Spionagesoftware hackt Telefone | Interview mit Dr. Shir Hever

Das Transkript gibt möglicherweise aufgrund der Tonqualität oder anderer Faktoren den ursprünglichen Inhalt nicht wortgenau wieder.

Zain Raza (ZR): Vielen Dank für Ihr Interesse und willkommen zu einer weiteren Folge von Die Quelle. Willkommen zum zweiten Teil mit Dr. Shir Hever und zur Fortsetzung unserer Diskussion. Wenn Sie den ersten Teil über die Aufstände im Westjordanland noch nicht gesehen haben, sollten Sie das unbedingt nachholen. In diesem Teil werden wir uns auf die Spionagesoftware Pegasus konzentrieren. Dr. Shir Hever, vielen Dank, dass Sie sich heute Zeit genommen haben.

Shir Hever (SH): Vielen Dank, dass ich hier sein darf.

ZR: Können Sie unseren Zuschauern zunächst die Eigenschaften dieser Pegasus-Spionagesoftware erläutern?

SH: Ja, gerne. Pegasus ist also nur eines der Programme, die von einem Unternehmen namens NSO Group entwickelt wurden. Es gibt etwa sechs israelische Spyware-Firmen, die verschiedene Arten von Software herstellen, mit der man sich in Telefone und Computer einhacken kann. Bei der Spyware handelt es sich um eine neuartige Technologie, die von israelischen Absolventen einer speziellen Geheimdiensteinheit, einer Signal Intelligence Unit, namens 8200, entwickelt wurde. Diese Einheit hackte Telefone von Menschen und spionierte sie aus, überwachte sie, die Palästinenser, um sie mit den von ihnen gesammelten Informationen zu erpressen und sie zu Kollaborateuren zu machen. Einige Mitglieder dieser Einheit waren schockiert und angewidert von den Aktivitäten der Einheit und enthüllten ihre Arbeitsweise.

Die überwiegende Mehrheit dieser Beamten hält es jedoch für absolut in Ordnung, die Privatsphäre von Menschen zu verletzen und sie zur Kollaboration zu erpressen. Schließlich waren sie überzeugt, dass dies eine großartige Möglichkeit zur Bereicherung darstellen

würde. Sie haben die Technologie, die vom israelischen Geheimdienst verwendet wurde, in ein Produkt verwandelt, das weltweit verkauft wird. Nach Angaben von Amnesty International, Forbidden Stories und Citizen Lab, die im vergangenen Juli einen sehr umfassenden Bericht veröffentlichten, wurde die Software von 45 Ländern gekauft und gegen Anwälte, Menschenrechtsaktivisten, Politiker und Zivilisten eingesetzt. Es handelt sich also nicht um ein militärisches Werkzeug, sondern tatsächlich um ein Werkzeug gegen Zivilisten, gegen die Zivilgesellschaft und gegen die Menschenrechte.

ZR: Es handelt sich um dieselbe Software, die von der saudischen Monarchie zur Lokalisierung von Jamal Khashoggi verwendet wurde, um mehr über dessen Aktivitäten herauszufinden und um zu erfahren, mit wem er korrespondierte, durch das Hacken seines Telefons, korrekt?

SH: Es ist dieselbe, auch wenn das Pegasus-Programm verschiedene Iterationen hat. Das Programm, das 2018 gegen Jamal Khashoggi eingesetzt wurde, ist eine ältere Version dessen, was jetzt auf dem Markt erhältlich ist. Eine der sehr beunruhigenden Entwicklungen dieses Programms besteht darin, dass es das Hacken von Geräten auf Distanz ermöglicht, ohne dass die Person, die das Gerät besitzt, irgendeine Möglichkeit hat zu wissen, dass das Gerät gehackt wurde. Ihr Telefon, mein Telefon, jeder von uns könnte also bereits gehackt worden sein. Wir können dies nicht wissen, ohne das Telefon tatsächlich zur forensischen Analyse an Citizen Lab oder eine ähnliche Organisation zu schicken, und selbst dann können sie nur feststellen, ob es gehackt wurde oder nicht. Das Beunruhigende an dieser Situation ist, dass nicht sein Telefon gehackt wurde, sondern das Telefon von jemandem, mit dem er korrespondierte. Er korrespondierte mit einem Menschenrechtsaktivisten in Kanada, und das Telefon in Kanada war dasjenige, das gehackt wurde.

