Daniel Leisegang

Pegasus oder: Der Angriff auf die Schwachstellen

Rund 60 Millionen Smartphones sind allein hierzulande in Gebrauch. Wie jedes einzelne dieser Geräte im Handumdrehen in eine leistungsfähige Wanze umgewandelt werden kann, zeigen die Enthüllungen über die mächtige Ausspähsoftware „Pegasus". Sie stützen sich auf Recherchen eines internationalen Journalistenkonsortiums, an dem hierzulande NDR, WDR, „Süddeutsche Zeitung" und „Die Zeit" in Kooperation mit der NGO Forbidden Stories und Amnesty International beteiligt sind.[1]

Pegasus wird von dem israelischen Unternehmen NSO vertrieben und gleicht weniger einem geflügelten als vielmehr einem trojanischen Pferd: Um eine Spähattacke auszuführen, genügt es, die Telefonnummer des Opfers zu kennen. Unbemerkt können Angreifer dann das Programm auf jedes beliebige Smartphone hochladen, aktivieren und so Zugriff auf nahezu alle Inhalte und Gerätefunktionen erhalten: SMS, E-Mails, Fotos sowie Kamera und Mikrofon. Selbst verschlüsselte Chatverläufe und Passwörter lassen sich auf diese Weise auslesen.

Mit ihrer „Spyware for hire" („Spionagesoftware zum Mieten") zählt das 2010 gegründete NSO längst zu den Marktführern in der Branche. Fast ebenso lang ist das Unternehmen berüchtigt dafür, bei der Auswahl seiner Kunden nicht besonders zimperlich zu sein. Weltweit verfügt NSO nach eigenen Angaben über mehr als 60 Kunden in 40 Ländern – unter anderem in Mexiko, Indien, Saudi-Arabien, Marokko, Aserbaidschan, Kasachstan, Ruanda sowie im EU-Mitgliedsland Ungarn. Um Pegasus nutzen zu können, mussten diese Staaten nur eines tun: Geld auf den Tisch legen. NSO verlangt eine pauschale Installationsgebühr in Höhe von 500 000 US-Dollar; weitere 650 000 Dollar kostet es, zehn iPhone- bzw. Android-Nutzer auszuspionieren.[2]

Digitale Waffe gegen Demokraten

Anders als von NSO behauptet, setzen diese Staaten Pegasus keineswegs nur „gegen die Bin Ladens dieser Welt" ein, sondern vor allem gegen Personen, die Demokratie, Menschen- und Grundrechte verteidigen. Das belegt eine brisante Liste von rund 50 000 Telefonnummern mit Pegasus-Opfern, die Forbidden Stories im Vorfeld der Enthüllungen zugespielt wurde.

Die Nummern gehören hunderten von Regierungsmitgliedern und -mitarbeiterinnen sowie 85 Menschenrechtsaktivisten und 189 Journalistinnen in aller Welt. Ausgespäht wurden unter anderem die Verlobte des 2018 mutmaßlich von der saudi-arabischen Regierung ermordeten Journalisten Jamal Khashoggi, der britische Menschenrechtsanwalt David Haigh, die aserbaidschanische Investigativjournalistin Sevinj Vagifgiz, Mexikos Präsident Andrés Manuel López Obrador, der sich zum Zeitpunkt der Überwachung noch in der Opposition befand, der indische Oppositionsführer Rahul Gandhi sowie der französische Präsi-

1 Vgl. www.forbiddenstories.org.

2 Vgl. Pegasus Hack: How Much Did it Cost to Spy on Citizens?, www.thecitizen.in, 23.7.2021.

dent Emmanuel Macron. Auch mehrere ungarische Journalistinnen und Lokalpolitiker zählen zu den Opfern.

Trotz dieser Belege weist NSO jede Verantwortung von sich: Einen Automobilhersteller würde man auch nicht dafür haftbar machen, wenn jemand mit einem von ihm gebauten Wagen betrunken einen Unfall baue. Der Vergleich führt allerdings in die Irre: Denn NSO verkauft kein Fortbewegungsmittel, sondern eine digitale Waffe, die sich gegen jede beliebige Person richten lässt. Vor allem aber belegen die Enthüllungen, welch immense Gefahr von Sicherheitslücken in Software und IT-Infrastrukturen ausgeht.

