Das ›Cyber Horse‹ am Campus der Universität Tel Aviv: Es besteht aus Tausenden PCs und Handys – allesamt mit Computerviren infiziert.

Colorpilker/shutterstock

Nach über sechs Jahren Ruhe stehen in Österreich wieder Trojaner vor der Tür. Sie sind in der Novelle zum Staatsschutz- und Nachrichtendienstgesetz versteckt, dessen Begutachtungsfrist Anfang Juni abgelaufen ist. Im Ministerrat herrscht bereits grundsätzliche Einigung zu diesem Gesetzesentwurf, der Anfang Juli mit ein paar Änderungen beschlossen werden soll. Wie schon beim letzten Versuch im Jahr 2018, Technologien und Methoden der organisierten Kriminalität als polizeiliche Ermittlungsinstrumente festzuschreiben, hagelte es negative Stellungnahmen. An die hundert trafen diesmal ein. Die aktuellen Passagen zur Überwachung von WhatsApp, Signal und Co. mittels Trojaner-Schadsoftware unterscheiden sich nämlich kaum von der Version, die der Verfassungsgerichtshof (VfGH) 2019 verworfen hat. Hauptgrund für die damalige Einstufung als verfassungswidrig war die Erkenntnis, dass es technisch nicht möglich ist, die Zugriffe von Trojanern auf Chat-Programme zu beschränken. Weil aber unverschlüsselte SMS und Telefonate durch verschlüsselte Chatprogramme weitgehend abgelöst wurden, bedürfe es einer Möglichkeit zur Überwachung auf dem Endgerät, bevor verschlüsselt übertragen wird: So hatten die Innenminister Wolfgang Sobotka, dann Herbert Kickl und jetzt Gerhard Karner nacheinander argumentiert. Der Einsatz von Trojaner-Schadsoftware wurde als bloße technische Fortschreibung der Überwachung von Telefonienetzen ins Internet-Zeitalter dargestellt.

Diese Analogie stimmt gleich auf mehreren Ebenen nicht. Es ist, als würde man eine richterlich genehmigte Hausdurchsuchung durch Polizeibeamte samt Protokoll, Dokumentation und Rechtsschutzbeauftragten mit einem bestellten Wohnungseinbruch durch internationale Berufseinbrecher gleichstellen. Dieser Vergleich ist keineswegs weit hergeholt. Die Herstellung und der Vertrieb von solcher Schadsoftware für Strafverfolger ist ein hochriskantes Geschäft, denn früher oder später kommt jedes dieser Unternehmen zwangsläufig mit EU-Recht oder US-Gesetzen in Konflikt. Der mutmaßliche Weltmarktführer NSO Group ist aktuell in eine ganze Serie von Prozessen verwickelt, bis hin zu einem prominenten Mordfall, in dem Trojaner-Spionagesoftware ebenfalls eine Rolle spielte. Die NSO Group, das Intellexa Consortium, Candiru und Paragon Solutions – allesamt aus Israel – teilen sich derzeit den europäischen Markt. Das geht aus zwei aktuellen Studien des NATO-nahen Thinktanks ›Atlantic Council‹ hervor.

Dieser Markt folgt zwar in etwa den Geschäftspraktiken und Usancen, die beim internationalen Vertrieb von herkömmlicher Software herrschen, weicht aber in einigen entscheidenden Punkten davon ab. Die Unternehmen auf dem Markt für Schadsoftware für staatliche Überwachungszwecke sind auch deutlich anders strukturiert als herkömmliche Software-Konzerne, nämlich als dezentrale arbeitsteilige Konsortien. Das hat vor allem juristische Gründe.

Wie aber funktionieren die Dienstleistungen, die diese Unternehmen Geheimdiensten in aller Welt anbieten, eigentlich genau? Und hätte der Staat Österreich, wenn er denn zugreift, überhaupt die technische Kontrolle darüber, was genau er sich mit einem Bundestrojaner einkauft?

