Wie eine Firma in Lausanne unfreiwillig bei Pegasus-Spionage-Attacken mitwirkte

Die Schweiz steckt tiefer im Skandal um die Überwachungssoftware als bisher bekannt: Nur in zwei anderen Ländern standen mehr Server für Operationen mit Pegasus bereit. Über die Schweizer Cloud lief 2020 eine Abhöraktion.

Eine Recherche von Adrienne Fichter und Patrick Seemann, 26.08.2021

«Das ist eine Branche, die nicht existieren sollte»: So umschreibt der berühmte Whistleblower Edward Snowden das Metier der NSO Group.

Die israelische Firma verkauft seit Jahren die Spionagesoftware Pegasus an verschiedene Staaten. Offiziell soll sie nur im Kampf gegen Terrorismus und Menschenhandel eingesetzt werden, wie das Technologieunternehmen stets beteuert hat. Doch de facto wird die Software von Staaten wie Saudiarabien, Ungarn, Mexiko oder Marokko eingesetzt, um Menschenrechtsaktivistinnen, Oppositionelle oder Journalisten auszuspionieren und zu verfolgen.

Der grossflächige Einsatz von Pegasus wurde Mitte Juli 2021 enthüllt und erschütterte die Welt. Die gemeinnützige Medienorganisation «Forbidden Stories» und Amnesty International mit ihrem Tech-Team haben in Kooperation mit Medien wie der «Süddeutschen Zeitung», «Die Zeit», «Le Monde», dem «Guardian» und der «Washington Post» auf der Basis einer Telefonliste Hunderte Opfer der Spionagesoftware recherchiert. Darunter sind Frankreichs Präsident Emmanuel Macron oder investigative Journalisten wie Mediapart-Gründer Edwy Plenel. 600 hochrangige Politikerinnen, 85 Aktivisten sowie 189 Journalistinnen waren gemäss den Recherchen weltweit von Pegasus-Angriffen betroffen. Aufgrund der Enthüllung sah sich das israelische Verteidigungsministerium gezwungen, eine Untersuchung beim Vorzeigeunternehmen durchzuführen.

Die Schweiz schien im Zusammenhang mit Pegasus bisher kaum eine Rolle zu spielen. Doch jetzt zeigen Recherchen der Republik: Sie steckt tiefer als bisher angenommen im Skandal um die mächtige Überwachungssoftware.

Die Rolle der Schweiz

Pegasus ist ein umfassendes Überwachungsprogramm. Einmal auf dem Smartphone installiert, aktiviert die Software Mikrofone und Kameras und

überträgt jede eintreffende SMS in Echtzeit. Sie kann auf Nachrichten, Bilder, Videos und sämtliche anderen Inhalte des Geräts zugreifen. Es ist, als ob einem jemand permanent über die Schulter auf den Bildschirm schaut.

Eingeschleust wird die Software oft ohne eigenes Zutun. Viele der Opfer haben weder einen verdächtigen Link angeklickt noch sich anderweitig angreifbar gemacht. Pegasus nutzt Sicherheitslücken in Betriebssystemen der Smartphone-Hersteller oder von Messenger-Apps wie Whatsapp.

Ich will es genauer wissen: Wie genau funktioniert die Infektion eines Smartphones mit der Schadsoftware Pegasus?

Für eine für die Überwachung oder Fernsteuerung von IT-Geräten verwendete Malware ist typischerweise Folgendes nötig:

1. Eine Methode, um die Malware auf dem Smartphone der Zielperson zu installieren (ein «Infektionslink»).
2. Ein im Internet erreichbarer Installationserver, der die Malware installierbar bereitstellt.
3. Ein Steuerserver, mit dem das Verhalten der Malware gesteuert werden kann.

Für die Installation wurde bei den vor 2018 eingesetzten Versionen von Pegasus der Angegriffene dazu verleitet, einen harmlos aussehenden Link anzutippen. Beim Laden der so aufgerufenen Webseite wurde die Installation ausgelöst. Moderne Versionen nutzen Lücken aus – etwa in iMessage von Apple –, um schon direkt beim Empfang einer Nachricht durch das Smartphone einen Softwarecode auszuführen (sogenannte Zero-Click-Angriffe).

