

# Israelisches Gericht bestätigt die berüchtigte Spionagefirma *NSO Group*

Tamara Nassar, [electronicintifada.net](http://electronicintifada.net), 14.07.20

Am Sonntag lehnte ein israelisches Gericht eine von Amnesty International unterstützte Petition ab, in der das israelische Verteidigungsministerium aufgefordert wurde, dem Cyberwarfare-Unternehmen *NSO-Group* die Exportlizenz zu entziehen.

Die Richterin, Rachel Lavi-Barkai entschied, dass die Antragsteller keine Beweise dafür vorgelegt hatten, dass die Technologie des israelischen Unternehmens zur Bespitzelung von Amnesty-Personal eingesetzt worden war.

„Ich bin davon überzeugt, dass die Kontrollverfahren und die Abfertigung von Genehmigungsanträgen für Exporte militärischen Materials sorgfältigst befolgt werden“, sagte Lavi-Barkai über den Prüfprozess der *NSO Group*, so die israelische Tageszeitung *Haaretz*.

**Der Eigentümer von *WhatsApp*,  
Facebook, hat die israelische  
Firma ebenfalls verklagt**

Obwohl es „Berge an Beweisen“ gibt, dass die von der *NSO-Group* hergestellten Überwachungsinstrumente gegen Journalisten und Menschenrechtsverteidiger eingesetzt wurden, hat das Gericht in dieser Weise entschieden, sagte Danna Ingleton, eine Technikspezialistin von Amnesty. Dieses „schändliche Urteil ist ein schwerer Schlag für Menschen auf der ganzen Welt, die durch den Verkauf der Produkte der *NSO Group* an berüchtigte Menschenrechtsverletzer gefährdet sind“. „So profitiert die *NSO-Group* weiterhin ungestraft von Menschenrechtsverletzungen“, fügte sie hinzu. Im Mai 2019 war die Klage gegen die *NSO Group* von etwa 30 Beschwerdeführern eingereicht worden.

Nachdem einer ihrer Mitarbeiter 2018 mit der hochentwickelten Cyber-Waffe *Pegasus*, der Firma *NSO-Group*, ins Visier genommen wurde, unterstützte *Amnesty International* die Klage. *Pegasus* ermöglicht es seinen Betreibern, unbemerkt Smartphones zu kapern und riesige Mengen privater Daten abzuschöpfen.

Die *NSO Group* begrüßte die Entscheidung des Gerichts mit den Worten: „Es gab keine beweiskräftige Grundlage für die Anschuldigungen“. Die *NSO Group* behauptet, dass ihre Produkte „ausschließlich von staatlichen Geheimdienst- und Strafverfolgungsbehörden zur Bekämpfung von Verbrechen und Terror“ verwendet werden.

Inzwischen wurde ein katalanischer Spitzenpolitiker das jüngste Ziel der Spionage-Software der *NSO Group*.

Einer gemeinsamen Untersuchung zufolge, die *The Guardian* und *El País* durchgeführt hatten, wurde das Telefon des Präsidenten des katalanischen Regionalparlaments, Roger Torrent, mit *Pegasus* infiziert. Der Messaging-Dienst *WhatsApp* alarmierte Torrent, dass sein Telefon gehackt und infiziert wurde, indem eine Schwachstelle ausgenutzt wurde, um die *Spyware Pegasus* zu installieren.

„Es erscheint falsch, dass Politiker in einer Demokratie mit Rechtsstaatlichkeit, ausspioniert werden“, sagte Torrent dazu. „Ich halte es auch für unmoralisch, große Mengen öffentlicher Gelder für den Kauf von Software auszugeben, die zur Verfolgung politischer Dissidenten verwendet werden kann“.

Auch zwei weitere katalanische Unabhängigkeitsbefürworter sind davon betroffen. Die ehemalige Abgeordnete des katalanischen Parlaments, Anna Gabriel, wurde von der kanadischen Cybersicherheitsorganisation *Citizen Lab* informiert, dass ihr Telefon infiltriert wurde. Jordi Domingo ist ebenfalls betroffen.

Obwohl Domingo die katalanische Unabhängigkeit unterstützt, glaubt er, dass er fälschlicherweise ins Visier genommen wurde und mutmaßt, dass das eigentliche Ziel „ein prominenter Anwalt war, der denselben Namen hat und an der Ausarbeitung der katalanischen Verfassung mitgewirkt hatte“, berichtet *The Guardian*.

Dadurch, dass die *NSO Group* darauf beharrt, dass sie ihre Software ausschließlich an Regierungen verkauft, glaubt Torrent, dass die spanische Regierung der Hauptverdächtige bei den jüngsten Hackerangriffen ist. Das Büro des spanischen Premierministers erklärte, es habe „keine Beweise“ dafür, dass die drei katalanischen Politiker „Ziel von Hackerangriffen auf ihre Handys waren“ und bestand darauf, dass jede Operation mit einem Mobiltelefon immer in Übereinstimmung mit der entsprechenden gerichtlichen Genehmigung durchgeführt wird“.

2019 gab *WhatsApp* eine aktualisierte Version heraus, bei der die Schwachstelle behoben war, die zur Ausspionierung von 1.400 Personen benutzt wurde. Laut *The Guardian* gibt es bisher keine Vermutungen darüber „dass irgendein europäisches Land die Software der *NSO Group* bei den Angriffen 2019 benutzt hat“.

Der Eigentümer von *WhatsApp*, Facebook, hat die israelische Firma ebenfalls verklagt.

Trotz der berüchtigten Rolle, die die *NSO-Group* bei der Verletzung der Rechte von Journalisten und Menschenrechtsverteidigern auf der ganzen Welt spielt, haben sich mehrere europäische Länder, u. a. die Niederlande und Schweden, der israelische Technologieindustrie angenähert, die eng mit *Cyberwarfare*- und Spionage-Technologie verflochten ist.

Übersetzung: M. Kunkel, Pako – palaestinakomitee-stuttgart.de

Quelle:

<https://electronicintifada.net/blogs/tamara-nassar/israeli-court-backs-notorious-spy-firm-nso-group>