Recursos sobre segurança criptográfica

Internet Society

7 de Outubro de 2021

Recursos sobre segurança criptográfica

Pergunta 1: quais as aplicações de mensagens que suportam criptografia extremo a extremo?

- **Resposta 1:** ver aqui https://getstream.io/blog/most-secure-messaging-apps
- **Resposta 2 ou aqui:** https://www.tomsguide.com/reference/best-encrypted-messaging-apps
- **Resposta 3 ou ainda aqui:** https://www.eff.org/deeplinks/2018/03/why-we-cant-give-you-recommendation

Pergunta 2: os sites a que eu acedo suportam acessos seguros (TLS)?

- **Resposta: p**ara que tráfego entre o seu browser e um site esteja protegido criptograficamente, é necessário que o mesmo suporte **TLS (Transport Layer Security)** com uma implementação de acordo com as melhores práticas recomendadas. Para começar, é necessário que o URL do site seja da forma **https://domain-name** e não **http://domain-name**. Também é conveniente que o nome de domínio do site seja autenticado através de **DNSSEC (Domain Name Security Extensions)**. Para além disso é conveniente que os gestores do site adoptem as melhores práticas de segurança do mesmo.

Pergunta 3: como posso saber se os sites a que acedo suportam segurança criptográfica de forma adequada?

- **Resposta:** teste esse site através de um dos sistemas de testes disponíveis.

Quais são eles?

- **Resposta: https://internet.nl** (acesso livre) – este sistema de testes faz testes profundos e dá explicações completas sobre o que está bem e o que tem de ser melhorado. Existem outros sistemas de testes como por exemplo **https://webcheck.pt** (acesso livre), **https://www.ssllabs.com/ssltest** (acesso livre) e **https://observatory.mozilla.org** (acesso livre).

Pergunta 4: qual é a versão de TLS que atualmente é recomendada?

- **Resposta:** consulte **este documento do IETF** e também esta explicação sobre porque é **perigoso usar TLS 1.0 ou TLS 1.1.**

Pergunta 5: se eu necessitar de informação sobre como melhorar o meu site onde me posso dirigir?

- **Resposta:** esta documentação da Internet Society ajuda a atingir esse objetivo.

Pergunta 6: qual o atual grau de adesão a segurança criptográfica na web mundial?

- **Resposta**: **este site do W3** permite ter uma visão do grau de adopção do HTTPS, assim como sobre as **tendências de utilização** de outras tecnologias, eventualmente recomendadas, para a implementação dos sites. O site da **Let's Encrypt** fornece igualmente alguns dados interessantes, nomeadamente os obtidos através do observatório Mozilla.

Pergunta 7: qual a situação em Portugal?

- **Resposta:** o Capítulo Português da Internet Society elaborou um **Diagnóstico da situação da segurança da Internet Portuguesa em Maio de 2021.** No mesmo são fornecidos dados muito detalhados da situação. O site **Why No HTTPS** apresenta os Top-100 mais populares sites no mundo que infelizmente **NÃO SUPORTAM HTTPS**. O mesmo site também permite obter uma visão da situação país a país. Aqui está **a visão deles sobre Portugal**. Caso decida contactar algum desses sites a reclamar, teste-o primeiro com as ferramentas indicadas na resposta à pergunta 3 acima.