So wurden die Gespräche mit Jamal Khashoggi der saudischen Regierung offengelegt, und die saudische Regierung entschied dann, dass ihr die Aussagen von Jamal Khashoggi nicht gefielen. Und sie, nun ja, aller Wahrscheinlichkeit nach, obwohl es vor Gericht nicht bewiesen wurde, aber ich denke, jedem ist bewusst, dass die Wahrscheinlichkeit sehr hoch ist, dass Jamal Khashoggi im saudischen Konsulat in Istanbul ermordet wurde, basierend auf den Informationen, die das israelische Unternehmen für die saudische Regierung gesammelt hat. Selbst wenn unser Telefon nicht gehackt wurde, könnten wir mit jemandem korrespondieren, dessen Telefon gehackt wurde. Und wieder einmal gelangen unsere Informationen in die falschen Hände, was extrem gefährlich und natürlich auch extrem illegal ist.

ZR: Das erinnert mich an die von Edward Snowden aufgedeckten NSA-Programme, die eigentlich ausländische Ziele überwachen sollten, aber wenn sie mit Amerikanern korrespondierten, waren sie in der Lage, diese abzufangen und auf die Inlandsebene auszuweiten. Zurück zu dieser Software. Natürlich werden sich die Menschen hier in Deutschland fragen: Was geht mich das an? Was macht Deutschland im Moment mit Israel? Kauft es die Software? Ist es in irgendeiner Weise beteiligt? Und der zweite Teil der Frage,

die Sie danach beantworten könnten, ist, dass die meisten Leute sagen würden: Ich habe nichts zu verbergen; die Regierung kann mich ruhig ausspionieren. Was sagen Sie dazu?

SH: Zunächst einmal hat eine Abteilung der deutschen Polizei, die deutsche Bundespolizei, Pegasus erworben. Sie hat die Software von der NSO Group gekauft. Als dies in den Medien aufgedeckt wurde und ihnen Fragen dazu gestellt wurden, was sie mit diesem Programm beabsichtigen und was sie ausspionieren, antworteten sie, dass sie nicht die Absicht hätten, es zu benutzen. Es handelt sich aber um eine sehr teure Software. Wenn sie also die Wahrheit sagen, so wurden Millionen von Euro verschwendet. Wenn sie lügen, dann spionieren sie deutsche Bürger aus. Das ist sehr beunruhigend und bedarf einer Untersuchung.

Zurzeit läuft eine Untersuchung durch das Europäische Parlament. Es gibt einen Ausschuss von Parlamentsmitgliedern, die auch nach Israel gereist sind, um mit Mitgliedern der NSO-Gruppe zu sprechen, sowie mit Opfern dieser Software, und um Informationen zu sammeln. Es wird ein Verfahren geben, in dem die EU-Beamten für den Kauf der Spionagetechnologie zur Rechenschaft gezogen werden, die normalerweise von Organisationen wie der von Ihnen erwähnten NSA für die Spionage von Staat zu Staat, für militärische Spionage, eingesetzt wird. Aber hier geht es um ein Unternehmen, ein privates Unternehmen, das Spionagetechnologie auf staatlicher Ebene einsetzt und sie an den Meistbietenden weitergibt. Das ist äußerst gefährlich.

Aber ich möchte das wichtigere Thema ansprechen, nämlich die Frage, ob es sich tatsächlich um ein Instrument für die Strafverfolgung handelt; die NSO-Gruppe selbst sagt gerne, dass es zur Bekämpfung von Terrorismus und Kriminalität eingesetzt würde. Zunächst einmal gibt es keinen einzigen dokumentierten Fall, in dem Spionageprogramme zur Aufklärung von Verbrechen oder zur Verhinderung von Straftaten beigetragen haben. Und dafür gibt es einen guten Grund. Denn das Programm selbst ist, technologisch gesehen, für die Strafverfolgung einfach nicht nützlich. Bei der Strafverfolgung geht es um Transparenz. Es geht um ganz klare Verfahren. Wenn man Beweise sammeln will, die vor Gericht verwertbar sind, dann braucht man ein Verfahren zum Sammeln dieser Beweise, das von den Gerichten zurückverfolgt und beobachtet werden kann. Andernfalls sind alle Beweise, die Sie sammeln, nutzlos. Das ist genau der Punkt, denn wie ich schon sagte, wenn Ihr Telefon dann in einem forensischen Labor analysiert wird, kann man zwar nachvollziehen, ob das Telefon gehackt wurde, aber man weiß nicht, wann und von wem, geschweige denn, was genau mit dem Telefon gemacht wurde.

