Pegasus bei BND und BKA

Pegasus bei BND und BKA

Nach und nach werden weitere Kunden der israelischen NSO Group bekannt. Offenbar haben auch deutsche Polizeibehörden und Nachrichtendienste die Spyware Pegasus gekauft.

Deutsche Behörden nutzen umstrittene Spyware

Nach und nach werden weitere Kunden der israelischen NSO Group bekannt. Offenbar haben auch deutsche Polizeibehörden und Nachrichtendienste die Spyware Pegasus gekauft.

Von Sylvester Tremmel

Das Bundeskriminalamt (BKA) und der Bundesnachrichtendienst (BND) setzen offenbar die Überwachungssoftware Pegasus ein. Das berichten Zeit, Süddeutsche Zeitung, WDR und NDR. Im Fall des BKA soll das Bundesinnenministerium über den Einsatz informiert gewesen sein, nicht aber Innenminister Horst Seehofer selbst. Beim BND war angeblich das Bundeskanzleramt eingeweiht. Das Parlamentarische Kontrollgremium, dem unter anderem die Kontrolle des BND obliegt, soll nicht informiert worden sein.

Pegasus war im Juli dieses Jahres durch Veröffentlichungen des Rechercheverbundes „Pegasus Project“ der breiten Öffentlichkeit bekannt geworden. Den Recherchen zufolge wird Pegasus von einer Vielzahl von Akteuren auf der ganzen Welt eingesetzt; nicht nur zur Bekämpfung schwerwiegender Kriminalität, sondern auch, um Politiker, Oppositionelle, Menschenrechtsaktivisten und Journalisten zu überwachen.

Das steht im krassen Gegensatz zu den Versicherungen des israelischen Herstellers NSO Group: Das Unternehmen schreibt, man lizenziere seine Software nur an „ausgewählte, genehmigte, bestätigte und berechtigte Staaten und staatliche Behörden“. Pegasus dürfe nur zur „nationalen Sicherheit“ und in „größeren Ermittlungen“ von Sicherheitsbehörden zum Einsatz kommen. Andererseits betont die NSO Group auch, nicht zu wissen, wie ihre Kunden Pegasus tatsächlich nutzen.

Laut NSO Group kommt Pegasus nur gegen Terror und Kriminalität zum Einsatz.

Pegasus fürs BKA zu mächtig

Dem BKA wollte die NSO Group ihre Software 2017 verkaufen, berichtet Tagesschau.de. Dazu sei es nicht gekommen, weil das BKA Vorbehalte gehabt habe: Deutsches Recht unterscheidet zwischen Online-Durchsuchungen und der Quellen-Telekommunikationsüberwachung (Q-TKÜ). Im ersten Fall werden auf einem Gerät gespeicherte Daten ausgeleitet. Bei der Q-TKÜ wird dagegen nur die Kommunikation abgegriffen, analog zur abgehörten Telefonleitung. Pegasus habe diese Unterscheidung nicht getroffen und noch weitere Probleme aufgewiesen.

Nach einem Bericht der Wochenzeitung Die Zeit änderte sich dies 2020. Die NSO Group habe dem BKA eine angepasste Version von Pegasus zur Verfügung gestellt, die mit deutschem Recht vereinbar sein soll – zumindest nach Ansicht des BKA. Wie genau der BND Pegasus einsetzt, ist nicht bekannt.

Mit dem Einsatz von Pegasus stellen sich deutsche Behörden in eine Reihe von fragwürdigen Käufern, die erhebliche Zweifel daran aufkommen lässt, dass die NSO Group ihre Kunden ausreichend sorgfältig überprüft. Anfang Oktober befand etwa

ein englisches Gericht, dass Muhammad bin Raschid Al Maktum, Herrscher des Emirats Dubai, die Software eingesetzt habe, um seine Exfrau und ihre Anwälte zu überwachen.

Bedenklich ist auch der Verdacht, die NSO Group könnte Einblick in die mit Pegasus durchgeführten Überwachungsoperationen haben – entgegen ihrer Aussagen. Gegenüber der Zeit erklärten BND und BKA, das technisch ausschließen zu können. Die Zeitung berichtet aber von entgegenstehenden Aussagen ehemaliger Mitarbeiter der NSO Group. Demnach würden die exfiltrierten Daten über Server des Unternehmens fließen.

Hinzu kommt ein moralisches Problem: Um Software wie Pegasus auf Zielgeräte ausspielen zu können, muss die NSO Group schwerwiegende Sicherheitslücken in aktuellen Versionen von iOS und Android kennen und geheim halten. Die daraus erwachsende Gefährdung sämtlicher Smartphone-Besitzer wird in Kauf genommen. Kunden der NSO Group finanzieren dieses Geschäftsmodell, statt die breite Masse ihrer Bürger zu schützen.

Im Fall von Android ist nicht bekannt, über welche Lücken Pegasus auf Geräte gelangt. Unter iOS war ein Einfallstor mutmaßlich eine Lücke in der App iMessage. Darüber konnte Pegasus ausgespielt werden, ohne dass die iPhone-Nutzer irgendetwas tun mussten – eine sogenannte Zero-Click-Lücke. Die hat Apple mittlerweile geschlossen, welche weiteren Lücken die NSO Group noch kennt, weiß nur sie selbst. *(syt@ct.de)*

Recherchen zu Pegasus: ct.de/yfzj

ct.de/yfzj

- **The Pegasus Project** Seite des Pegasus Projekts beim Journalismus-Netzwerk Forbidden Stories.
- **Forensic Methodology Report: How to catch NSO Group's**

Pegasus Forensischer Bericht zu Pegasus des Security Labs von Amnesty International.

c’t-Berichterstattung zum Thema Pegasus

- **Infiziert ohne Klick: Amnesty International deckt Massenüberwachung durch Pegasus auf**
- **Rüffel vom Fachmann: Sicherheitsforscher fordert grundlegende iOS-Überarbeitung**
- **Spyware-Entdecker: Geheimdienst-Spionagetool Pegasus auf dem iPhone enttarnen**

Pegasus an deutschen Behörden

- **BKA bekam maßgeschneiderten Trojaner** Tagesschau.de zum Pegasus-Einsatz beim BKA.
- **Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein** Zeit-Bericht zum Einsatz von Pegasus beim BND.
- **Bundesnachrichtendienst spitzelt mit Pegasus** Tagesschau.de zum Pegasus-Einsatz beim BND.