Um das zu beantworten, lohnt ein Blick auf die Hersteller. Alle vier genannten Unternehmen sind multinationale Syndikate aus Sub- und Partnerfirmen und dabei auch in einem oder mehreren EU-Staaten niedergelassen. Die Entwicklung der Schadsoftware selbst findet jedoch bei allen außerhalb des EU-Raums statt, denn Entwicklung, Vertrieb und der Einsatz von Schadsoftware ist in allen EU-Staaten grundsätzlich einmal verboten. NSO, Candiru und Paragon entwickeln ihre Trojaner in Israel, wo sich auch ihre Zentralen befinden. Nur Intellexa ist in Griechenland niedergelassen, seine ›Predator‹-Trojanersuite wird jedoch von einem Partnersyndikat in Nordmazedonien entwickelt. Eigentümer, Management und die leitenden Techniker sind Israelis und fast alle sind Reservisten der Unit 8200, der in den Medien gern als ›Israels NSA‹ bezeichnet wird. Dasselbe gilt auch für die anderen drei Syndikate, denn die gesamte Branche der EU-Trojanerlieferanten besteht im Grunde aus ein paar Bataillonen von Reservisten dieser technischen Spionage-Einheit der israelischen Armee. Und jedes dieser vier Syndikate stand schon mindestens einmal im Zentrum eines Überwachungsskandals in Europa, oder in den USA auf schwarzen Listen bzw. vor Gericht.

SICHERHEIT

Einbruch auf Bestellung

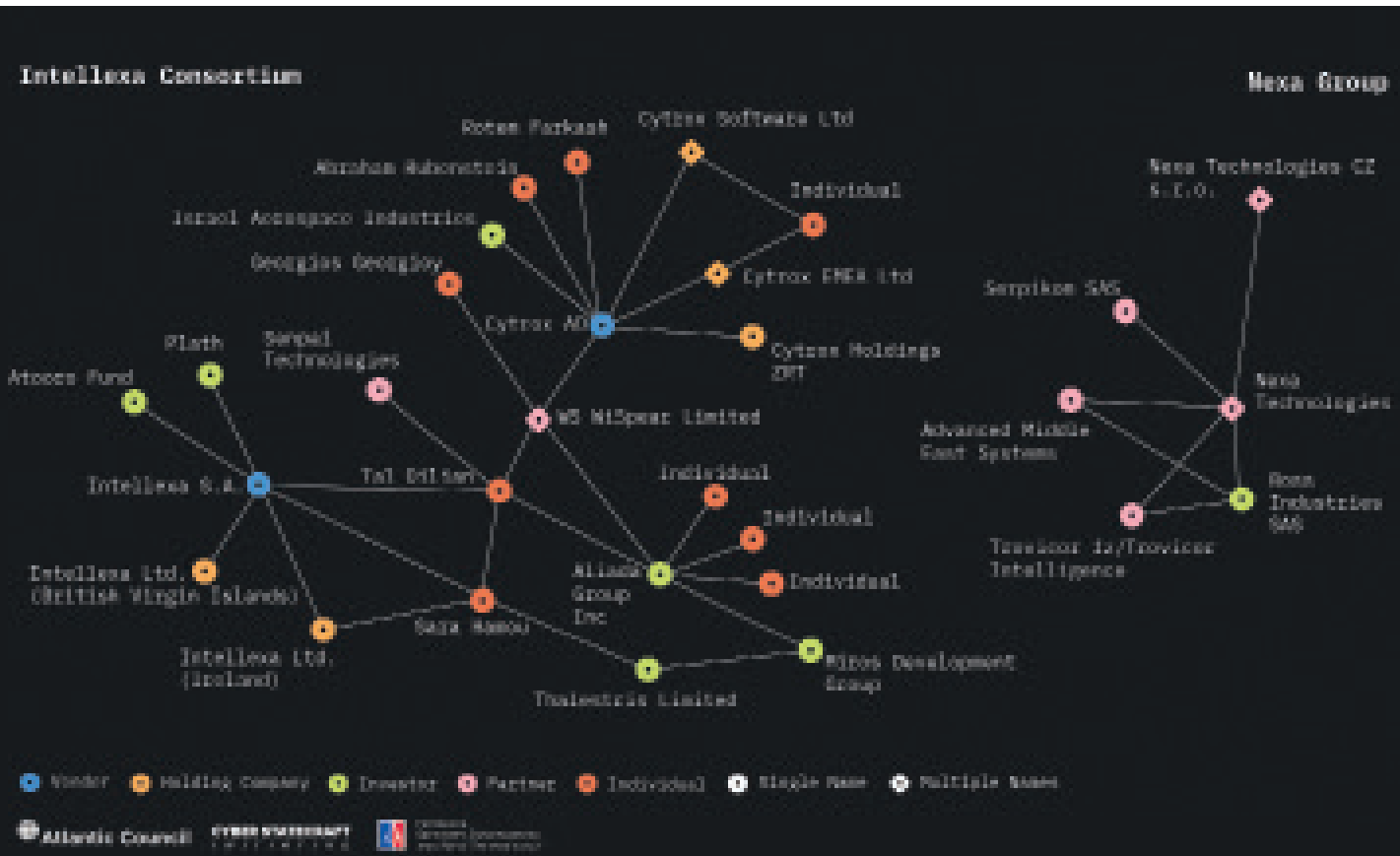
Der Bundestrojaner ist zum zweiten Mal seit 2018 in aller Munde. Wer aber sind die Unternehmen, die Geheimdiensten ihre hochspezialisierten Überwachungsdienste anbieten? Und darf die Republik ihnen vertrauen?

