KULTUR NEU ENTDECKEN

SWR KULTUR

Das Wissen

Spähsoftware im Handy – Wie Staaten uns heimlich überwachen

Von Benjamin Breitegger

Sendung vom: Montag, 19. Januar 2026, 8:30 Uhr
Redaktion: Lukas Meyer-Blankenburg
Regie: Günter Maurer
Produktion: SWR 2026

Unter Auflagen können Sicherheitsbehörden Spähsoftware benutzen, um Kriminelle zu überführen. Doch in der EU häufen sich Fälle, in denen etwa Regierungs-Kritiker illegal ausspioniert werden. Eine Gefahr für die Demokratie.

Das Wissen können Sie auch im **Webradio** unter swrkultur.de und auf Mobilgeräten in der **SWR Kultur App** hören – oder als **Podcast** nachhören:
https://www.swr.de/swrkultur/programm/podcast-swr-das-wissen-102.html

---

MANUSKRIPT

Musikakzent

Sprecher:
Man sieht sie nicht. Man weiß nicht, dass sie da sind. Wie lange sie da sind. Und was genau sie machen: Digitale Spione nisten sich unbemerkt in Handys ein und bleiben unsichtbar. Ihr Absender kann Chatnachrichten lesen, auch wenn sie eigentlich verschlüsselt sind. Er kann Gespräche mithören. Er kann sich private Fotos anschauen. Das Mikrofon einschalten und zuhören, was man gerade mit wem bespricht. Er kann via Kamera zuschauen und weiß dank GPS auch, wo man ist.

Das alles ist technisch möglich. Ein mit Spähsoftware infiziertes Handy wird zum perfekten Überwachungstool. Das macht Spähsoftware zum mächtigen Werkzeug in den Händen der Richtigen. Und zum gefährlichen in den Händen der Falschen.

Ansage:
Spähsoftware im Handy – Wie Staaten uns heimlich überwachen. Von Benjamin Breitegger.

Sprecher:
Der deutsche Staat darf sich in Handys hacken. Er setzt Spionagesoftware im Kampf gegen Terroristen und organisierte Kriminalität ein. Das ermöglicht zum Beispiel, WhatsApp-Nachrichten mitzulesen. Der Staat spricht allerdings nicht vom „Hacken“, sondern von der „Quellen-Telekommunikationsüberwachung“ und von der „Online-Durchsuchung“. Das Gesetz regelt, wen Nachrichtendienste und Strafverfolger wie überwachen dürfen und unter welchen Voraussetzungen. Und weil diese Überwachung einen extremen Eingriff in die Privatsphäre darstellt, sind die Auflagen seit August 2025 strenger.

Atmo 01: Tagesschau:
Der Einsatz sogenannter Staatstrojaner durch Strafverfolger ist nur bei schweren Straftaten zulässig. Das hat das Bundesverfassungsgericht in Karlsruhe entschieden.

Sprecher:
Der Einsatz des Staatstrojaners sei zwar grundsätzlich erlaubt, allerdings nur zur Aufklärung von Straftaten mit mehr als drei Jahren Freiheitsstrafe. Geklagt hatte eine Gruppe von Anwälten, Künstlern und Journalisten. ARD-Rechtsexperte Philip Raillon ordnete das Urteil im Interview mit der Tagesschau ein.

O-Ton 01 Philip Raillon, ARD-Journalist:
Bislang war so eine sogenannte Quellen-Telekommunikationsüberwachung auch bei eher kleineren Delikten möglich. Zum Beispiel bei allen Arten der Volksverhetzung oder bei allen Formen des Geheimnisverrates. Und da sagt das Gericht, solche eher kleineren Delikte, die zählen teilweise noch zur sogenannten Massenkriminalität. Und da ist so ein krasses Mittel wie so eine Telekommunikationsüberwachung unverhältnismäßig und deswegen verfassungswidrig. Bei schwereren Straftaten hingegen ist das in Ordnung. Da hat das Gericht gesagt, da muss man abwägen und dann kann die Polizei im Einzelfall auch so ein Mittel einsetzen. Es geht dabei

einerseits um die Überwachung des Gesprächs, und gleichzeitig kann man so einen Staatstrojaner auch einsetzen, um sämtliche Dateien auf einem Handy oder auf einem Computer zu durchsuchen. Das ist dann die sogenannte Online-Durchsuchung.

