Ehemalige israelische Spione betreuen nun die Cybersicherheit der US-Regierung

thegreyzone.com, 03.12.25

Das Pentagon, das Finanzministerium, das Heimatschutzministerium und eine Reihe weiterer US-Behörden vertrauen bei der Konsolidierung und dem Schutz ihrer Daten inzwischen auf ein Unternehmen, das von ehemaligen Mitarbeitern des israelischen Militärgeheimdienstes gegründet wurde.

Ein Unternehmen mit engen Verbindungen zum israelischen Geheimdienst überwacht die Cybersicherheit in mehr als siebzig US-Regierungsbehörden, darunter das Verteidigungsministerium und das Ministerium für Innere Sicherheit.

Die US-Behörden haben ehemaligen Spionen aus einem Land, das bekanntermaßen Spionage innerhalb der USA betrieben hat, erlaubt, einen Cyberspionage-Zugang zu fast dem gesamten Apparat der Bundesregierung aufzubauen.

Axonius wurde von ehemaligen Spionen der israelischen Einheit 8200 gegründet. Die Software des Unternehmens ermöglicht dem Anwender „Sichtbarkeit und Kontrolle jeglichen Geräte-Typs in beliebiger Anzahl," 1, des Weiteren sammelt und analysiert sie die digitalen Daten von Millionen von US-Bundesangestellten.

Das erklärte Ziel der *Axonius*-Plattform ist es, IT-Tools zu zentralisieren, um Sicherheitslücken zu identifizieren und zu beheben. Als Produkt des israelischen Geheimdienstes wirft die Verbreitung von *Axonius* innerhalb der US-Regierung jedoch ernsthafte Fragen auf.

Axonius wurde von den Israelis Dean Sysman, Ofri Shur und Avidor Bartov gegründet und wird derzeit von ihnen geleitet. Die drei lernten sich in den 2010er Jahren kennen, als sie im selben Team des israelischen Geheimdienstes *Unit 8200* 2 arbeiteten. In seinem *LinkedIn*-Profil gibt Sysman nur wenige Details über seine Tätigkeit für die israelische Armee preis und beschreibt sie lediglich als „weitreichend".

Sysman verließ die israelische Armee 2014 nach fünf Jahren und gründete eine Cyber-Hacking-Gruppe, während Shur und Bartov bis 2017 blieben, einem Zeitraum, in den Israels Angriffskrieg gegen Gaza im Jahr 2014 fällt, wo die israelische Armee mehr als zweitausend palästinensische Zivilisten ermordete.

Die Gründung von *Axonius* ging mit bemerkenswerter Geschwindigkeit voran. Nachdem sie 2017 die israelische Armee verlassen hatten, taten sich Shur und Bartov erneut mit Sysman zusammen und erhielten zur Gründung von *Axonius* sofort 4 Millionen US-Dollar Startkapital von Yoav Leitersdorf, einem in San Francisco lebenden israelisch-amerikanischen Veteranen der *Einheit 8200*. Leitersdorf, geschäftsführender Gesellschafter der US-amerikanisch-israelischen Risikokapitalgesellschaft *YL Ventures*, ist ein erfolgreicher Gründungsinvestor in Cyber-Start-ups der *Einheit 8200*. Im selben Jahr erhielten Sysman, Shur und Bartov auch Millionen an Startkapital von der israelischen Firma *Vertex Ventures*, die von Veteranen der israelischen Spionageeinheiten geführt wird. Tami Bronner, Teilhaberin bei *Vertex*, war vier Jahre lang im israelischen Militärgeheimdienst tätig.

Nach dieser frühen Finanzierung durch dem israelischen Geheimdienst nahestehende Investoren erhielt das Unternehmen weitere Investitionen in Höhe von mehreren hundert Millionen Dollar von einem Netzwerk US-amerikanischer Risikokapitalgesellschaften, die Verbindungen zum israelischen Geheimdienst haben.

Dazu gehört auch das in Palo Alto ansässige Unternehmen *Accel Partners*, das in mehr als dreißig israelische Technologieunternehmen investierte, darunter auch *Oasis*, ein weiterer Ableger der Cyber-*Einheit 8200*. Nir Blumberger, ein Israeli, der in der israelischen Armee gedient hatte, wurde 2016 von *Accel* von *Facebook* abgeworben, um das Büro in Tel Aviv zu eröffnen.