TEXT: Erich Moechel

Auf den bisherigen Marktführer in Europa, die israelische NSO Group, treffen gleich alle diese Punkte zu. Das mit zuletzt 700 Mitarbeitern wohl umsatzstärkste Unternehmen der Branche hatte seine Überwachungs-Suite mit Stand 2022 schon an Behörden in 14 EU-Staaten geliefert. Das kam im NSO-Untersuchungsausschuss des EU-Parlaments ans Licht, der nach einer Serie von Überwachungsskandalen eingesetzt wurde. Bei forensischen Untersuchungen an kompromittierten Smartphones waren 2021 Teile einer Liste von weiteren Zielgeräten aufgetaucht, darunter Smartphones aus dem Umfeld des französischen Präsidenten Emmanuel Macron sowie des spanischen Premiers Pedro Sánchez. In beiden Fällen führten die Spuren des Trojaners nach Marokko. Heftig kritisiert wurde in diesem Ausschuss die Nicht-Kooperation der israelischen Regierung, die in allen Fällen eine Exportlizenz erteilt hatte. Die mächtige ›Pegasus‹-Trojanersuite der NSO Group wird in Israel als militärische Waffe eingestuft, für jede Lieferung an einen Drittstaat braucht es eine Exportlizenz. Die Skandale entstehen immer dann, wenn derartige Schadsoftware an autoritär regierte Staaten geliefert wird, die sich nicht an die Auflagen der Lieferanten halten. Statt Kriminellen oder Terroristen werden dann heimische Oppositionelle und Dissidenten im Exil überwacht. Die Trojaner-Lieferanten geraten regelmäßig in die Bredouille, wenn diese grenzüberschreitende Überwachung durch Behörden eines Drittstaats im EU-Raum oder in den USA passiert. Auf die Skandale folgen dann Gerichtsverhandlungen, allein im Mai spielten sich rund um die NSO-Trojaner eine Reihe von Prozessen vor diversen Gerichten in Europa und den USA ab.

Das ungarische Verfassungsgericht etwa gab der Klage eines Fotojournalisten auf Auskunft statt, der mit einer Reihe von Journalisten, Oppositionspolitikern, Bürgerrechtsaktivisten und Anwälten 2021 mit dem Pegasus-Trojaner der NSO ausspioniert worden war. Diese Berufsgruppen und Akteure werden rund um den Globus weitaus am häufigsten mit Trojanern angegriffen. So auch Dschamal Kashoggi, Journalist der *Washington Post* mit saudi-arabischen Wurzeln. Kashoggi war nach dem Betreten des Istanbuler Konsulats seines Herkunftslands im Jahr 2018 spurlos verschwunden. Man geht davon aus, dass er im Konsulat umgebracht und zerstückelt wurde. Eine forensische Untersuchung der Smartphones im familiären Umfeld Kashoggis förderte Spuren des Pegasus-Trojaners zutage, und die führten in die Emirate sowie nach Saudi-Arabien. Kashoggis Ehefrau Hanan Elatr hatte in der Folge eine Klage wegen Beihilfe gegen die NSO Group in den USA eingereicht, in erster Instanz verloren, im Mai wurde auch ihre Berufung abgelehnt. Für das Gericht war nicht nachgewiesen, dass die Trojanerfirma von den Vorgängen Kenntnis hatte.