Sprecher:
Wie genau das getan wird und welche Werkzeuge dabei genutzt werden, verrät der Staat nicht. Das Bundespolizeipräsidium schreibt auf Anfrage von „Das Wissen“:

Sprecherin:
(Zitat Bundespolizeipräsidium):
Die Bundespolizei steht für ein Interview nicht zur Verfügung. Wenden Sie sich bitte an das Bundeskriminalamt.

Sprecher:
Das Bundeskriminalamt schreibt, man könne:

Sprecher 2:
(Zitat BKA):
…leider kein Interview zu der angefragten Thematik anbieten.

Sprecher:
Und der Bundesnachrichtendienst lässt wissen, er nehme…

Sprecherin:
(Zitat Bundesnachrichtendienst):
…zu Angelegenheiten, die etwaige nachrichtendienstliche Erkenntnisse oder Tätigkeiten betreffen, grundsätzlich nicht öffentlich Stellung.

Sprecher:
Der Journalist und Aktivist Arne Semsrott wollte sich mit dieser Antwort nicht zufriedengeben und klagte. Er wollte wissen, ob der BND die Spähsoftware „Pegasus“ nutzt. Im November 2024 urteilte das Bundesverwaltungsgericht: Der BND muss sich dazu nicht äußern.

Die Nachrichtendienste und Behörden wollen sich nicht in die Karten schauen lassen. Ihre Argumentation: Je weniger Details öffentlich bekannt sind, desto weniger können sich Kriminelle informieren und davor schützen, überwacht zu werden. Aber auch die Hersteller der Spionagesoftwares wollen geheim bleiben. Schon 2018 sagte ein Staatssekretär im Innenausschuss laut geleakten Protokollen:

Sprecher 2:
(Zitat Staatssekretär im Innenausschuss):
Die Unternehmen wollen nicht, dass es offenbar wird, dass sie mit der Bundesregierung oder mit Sicherheitsbehörden des Bundes kooperieren. Wenn dies der Fall ist, dann beenden sie ihre Geschäftsbeziehungen mit uns. Ich sage es hier ganz offen, die sind verbrannt, wenn die Namen zirkulieren und öffentlich werden.

Sprecher:
Das scheint sich seit 2018 nicht verändert zu haben. Ein Sprecher des Bundesinnenministeriums bestätigt: Der Einsatzzweck wäre gefährdet, würde man verraten, welche Softwareprodukte Sicherheitsbehörden verwenden. Auch wieviel Geld man dafür ausgibt, verrät die Bundesregierung nicht.

Was bekannt ist, kommt oft von Journalistinnen und Journalisten: Recherchen haben gezeigt, dass Behörden gleich mehrere Spähsoftwares einsetzen. Sie entwickeln sie teils selbst, teils erwerben sie Software von kommerziellen Überwachungsunternehmen. Aktuell zum Einsatz kommen dürfte unter anderem eine an das deutsche Gesetz angepasste Version des umstrittenen Spionagetools „Pegasus“. Mit ihr wurden in der Vergangenheit Politiker und Journalisten weltweit ausgespäht.

Musikakzent

Spionagesoftware, Spähsoftware oder internationale Spyware, Staatstrojaner oder Bundestrojaner: Es zirkulieren viele Namen. Gemeint sind immer hochkomplexe digitale Spionagewerkzeuge, die sich auch übers Internet auf Geräte wie Handys spielen lassen. Das funktioniert nur, weil die Spähsoftware bislang unbekannte Sicherheitslücken ausnutzt. Das Problem dabei: Nicht nur der Staat, sondern auch Kriminelle können Sicherheitslücken ausnutzen. Deswegen ist Spähsoftware umstritten.

Umstritten ist sie auch, weil die Hersteller der Spähsoftware undurchsichtig agieren und zivilgesellschaftliche Organisationen regelmäßig Missbrauch aufzeigen. Der geschieht nicht nur in diktatorischen Regimen, sondern auch mitten in der EU. Anruf bei Francesco Cancellato in Rom.

Atmo 02: Signal-Anruf

O-Ton 02 Francesco Cancellato, italienischer Journalist:
I am Francesco Cancellato, I am 45 years old, and I am the editor in chief of the online media outlet fanpage dot it which is one of the biggest media outlets in Italy. It has 2.5 million unique readers per day.

Sprecher:
Francesco Cancellato ist ein italienischer Investigativjournalist. Er leitet die Onlinezeitung fanpage Punkt it, die 2024 etwa verdeckt zur Regierungspartei Fratelli d'Italia von Georgia Meloni und deren Verbindungen zu neofaschistischen Gruppen recherchierte. Ein halbes Jahr später, im Januar 2025, schickte WhatsApp Cancellato eine Warnung: Sein Handy sei über eine WhatsApp-Lücke möglicherweise mit Spionagesoftware infiziert worden.