Diese Spyware ermöglicht jemandem die volle Kontrolle über ein Gerät, d. h. er kann aus der Ferne Kamera und Mikrofon aktivieren und sämtliche Vorgänge in der Umgebung des Telefons verfolgen. Sie können auch Daten vom Telefon herunterladen, aber sie können auch auf dem Telefon programmieren. Sie können auf Ihrem Social-Media-Konto unter Verwendung Ihres Kontos so schreiben, dass es aussieht, als hätten Sie etwas verfasst, was Sie nicht beabsichtigt haben. Das gibt der Polizei oder jedem, der Zugang zu der Software

hat, eine Menge Macht. Im Grunde könnten sie unschuldige Menschen mit gefälschten Beweisen belasten; es besteht keine Möglichkeit, dies herauszufinden. Und da es keine Möglichkeit gibt, herauszufinden, wann genau das Programm benutzt wurde und was auf dem Telefon oder dem Computer programmiert wurde, können Strafverfolgungsbehörden dies eigentlich nicht verwerten.

Eine solche Praxis funktioniert nur bei zwei Anlässen: Bei autoritären Regimen, die keine interne Rechenschaftspflicht haben. Wenn man sich mal ansieht, wer die größten Kunden der NSO Group und von Pegasus sind, dann handelt es sich um absolut autoritäre Regime in Ländern, die nicht einmal annähernd demokratisch sind. Wir haben über Saudi-Arabien gesprochen, wir sollten auch die Vereinigten Arabischen Emirate erwähnen. Wir sollten Honduras erwähnen. Wir sollten Uganda und den Tschad, Ungarn und Weißrussland anführen. Dies sind Orte, an denen israelische Spionageprogramme gegen Menschen eingesetzt wurden. Und natürlich Hongkong, wo die Spyware-Technologie den chinesischen Behörden zur Verfügung gestellt wurde, um die dortige Freiheitsbewegung zu unterdrücken.

ZR: Die Privatsphäre ist meiner Meinung nach ein Thema, das nach den großen Enthüllungen von Edward Snowden und Glenn Greenwald über die NSA-Leaks in den Hintergrund getreten ist. Auch WikiLeaks enthüllte Dokumente, z. B. Vault 7 der CIA, in denen sie einen Samsung-Fernseher zur Überwachung verwenden konnten, ohne dass der Fernseher überhaupt eingeschaltet war. Wie wird diese Situation in Bezug auf die bürgerlichen Freiheiten von der israelischen Gesellschaft und den Medien gesehen? Und der zweite Teil der Frage: Gab es irgendwelche internationalen Reaktionen hierauf?

SH: In der israelischen Gesellschaft ist das ein sehr komplexes Thema, weil die meisten Israelis glauben, dass die israelischen Geheimdienste diese Art von Technologie auf keinen Fall gegen israelische Bürger einsetzen würden. [Ironisch:] Schließlich müssen wir Israelis uns über diese Dinge keine Sorgen machen. Und dann gab es eine sehr geschickt inszenierte Enthüllung in den israelischen Medien, die aufdeckte, dass die israelische Polizei tatsächlich Spionagesoftware eingesetzt hatte, um israelische Bürger auszuspionieren. Aber der Journalist, der dies aufdeckte, erhielt absichtlich falsche Informationen und veröffentlichte gefälschte Beweise und falsche Zeugenaussagen, als würde die Polizei diese Überwachung nutzen. Es handelte sich um eine äußerst raffinierte Operation. Sie diente vor allem dazu, die Glaubwürdigkeit einiger Zeugen zu untergraben, die gegen den ehemaligen israelischen Ministerpräsidenten Netanjahu ausgesagt hatten, der sich mit Korruptionsvorwürfen konfrontiert sieht.

Dieses Exposé wurde benutzt, um zu sagen: Seht her, die Staatsanwaltschaft benutzt Pegasus, um Beweise gegen Netanjahu zu platzieren. Das bedeutet, dass Beweise gegen ihn nicht anerkannt werden müssen. Und nachdem Netanjahu in seinem Prozess davon Gebrauch gemacht hatte, stellte sich später heraus, dass die Informationen gefälscht waren, dass sie unzutreffend waren und dass die Journalisten die Anschuldigungen zurücknehmen mussten.

Daraufhin zogen alle den Fehlschluss, dass die Spionagesoftware in Wirklichkeit nie gegen israelische Bürger eingesetzt wurde. Aber das war ein Trugschluss. Es war eine sehr geschickte Art und Weise der Verantwortlichen, eine Gegenreaktion auszulösen: Oh, der Bericht war also gefälscht, was bedeutet, dass wir in Sicherheit sind. Nein, tatsächlich hat die israelische Polizei später in einem viel weniger bekannten Dokument zugegeben, dass sie diese Technologie gegen Demonstranten, gegen Menschenrechtsaktivisten in Israel und gegen israelische Bürger einsetzte. Wie war der zweite Teil Ihrer Frage?