Der damalige CEO der NSO Group, Shalev Hulio, hatte jede Mitverantwortung zurückgewiesen. Man habe den Fall überprüft und keine Hinweise gefunden, dass Frau Elatrs Smartphone mit dem Pegasus-Trojaner überwacht worden sei. Wie aber konnte das die Firma überprüfen, wenn die Pegasus-Software von Be-



hörden der Emirate oder Saudi-Arabiens eingesetzt wurde? Ganz einfach, weil die Trojaner-Software auf einem befallenen Smartphone in der Regel über Server der Lieferfirmen gesteuert wird. Die Trojanersoftware auf dem Zielgerät ist ja nur ein Teil einer weit größeren Software-Suite, die weiters aus einem externen Command-Control-Netzwerk und der Auswertungssoftware bei den Behörden besteht. Wie bei den meisten anderen hochspezialisierten Software-Anwendungen ist auch die Überwachung mit Trojanern primär ein Dienstleistungsgeschäft.

Ganz deutlich wird der Dienstleistungscharakter in einem weiteren Fall, der ebenfalls im Mai bei einem US-Berufungsgericht eingereicht wurde. Geklagt hatten mehrere Journalisten aus El Salvador, die mit dem Pegasus-Trojaner ausspioniert worden waren. Die Klage wurde deshalb in Kalifornien eingereicht, weil die Spionagesoftware über Server von Apple auf die iPhones der Journalisten geschmuggelt worden war. NSO-Mitarbeiter hatten Server des iPhone-Herstellers gehackt, um ihre Spionagesoftware einfach und unauffällig auf die Zielgeräte aufzubringen. Der Prozess, den Apple selbst in dieser Angelegenheit gegen NSO angestrengt hatte, wurde im Herbst 2024 hingegen überraschend eingestellt. Beobachter gehen davon aus, dass Apple das Angebot von NSO auf eine stille Einigung akzeptierte, um eine öffentliche Diskussion über seine Sicherheitsstandards zu vermeiden.

Begonnen hatte der Mai 2025 jedoch mit einem Paukenschlag, der das Ende der NSO Group einläuten könnte. Ein kalifornisches Gericht verurteilte das Unternehmen zur Zahlung von 168 Millionen Dollar an Mark Zuckerbergs Meta-Konzern. NSO wurde schuldig gesprochen, ein parasitäres Geschäftsmodell auf der Infrastruktur von Meta aufgezogen zu haben. Wie im Fall Apple wurde die NSO-Schadsoftware über gehackte Server ausgebracht, in diesem Fall über solche von WhatsApp. Der aktuelle CEO des Unternehmens, Yaron Shohat, gestand den Sachverhalt zwar ein, zeigte sich aber außerstande, die Strafe zu bezahlen. Das Unternehmen komme bei monatlichen Fixkosten von zehn Millionen Dollar gerade so über die Runden, sagte Shohat. Und die Aktiva von 158 Millionen in der Bilanz – NSO musste seine Bücher teilweise offenlegen – seien Forderungen an Partnerfirmen, die leider uneinbringlich seien. Anfang Juni reichte die NSO Group Berufung ein, mit dem erklärten Ziel einer Reduktion der Strafe. Eine Sprecherin des Meta-Konzerns gab dagegen an, man wolle nun erreichen, dass die NSO Group nie wieder in der Lage sein werde, WhatsApp und seine User anzugreifen.

Sollte die zweite Instanz dieses Urteil bestätigen, dann wird die 2010 gegründete NSO Group das in ihrer derzeitigen Form wohl nicht überleben. Die Fixkosten in dieser Branche sind tatsächlich sehr hoch, und sie betreffen vor allem die Entwicklung. Jede geschlossene Sicherheitslücke, jedes Stück ihrer Schadsoftware, das von Anti-Virus-Firmen veröffentlicht wird, entwertet Teile ihres Arsenals. ›Exploits‹ für drei verschiedene Betriebssysteme müssen neu zugekauft oder selbst entwickelt (siehe Kasten) und Passagen der Software umgeschrieben werden, um den Virusscannern zu entgehen. Dazu kommen die Kosten der Prozesse, in die man unweigerlich verwickelt wird. Aktuell dürfte die NSO allerdings über genügend flüssige Mittel verfügen, denn Anfang Juni gab man auf der weltgrößten Überwachungsmesse ISS World in Prag wie jedes Jahr den Hauptsponsor. Die Eigentümerstruktur der NSO Group aber hatte sich schon 2022 verändert, die Luxemburger Dufresne Holding hält seitdem alle Anteile und es gab Entlassungen. Shalev Hulio, der die riskante Strategie, auf Server von Weltkonzernen einzubrechen, als CEO zu verantworten hatte, verließ das Unternehmen. Ein Jahr später gründete er mit einem Partner aus dem NSO-Syndikat sowie Sebastian Kurz das KI-Start-Up ›Dream Security‹.