O-Ton 03 Francesco Cancellato (engl.):
I thought it was a scam … but I realized I could be at target when I became at target, not before that.

Sprecher 2:
(Voiceover):
Ich habe zuerst gedacht, das ist ein Scam, eine Betrugsmasche. Aber da ist nur diese Nachricht ohne Link gewesen, ich sollte nirgends draufklicken, nur eine E-Mail an jemanden schreiben. Mein Co-Chefredakteur und mein Medienunternehmen haben auch zuerst an einen Scam gedacht. Aber gleichzeitig ist klar gewesen: Es ist jetzt nicht Science-Fiction, dass ein Journalist ausspioniert wird, sondern naheliegend. Natürlich fragt man sich als Erstes: Warum ich? Obwohl es offensichtlich ist – wir sind ein großes Investigativmedium. Aber mir ist erst klar geworden, dass ich ein Spionageziel sein könnte, als ich eines geworden bin.

Sprecher:
Francesco Cancellato kontaktierte das Citizen Lab, ein interdisziplinäres Forschungslabor an der Universität Toronto in Kanada. Seine Mitarbeiter decken Spionagefälle weltweit auf. Sie analysieren Handys und Computer von mutmaßlichen Opfern und forschen zu digitalen Bedrohungen.

Die Experten dort konnten mit technisch-forensischen Methoden zwar keine Infektion auf Cancellatos Android-Handy nachweisen, schreiben in einer Analyse aber, dass dies nicht bedeute, dass – Zitat – „das Telefon nicht erfolgreich gehackt wurde“. Ein Nachweis einer Infektion ist auf Apple-Handys einfacher. Beweise für einen Hack fand das renommierte Citizen Lab auf dem iPhone von Ciro Pellegrino, Cancellatos Kollegen. Dessen Handy wies Spuren der Spähsoftware von „Paragon“ auf. Das deute auf den Versuch hin, so die kanadischen Experten, ein Medienunternehmen ins Visier zu nehmen.

Francesco Cancellato machte seinen Fall öffentlich. Das brachte ihm nicht nur Unterstützung, sondern auch öffentliche Kritik ein, erzählt er. War die mutmaßliche Überwachung vielleicht legitim? Hat er womöglich was zu verstecken?

O-Ton 04 Francesco Cancellato (engl.):
I didn't sleep for two months … that someone on the other side that convinced the public opinion I was an imposer.

Sprecher 2:
(Voiceover):
Zwischen Ende Februar und April habe ich fast zwei Monate lang nicht geschlafen. Ich bin jede Nacht mit Angstzuständen aufgewacht oder mit Panikattacken. Mein Herz hat jede Nacht gerast, weil ich große Angst davor hatte, dass jemand die Öffentlichkeit davon überzeugt, ich sei ein Betrüger.

Sprecher:
Bekannt ist, dass Italiens Regierung die Paragon-Spähsoftware einsetzt. Sie überwachte damit unter anderem zwei Seenotrettungs-Aktivisten, denen Beihilfe zur illegalen Einwanderung vorgeworfen wird. Andere Überwachungsfälle wie der von Francesco Cancellato bleiben offiziell unbestätigt.

O-Ton 05 Francesco Cancellato (engl.):
The Secret Service told that there wasn't an authorized activity to spy on me. … they didn't convince me at all.

Sprecher 2:
(Voiceover):
Der Geheimdienst hat mir mitgeteilt, dass es keine autorisierte Überwachung gab. Und die Regierung hat keinerlei Solidarität gezeigt. Sie haben mich nicht mal angerufen. Sie haben mir sogar gedroht: „Wenn Sie behaupten, wir hätten Sie ausspioniert, verklagen wir Sie." Als Georgia Meloni im Parlament auf meinen Fall angesprochen worden ist, hat sie gesagt: „Ich möchte nur wichtige Fragen beantworten." Für sie ist es also nicht so wichtig gewesen. Dieses feindselige Verhalten hat mich sehr nachdenklich gemacht. Ich kann zwar nicht behaupten, dass es die Regierung war, die mich ausspioniert hat. Aber sie hat mich auch nicht davon überzeugt, dass sie es nicht getan hat. Sie hat mich überhaupt nicht überzeugt.

