NSO muss Quellcode der Spyware Pegasus herausrücken

Die Spionagefirma NSO soll WhatsApp den Quellcode ihrer Software Pegasus übergeben. Das hat der WhatsApp-Konzern Meta vor Gericht erstritten.

WhatsApp konnte vor Gericht einen Erfolg gegen die Spionagefirma NSO verbuchen: Laut den Gerichtsakten muss die israelische NSO Group den Quellcode ihrer Software Pegasus sowie die dafür benötigten Grundlagen von April 2018 bis Mai 2020 an WhatsApp überreichen. NSO soll 2019 über einen Zeitraum von zwei Wochen Server von WhatsApp benutzt haben, um die Spionagesoftware auf über 1400 Geräten von WhatsApp-Nutzern zu installieren. Darunter sollen auch Journalisten, Regierungsbeamte und Menschenrechtsaktivisten gewesen sein.

Die Pegasus-Software nutzte damals eine Lücke in WhatsApp aus (CVE-2019-3568), um den Schadcode auf den Geräten der Opfer zu installieren. Dazu genügte ein Sprachanruf via WhatsApp, die Zielperson musste den Anruf nicht mal annehmen. Weil NSO dafür WhatsApp-Accounts erstellen musste, verstießen sie bei den Angriffen gegen die Regeln von WhatsApp. Deswegen reichte WhatsApp 2019 eine Klage gegen NSO ein. Mit dem nun zu übergebenden Quellcode will WhatsApp unter anderem nachvollziehen, welche Daten Pegasus extrahieren konnte.

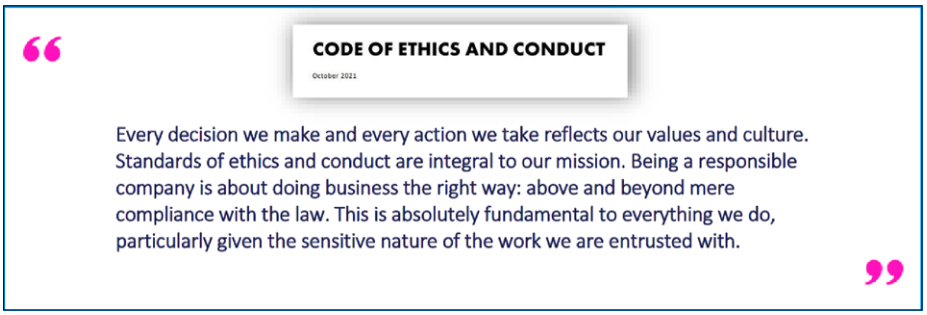
Der Fall WhatsApp gegen NSO Group ist vor dem US-Bundesbezirksgericht für das nördliche Kalifornien verhandelt worden. Das Verfahren trägt das Aktenzeichen 19-cv-07123, eine Übersicht des gesamten Verfahrens inklusive der Dokumente und den Entscheidungen finden Sie über ct.de/ywb2. In anderen Anklagepunkten entschied die Richterin Phyllis J. Hamilton für NSO, so muss die Spionagefirma die Namen seiner Kunden und den Aufbau der Server-Architektur nicht offenlegen.

NSO wehrte sich vehement gegen die Klage und versuchte vor Gericht einen Immunitäts-Status zu erlangen. Die Spionagefirma argumentierte, man würde Nachrichtendiensten helfen, Kriminelle festzunehmen, und Staaten beim Schutz der nationalen Sicherheit unterstützen. Zudem habe NSO als Agent für nicht identifizierte ausländische Regierungen gearbeitet und sei ihrer eigenen Erklärung zufolge immun gegen eine Klage. Das Gericht folgte dieser Argumentation nicht und verweigerte den Immunitäts-Status.

Nach vielen Protesten seitens NSO wurde die Klage vergangenes Jahr schließlich vom Supreme Court der USA zugelassen. Die Entscheidung des Gerichts ist ein herber Schlag für die Spionagefirma, die die Funktionsweise von Pegasus ungern offenlegen will. Selbst Käufer der Software erhalten keinen Einblick. Durch seltene Analysen von Spyware-Samples weiß man, dass Pegasus eine ausgeklügelte Software ist (siehe c't 3/2022, S. 38): Einige Pegasus-Versionen nutzen sogenannte Zero-Click-Sicherheitslücken aus. Dadurch können sie sich auf einem Gerät einnisten, ohne dass dessen Besitzer auch nur einen Link anklickt. Die Opfer müssen also in keiner Weise selbst aktiv werden, um die Schadsoftware herunterzuladen.

NSO beteuert, seine Kunden sorgfältig auszusuchen und ausschließlich an Regierungen zu verkaufen: zur Bekämpfung von Terrorismus oder zur Stärkung der inneren Sicherheit. Dass das in der Realität oft anders aussieht und politische Gegner oder Journalisten Ziele sind, zeigt auch ein bekannter Fall in Polen: Dort soll die Vorgängerregierung unter PiS die Opposition mit Pegasus belauscht haben. Der Skandal ist als „Polens Watergate“ bekannt geworden. *(wid@ct.de)*

Gerichtsdokumente: ***ct.de/ywb2***



Im Transparenzbericht von 2023 lobt sich NSO für seinen hohen Ethik-Standard. Vor Gericht hat ihnen das nicht weitergeholfen.