Ab 2019 bekam die NSO Group, die jahrelang im EU-Raum dominiert hatte, Konkurrenz als beliebtester Trojanerlieferant europäischer Behörden, als das ›Intellexa Consortium‹ auf der Bildfläche erschien. Dieses Syndikat ist in Zypern, Griechenland, Frankreich, Deutschland, Tschechien, der Schweiz et al. niedergelassen und nutzte das, um seinen Trojaner als ›europabasiert und unter europäischer Regulation‹ zu vermarkten. Ein Teil der Softwareentwicklung passiert in Griechenland, dem derzeitigen Hauptquartier, die heiklen Elemente der Trojanersoftware ›Predator‹ wurden anfangs in der ungarischen Dependance entwickelt, aber schon bald wurde die Produktion in ein Partnersyndikat namens Cytrox nach Nordmazedonien ausgelagert.

Als Folge der Serienangriffe mit Verschlüsselungstrojanern durch internationale Erpresserbanden hatte sich nämlich abgezeichnet, dass die einschlägigen Strafrechtsparagrafen EU-weit bald verschärft würden. So auch in Österreich, wo der Strafrahmen für ›widerrechtlichen Zugriff auf ein Computersystem‹ etwas verspätet 2023 angehoben wurde. ›Wer sich zu einem Computersystem... durch Überwindung einer spezifischen Sicherheitsvorkehrung ... in der Absicht Zugang verschafft, sich ... Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt ... ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen‹, heißt es im § 118a StbG. Geschieht dies im Rahmen organisierter Kriminalität, steigt der Strafrahmen auf fünf Jahre.

Die in dieser Grafik abgebildete Firmenstruktur des **Intellexa Consortiums** ist in ihrer Dezentralisierung typisch für die gesamte Branche. Finanz- und Vertriebszentrum ist die **Intellexa S.A**. in Griechenland, die Holdings sind jedoch in Steuerparadiesen angesiedelt. Die Predator-Schadsoftware wird von der **Cytrox AD** in Nordmazedonien entwickelt, und die wird von drei Holdings kontrolliert. Wichtigster Investor sind die **Israel Aerospace Industries**. Ganz rechts ist das **Nexa-Partnersyndikat** abgebildet, dem unter anderen die deutsche Trovicor angehört. Dieses Konsortium vertreibt vor allem Hard- und Softwares zur Überwachung von Mobilfunknetzen sowie des Internetverkehrs.

Die Stellen im Gesetzestext treffen sowohl auf Trojaner von Cyberkriminellen wie auf Polizeitrojaner zu. Die ›spezifischen Sicherheitsvorkehrungen‹, die etwa auf der Android-Plattform überwunden werden müssen, sind zum Beispiel Google Play Protect oder diverse Anti-Virusprogramme, die verhindern sollen, dass ein Programm aus seiner ›Sandbox‹ ausbricht und verdeckt die Kontrolle über das gesamte Smartphone übernimmt. Und das tun sowohl die Pegasus-Suite von NSO wie auch die Predator-Schadsoftware von Intellexa. Beides sind Universaltrojaner, die von der Protokollierung aller Tastatureingaben, Freischalten von Mikrofon und Kamera, bis zur Speicherdurchsuchung alles überwachen können. In ihrer Funktion beschränken lassen sich solche Schadsoftwares grundsätzlich kaum.