Sprecher:
Der Journalist Cancellato nennt die Spähsoftware den „Feind im Inneren". Er hat ein Buch geschrieben über den Skandal. Die italienische Regierung und Paragon sagen, sie haben ihre Zusammenarbeit beendet. Paragons Spähsoftware kommt aber auch anderswo zum Einsatz. Insgesamt kontaktierte WhatsApp mehr als 90 mutmaßliche Spionageopfer in nicht weniger als 14 EU-Ländern, darunter auch Deutschland. Möglich, dass ein Teil dieser Fälle aus Produktvorführungen bei Behörden stammt.

Musikakzent

Sprecher:
Die Denkfabrik Atlantic Council beobachtet den globalen Markt für Spionagesoftware. Ihre Analyse zeigt: Italien gehört, neben den USA und Israel, zu den wichtigsten Standorten für Spähsoftware-Anbieter und -Investoren. Weitere Spionageunternehmen haben sich ebenfalls in europäischen Ländern angesiedelt – und werden mitunter mit EU-Geld gefördert. Das berichtete das europäische Investigativmedium „Follow the Money" im September 2025. Als Reaktion auf die Recherchen kündigte die EU-Kommission an, „unverzüglich" zu handeln und Personen oder Organisationen, die in – Zitat – „schweres berufliches Fehlverhalten" verwickelt sind, nicht mehr zu finanzieren. Strafverfolger und Geheimdienste, so die Kommission, dürften Spionagesoftware aber für legitime Zwecke rechtmäßig einsetzen.

Welche europäischen Behörden welche Unternehmen beauftragen, ist weiterhin nicht bekannt. Und auch der Markt für Spionagesoftware bleibt undurchsichtig. Unternehmen benennen sich um und tauchen in neuen Ländern auf. Oft haben sie keine Webseite. „Das Wissen" hat mehrere europäische und internationale Anbieter kontaktiert – so sich denn eine E-Mail-Adresse des Unternehmens oder ein LinkedIn-Profil der Geschäftsführung im Internet findet. Kein einziges Unternehmen hat auf die Anfragen geantwortet.

O-Ton 06 John Scott-Railton, Forscher am Citizen Lab in Kanada (engl.):
Today I think most people recognize that there are risks to their phone … how much Europe specifically is experiencing a spyware crisis.

Sprecher 2:
(Voiceover):
Heute ist den meisten Menschen wohl bewusst, dass ihr Smartphone Risiken birgt und dass ein Hackerangriff auf ihr Smartphone enorme persönliche Folgen haben kann. Man kann sein Geld verlieren. Man kann seine Privatsphäre verlieren. Aber was die Menschen meiner Meinung nach noch immer nicht ganz verstehen, ist, wie sehr gerade Europa von einer Spähsoftware-Krise betroffen ist.

Sprecher:
Das sagt John Scott-Railton. Er arbeitet für das Citizen Lab, jenes kanadische Forschungslabor, das die Handys der italienischen Journalisten untersucht hat. „Das Wissen“ erreicht den IT-Sicherheitsexperten per Videocall. Wo er sich gerade befindet, verrät er nicht. Er und ein kleines Team in Kanada kämpfen gegen eine mächtige globale und milliardenschwere Überwachungsindustrie – da kann Vorsicht nicht schaden.

O-Ton 07 John Scott-Railton (engl.):
When I say spyware crisis … in ways that I think are dangerous to European democracy.

Musikakzent

Sprecher 2:
(Voiceover):
Wenn ich von Spähsoftware-Krise spreche, meine ich den Einsatz von raffinierter Hacking-Technologie, die oft unsichtbar ist, weil die Opfer nicht mal einen Fehler machen müssen. Sie müssen nicht mal einen falschen Klick machen, um infiziert zu werden. Und diese Technologie wird von Regierungen eingesetzt, darunter europäische Regierungen, und das ist meiner Meinung nach demokratiegefährdend.

Sprecher:
Früher hätten nur eine Handvoll Regierungen die Spezialfähigkeit, sich in Handys zu hacken. Heute sollen 14 EU-Staaten die Spähsoftware Pegasus der NSO Group erworben haben. Weitere Staaten wollen in Zukunft Hacking-Dienstleistungen zukaufen. Das österreichische Parlament hat erst im Sommer 2025 beschlossen, in Zukunft Spähsoftware zu erwerben. Und Griechenland hat die gesetzliche Grundlage dafür Ende 2022 geschaffen – und das nach einem massiven Überwachungsskandal.

