Carta aberta aos líderes de governos do mundo

Access Now

Data da publicação:

Outubro de 2016

Esta carta é uma iniciativa da organização não-governamental Access Now, que atua em defesa dos direitos digitais ao redor do mundo e desde janeiro de 2016 está sendo enviada para líderes de diversos países que discutem legislações ou outras medidas que podem minar o uso da criptografia. Além de fundamentais para a comunicação segura na rede, a criptografia e o anonimato permitem a privacidade necessária para a liberdade de expressão e opinião na era digital, como ressaltou o Relator Especial da ONU para a Liberdade de Expressão, David Kaye. A carta conta com o apoio de mais de 150 organizações ao redor do mundo e já foi enviada para governos de países como Estados Unidos, Reino Unido, Austrália, França e aos membros da União Europeia. Ela segue aberta para adesão em https://www.SecureTheInternet.org

Exortamos as senhoras e senhores a proteger a segurança de seus cidadãos, sua economia e seu governo, apoiando o desenvolvimento e a utilização de ferramentas e tecnologias de comunicações seguras, rejeitando políticas que possam impedir ou prejudicar o uso de criptografia forte e instigando outros líderes a fazerem o mesmo.

Ferramentas, tecnologias e serviços de criptografia são essenciais para proteger nossa infraestrutura digital de comunicações pessoais contra danos e defendê-la de acessos não autorizados. A capacidade de se desenvolver e utilizar criptografia livremente consiste na pedra fundamental para a economia global de hoje. O crescimento econômico na era digital é alimentado pela capacidade de confiar e autenticar nossas interações e de se comunicar e realizar negócios com segurança, dentro e através das fronteiras.

Alguns dos técnicos e especialistas em criptografia mais notáveis do mundo explicaram recentemente que leis ou políticas que minam a criptografia podem “forçar um retrocesso nas melhores práticas implementadas para tornar a Internet mais segura”, “aumentar substancialmente a complexidade do sistema” e os custos associados e “criar alvos concentrados que podem atrair atores maliciosos”1. A ausência de criptografia facilita o acesso a dados pessoais sensíveis, incluindo informações financeiras e de identidade, por parte de criminosos e outros agentes

maliciosos. Uma vez obtidos, esses dados sensíveis podem ser vendidos, expostos publicamente ou utilizados para chantagear ou constranger as vítimas. Além disso, dispositivos ou equipamentos com criptografia frágil são os principais alvos de criminosos.

O Relator Especial das Nações Unidas para a Liberdade de Expressão apontou que “a criptografia, o anonimato e os conceitos de segurança a eles relacionados, oferecem a privacidade e segurança necessárias para o exercício do direito à liberdade de opinião e de expressão na era digital”. Ao avançarmos para conectar o próximo bilhão de usuários, restrições à criptografia em qualquer país provavelmente terão um impacto global. Ferramentas e tecnologias de criptografia ou anonimização permitem que advogados, jornalistas, denunciantes e organizadores comuniquem-se livremente através das fronteiras e trabalhem para melhorar suas comunidades. Elas também garantem aos usuários a integridade de seus dados e autentica indivíduos, empresas e governos.

Encorajamos o apoio à proteção e segurança dos usuários através do fortalecimento da integridade das comunicações e sistemas. Todos os governos devem rejeitar leis, políticas ou outros mandatos ou práticas, incluindo acordos secretos com empresas, que limitem o acesso ou prejudiquem a criptografia e outras ferramentas e tecnologias seguras de comunicação. Os usuários devem ter a opção de usar – e as empresas a opção de fornecer – a criptografia mais forte disponível, incluindo a criptografia fim-a-fim (end-to-end), sem medo de que os governos obrigarão o acesso ao conteúdo, metadados ou chaves de criptografia sem o devido processo e o respeito aos direitos humanos. Assim:

- Governos não devem, de nenhuma maneira, banir ou limitar o acesso do usuário à criptografia ou proibir a aplicação ou uso de criptografia por grau ou tipo;
- Governos não devem tornar obrigatória a concepção ou implementação de backdoors ou vulnerabilidades em ferramentas, tecnologias ou serviços;
- Governos não devem exigir que ferramentas, tecnologias ou serviços sejam concebidos ou desenvolvidos para permitir o acesso de terceiros a chaves de criptografia ou a dados não criptografados;
- Governos não devem tentar enfraquecer ou minar os padrões de criptografia ou influenciar intencionalmente o estabelecimento de padrões de criptografia, exceto para promover um nível mais elevado de segurança da informação. Nenhum governo deve ordenar que algoritmos, padrões, ferramentas ou tecnologias de criptografia sejam inseguros; e
- Governos não devem, seja por acordos privados ou públicos, obrigar ou pressionar qualquer entidade para exercer qualquer atividade que seja incompatível com os princípios acima.

A existência de criptografia forte, assim como de ferramentas e sistemas seguros que se apoiem nela, são fundamentais para aprimorar a segurança no ciberespaço, fomentar a economia digital e proteger os usuários. Nossa capacidade de potencializar o uso da Internet para o crescimento global e prosperidade e como ferramenta para organizadores e ativistas requer a capacidade e o direito de se comunicar de forma privada e segura através de redes confiáveis.
Estamos ansiosos para trabalhar juntos em direção a um futuro mais seguro.

Categoria:

- poliTICs 24