In beiden Fällen wird mit dem ersten Link (oder der Zero-Click-Lücke) meist nur ein erster Teil der Malware auf dem Gerät installiert. Dieses Codestück lädt und installiert dann selbstständig und ohne dass die Benutzerin dies bemerkt die weiteren notwendigen Teile, um das Smartphone vollständig unter Kontrolle zu bekommen. Dabei werden oft je nach verwendeter Betriebssystemversion unterschiedliche Softwarestücke nachgeladen, die jeweils spezifische Lücken in der verwendeten Betriebssystemversion ausnutzen.

Nach erfolgter Installation und der Übernahme beginnt die Malware, mit einem Steuerserver zu kommunizieren, um einerseits die Übernahme des Geräts zu signalisieren und anderseits Befehle für weitere Datenextraktionen entgegenzunehmen. Zumindest grundsätzlich kann der Steuerserver auch sicherstellen, dass effektiv nur die Zielperson ausgespäht wird.

Im Falle von Spionagesoftware wie Pegasus kann davon ausgegangen werden, dass jeder Kunde – oft Regierungen oder Geheimdienste – eigene Steuerserver einsetzt, allenfalls auch eigene Installationsserver. Schliesslich wollen die Anwender von Pegasus ihre Angriffsziele vor anderen geheim halten.

Auch wenn die Schweiz in der Berichterstattung über Pegasus bisher nicht gross vorkam, ist ihre Rolle grösser als allgemein bekannt. Mehrfach schon führten in der Vergangenheit Spuren des Spionagetools in die Schweiz:

– Die kanadischen Forscherinnen vom Citizen Lab der Universität Toronto belegten bereits 2018, dass die Schweiz Schauplatz von Pegasus-Attacken war. Das zeigten entsprechende Spuren im Swisscom-Netz. Der Bericht erregte in der Schweiz wenig Aufsehen. Die Swisscom wiegelte ab: Man habe keine «Kommunikation» feststellen können.

– Die Credit Suisse finanzierte das umstrittene Cyberunternehmen NSO-Group mit einem Kredit von 500 Millionen Franken.
– Die im Genfer Exil lebende spanische Oppositionspolitikerin Anna Gabriel wurde Opfer einer Pegasus-Attacke – und zwar in der Zeit, als sie bereits in der Schweiz lebte, wie eine ihr nahestehende Person gegenüber der Republik bestätigt. Hinter der Attacke, so schreibt «El País», wird der spanische Geheimdienst vermutet.
– Der Nachrichtendienst des Bundes, das Bundesamt für Polizei (Fedpol) und kantonale Strafverfolgungsbehörden haben die Software 2017 und 2018 getestet. Die NZZ vermutet, gestützt auf anonyme Quellen, dass sie heute noch im Einsatz ist. Somit dürfte es weitere ausspionierte Personen in der Schweiz geben.

Ich will es genauer wissen: Wie wurden Pegasus-Spuren gefunden, die bereits 2018 in die Schweiz führten?

Eine Gruppe von Wissenschaftlern des Citizen Lab der Uni Toronto beobachtet die NSO Group seit Jahren. Dabei hat sie bereits viele bekannte Opfer der Pegasus-Software identifiziert, unter anderem den Aktivisten Ahmed Mansoor oder den im Oktober 2018 ermordeten Journalisten Jamal Khashoggi. 2018 haben die Wissenschaftlerinnen 45 Staaten identifiziert, in denen es zu Pegasus-Attacken gekommen ist – darunter auch die Schweiz. Wie sind sie vorgegangen?

Die Spurensuche beginnt mit dem entlarvten Softwarecode von Pegasus selbst. Gelangt man in den Besitz des Installationslinks (zum Beispiel durch die Analyse des Smartphones eines Opfers), kann der Code in ein abgesichertes Testumfeld geladen und dort dessen Verhalten analysiert werden. In der Malware sind auch die URLs für den Zugriff auf verwendete Installations- und Steuerserver enthalten.

Der Name eines einzelnen Servers allein hilft noch nicht wirklich weiter. Um den Einsatz von Pegasus zu untersuchen, kommt ein weiteres Werkzeug zum Einsatz: das sogenannte Fingerprinting von Webservern. Analog zum Browser-Fingerprinting (bei welchem Benutzer aufgrund von Browserversion, Fenstergrösse, Betriebssystemversion, installierten Zeichensätzen und weiteren Merkmalen auch ohne Cookies identifiziert werden können) lassen sich auch für Server im Internet Fingerprints definieren, im einfachsten Fall aufgrund von URLs, welche nur auf diesem einen Server ein Ergebnis liefern (und auf allen anderen eine Fehlermeldung).