Das ›europäisch regulierte‹ Image kam dem Intellexa-Syndikat, dessen Schadsoftware sich bei Europas Polizeibehörden anfangs großer Beliebtheit erfreute, in Rekordzeit abhanden. Drei Jahre nach der Gründung stand das Syndikat bereits im Zentrum des ›Predatorgate‹ genannten Überwachungsskandals in Griechenland. Rund fünfzig Personen des öffentlichen Lebens – Militärs, Journalisten, Anwälte und Oppositionspolitiker – waren vom griechischen Geheimdienst EYP 2022 illegal überwacht worden. Anfang April 2025 begann der zugehörige Strafprozess, angeklagt sind allerdings nicht die Auftraggeber, die aus Regierungskreisen stammen müssen, sondern die Eigentümer des Syndikats. Tal Dilian, ehemaliger Kommandeur einer technischen Spezialeinheit der israelischen Armee, und seine Ex-Gattin Sara Hamou stehen deshalb persönlich vor Gericht. Laut Anklage bot Intellexa als besonderen Service nämlich an, die Angriffe auf Zielpersonen mit dem Predator-Trojaner selbst durchzuführen. Aufträge dieser Art wurden mutmaßlich auch für Diktaturen wie Singapur, Sudan, Vietnam, Angola oder Indonesien erledigt, die Journalisten und Dissidenten im Exil überwachten. Nachdem immer mehr Fälle in Deutschland wie in den USA aufgeflogen waren, brachten forensische Untersuchungen von Amnesty International erneut Listen mit Telefonnummern von prominenten Zielpersonen ans Licht. Sowohl Roberta Metsola, die Präsidentin des EU-Parlaments, wie Tsai Ing-wen, der Präsident Taiwans, fanden sich da, sowie zwei US-Kongressabgeordnete oder die deutsche Botschafterin in den USA. 2024 landete auch Intellexa auf der schwarzen Liste des US-Finanzministeriums. Neben fünf Subfirmen des Syndikats wurden Hamou und Dilian persönlich sanktioniert.

Wenn in der DSN eine Software zum Einsatz kommen soll, die von Reservisten militärischer Geheimdienste eines Drittstaats entwickelt wurde, sollte eine gründliche technische Überprüfung eigentlich obligatorisch sein.

Mit Candiru steht bereits der dritte mögliche Lieferant für einen österreichischen Polizeitrojaner auf der schwarzen Liste der USA. Eine Behörde eines Drittstaats hatte mit dem Candiru-Trojaner im Jahr 2021 US-Staatsbürger überwacht. Einer der verseuchten Windows-Rechner wurde in Folge im ›Citizen Lab‹ der Universität Toronto untersucht. Dabei wurden die Kosten- und Abrechnungsstruktur des Candiru-Syndikats sichtbar. Das Startpaket kommt auf 16 Millionen Dollar und enthält unlimitierte Infektionsversuche, allerdings nur in einem einzigen Staatsgebiet, die Zahl der gleichzeitig überwachten Geräte ist auf zehn beschränkt. Für 1,5 Mio. zusätzlich können in zwei Ländern 15 weitere PCs oder Smartphones überwacht werden. Auch alle anderen Trojaner-Suites beinhalten ein ähnliches Lizenzierungssystem, das über das Command/Control-Netzwerk der Lieferfirma geschaltet und in Teilen auch auf dem verseuchten Endgerät abgebildet wird. Das erklärt, warum immer wieder ›Target Lists‹ mit Telefonnummern oder anderen Identifikatoren gefunden werden. Es sind ganz einfach jene Nummern, die im Rahmen eines solchen Zehner-Lizenzpakets zur Überwachung freigeschaltet wurden. Damit lässt sich allerdings nicht sagen, ob das betreffende Endgerät tatsächlich überwacht wurde – sondern nur, dass ein Geheimdienst oder eine Polizeibehörde eines Drittstaats eine Lizenz zur Überwachung dieses Geräts gelöst hat und über die entsprechenden technischen Mittel dafür verfügt.

