SWR2 MANUSKRIPT
ESSAYS FEATURES KOMMENTARE VORTRÄGE

SWR2 Wissen
Spionage-Trojaner im Staatsdienst

Von Dieter Bauer

Sendung: Montag, 17. September 2018, 8:30 Uhr
Redaktion: Charlotte Grieser
Regie: Andrea Leclerque
Produktion: SWR 2018

Staaten und Staatsorgane wie Polizei und Geheimdienste nutzen Trojaner, um Gegner auszuspionieren. Die neueste Generation dieser Tools ist besonders perfide und schwer zu erkennen.

MANUSKRIPT

Atmo – Tagesschau 1.3.18, 22.15 Uhr:
„Noch ist nicht ganz klar, wer den Angriff auf das Computernetz der Bundesregierung verantwortet hat, wie groß das Ausmaß des Datenklaus wirklich war oder wie viele Ministerien und Behörden es getroffen hat. Aber eines ist ziemlich klar geworden: Wenn es um digitale Sicherheit geht, sollten wir uns alles andere als zu sicher wähnen.“

Sprecherin 2:
Sie bedrohen die deutsche Regierung ebenso wie Menschenrechtsaktivisten im Nahen Osten.

O-Ton - Ala’a Shehabi, darüber Übersetzerin:
Ich dachte mir, dass die Regierung versuchen könnte, Oppositionelle mit gefälschten Mails hereinzulegen. Mit individuell aufgemachten Mails.

Sprecher 1:
Die Urheber sprechen nicht gern über sie.

O-Ton Autor/Gamma im Gespräch, darüber Übersetzer:
Gamma: Wollen Sie, dass ich den Sicherheitsdienst hole? Ich mach‘ das! –
Autor: Die Aufsicht? –
Gamma: Ich fordere Sie auf, zu gehen und nicht mehr länger mit mir zu sprechen. Bitte. Ihre Entscheidung.

Ansage:
Spionage-Trojaner im Staatsdienst. Eine Sendung von Dieter Bauer.

Sprecher 1:
Cyber-Spione, sogenannte Trojaner, verkauft von privaten Unternehmen: Sie können mitlesen, -hören oder -sehen, was User auf ihren Computern, Tablets und Smartphones tun. Werden sie von Regierungen, Regimes oder Regierungsorganen eingesetzt, spricht man von Staats-Trojanern.

Sprecherin 2:
Ein Trojaner ist eine Schad-Software, die Nutzer auf ihren eigenen Geräten ausspioniert, Textbotschaften mitliest und Passwörter erfasst. Kriminelle setzen Trojaner ein, um Kontodaten oder Kreditkarten auszuspähen. Aber auch Regierungen, Polizei und Geheimdienste haben ein starkes Interesse an ihnen: Ein Mausklick und die Überwachungs-Software liest den aktuellen Standort Verdächtiger oder auch nur missliebiger Personen aus, kopiert Adressbücher oder schaltet heimlich die Mikros und Kameras von Smartphones an. Das spart die mühsame Installierung von Abhör-Wanzen oder gar den aufwendigen Einsatz eines teuren Überwachungsteams. Der Informatiker Eric King von der Londoner Nichtregierungsorganisation „Privacy International“ forscht seit langem zu dieser Form der elektronischen Überwachung:

O-Ton Eric King, darüber Übersetzer:
Trojaner werden an einen Computer oder ein Smartphone gesendet, um diese Geräte zu hacken. Anschließend kann der Absender des Trojaners das Gerät heimlich steuern. Er kann die Emails mitlesen, den Kalender ausspähen, aber noch viel mehr: zum Beispiel die getippten Tasten protokollieren und auf diese Weise verschlüsselte Passwörter ermitteln. Der Trojaner kann auch Sicherheits-Software umgehen, die Kamera anschalten, Fotos und Videos aufnehmen. Auch das Telefon-Mikro kann aus der Ferne angeschaltet werden. Dann trägt man ahnungslos eine Abhör-Wanze mit sich herum und lädt sie auch noch selber jede Nacht neu auf.

Sprecher 1:
Eric King hat viel zu tun: Immer mehr hochspezialisierte, kleine Privatunternehmen drängen auf den Markt für die sogenannte „Spyware“ und bieten immer ausgefeiltere Produkte an. Prinzipiell lassen sich die Spionage-Werkzeuge gegen jeden einsetzen: Schwerverbrecher und Terroristen, aber auch ahnungslose Normalbürger, Politiker, Konzernchefs, Militärs – oder, besonders perfide, gegen politisch aktive Bürger, die sich in einer Diktatur für Menschenrechte einsetzen. Neu ist diese Art der Spionage nicht:

O-Ton Eric King, darüber Übersetzer:
Bösartige Software wie diese Trojaner existieren, seit es Computer gibt. In jüngster Zeit beobachten wir aber einen neuen Trend: Privatunternehmen entwickeln solche Technologien gezielt und verkaufen sie an Strafverfolgungsbehörden. Dabei ist die Rechtslage unklar: Denn nur wenige Länder haben diese Art der Überwachung juristisch geregelt. Dabei muss man sich nur mal die Möglichkeiten vorstellen: Trojaner können Dateien verändern, Beweismittel unterschieben, alles Mögliche tun. Wir wissen nicht einmal, wie viele europäische Länder solche Tools einsetzen.

Sprecher 1:
Im Herbst 2017 entdecken auf Computerviren spezialisierte Wissenschaftler aus Deutschland, der Schweiz und der Slowakei fast gleichzeitig eine neue Version des Trojaners „Finfisher“, der von einer gleichnamigen GmbH aus München verkauft wird.