Mit den aus der Malware extrahierten URLs konnten die Wissenschaftler von Citizen Lab Fingerprints der von Pegasus verwendeten Server erstellen und das Internet nach weiteren Instanzen absuchen (was aufwendiger klingt, als es ist, die über IP erreichbaren Server im Internet lassen sich innert weniger Stunden abklappern). Insgesamt konnten dabei 2016 knapp 200 Server und 2018 gut 500 Server als Teil des NSO-Netzwerks identifiziert werden.

Wie erwähnt kann davon ausgegangen werden, dass jede NSO-Kundin ihre eigenen Installations- und Steuerserver einsetzt. Citizen Lab konnte Unterschiede in den von den Servern verwendeten Zertifikaten und Proxy-Konfigurationen ausnutzen, um die gefundenen Server in 36 Gruppen einzuteilen. Vermutlich wurde jede Gruppe von einem spezifischen Angreifer/Operator – also einem NSO-Kunden – betrieben, um die jeweiligen Zielpersonen anzugreifen.

Damit sind die Täter mutmasslich identifiziert, jedoch noch nicht deren Opfer.

Die meisten Einsätze von Pegasus sind regional oder national begrenzt und richten sich gegen innenpolitisch relevante Ziele. Wie findet man nun heraus, in welcher geografischen Region ein einzelner Operator aktiv war?

Dazu braucht es einen kleinen Exkurs in die Technik des Internets. DNS (Domain Name System) ist quasi das Telefonbuch des Internets, das menschenlesbare Servernamen in technische IP-Adressen übersetzt (und aus republik.ch zum Beispiel 54.247.69.169 macht). Bei jedem Internetzugriff greift ein Browser (beziehungsweise das Betriebssystem) auf einen DNS-Server zu, um die IP-Adresse des entsprechenden Servers zu ermitteln. Typischerweise wird der DNS-Server vom jeweiligen Internetprovider (wie Swisscom) bereitgestellt, genutzt werden können aber auch alternative Angebote, etwa von Google oder Cloudflare. Ein DNS-Server weiss normalerweise nicht über alle IP-Adressen Bescheid, dafür aber, welchen anderen DNS-Server er fragen muss. Um nicht jede Anfrage weiterleiten zu müssen, werden Adressen für eine gewisse Zeit in einem Cache aufbewahrt. Dies führt dazu, dass bei mehreren Anfragen für eine Adresse die Antwortzeit beim ersten Mal länger ist als bei darauffolgenden Anfragen.

Diese Zeitdifferenz lässt sich mit einem sogenannten DNS-Probing ausnutzen, um zu erkennen, ob ein Servername schon im Cache eines DNS-Servers vorhanden ist. Ist dies der Fall, kann mit hoher Wahrscheinlichkeit geschlossen werden, dass in den letzten Stunden oder Tagen bereits jemand anderes auf denselben Server zugegriffen hat. Im Falle der Pegasus-Server liegt die Vermutung nahe, dass ein entsprechend infiziertes Smartphone im Netz des jeweiligen Providers aktiv war.

Die Forscherinnen von Citizen Lab haben die öffentlich erreichbaren DNS-Server der grossen Netzanbieter weltweit mittels DNS-Probing untersucht, um einzelne Operatoren geografisch verorten zu können. Für einen der Operatoren wurden ausschliesslich DNS-Einträge in den DNS-Servern der Swisscom gefunden. Details zu vertieften Analysen von Logfiles, anhand deren etwa erkennbar wäre, welche Swisscom-Kunden allenfalls Ziel einer Überwachung waren, konnte oder wollte Swisscom nicht mitteilen: «Wir haben unsere Logs nach Verbindungen zu den uns bekannten Indikatoren [-von Pegasus] durchsucht, ohne entsprechende Hinweise auf entsprechende Kommunikation zu finden.»

Als Erklärung dafür schob die Swisscom nach: «Da unsere DNS-Server auch auf Anfragen von ausserhalb des Swisscom-Netzes reagieren, könnte ein Operator auch unsere DNS-Server verwendet und somit den Anschein erweckt haben, dass ein Operator im Swisscom AS3303 aktiv ist.» Dies scheint allerdings wenig plausibel, da der DNS-Server ja typischerweise beim Einloggen ins Swisscom-Netzwerk direkt auf dem Gerät des Kunden gesetzt wird. Ob es sich als Auftraggeber um den spanischen Nachrichtendienst handelte (Fall Anna Gabriel), den NDB oder eine andere Institution, ist offen.