Atmo 03: Ansage der Metro-Station Kallithea

Sprecher:
Athen im September 2025. Eine Konferenz für internationale Investigativjournalistinnen und -journalisten. Unter den Gästen ist Thanasis Koukakis. Der 47-jährige griechische Finanzjournalist hat in der Vergangenheit für CNN und die Financial Times geschrieben, recherchierte zu finanziellen Unregelmäßigkeiten bei einer Bank und zeigte auf, dass Griechenlands Gesetze Geldwäsche und Steuerhinterziehung begünstigen.

Heute ist klar: Die griechischen Behörden überwachten Koukakis einerseits mit konventionellen Methoden: Sie hörten seine Telefonate ab. Andererseits wurde sein Handy später illegal mit Spähsoftware infiziert. Das Citizen Lab in Kanada fand Spuren einer Software namens „Predator“, zu Deutsch: Raubtier.

O-Ton 08 Thanasis Koukakis, griechischer Finanzjournalist (engl.):
The Helenic Data Protection Authority … in order to have me in a constant surveillance.

Sprecher 2:
(Voiceover):
Die griechische Datenschutzbehörde Heleni hat mir später zusätzlich bestätigt, dass sie insgesamt sieben Infektionen mit dem Schadprogramm „Predator“ festgestellt hat. Mir sind zwischen Sommer 2020 und November 2021 sieben Links zu vermeintlichen Nachrichtenseiten geschickt worden, um mich permanent und durchgehend zu überwachen.

Sprecher:
Im August 2022 enthüllte der Sozialdemokrat Nikos Androulakis – der heutige griechische Oppositionsführer –, dass es einen Versuch gab, sein Telefon mit Predator-Spyware zu hacken. Der Überwachungsskandal weitete sich aus, betroffen war die griechische Elite.

O-Ton 09 Thanasis Koukakis (engl.):
We have also documentation … other journalists and entrepreneurs.

Sprecher 2:
(Voiceover):
Die griechische Datenschutzbehörde hat insgesamt 87 andere Personen informiert. Die meisten von ihnen sind Minister der aktuellen Regierung, Politiker, ehemalige Oberbefehlshaber der griechischen Armee, Staatsanwälte, Journalisten und Unternehmer.

Sprecher:
Medien tauften den Skandal „Griechenlands Watergate“, anlehnend an den Missbrauch von Regierungsgewalt unter US-Präsident Richard Nixon in den siebziger Jahren. 27 der 87 Personen standen gleichzeitig unter legaler Telefonüberwachung, offiziell aus „nationalen Sicherheitsgründen“. Infolge der Enthüllungen traten der Chef des griechischen Geheimdienstes und der oberste

Berater des Premierministers, gleichzeitig sein Neffe, zurück. Der griechische Premier Kyriakos Mitsotakis hatte den Geheimdienst 2019 seiner Kontrolle unterstellt, bestritt aber, von der Überwachung gewusst zu haben. Ebenso, dass die Spionagesoftware Predator eingesetzt wurde.

Kyriakos Mitsotakis ist bis heute im Amt. Die juristische Aufarbeitung des Skandals läuft derweil schleppend. Zwei Staatsanwälte wurden von den Ermittlungen abgezogen und kein Regierungsbeamter angeklagt. Erst im Herbst 2025 standen dann zwei Griechen und zwei Israelis vor Gericht. Sie hatten die Überwachungssoftware Predator in Griechenland vermarket. Der Skandal habe sich somit gewandelt, findet der Journalist Thanasis Koukakis.

O-Ton 10 Thanasis Koukakis (engl.):
As we speak, the Greek Watergate scandal has been minimized to a misdemeanor … this scandal infected the independent authorities and the Greek judiciary.

Sprecher 2:
(Voiceover):
Der griechische Watergate-Skandal ist durch diese Anklage auf ein simples Vergehen reduziert worden. Es hat als politischer Skandal zu illegalen und legalen Überwachungen über das Büro des Premierministers begonnen. Doch im Zuge der Ermittlungen zu den Überwachungen hat dieser Skandal die unabhängigen Behörden und die griechische Justiz erfasst.

Der Missbrauch von Spionagesoftware ist nicht neu. Schon ab 2021 berichteten zahlreiche Medien, dass mit der Spionagesoftware Pegasus weltweit Politiker, Journalisten und Menschenrechtsaktivisten ins Ziel gerieten. Der französische Präsident Emmanuel Macron war darunter und auch das Umfeld des saudischen Dissidenten Jamal Khashoggi, den ein Mordkommando im saudi-arabischen Konsulat in Istanbul zerstückelt hatte. Das Europäische Parlament setzte infolge der Enthüllungen einen Untersuchungsausschuss zu Spionagesoftware ein. Im Sommer 2023 präsentierte das Parlament seinen Abschlussbericht. Die liberale niederländische Abgeordnete Sophie in‘t Veld sagte damals im Plenum: Man spreche oft von europäischen Watergates. Doch eigentlich sei der Watergate-Vergleich schief. Der Begriff „Stasi-Methoden“ passe besser.