Es ist davon auszugehen, dass Preise und Staffelung bei allen Anbietern ähnlich sind, wie etwa auch bei Paragon Solutions. Deren Schadsoftware unterscheidet sich von den übrigen Lieferanten insofern, als kein universaler Keylogger zum Einsatz kommt, der sämtliche Tastatureingaben mitschreibt. Im Hintergrund werkt der ›Graphite‹-Trojaner wie alle anderen natürlich quer durch das Betriebssystem. Allein zur Überprüfung, ob auch das richtige Zielgerät erwischt wurde, müssen die Hardware und die SIM-Card ausgelesen werden. An die Behörden ausgeleitet werden angeblich aber nur die Inhalte aus Chat-Programmen, die der Graphite-Trojaner allesamt befällt. Und genau diesen Trojaner hatten die Beamten des BMI bei der Abfassung des Ministerialentwurfs offensichtlich im Auge. ›Die einzubringende Software ist technisch regulierbar, sodass nur gezielte und von der Bewilligung umfasste Nachrichten aus bestimmten Applikationen ausgeleitet werden können‹, heißt es denn auch in den Erläuterungen zum BMI-Entwurf. Und das trifft eben nur auf Graphite-Trojaner von Paragon Solutions zu.

Seit seiner Gründung 2019 war dieses israelische Unternehmen im Vergleich zu anderen dieser Branche kaum negativ aufgefallen, doch im Dezember 2024 änderte sich das Bild. Da wurden Techniker von WhatsApp auf eine Kampagne aufmerksam, bei der insgesamt 90 Benutzerkonten mit dem Paragon-Trojaner

Perekotypole/Shutterstock.

verseucht worden waren. Wie sich herausstellte, wurden keine Kriminellen, sondern Mitarbeiter der Seenotretter-NGO ›Mediterranea‹, also Aktivisten der Flüchtlingshilfe, mit maßgefertigten ›Zero-Clicks-Exploits‹ auf der WhatsApp-Plattform angegriffen. Der Zuckerberg-Konzern kündigte rechtliche Schritte gegen die Ausbringer der Schadsoftware an, auf öffentlichen Druck setzte die postfaschistische Regierung Giorgia Melonis im Februar 2025 einen Untersuchungsausschuss ein. Dort wurde allerdings weniger untersucht, sondern vielmehr gemauert. Als die Vertreter der Regierung es ablehnten, sich mit den Fällen der überwachten Journalisten überhaupt zu befassen, kündigte Paragon Solutions den Vertrag. Das Unternehmen kann derzeit keine Skandale brauchen. Paragon ist nämlich gerade dabei, den US-Markt zu erobern, wo die gesamte Konkurrenz wie beschrieben auf einer schwarzen Liste steht.

Die Anfälligkeit dieses neuen verdeckten ›Ermittlungsinstruments‹ für Missbrauch scheint auch den Autoren des Ministerialentwurfs bis zu einem Grad bewusst zu sein. In den Erläuterungen ist mehrfach von der ›Sonderstellung‹ und der ›spezifischen Eingriffsintensität‹ die Rede, denen Rechnung getragen werden müsse. Als allererste Absicherungsmaßnahme fiel den Beamten allerdings ein, die Auskunftsrechte zu beschneiden, weil ›mit der Ermächtigung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten‹ seien. Des Weiteren ist viel von einem ›neuartigen Rechtsschutzsystem‹ und einem ›besonderen Bewilligungs- und Kontrollverfahren‹ samt Einbindung des Verwaltungsgerichtshofs die Rede. Es handelt sich dabei ausschließlich um Sicherungsmaßnahmen juristischer Natur. Von technischer Absicherung oder Kontrolle ist in den Erläuterungen nicht ein einziges Mal die Rede, wie etwa, dass der Quellcode dieser Software überprüft oder die gesamte Suite einem Live-Audit durch IT-Sicherheitsexperten unterzogen werden könnte.

Wenn in der Direktion Staatsschutz und Nachrichtendienst, dem Zentrum der heimischen Spionageabwehr, eine Software zum Einsatz kommen soll, die von Reservisten militärischer Geheimdienste eines Drittstaats entwickelt wurde, sollte eine gründliche technische Überprüfung doch eigentlich obligatorisch sein. Und ganz besonders dann, wenn einer der Gründer der Lieferfirma Paragon Solution Ehud Schneorson ist, Ex-Kommandeur der Unit 8200 im Brigadiersrang; und ein weiterer Gründer Ehud Barak heißt: Ex-Kommandant einer Mossad-Spezialeinheit, dann Generalstabschef, Verteidigungsminister und ehemaliger Ministerpräsident Israels. •

Der Autor empfiehlt
die Studie ›Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights‹ des Thinktanks ›Atlantic Council‹.