Recherchen der Republik zeigen nun erstmals: Die Schweiz spielt ausserdem auch als Infrastrukturstandort für Pegasus-Attacken eine Rolle. 2020 kam es mittels eines infizierten Servers in der Schweiz zu einer Abhöraktion.

Im forensischen IT-Bericht von Amnesty Tech stehen erstens Deutschland mit 212 Servern und zweitens Grossbritannien mit 79 Servern auf den ersten beiden Positionen im Standortländer-Ranking, das aufzeigt, von wo aus Pegasus-Attacken ausgingen. Dabei handelt es sich mutmasslich um Rechenzentren von amerikanischen Cloud-Anbietern, die von der NSO Group gemietet wurden.

Doch gleich dahinter, auf Rang drei, folgt die Schweiz – mit der Firma Akenes SA aus Lausanne. Das Unternehmen, hierzulande besser bekannt unter seinem Produktnamen Exoscale, steht an vierter Stelle des «NSO-Server-Rankings» von Amnesty International – hinter den US-Konzernen Amazon, Digital Ocean und Linode. Akenes – in vielen Medienberichten fälschlicherweise als amerikanisches Unternehmen bezeichnet – stellte seine Server also für Operationen mit der Spionagesoftware zur Verfügung.

Dies belegen Ergebnisse einer Untersuchung, die das Amnesty-Tech-Team durchführte und die der Republik vorliegen. Amnesty-Tech-Sprecher Etienne Maynier bestätigt auf Anfrage, dass 2020 auf einem Akenes-Server mit einer bestimmten Webadresse eine effektive Pegasus-Infektion eingetreten ist. Genauer: Die angegriffene Person habe auf den Infektionslink geklickt oder habe die Infektion via einen anderen Kanal wie Whatsapp erhalten.

Damit ist klar: Eine Person wurde 2020 Opfer einer erfolgreichen Pegasus-Attacke über Schweizer Server. Es gibt keine Hinweise auf das Opfer, auch nicht darauf, ob es aus der Schweiz stammt. Ebenso wenig lässt sich sagen, ob der Nachrichtendienst oder das Fedpol hinter der Attacke steckt.

Maynier sagt: «Es ist wichtig zu beachten, dass der Standort eines Servers nichts darüber aussagt, welcher Kunde oder welches Land diesen Server nutzt. Einige dieser Server wurden in der Schweiz gehostet, aber das bedeutet nicht, dass sie mit der Schweiz oder einem europäischen Kunden in Verbindung stehen.»

Zudem, sagt Maynier, seien 57 weitere Akenes-Server als «Komponenten», als Teile des Infektionssystems der NSO Group, genutzt worden.

Schweizer Alternative zu Amazon

Mitbegründet wurde die Firma Akenes 2011 von Antoine Coetsier, dem heutigen CEO. 2017 kaufte die Telekom Austria grosse Teile des Unternehmens. Seither ist das Cloud-Unternehmen auf Wachstumskurs und unterhält auch Rechenzentren in Österreich und Deutschland. Kunden sind unter anderem die Forschungseinrichtung Cern und die Plattform «Dein Deal». Exoscale aka Akenes positioniert sich als europäische Cloud-Alternative, die sich den strengen europäischen Datenschutzgesetzen verpflichtet sieht.

Was für einen berüchtigten Kunden Akenes mit der NSO Group hatte, war den Westschweizern offenbar kaum bekannt. Dies geht aus Gesprächen hervor, welche die Republik mit mehreren ehemaligen Angestellten geführt hat. Alle zeigten sich überrascht, niemand wusste von der Kundenbeziehung mit der NSO Group. Doch die meisten sagen auch, dies liege in der Natur der Sache. Akenes stelle lediglich Rechenleistung zur Verfügung. «Wir haben nichts mit dem Produkt des Kunden zu tun, und man hat schon gar keinen Zugriff auf die Daten», sagt eine Quelle.

Auf die Hinweise von Amnesty Tech reagierte Akenes, indem die Firma versuchte, die Nutzungsstrategien von NSO zu durchleuchten – jedoch ohne Erfolg. Akenes-CEO Antoine Coetsier sagt der Republik, er habe mit dem «Amnesty-Forschungsteam Kontakt aufgenommen, um weitere Untersuchungen mit anderen historischen Daten durchzuführen, die ihnen zur Verfügung standen, aber es hat sich kein Muster herauskristallisiert».