O-Ton 11 Sophie in‘t Veld, frühere Abgeordnete des Europäischen Parlaments (engl.):
I firmly believe that democracy is about checks and balances … It is a democracy crisis, you might say now.

Sprecherin:
(Voiceover):
Ich bin fest davon überzeugt, dass Demokratie auf Gewaltenteilung, Rechenschaftspflicht und Kontrolle basiert. Nimmt man diese weg, ist die Demokratie tot. Wenn es keine ausgleichenden Kräfte mehr gibt, ist die Demokratie tot. Und genau das ist das Ziel der Regimes, die Spähsoftware gegen einige ihrer eigenen Bürger einsetzen. Und das geschieht nicht nur in Saudi-Arabien oder Mexiko, nein,

es geschieht direkt vor unserer Haustür, innerhalb der Europäischen Union, durch EU-Regierungen. Man könnte sagen: Es handelt sich um eine Krise der Demokratie.

Sprecher:
In ihrem Abschlussbericht forderten die Parlamentarier ein bedingtes Moratorium für Spähsoftware, bis Missbrauchsfälle aufgeklärt sind. Sie empfohlen EU-Standards, die regeln, wie Mitgliedstaaten Spähsoftware legal einsetzen können, und striktere Exportkontrollen. Außerdem forderten sie Rechtshilfe für die Opfer von Missbrauch. – Aber:

O-Ton 12 Aljosa Ajanovic, Autor des Spyware-Policypapers von EDRI (engl.):
So the Commission hasn't taken any of the measures … we agreed with many of them.

Sprecher 2:
(Voiceover):
Die Europäische Kommission hat keine der Maßnahmen ergriffen, die das Europäische Parlament empfohlen hat und denen wir in vielen Punkten zugestimmt haben.

Sprecher:
Das sagt Aljosa Ajanovic. Er arbeitet bei Edri, einem europäischen Netzwerk von mehr als 50 Organisationen, das sich für digitale Rechte einsetzt. Vonseiten der EU-Kommission hieß es im Sommer 2025, die Ermittlungen zum mutmaßlichen Missbrauch von Spionagesoftware seien Sache der nationalen Behörden. Doch genau die nationalen Behörden werden oft des Missbrauchs beschuldigt, wie im Falle von Griechenland und Italien. Was tun? Das NGO-Netzwerk Edri kommt in einem Positionspapier zum Schluss: Spähsoftware müsse verboten werden. Die Technologie könne nicht menschenrechtskonform eingesetzt werden.

O-Ton 13 Aljosa Ajanovic (engl.):
Through these tools that are highly invasive … can be compared to a weapon and therefore forbidden.

Sprecher 2:
(Voiceover):
Spionagesoftwares sind äußerst invasive Instrumente, die per Definition nicht die Anforderungen an Notwendigkeit und Verhältnismäßigkeit erfüllen können. Sie sind gefährlich und können wegen ihrer Auswirkungen mit Waffen verglichen werden.

Sprecher:
Aljosa Ajanovic erklärt, Spionagesoftware nutze bisher unbekannte Sicherheitslücken in technischen Geräten aus. Einen sicheren Weg, damit nur Kriminelle ins Visier zu nehmen, gebe es nicht.

O-Ton 14 Aljosa Ajanovic (engl.):
There is no safe ways. once you open vulnerability … and that's their defense also against foreign interference, for example.

Sprecher 2:
(Voiceover):
Sobald Sie eine Schwachstelle in einem Gerät offenlassen, ist sie für alle offen. Die Türe, die man nutzt, um die bösen Typen auszuspionieren, kann auch von böswilligen Akteuren genutzt werden. Eine Schwachstelle kann alle Nutzer in Gefahr bringen. Sie kann auch das eigene Land in Gefahr bringen. Schließlich verwendet die Polizei verschlüsselte Chats für die interne Kommunikation. Auch Regierungsbeamte nutzen sie, um sich zum Beispiel gegen ausländische Einmischung zu schützen.

Sprecher:
Daher sollten Schwachstellen, sobald sie entdeckt werden, sofort beseitigt werden. Doch das passiere nicht immer, sagt Aljosa Ajanovic.