Zu den weiteren Geldgebern von *Axonius* gehört das in San Francisco ansässige Unternehmen B*essemer Venture Partners*, das ehemalige israelische Geheimdienstmitarbeiter in einem Büro in Tel Aviv unter der Leitung von Adam Fisher beschäftigt. Fisher, ein Amerikaner, der 1998 nach Israel emigrierte, fungierte als Vermittler zwischen Zionisten im Silicon Valley und der israelischen Armee und hielt während des Völkermords einen Vortrag darüber, wie Israel den Online-Krieg gewinnen kann. Der Israeli Amit Karp, Partner bei *Bessemer Ventures* und ebenfalls ehemaliger israelischer Geheimdienstoffizier, sitzt im Vorstand von *Axonius*.

Das in Menlo Park ansässige Unternehmen *Lightspeed Venture Partners*, das *Axonius* in mehreren Finanzierungsrunden mit rund 200 Millionen Dollar unterstützte, unterhält ebenfalls enge Beziehungen zu israelischen Spionageeinheiten. Yonit Wiseman, Teilhaberin bei *Lightspeed*, war sechs Jahre lang im israelischen Militärgeheimdienst tätig und schied 2018 aus. Ihr Kollege Tal Morgenstern war Kommandeur einer Spezialeinheit der israelischen Streitkräfte.

Angesichts der Beweise, dass *Axonius* ein direkter Abkömmling des israelischen Geheimdienstes ist, ist das Ausmaß seiner Vernetzung innerhalb der Struktur der US-Bundesregierung außergewöhnlich.

Das Unternehmen gibt an, dass seine Plattform „in mehr als 70 Bundesbehörden eingesetzt wird“ und dass sie vier der fünf großen Dienststellen des US-Verteidigungsministeriums nutzen. Die

Website der US-Bundesregierung für die Vergabe von Aufträgen zeigt, dass *Axonius* Aufträge für die Armee, die Marine, die Luftwaffe und das Marine Corps erhalten hat, was allein schon Millionen von Mitarbeitern und den dazugehörigen Geräten entspricht.

Im November 2024 wurde das Unternehmen vom Ministerium für Innere Sicherheit ausgewählt, um dessen Fähigkeit zur Cybersicherheit zu modernisieren, indem „Daten aus Hunderten von separaten Datenquellen, die sich über Dutzende von Bundes-, Zivil- und Exekutivbehörden verteilen", zentralisiert werden. Nur einen Monat später, im Dezember 2024, wurde das Unternehmen vom Verteidigungsministerium beauftragt, sein System zur Rund-um-die-Uhr-Überwachung zu modernisieren, das alle internen und externen Computer und IT-Netzwerke des Verteidigungsministeriums überwacht – eine Funktion, die als „kontinuierliche Überwachung und Risikobewertung" bekannt ist. Und im April dieses Jahres erhielt *Axonius* die Lizenz für alle US-Bundesbehörden, sein cloudbasiertes Cyberüberwachungssystem zu nutzen.

Weitere Bundesbehörden, die *Axonius*-Software integrieren, sind unter anderem die Bereiche Energie, Verkehr, das US-Finanzministerium und viele andere. Daten der US-amerikanischen Website für Fördermittelvergabe zeigen, dass die *US Defense Logistics Agency*, zuständig für die Verwaltung der globalen Waffenlieferkette der USA, mit Ausgaben in Höhe von 4,3 Millionen US-Dollar allein im Jahr 2023 der größte Einzelkunde von *Axonius* war. Das Landwirtschaftsministerium hat fast 2 Millionen Dollar für *Axonius*-Tools ausgegeben, und das Ministerium für Gesundheit und Soziales hat seit 2021 1,3 Millionen Dollar dafür aufgewendet.

Axonius wird gemeinhin als amerikanisches Unternehmen beschrieben. Während sich der Hauptsitz und die Verwaltungsbereiche in New York befinden, sind die Gründer, Führungskräfte und Hauptfinanzierer alle Israelis, und vor allem sind die Software- und Engineering-Funktionen in Tel Aviv angesiedelt. *Axonius* hat mehr als achthundert Beschäftigte, und eine Suche in *LinkedIn*-Profilen bestätigt, dass die Mehrheit der Ingenieure von Axonius in Tel Aviv einen Hintergrund im israelischen Militärgeheimdienst hat.

Das *Axonius*-System zeichnet sich dadurch aus, dass es Daten aus allen Sicherheits- und IT-Tools, die ein Unternehmen nutzt, an einem Ort zentralisiert, um die Analyse, Kontrolle und Fehlerbehebung zu vereinfachen. Dieser Ort ist Tel Aviv, wo Hunderte ehemaliger israelischer Spione, die als Ingenieure für Axonius arbeiten, beispiellosen Zugang und Einblick in Lebensweisen und Bewegungen von Millionen von Mitarbeitern der US-Bundesregierung haben. Mit dieser Transparenz kann ein *Axonius*-Operator einzelne Geräte mit individuellen IDs verbinden und alle Anmelde-/Abmeldedaten sowie die Website-Nutzung einsehen. Ein Operator kann auch die Deaktivierung eines Kontos, die Quarantäne eines Geräts oder die Entfernung eines Benutzers aus einer Gruppe anordnen.