Auch Amnesty Tech vermutet, dass Akenes seinen zwielichtigen Kunden nicht gekannt hat. Dies liege an den Taktiken der israelischen Firma.

«Die NSO Group mietet regelmässig operative Infrastruktur unter Verwendung pseudonymer E-Mail-Konten und Zahlungsmethoden», sagt Amnesty-Tech-Sprecher Maynier. Weil die NSO-Gruppe mit Tarnfirmen operiert, vermochte CEO Coetsier auch die Frage nach der Dauer der Geschäftsbeziehung nicht zu beantworten. «Die Cloud ist eine sehr volatile Umgebung, und IP-Adressen können im Laufe der Zeit mehreren Mietern zugewiesen werden», sagt er.

Ist Akenes damit nun ein typisches Opfer der NSO Group, oder versagten ihre Mechanismen zur Durchleuchtung dubioser Kunden?

Lob und Kritik am Schweizer Cloudbetreiber

Was sich sicher sagen lässt: Es gibt in der Schweiz kaum Überwachungspflichten für Hostingprovider wie Akenes, bloss Selbstverpflichtungen. Dazu gehört etwa der «Code of Conduct» des Branchenverbands Swico. Üblicherweise gelangen die Schweizer Behörden mit konkreten Anfragen bei strafrechtlichen Inhalten wie Kinderpornografie an die Unternehmen.

Im Fall von Pegasus dürfte dieses Prozedere kaum zur Anwendung kommen: Hier sind Schweizer Behörden wie der Nachrichtendienst, das Fedpol und die Kantone selbst die mutmasslichen Käuferinnen der Spionagesoftware.

Richtig ist auch: Die Geschäftsbedingungen von Akenes untersagen die Nutzung ihrer Server für die Verbreitung von Schadsoftware. Ein Verstoss führe zur direkten Beendigung einer Geschäftsbeziehung, sagt CEO Coetsier, weshalb man den Fall genau untersuche. Amnesty-Sprecher Maynier sagt, dass sich Akenes kooperativ zeigte: «Sie haben schnell reagiert und versprochen, die Befunde schnell zu untersuchen.» Und dennoch wird auch Kritik laut. Als aufstrebendes Start-up müsse man prüfen, wer seine Server nutze, sagt ein Ex-Kadermitglied: «Wenn man sich als Schweizer Alternative zu Amazon aufstellt, sollte man genauer hinschauen bei seinen Kunden.»

Die Spionageoperationen mit – unfreiwilliger – Schweizer Mithilfe sind nun allerdings schon Geschichte. Seinem Wissensstand nach, sagt Maynier von Amnesty Tech, habe die NSO Group bereits damit begonnen, die vierte und letzte bekannte Version ihrer Schadsoftware grösstenteils oder vollständig abzuschalten, bevor Amnesty Tech ihren Bericht veröffentlicht habe.

Die NSO Group hat also bereits vor den Enthüllungen im Sommer durch Medien weltweit ihre gesamte Infrastruktur deaktiviert – so, wie sie es in den vergangenen Jahren praktisch bei jedem aufsehenerregenden Medienbeitrag getan hat, um dann einige Wochen oder Monate später mit neuen Verschleierungsmethoden und neuem Schadcode wieder aktiv zu werden.

Die Suche nach Spuren der Pegasus-Spionagesoftware bleibt ein ewiges Katz-und-Maus-Spiel. Und dürfte bald in eine neue Runde gehen.

Ich will es genauer wissen: Welches sind die betroffenen Domain-Adressen der Schweizer Firma Akenes?

Eine Auswahl der Domain-Namen und IP-Adressen, die entweder Teile des Infektionssystems darstellen oder Pegasus-Infektionsserver waren:

89.145.167.181 - drp2j4sdi.safecrusade.com

159.100.244.53 - info3mkx72.meanspursuit.com

159.100.244.78 - api456sd.blindlydivision.com

159.100.245.78 - img283jda.reachcomputer.com

159.100.249.83 - img5t7j3d5.stationfunds.net

194.182.181.131 - js30jd2mdpi.panelbreed.com

194.182.182.51 - srv768s1.last-chainleash.net

194.182.182.150 - mongo87a.sweet-water.org

194.182.183.95 - cpu52gh33.standartsheet.com

Quelle: Amnesty Tech, zusammengestellt exklusiv für die Republik