O-Ton 15 Aljosa Ajanovic (engl.):
So we have proof that in the year 2023 … have reasons to believe that they are the main actors of this vulnerability market.

Sprecher 2:
(Voiceover):
Wir wissen, dass im Jahr 2023 von 25 Schwachstellen, die Google gefunden hat, 20 irgendwann von Spyware-Unternehmen ausgenutzt worden waren. Daher haben wir Grund zu der Annahme, dass die Spyware-Firmen die Hauptakteure auf dem Markt für Schwachstellen sind.

Sprecher:
Hersteller wie Google oder Apple zahlen Geld an Forscher, wenn diese neue Schwachstellen entdecken. Die Hersteller schließen die Lücken dann. Doch parallel existieren ein Grau- und Schwarzmarkt, auf dem Schwachstellen angeboten werden. Dort zahlen Akteure teils Millionenbeträge. Die Hersteller erfahren von den Schwachstellen nichts, Spähsoftwares können sie ausnutzen.

Dieses Geschäft werde durch die staatliche Nachfrage nach Spähsoftware gefördert, argumentiert Aljosa Ajanovic vom European Digital Rights Network. Die EU-Staaten schwächen so indirekt die digitale Sicherheit ihrer Bürgerinnen und Bürger, statt sie zu stärken.

O-Ton 16 Aljosa Ajanovic (engl.):
All the money that is being used now for this type of tools … let's build a safe digital world for everyone.

Sprecher 2:
(Voiceover):
Das gesamte Geld, das derzeit für diese Art von Tools ausgegeben wird, sollte stattdessen in die Verbesserung unserer Cybersicherheit fließen. Um unsere Systeme widerstandsfähiger zu machen, um Unternehmen stärker zu sensibilisieren und sie zu verpflichten, nach Schwachstellen zu suchen und Anreize dafür zu

schaffen, damit diese Schwachstellen dann geschlossen werden können. Also als Fokus nicht die Überwachung, sondern eine sichere digitale Welt für alle.

Sprecher:
Kurzfristig könnte die EU Sanktionen aussprechen gegen Spähsoftware-Unternehmen und Personen, die Menschenrechtsverletzungen begangen haben. Das geschah etwa in den USA unter Präsident Joe Biden.

Musikakzent

Sprecher:
US-Sanktionen gegen mehrere Spähsoftware-Unternehmen sind bis heute aufrecht, die Hersteller stehen auf der „schwarzen Liste“ des US-Handelsministeriums. Zudem verurteilte ein Gericht die NSO Group, die hinter Pegasus steht, zu einer 167-Millionen-Dollar-Strafe. Geklagt hatte WhatsApp, über dessen Server die Schadsoftware verbreitet worden war.

Doch US-Investoren haben die Spähsoftware-Branche entdeckt. Die NSO Group ist seit kurzem in amerikanischer Hand. Neuer Vorstandsvorsitzender ist ein ehemaliger, von Donald Trump eingesetzter Botschafter. Es ist nicht ausgeschlossen, dass die Firma wieder am amerikanischen Markt tätig werden kann. Andere Spähsoftware-Hersteller sind bereits aktiv. So wird die US-Einwanderungsbehörde ICE wohl jene Spähsoftware einsetzen, mit der mutmaßlich die Handys der beiden italienischen Journalisten überwacht wurden. Paragon, das Unternehmen dahinter, wurde laut israelischen Medien ebenfalls von amerikanischen Investoren übernommen.

Sprecher:
Stellt sich die Frage: Wie kann man sich vor ausgeklügelter Handyspionage schützen? Der IT-Experte John-Scott Railton vom Citizen Lab in Kanada sagt, natürlich solle man aktuelle Sicherheitsupdates auf allen Geräten installieren, doch hundertprozentigen Schutz gebe es eben nicht.

O-Ton 17 John Scott-Railton (engl.):
The reason that spyware scares me so … more expensive to hack.

Sprecher 2:
(Voiceover):
Spähsoftware macht mir so viel Angst, weil es kein Patentrezept dagegen gibt. Es gibt nichts, was ein Normalbürger tun kann, um sicherzustellen, dass sein Gerät nicht gehackt werden kann. Aber es gibt bestimmte Maßnahmen, die man ergreifen kann, um das Hacken teurer zu machen.