Außerdem verfügt *Axonius* über eine separate Forschungs- und Entwicklungsabteilung innerhalb des Unternehmens namens *AxoniusX*, eine *Skunkworks*-Einheit, die sich auf die Entwicklung neuer Cyber-Werkzeuge konzentriert und von einem weiteren Spion der *Einheit 8200*, Amit Ofer, geleitet wird.

Vielleicht spielt all das keine Rolle, und *Axonius* ist lediglich ein Beispiel für die zwielichtige, symbiotische Natur der Beziehung zwischen den USA und ihrem kolonialen Außenposten. Der Einwand wäre berechtigt, gäbe es da nicht Israels lange Geschichte der Spionage in den Vereinigten Staaten.

Von der Anwerbung von Hollywood-Produzenten, die Scheinfirmen leiteten, die Nukleartechnologien stahlen, bis hin zum Verkauf von verwanzter Software an ausländische Regierungen – Spionage (insbesondere Cyberspionage) war schon immer ein zentraler Bestandteil der israelischen Außenpolitik. Robert Maxwell, der Vater von Ghislaine Maxwell, war ein Spion für Israel, und eine Vielzahl von Indizien deutet darauf hin, dass auch Jeffrey Epstein ein Agent des israelischen Militärgeheimdienstes war. In jüngerer Zeit, während Trumps erster Amtszeit, platzierte Israel Miniatur-Spionagegeräte 3 rund um das Weiße Haus und andere US-Regierungsgebäude in Washington DC, um US-Beamte zu überwachen.

Die US-Behörden haben also ehemaligen Spionen aus einem Land, das bekanntermaßen Spionage innerhalb der Vereinigten Staaten betrieben hat, erlaubt, einen Cyberspionage-Zugang zu fast dem gesamten Apparat der Bundesregierung aufzubauen. Mit anderen Worten: Die USA haben ihre Cybersicherheitsinfrastruktur auf Bundesebene faktisch an den israelischen Geheimdienst ausgelagert.

Ob *Axonius* seinen beispiellosen Zugang missbräuchlich nutzte oder dies beabsichtigt, lässt sich nicht sagen. Wer jedoch mit der Geschichte der Spionageaktivitäten Israels vertraut ist, sollte angesichts der Einbettung von Cybersoftware ehemaliger israelischer Spione in das Computersystemnetzwerk der US-Bundesbehörden ernsthaft besorgt sein.

Allgemeiner betrachtet zeigt *Axonius*, wie ein militarisierter israelischer Staat jedes Jahr Milliarden an amerikanischen Geldern erhält, um seine digitale Architektur der Apartheid und des Völkermords aufzubauen, und dann diese Fähigkeiten an die USA zurückverkauft. Die amerikanischen Steuerzahler bezahlen Israel also praktisch doppelt. Und mit dem Rückkauf der Technologien, ursprünglich finanziert von ihren Steuerzahlern, ermöglichen die USA die Einführung von Trojaner-Funktionen und bereichern dabei israelische Kriegsverbrecher.

Die gute Nachricht ist, dass Millionen gewöhnlicher Amerikaner langsam erkennen, dass Israel für die USA gar nicht so vorteilhaft ist, wie es ihnen von ihren politischen Führern seit langem verkauft wird. Die Geschichte von *Axonius* bestätigt einmal mehr, wie schlecht dieser Deal ist.

1. https://cyberscoop.com/axonius-4-million-seed-funding-unit-8200/
2. https://www.linkedin.com/pulse/two-weeks-term-sheet-axonius-funding-story-yoav-leitersdorf
3. https://www.politico.com/story/2019/09/12/israel-white-house-spying-devices-1491351
4. https://www.brookings.edu/articles/support-for-israel-continues-to-deteriorate-especially-among-democrats-and-young-people/

(Innerhalb des Originalartikels gibt es weitere Links)

Dieser Artikel wurde ursprünglich von ¡Do Not Panic! veröffentlicht.

Quelle: https://thegrayzone.com/2025/12/03/israeli-spies-run-us-cybersecurity/

Übersetzung für Pako: A. Riesch – palaestinakomitee-stuttgart.de