Vulnerabilidade no WhatsApp compromete criptografia das mensagens

POR **CLAUDIO YUGE** | @CLANGCOMIX
EM **WHATSAPP**
13 JAN 2017 — 14H23

Uma vulnerabilidade no **WhatsApp** pode ser usada para interceptar e ler as mensagens criptografadas dos usuários. A brecha de segurança foi encontrada pelo pesquisador Tobias Boelter, da Universidade da Califórnia, e revelada pelo periódico britânico The Guardian.

De acordo com o jornal, a descoberta foi feita no ano passado e comunicada ao **Facebook**, proprietário do comunicador instantâneo, mas nada foi feito para corrigir a falha. Ainda que não admitam a existência do problema, estudos indicam que a rede social e instituições governamentais — ou até mesmo hackers — podem ter acesso a todo o conteúdo que você compartilha por ali.

Como isso acontece?

Em abril do ano passado, o Whatsapp implementou o sigilo com a chamada "criptografia de ponta-a-ponta", que deveria embaralhar as mensagens no começo e decodificar no destino. Assim, o conteúdo não poderia ser interceptado por terceiros e nem mesmo pela própria companhia. As chaves de segurança foram desenvolvidas pela Open Whisper Systems, a partir do protocolo Signal, usado também por outros aplicativos, como o Telegram.

Se o WhatsApp for questionado pelo governo para revelar o registro das mensagens, pode garantir acesso devido a essa mudança de chaves

Em teoria isso impede que qualquer um, até mesmo especialistas, consigam obter informações de sua conta. Porém, a investigação de Boetler mostrou que o serviço de mensagens adaptou o Signal para forçar processos de usuários offline: todas as mensagens não entregues são criptografadas com uma nova chave e enviadas novamente.

Essa recodificação e reenvio de dados permite que as mensagens possam ser interceptadas. "Se o WhatsApp for questionado pelo governo para revelar o registro das mensagens, pode garantir acesso devido a essa mudança de chaves", explica o Boelter.

Resposta do WhatsApp

Questionado pelo The Guardian, um porta-voz da empresa afirmou: "Mais de 1 bilhão de pessoas usam o WhatsApp diariamente, porque ele é simples, rápido, confiável e seguro. Aqui sempre acreditamos que as conversas devem ser privadas e seguras. No ano passado oferecemos a todos os usuários um nível melhor de segurança, fazendo com que toda mensagem, foto, vídeo, arquivo e chamada fossem encriptadas de ponta-a-ponta por padrão. Quando introduzimos esses recursos, focamos em manter o produto simples, considerando como ele é usado diariamente em todo o mundo".

O aplicativo possui uma notificação de segurança (Configurações > Conta > Segurança > Mostrar notificações de segurança) que pode ser acionada para avisar os usuários sobre mudanças em códigos,

principalmente nos casos de troca de aparelho ou reinstalação. “Fazemos isso porque em muitas partes do mundo as pessoas trocam frequentemente de dispositivos e cartões SIM. Nessas situações, queremos ter certeza de que as mensagens não sejam perdidas no caminho.”

Perguntada se o Facebook tem acesso ao conteúdo ou agências governamentais podem obter esses dados, a companhia foi evasiva e afirmou que esses detalhes **estão em uma página a respeito na rede social**.

Mas o WhastApp continua seguro?

Ainda é muito difícil conseguir os dados encriptados do WhatsApp e é preciso especialistas no assunto para tentar burlar o sistema. Contudo, essa brecha levanta novamente a questão de privacidade do cidadão diante do governo.

Recentemente, o Investigatory Powers Act foi aprovado no Reino Unido e permite que o Estado intercepte informações de companhias privadas no caso de suspeita de crimes. Algo parecido com o que a Agência de Segurança Nacional dos Estados Unidos alegou quando o analista de sistemas Edward Snowden revelou um vazamento de dados que deveriam ser sigilosos.

Fato é que o medo de que isso aconteça existe desde que o Facebook adquiriu o WhatsApp, em 2014. Na época, a rede social afirmou que não usaria a mesma política de uso das informações de usuários para explorar publicidade e que manteria a segurança do aplicativo.

Publicada em: *https://www.tecmundo.com.br/whatsapp/113440-vulnerabilidade-whatsapp-compromete-criptografia-mensagens.htm*

WhatsApp vive em guerra com a Justiça brasileira

A privacidade dada aos milhões de usuários do WhatsApp já foi alvo de combate entre o aplicativo e a Justiça brasileira. Por ordem judicial, o serviço de troca de mensagens já foi bloqueado em três oportunidades no país.

A disputa envolve o pedido da Justiça para que o WhatsApp divulgue dados de usuários no aplicativo em processos criminais, por exemplo. A empresa dona do aplicativo se nega a fornecer as informações pedidas pela Justiça com a alegação de que não tem acesso e posteriormente ocorre o bloqueio.

Especialistas de polícia e do Ministério Público alegam que o WhatsApp precisa de mais controle. A questão do bloqueio ou não do aplicativo, ação que prejudica milhões de usuários, é discutido pela Justiça brasileira.

Trecho publicado em: *https://tecnologia.uol.com.br/noticias/redacao/2017/01/13/brecha-no-whatsapp-permite-espiar-mensagens-criptografadas-diz-jornal.htm*

Questões:

1 – Quais processos de segurança empresas de troca de mensagem, como whatsapp, precisam implementar para garantir um bom serviço para seus usuários?

2 – Deixar uma maneira para recuperar as informações, para casos específicos como investigações criminais, não é uma forma de investir em segurança pública, justifique a resposta?

3 – Baseado em suas rotinas, cite problemas de segurança de informação (ao menos um) que vocês tem notado, quais as implicações deste problema e se vocês já pensaram em uma possível solução.