Lücken im System

Denn Pegasus nutzt Programmierfehler, um auf fremde Smartphones zu gelangen – im besten Fall sogenannte Zero-Exploit-Schwachstellen, die selbst den Herstellern der auf den Smartphones installierten Betriebssysteme unbekannt sind. Mitunter soll NSO gleich mehrere dieser „Zero Days" nacheinander verwenden, um ein Smartphone zu infiltrieren.

Insofern sind die Pegasus-Enthüllungen auch ein gewaltiges PR-Desaster für Apple und Google. Beide Konzerne sind eigentlich für die Sicherheit jener Geräte verantwortlich, auf denen ihre Betriebssysteme, iOS und Android, laufen. Eben damit werben sie auch vollmundig: „What happens on your iPhone, stays on your iPhone", lautet etwa ein Werbespruch von Apple. Tatsächlich aber hebelt Pegasus die vermeintlich unüberwindbaren Schutzvorkehrungen auf Apples Smartphones, von denen der Konzern allein im vergangenen Jahr weltweit knapp 190 Mio. Stück verkaufte, kurzerhand mit einer „stillen Nachricht" über Apples hauseigenen Chat-Dienst *iMessage* aus. IT-Experten zeigten sich davon allerdings nicht sonderlich überrascht: Bereits seit längerem ist bekannt, dass iMessage gefährliche Schwachstellen aufweist.[3]

Bei Android sieht es nicht viel besser aus: Googles Betriebssystem beruht zwar zu einem Großteil auf Open-Source-Programmcode, der offen einsehbar und damit auch von Experten geprüft und korrigiert werden kann – allerdings nur, wenn diese die von ihnen gefundenen Schwachstellen publik machen und nicht zu einem hohen Preis an Unternehmen wie NSO verkaufen. Hinzu kommt, dass Google die Apps im *Google Play Store* weniger streng prüft als Apple und auf vielen älteren Android-Smartphones häufig Versionen des Betriebssystems laufen, für die die Betreiber keine Updates mehr bereitstellen und die daher zusätzliche Einfallstore für Schadsoftware bieten. Das erklärt auch, warum die Ausnutzung von Sicherheitslücken bei Android-Smartphones im vergangenen Jahr um sage und schreibe das Siebzehnfache zunehmen konnte.[4]

Angesichts dieser fahrlässigen Geschäftspraxis müsste die Politik das Duopol aus Apple und Googles Mutterkonzern Alphabet eigentlich erheblich stärker in die Pflicht und in Haftung nehmen. Das aber setzt voraus, dass Regierungen der Sicherheit von IT-Systemen und -Infrastrukturen einen entsprechenden Stellenwert einräumen. Dass wir davon derzeit noch meilenweit entfernt sind, belegt die rasante Zunahme sogenannter Ransomware-Angriffe – in den USA, aber auch hierzulande. Und auch bei diesen Attacken spielen Sicherheitslücken eine entscheidende Rolle.

Denn durch sie gelangen Hacker in Computersysteme, wo sie dann sämtliche Daten verschlüsseln. Nur wenn die Opfer den meist beträchtlichen Lösegeldforderungen der Angreifer nach-

3 Vgl. Remote iPhone Exploitation Part 1: Poking Memory via iMessage and CVE-2019-8641, https://googleprojectzero.blogspot.com, 9.1.2020.