ZR: Wie wird dies international beurteilt? Gab es Verurteilungen seitens bestimmter Länder? Die NSA-Enthüllungen waren zum Beispiel ziemlich umfangreich und sie hatten große diplomatische Auswirkungen. Wie waren die Auswirkungen in diesem Fall oder duldet man die Software einfach als ein Produkt auf dem Markt, das gekauft und verkauft werden kann?

SH: Ein Teil des Problems besteht meiner Meinung nach darin, dass Menschen, die davon sehr betroffen und darüber wütend sind – es gibt Menschen, die in Bahrain und Marokko gefoltert wurden, weil die Behörden Pegasus zur Festnahme von Menschenrechtsaktivisten, insbesondere von Frauenrechtsaktivisten, eingesetzt haben. In Mexiko wurden im Zuge der Ermittlungen zu den 43 verschwundenen Studenten, die in Wirklichkeit ermordet wurden, Rechtsanwälte und Menschenrechtsaktivisten durch Pegasus gezielt zum Schweigen gebracht. Diese Art von berechtigter Wut gegen den Einsatz einer Spionagesoftware, einer israelischen Spionagesoftware, um Menschenrechtsaktivisten zum Schweigen zu bringen, geht um die ganze Welt. Menschen aus all diesen Ländern müssen zusammenarbeiten und die Informationen bereitstellen, die sie haben, um eine globale Kampagne gegen ein globales Problem zu führen.

Außerdem wurde auch das Telefon des französischen Präsidenten Macron von israelischer Spionage-Software gehackt. Dies schien ein Moment zu sein, in dem es vielleicht zu einer internationalen Gegenreaktion hätte kommen können, da der Präsident eines mächtigen westlichen Landes gehackt worden war. Der israelische Verteidigungsminister flog nach Paris, um sich persönlich bei Macron zu entschuldigen, und Frankreich ließ die Sache auf sich beruhen und ermöglichte eine Fortsetzung des Geschehens. Das ist wirklich ein ernstes Problem.

Wir beobachten auch ein Problem mit Konzernen. Zwei sehr große Konzerne haben gegen die NSA Group geklagt: Apple und Facebook. Das liegt daran, dass ihre eigenen Geräte, ihre eigene Technologie, Facebook, das jetzt Meta heißt, und WhatsApp gehackt worden sind. Auch Apple-Telefone, iPhones, wurden von Pegasus gehackt. Sie haben also Klagen gegen das Unternehmen angestrengt, und man dachte: Wenn die großen Konzerne auf unserer Seite sind, dann werden wir gewinnen. Aber so einfach ist es leider nicht, denn sie ziehen den Prozess in die Länge. Und in der Zwischenzeit wirbt Apple bereits mit einer neuen Produktreihe, in der sie Telefone vermarkten, die gegen Spionageprogramme resistent sind. Sie zahlen also das Doppelte und erhalten ein Produkt, das sie vor Spionageprogrammen

schützen soll. Aber in Wirklichkeit machen sie Profit damit. Sie verwandeln die drohende Spyware in eine weitere Gewinnquelle. Es entsteht eine Nachfrage nach einem neuen Produkt, welches sie mit Freude zur Verfügung stellen. So haben sie jetzt ein Interesse daran, dass ihr Prozess gegen die NSO Group niemals endet.

Die Verantwortung liegt wieder einmal bei uns als Bürger eines jeden Landes der Welt, wobei wir jetzt im Rahmen von Deutschland sprechen, um dem ein Ende zu setzen, Kampagnen und Proteste zu starten, damit wir sicherstellen, dass diese Unternehmen nicht von der Verletzung unserer Privatsphäre und von Menschenrechten profitieren können.

ZR: Ich denke, das ist ein guter Schlusspunkt. Hoffen wir, dass unsere Zuschauer etwas unternehmen und ein Bewusstsein für dieses Thema entwickeln werden. Shir Hever, unabhängiger Journalist, Wirtschaftswissenschaftler und Autor, vielen Dank, dass Sie heute bei uns waren.

SH: Vielen Dank.

ZR: Und ich danke Ihnen für Ihr Interesse an der heutigen Sendung. Vergessen Sie nicht, unseren YouTube-Kanal zu abonnieren und zu spenden, damit wir weiterhin unabhängige, gemeinnützige Nachrichten und Analysen produzieren können. Ich bin Ihr Gastgeber Zain Raza, bis zum nächsten Mal.

ENDE