Criptografia Global Sob Ameaça
Criptografia Para Todos

Junho 2020

Criptografia Global Sob Ameaça

Os criminosos também podem usar criptografia. Algumas autoridades estão preocupadas que a criptografia as impeça de obter os elementos probatórios ou informações que necessitam. Para resolver essas preocupações, alguns governos estão a tentar fazer com que as empresas lhes criem maneiras de aceder ao conteúdo cifrado pelos sistemas das empresas (uma prática conhecida por "acesso excecional").

Independentemente do método, não existe acesso “excecional”. Os criminosos poderiam descobrir e usar a mesma maneira de aceder.

Como as Forças Policiais Planeiam Aceder Aos Nossos Dados?

A autoridades têm proposto várias formas de se obter o “acesso excecional” aos dados cifrados. Estas incluem:

- **Um *backdoor* criptográfico**, que é uma alteração num protocolo, aplicação ou serviço de criptografia que supostamente permitirá o acesso autorizado de terceiros a dados cifrados. Uma das formas de o fazer é enfraquecendo os mecanismos criptográficos ou os sistemas que os suportam.
    - **O problema:** os *backdoors* podem ser abertos por qualquer pessoa que os descubra.
- **Custódia de chaves (*key escrow*)**, quando as chaves de decifração são guardadas sob a custódia de uma terceira entidade de confiança para uso posterior pelas forças policiais.

- **O problema:** as chaves podem ser perdidas, copiadas ou roubadas.

Se as Autoridades Podem Aceder Aos Nossos Dados, Quem Mais Também o Pode Fazer?

Os especialistas em segurança da informação concordam que, embora os *backdoors* e os principais sistemas de custódia de chaves facilitem o acesso das autoridades aos dados cifrados, também facilitam o acesso de terceiros, tais como criminosos.

Os backdoors podem ser abertos por qualquer pessoa que os encontrar.
As chaves podem ser perdidas, copiadas ou roubadas.

Pelo Menos Apanhávamos os Maus da Fita, Certo?

Infelizmente, não.

Os especialistas concordam que é improvável que o acesso excecional impeça os criminosos de comunicar secretamente.

- Mesmo que a criptografia sem acesso excecional fosse ilegal, os criminosos ainda poderiam encontrar ferramentas no mercado negro ou criar suas próprias ferramentas.

- Os utilizadores comuns que cumprem a lei podiam ficar vulneráveis a criminosos que tenham descoberto como explorar sistemas de acesso excecional.

O acesso excecional coloca a pessoa comum em maior risco, sem contudo resolver o problema que pretendia corrigir!