4 Vgl. Victor Chebyshev, Mobile malware evolution 2020, www.securelist.com, 1.3.2021.

kommen, erhalten sie mit viel Glück ihre entschlüsselten Daten zurück. Schätzungen zufolge wurden auf diese Weise im vergangenen Jahr weltweit mehr als 400 Mio. US-Dollar erpresst – vier Mal mehr als 2019.[5]

Die Auswirkungen solcher Ransomware-Angriffe sind meist desaströs – nicht nur für einzelne Unternehmen, sondern auch für die kritische Infrastruktur ganzer Staaten. Das zeigte sich eindrücklich im Mai in den USA, als die Hacker-Gruppe „DarkSide" die *Colonial Pipeline* lahmlegte, durch die knapp die Hälfte aller an der US-Ostküste verbrauchten Kraftstoffe geleitet werden. Die Folgen waren steigende Mineralölpreise, ein regionaler Notstand, Panikkäufe und Chaos an den Tankstellen. Die Betreiber der Pipeline waren allerdings vorgewarnt: Nur drei Jahre vor dem Angriff hatte ein bei ihnen durchgeführtes Sicherheits-Audit „grauenhafte" Praktiken des Informationsmanagements und „einen Flickenteppich schlecht verbundener und gesicherter Systeme" offengelegt.[6]

Schon im Dezember 2020, noch in der Amtszeit von Joe Bidens Vorgänger Donald Trump, war ein großangelegter Angriff auf Unternehmen und Behörden im ganzen Land erfolgt. Mehr als 18 000 Mal wurde dabei über die Computerverwaltungssoftware der IT-Wartungsfirma SolarWinds Schadsoftware an die Opfer ausgespielt. Zu ihnen gehörte auch die *National Nuclear Security Administration*, jene US-Behörde, die für die Sicherheit und den Betrieb der US-Atomwaffen verantwortlich ist. Anfang dieses Jahres sorgte schließlich ein dritter landesweiter Angriff auf Microsoft Exchange Server für Schlagzeilen: Er traf Forschungseinrichtungen, Behörden, Rüstungskonzerne sowie zahlreiche weitere Unternehmen.

5 Uli Ries und Christian Wölbert, Warum Cybergangster mit Ransomware immer höhere Lösegelder erpressen, www.heise.de, 5.7.2021.

6 Frank Bajak, Tech audit of Colonial Pipeline found 'glaring' problems, www.apnews.com, 13.5.2021.

Trotz dieser überaus alarmierenden Vorfälle nahm die Trump-Regierung das Problem nicht ernst, sondern kehrte es unter den Teppich.[7] Die Biden-Administration geht es demgegenüber deutlich offensiver an: Sie beschuldigt chinesische Hacker, für einen Teil der Attacken verantwortlich zu sein. Darüber hinaus stellte die US-Regierung jüngst Pläne vor, wie sie systemrelevante Einrichtungen und Behörden besser schützen will. Vor allem die Unternehmen sollen dafür in die Pflicht genommen werden, in deren Hand fast 90 Prozent der kritischen Infrastruktur in den USA liegen.

Der Bundestag im Visier

So weit ist man hierzulande noch lange nicht – obwohl auch in Deutschland Angriffe auf IT-Systeme und -Infrastrukturen massiv zunehmen.

Schätzungen zufolge gelang es Hackern bundesweit in mehr als 100 Fällen, die Server von Behörden, Kommunalverwaltungen sowie anderen staatlichen und öffentlichen Stellen anzugreifen und deren Daten zu verschlüsseln.[8] Genaue Zahlen fehlen, weil es hierzulande weder eine offizielle Statistik noch eine Meldepflicht für derartige Angriffe gibt. Aus diesem Grund tauchen meist nur Einzelfälle in der Presse auf, wie etwa der Angriff auf das Berliner Kammergericht, das im Jahr 2017 Hackern ein verlockendes Ziel bot: Das Gericht setzte damals noch „Windows 95" ein – ein Betriebssystem aus dem Jahr 1995 für das Microsoft schon 2001 den technischen Support eingestellt hat.[9] Inzwischen steigt die Zahl derartiger Angriffe rasant an: Allein im Juli legten Hacker ein Klini-

7 Vgl. Sandra Joyce, Ransomware: The threat we can no longer afford to ignore, www.fireeye.com, 29.10.2020.

8 Maximilian Zierer und Hakan Tanriverdi, Mehr als 100 Behörden erpresst, www.tagesschau.de, 29.6.2021.

9 Vgl. Sascha Lobo, Die nächste Pandemie wird digital, www.spiegel.de, 14.7.2021.

kum in Wolfenbüttel sowie die Stadtverwaltungen in Anhalt-Bitterfeld und Geisenheim lahm. Deren Mitarbeiter mussten mitunter über Wochen auf Stift, Papier und Faxgerät umsteigen.

