Ficha para decisores políticos: 6 razões pelas quais o "acesso por vias legais" a informações cifradas compromete a segurança

O que é a criptografia?

A **criptografia** é um processo de ocultação de informações, utilizando cifras, para que essas informações só possam ser lidas por alguém que possua a chave certa. **A cifra extremo a extremo (E2E) fornece um nível mais elevado de segurança e confiabilidade**, dado que só o destinatário final tem a chave certa para decifrar a mensagem.

As tecnologias criptográficas são ferramentas que ajudam as pessoas a estarem seguras online, pois protegem a integridade e a privacidade dos seus dados e das comunicações digitais. Elas permitem proteger a navegação na web, os serviços de *homebanking* e serviços públicos críticos, como por exemplo as redes elétricas, eleições, hospitais e transportes, e os cidadãos que deles dependem. Em 2018, mais de 1700 milhões de utilizadores usaram serviços de mensagens cifradas E2E para proteger as suas comunicações.[1]

Alguns governos temem que a criptografia torne mais difícil a recolha de informações para prevenir ou punir terroristas e criminosos. Estes governos foram céleres na aprovação de **legislação de "autorização de acesso por vias legais"** para dar às autoridades o poder de acederem e intercetarem comunicações cifradas, ou exigir que empresas o façam por elas. **Estas medidas colocam em risco todos os indivíduos que se encontram ligados online.**

Embora se argumente frequentemente que esta legislação não afetará a criptografia propriamente dita, pois, em vez disso, baseia-se noutras formas de acesso, a segurança dos utilizadores estará sempre em risco. Qualquer ponto de entrada ou de enfraquecimento dum serviço seguro constitui sempre uma fragilidade de segurança.

As medidas de "autorização de acesso por vias legais" enfraquecem a segurança da Internet e põem em perigo, não apenas a economia global, mas também os serviços essenciais dos quais dependemos, e adicionalmente a vida de todos os cidadãos em situações de fragilidade. A saber:

1. **Fragilidades obrigatórias enfraquecem-nos a todos**: não há nenhuma fechadura digital que só pode ser aberta pelos "bons", mas não pelos "maus". Fechaduras

[1] https://telegram.org/blog/200-million; https://techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad/

de "autorização de acesso por vias legais" tornarão mais fácil a outros, como por exemplo criminosos e governos hostis, obter acesso a dados confidenciais.

2. **A segurança nacional e individual estarão em risco**: ao diminuírem a segurança de informações pessoais e corporativas, de dados bancários e de informações governamentais, medidas de "autorização de acesso por vias legais" podem facilitar involuntariamente a espionagem, o roubo de identidade, chantagem, manipulação de mercados e muito mais.

3. **Os terroristas encontrarão novas alternativas**: se terroristas e criminosos souberem que as suas mensagens serão acedidas pelas autoridades, de certeza que passarão a usar alternativas próprias. Desta forma, as comunicações dos criminosos vão continuar ocultas, enquanto as dos utilizadores comuns se tornarão vulneráveis.

4. **Vidas em perigo**: comunicações cifradas E2E protegem a identidade de jornalistas, ativistas, testemunhas protegidas, autoridades camufladas e muitas outras pessoas em perigo. A vulnerabilidade das comunicações coloca as suas vidas em risco.

5. **Riscos acrescidos para as infraestruturas da Internet**: as medidas de "autorização de acesso por vias legais" ameaçam os principais componentes de segurança da infraestrutura da Internet, nomeadamente os mecanismos de autenticação, que são críticos para a nossa segurança.

6. **Impacto no comércio e no investimento**: as medidas de "autorização de acesso por vias legais" podem afetar significativamente a economia global. Para a maioria das empresas multinacionais, uma parte significativa da sua faturação e crescimento potencial é gerada em mercados emergentes. No entanto, os consumidores podem ter relutância em comprar produtos ou usar serviços de países cujos governos têm a capacidade de aceder às suas informações e comunicações privadas.

Cada país tem o direito e o dever de proteger os seus cidadãos. Contudo, as tentativas precipitadas de facilitar o acesso a dados cifrados, mesmo as bem-intencionadas, representam um grande risco para a segurança dos cidadãos cumpridores da lei e para a Internet em geral, ao mesmo tempo que não resolvem o problema que motivou a sua introdução.

Não eliminem os meios mais poderosas que servem para nos proteger, para proteger os nossos países, e as nossas economias. Expliquem aos líderes mundiais que devem apoiar o uso de criptografia forte por todos.