authorization*

RPKI *Resource Public Key Infrastructure*

SMTP *Simple Mail Transfer Protocol*

START/TLS *SMTP will be executed over TLS/SSL*

SSL *Secure Socket Layer*

SPF *Sender Policy Framework*

TLS *Transport Layer Security*