1º Relatório Do Projeto Open Security Standards Everywhere (OSSE)

1º Relatório do Projeto Open Security Standards Everywhere (OSSE)

O Capítulo Português da Internet Society acabou de publicar o Primeiro **Diagnóstico do Estado da Adopção de Normas de Segurança na Internet Portuguesa** que dá uma panorâmica do progresso de adopção dessas normas, definidas pela IETF (Internet Engineering Task Force), por diversos sectores da Internet portuguesa, nomeadamente:

- Como as empresas de suporte a serviço de hosting (hosters) suportam essas normas;
- Qual o grau de segurança dos 100 sites mais populares em Portugal (Lista Alexa Top 100 Portugal);
- De que forma cerca de 1000 sites dos mais diversos sectores de actividade, desde os sites do Governo, de instituições públicas e do sector privado (Lista Portugal 1000), estão do ponto de vista da segurança;
- Como os ISPs portugueses contribuem para a adopção de IPv6, o uso de DNSSEC e como implementam as normas ROA, ROV e RPKI para suporte da segurança do routing.

Workshop de apresentação pública do relatório – Dia 19 de Maio de 2021 pelas 17h00

Zoom Meeting: https://us02web.zoom.us/j/83104384395?pwd=KytUWnNOQUZ4RVNpd1MwMXl5VjBkdz09

Meeting ID: 831 0438 4395
Passcode: 143751

Obtenha o Relatório "Diagnóstico do Estado de Adopção de Normas de Segurança na Internet Portuguesa – 30/4/2021 em pdf

Com o apoio da

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 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 ISP 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 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 ferramentas 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 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 TLS, o DNSSEC não é necessário. Antes pelo contrário, dada a a tendência actual de usar o DNS para publicar informações de segurança para os servidores HTTP e SMTP, através das entradas DANE, SPF, DKIM e 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 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 OCSP e 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 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 SPF, DKIM e DMARC. 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 ISP 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 ISPs 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 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.

Referências na imprensa

Expresso Online em 5/5/2021

Associação ISOC Portugal Chapter

Departamento de Informática, Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa
Campus da Caparica
2829-516 Monte da Caparica Portugal

secretariado at isoc.pt
direcao at isoc.pt

Copyright © 2021 ISOC.PT. Todos os direitos reservados.
Screenr parallax theme por FameThemes