Sprecher:
Wer ein aktuelles Android-Handy hat, könne sich für das „Erweiterte Sicherheitsprogramm“ von Google registrieren. Wer ein Google-Handy nutze, könne außerdem das alternative und extra abgesicherte Betriebssystem GrapheneOS installieren. Doch das setzt technische Expertise voraus. Seine Lieblingsfunktion, sagt John-Scott Railton, finde sich auf iPhones und MacBooks: der Lockdown-Modus, auf Deutsch Blockiermodus genannt.

O-Ton 18 John Scott-Railton (engl.):
It's a simple mode that can be found in privacy settings … not perfect, but we see it blocking attacks.

Sprecher 2:
(Voiceover):
Das ist ein einfacher Modus, ganz unten in den Datenschutzeinstellungen. Wenn der aktiviert ist, sind viele der digitalen Türen, die Hacker gerne nutzen, verschlossen. Das macht es schwieriger, dich zu hacken. Das ist so, als würde man gute Türen installieren und alle Fenster mit wirklich guten Gittern versehen. Das ist zwar nicht perfekt, aber wir sehen, dass Angriffe mit diesem Modus blockiert werden.

Sprecher:
Der italienische Journalist Francesco Cancellato hat diese Sicherheitsmaßnahme ergriffen. Er hat sein Android-Handy gegen ein aktuelles iPhone getauscht, das nun im Lockdown-Modus läuft. Er ist extra wachsam geworden.

O-Ton 19 Francesco Cancellato (engl.):
Every anomaly right now, I pick up the phone … But I'm pretty sure that I am more aware right now.

Sprecher 2:
(Voiceover):
Natürlich greife ich jetzt bei jeder Unregelmäßigkeit sofort zum Telefon und sage: ‚Hallo Citizen Lab, ich habe eine Unregelmäßigkeit festgestellt, kann ich euch meine Systemdiagnose schicken? Kann ich euch meine Chat-Sicherung schicken? Könnt ihr das für mich analysieren?‘ Ich bin mir nicht sicher, dass man mich nicht noch einmal ausspionieren könnte. Das könnte wieder passieren. Aber ich bin mir dessen jetzt bewusster.

Sprecher:
Auf der Konferenz in Griechenland holt der Journalist Thanasis Koukakis sein iPhone aus der Hosentasche. Auch er hat den Lockdown-Modus aktiviert. Sein Smartphone ist damit zum Dumb-Phone geworden, sagt er. Vom smarten zum dummen Gerät.

O-Ton 20 Thanasis Koukakis (engl.):
The lockdown mode, it's something that, that makes the smartphone dumb phone… But it's a necessity to do so if you want to use an iPhone.

Sprecher 2:
(Voiceover):
Man kann nicht einmal mehr seine Textnachrichten durchsuchen. Solche Funktionen gehen verloren. Aber es ist jetzt notwendig, wenn man ein iPhone benutzen möchte.

Sprecher:
Er sei vorsichtiger geworden, was er über sein Handy sage und schreibe, selbst wenn es verschlüsselt passiere, sagt Koukakis. Er würde sich jetzt öfter persönlich mit seinen Informanten treffen, ohne Handy.

Musikakzent

Sprecher:
Seit dem Pegasus-Skandal hat sich die Branche weiterentwickelt. Den Markt dominieren mehrere internationale Spionageunternehmen. Ihre Softwares nutzen immer neue Sicherheitslücken, die Tech-Konzerne zu schließen versuchen. Es ist ein ständiger Wettlauf. Europäische Staaten greifen auf diese kommerziellen Spionagedienste zurück – und unterstützen so das Geschäft mit der IT-Unsicherheit. Wer wen ausspioniert und welche Daten wohin abfließen, bleibt meist unbekannt. Dieselbe Software, die Behörden gegen Kriminelle einsetzen, kann jederzeit gegen Verteidiger der Demokratie gerichtet werden.

Abspann:

Das Wissen (über Soundbett)

Sprecher:
Spähsoftware im Handy – Wie Staaten uns heimlich überwachen. Von Benjamin Breitegger. Sprecher: Marcus Westhoff. Redaktion: Lukas Meyer-Blankenburg. Regie: Günter Maurer.

Abbinder

*****

Literatur:

Ronald J. Deibert:
„Chasing Shadows“, Direktor Citizen Lab (2025)

Links:
Positionspapier EDRI, Spyware and State Abuse (2025):
EDRi_Spyware-position-paper.pdf

Abschlussbericht des EU-Parlaments (2023): TA MEF

Wissenschaftliche Dienste des Deutschen Bundestags: Sachstand zu sogenannter Spionagesoftware (2022):
Fragen zu sogenannter Spionagesoftware