Hoe veilig is WhatsApp nou eigenlijk?

16 maart 2016 16:37

Naast Apple wil het Amerikaanse Ministerie van Justitie nu achter WhatsApp aan. De versleuteling van die app zou namelijk voor problemen zorgen in de opsporing van criminelen. Hoe zat het ook alweer met de beveiliging van WhatsApp? Hoe veilig en anoniem is 's werelds meestgebruikte chat-app eigenlijk?

Slechte resultaten uit het verleden

WhatsApp heeft in het verleden nogal eens beveiligingsproblemen gehad, inclusief accountkapingen en onveilige opslag van berichten. De overname door Facebook heeft de zorgen om privacy vergroot, waarna veel gebruikers leken over te stappen naar het veiliger geachte Telegram. Die beveiligde open source chat-app gebruikt eigen encryptie, waar experts al zo hun twijfels over hadden. Het versleutelen van informatie is namelijk een complex geheel, waarbij zowel de wiskundige ondergrond voor het versleutelingsalgoritme meespeelt als ook de zorgvuldigheid van de ingebruikname daarvan.

De ingebruikname betreft niet eens de inzet door de daadwerkelijke eindgebruiker, maar de manier waarop versleuteling is doorgevoerd in de software. Zoals dus een app voor beveiligde communicatie. Dit heet in ICT-termen de implementatie. Fouten daarin kunnen de gebruikte encryptie - hoe krachtig die wiskundig gezien ook is - ondermijnen.

Zijdeur in plaats van achterdeur

WhatsApp is niet via brute force te kraken

Implementatiefouten of -slordigheden hebben eerder al de Amerikaanse inlichtingendienst NSA veel van zijn kraakwerk laten verrichten. Onmogelijk geachte decodering van versleutelde informatie bleek vaak doenbaar via een 'zijdeur', niet via het bruut kraken van wiskundig goed onderbouwde encryptie. Zijdeuren bestaan in diverse vormen en maten. Een voorbeeld is de categorie van man-in-the-middle aanvallen zoals diepgaand onderzocht en al vaak gedemonstreerd door de beruchte securityhacker Moxie Marlinspike.
Het gevaar van implementatiefouten speelt niet alleen bij relatieve nieuwkomers zoals Telegram, maar ook voor het in 2009 opgerichte WhatsApp. Die chat-app is begin 2014 voor 19 miljard dollar opgekocht door Facebook en heeft later dat jaar end-to-end encryptie ingevoerd. Daarvoor heeft het aangeklopt bij het door Moxie Marlinspike opgerichte Open Whisper Systems, dat open source software voor beveiligde communicatie maakt.

Stapje voor stapje

Whisper is bekend van communicatie-app Signal, die de opvolger is van de beveiligde telefonie-app RedPhone en de beveiligde chat-app Textsecure. WhatsApp heeft laatstgenoemde geïntegreerd, maar eerst alleen in zijn Android-app. Ondersteuning in de iOS-app moet nog volgen. Hierdoor is WhatsApp-communicatie met iPhone-gebruikers dus niet end-to-end beveiligd.

Berichten blijven alleen op WhatsApps servers staan terwijl ze verzonden worden

Vóór de invoering van deze begin-tot-eind versleuteling had het bedrijf de mogelijkheid om berichten in te zien wanneer die door zijn servers werden ontvangen en doorgestuurd. WhatsApps servers bewaren namelijk berichten terwijl ze 'onderweg' zijn van verzender naar ontvanger. Dit is een tijdelijk bewaren; totdat het bericht bezorgd is. Van een ware back-up is dus geen sprake, daarvoor moet een gebruiker zelf andere middelen aanwenden. Telegram daarentegen is puur een clouddienst en bewaart dus niets lokaal.

Vingers in de dijk

Na de invoering van Whisper Systems' end-to-end encryptie leek WhatsApp een stuk veiliger. Begin vorig jaar hebben Duitse onderzoekers echter kwetsbaarheden gevonden in deze beveiliging. Concreet: in de implementatie. Het bleek mogelijk berichten te onderscheppen via een zogeheten man-in-the-middle aanval. Het kernprobleem was volgens de onderzoekers dat het niet duidelijk was wannéér WhatsApp-conversaties echt met end-to-end encryptie zijn beveiligd. Sinds deze maand toont de WhatsApp-app een melding dat berichten op deze manier

zijn beveiligd.

Open source is geen garantie voor veiligheid

Toch is het daarmee niet honderd procent gegarandeerd dat WhatsApp volledig veilig is. De chat-app scoort relatief slecht op het overzicht van de digitale burgerrechtenbeweging EFF. Telegram scoort daar weer beter, hoewel in november experts opnieuw kritiek hadden op dit WhatsApp-alternatief. Het feit dat het open source is, is geen garantie dat het veilig is. Dit is wel aangetoond door recente grote gaten in bekende open source-producten, waaronder ook juist encryptiesoftware. Er blijft werk aan de winkel, wat ook geldt voor een closed source-product als WhatsApp.