Wie verwundbar selbst die digitale Infrastruktur der bundesdeutschen Verfassungsorgane ist, belegte bereits ein offenbar politisch motivierter Angriff im Jahr 2015: Damals wurde das interne Netzwerk des Deutschen Bundestages großflächig angegriffen. Hacker, die mutmaßlich im Auftrag des russischen Geheimdienstes GRU handelten, stahlen rund 16 Gigabyte Daten; die gesamte IT des Parlaments musste daraufhin zwei Wochen lang neu aufgesetzt werden. Und im vergangenen März gerieten einzelne Bundestagsabgeordnete erneut ins Visier von Angreifern, die es diesmal auf ihre privaten Postfächer abgesehen hatten.

Staaten hacken mit

Bund, Länder und Kommunen hätten viele der bestehenden Sicherheitslücken mit vergleichsweise einfachen Maßnahmen längst schließen können – indem sie die digitale Sicherheit weit oben auf die politische Agenda setzen, Fachkräfte einstellen, ihre IT-Infrastruktur modernisieren – und diese regelmäßig „updaten".

Damit allein ist es allerdings nicht getan, und hier schließt sich der Kreis zu den Pegasus-Enthüllungen. Denn zahlreiche Staaten tragen durch eigene Ausspähpraktiken ebenfalls aktiv zur wachsenden Datenunsicherheit bei: Jahr für Jahr geben Geheimdienste weltweit Millionen dafür aus, um iPhones und Android-Telefone zu hacken. Auch das Bundeskriminalamt darf seit 2009 sogenannte Staatstrojaner im „Kampf gegen den internationalen Terrorismus" einsetzen. Und erst im Juni verabschiedeten CDU/CSU und SPD gemeinsam im Bundestag ein Gesetz, das auch dem Bundesverfassungsschutz mehr Rechte bei der Überwachung mit Hilfe der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) einräumt. Die dafür erforderlichen Sicherheitslücken kaufen die Behörden ebenso wie NSO auf dem „freien Markt" ein und müssen diese ebenfalls nicht den Softwareherstellern melden.

Immerhin hat das Bundesverfassungsgericht kürzlich angemahnt, dass Behörden die Nutzung von Sicherheitslücken sorgfältig gegen jene Risiken abwägen müssen, die sich daraus für Bürger, Wirtschaft und Staat ergeben. Auch müssten sie Softwareherstellern Schwachstellen melden, „wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt".[10] Diese grundsätzlich begrüßenswerte Vorgabe hat indes einen Haken: Sie überlässt die Risikoabwägung weiterhin den staatlichen Behörden. Allzu leicht können sie den Gebrauch von Schwachstellen weiterhin damit rechtfertigen, dass sie andernfalls beim globalen Ausspähwettrüsten ins Hintertreffen geraten – auch gegenüber kommerziellen Anbietern wie NSO.

Eine effektive Exportkontrolle von Spähsoftware ist somit überfällig. Weitaus wirksamer wäre jedoch ein konsequentes Abrüsten – also ein weltweites Verbot der behördlichen und kommerziellen Nutzung von Sicherheitslücken, insbesondere von Zero-Day-Exploits. Daneben bedarf es einer Meldepflicht neuer Schwachstellen sowie eine Verpflichtung der Techkonzerne, diese innerhalb einer kurzen Frist zu beheben.

Nur so kann verhindert werden, dass Kriminelle und autoritäre Regime Sicherheitslücken ausnutzen – zulasten unserer Sicherheit, unserer Privatsphäre und der Demokratie. Und die Bezeichnung Pegasus wäre damit auch wieder allein den geflügelten Fabelwesen aus der griechischen Mythologie vorbehalten.

10 Vgl. Stefan Krempl, Staatstrojaner: Verfassungsgericht auf Holzweg oder in dubio pro IT-Sicherheit?, www.heise.de, 31.7.2021.