Sprecherin 2:
Dieser Trojaner ist von neuer Qualität: Bislang mussten Nutzer selbst einen Fehler machen, um sich einen Trojaner auf ihrem Smartphone oder Computer einzufangen – zum Beispiel eine verseuchte PDF-Datei oder ein angehängtes Foto öffnen. Die neue Finfisher-Version kommt nun noch heimtückischer daher: ganz ohne klickbare Anhänge, erklärt Candid Wüest aus Zürich, der ebenfalls Schadsoftware erforscht und zu den Entdeckern der neuen Finfisher-Generation gehört.

O-Ton – Candid Wüst:
Es kann sein, dass ich zu Hause am Surfen bin und will mir die neueste Version von irgendetwas herunterladen – WhatsApp, Firefox …

Sprecherin 2:
Ganz gewöhnliche Software, die täglich heruntergeladen wird und später immer wieder aktualisiert werden muss. Sie dient als Einfallstor für den Finfisher-Trojaner.

O-Ton – Candid Wüst:
… und ich werde dann beim Provider weitergeleitet und merke wahrscheinlich gar nicht, dass ich nicht auf dem Originalserver lande, sondern auf dem, der mir ein Zusatz-Paket – eben diesen Finfisher-Trojaner – mitliefert.

Sprecher 1:
Candid Wüest arbeitet für die Symantec Corporation – ein privates Unternehmen, das Antivirenprogramme verkauft. Kurz nach seiner Entdeckung meldet sich die Konkurrenz aus Bratislava: Dort finden die Forscher des Unternehmens ESET manipulierte Download-Links, ebenfalls für weitverbreitete Programme:

Sprecherin 2:
Videotelefonie per Skype, Schutzsoftware wie Avast, Dateienpackprogramme wie WinRAR oder der VLC Player, mit dem sich Videos und Musik abspielen lassen. Wer Updates dieser Programme laden möchte, kann von Finfisher auf eine gefälschte Webseite weitergeleitet werden, die dem Original täuschend ähnlich sieht. Dort wartet zwar das gewünschte Update, aber mit Finfisher als heimlicher Zugabe.

Sprecher 1:
Laut ESET, das wie Symantec diverse Antivirenprogramme verkauft, sollen bei der Umleitung auf gefälschte Webseiten „einige Telekommunikations-Unternehmen eine entscheidende Rolle (spielen)“. Das hieße: Die Internet- oder Telefonanbieter wären an der Verbreitung der Schadsoftware beteiligt. Aber ESET nennt weder die Unternehmen noch die Staaten, in denen die entsprechenden Router stehen, über die die Daten laufen. Symantec geht einen Schritt weiter. Candid Wüest:

O-Ton – Candid Wüst:
Also meines Wissens passiert es nicht bei den großen Providern und bei keinem Provider in Deutschland. Aber in gewissen Staaten kann es natürlich sein, dass das Regime Druck ausüben kann, um einen solchen Austausch der Software durchzuführen. Wir haben Indizien gesehen, dass in der Türkei und in Ägypten betroffene Fälle vorhanden sind, wo Finfisher eingesetzt wurde. Die Fälle, die wir gesehen haben, waren eher bei kleineren, lokalen, klassisch-städtischen Providern – keiner der ganz Großen.

Sprecher 1:
Kurz vor Redaktionsschluss dieses Features liefert eine Nichtregierungsorganisation aus New York City wieder Hinweise zu einem Finfisher-Trojaner neuen Typs: Laut „accessnow“ begann einer der Angriffe im Juli 2017 in der Türkei – in dem Land, vor dem der damalige deutsche Außenminister Sigmar Gabriel noch im selben Monat wegen willkürlicher Verhaftungen deutscher Staatsbürger warnte.

Sprecherin 2:
Auf mehreren gefälschten Twitter-Accounts, die scheinbar über Aktionen von Regierungsgegnern informierten, sei für kritisch aussehende Websites geworben worden, so accessnow. Diese Websites hätten schließlich eingeladen, über Android-Apps zu anderen Oppositionellen Kontakt aufzunehmen. In diesen Apps sei dann Finfisher versteckt gewesen.

Atmo:
Protestrufe

Sprecher 1:
Zu den Opfern früherer Finfisher-Versionen gehören Bürgerrechtler aus Bahrain. Das dortige Regime wird von Organisationen wie Amnesty International beschuldigt, willkürlich Menschen zu inhaftieren und sogar Kinder zu foltern. Dort setzte sich die Aktivistin Ala'a Shehabi für die Menschenrechte ein – und wurde deshalb mit einem Finfisher-Trojaner angegriffen. Damals musste man noch versehentlich auf einen ausführbaren Programmcode klicken, um den Trojaner zu aktivieren: zum Beispiel einen Mailanhang mit einer getarnten „exe“-Datei.

O-Ton – Ala'a Shehabi, darüber Übersetzerin:
Ich schaute mir damals meine Mails an. Dabei fiel mir eine sofort ins Auge: Denn der Absender sah aus, als wäre die Mail von einem bekannten Führer einer Oppositions-Partei verschickt worden. Man solle die Anlage anklicken: eine Agenda für einen

Dialog mit dem König. Ich dachte: Wow, das könnte eine sehr wichtige Nachricht sein. Aber als ich die Anlage öffnete, erschien nur eine leere Seite.

Sprecherin 2:
Ala'a Shehabi löschte die Mail mitsamt Anlage – die Sache schien erledigt zu sein. Doch mit dem Klick auf die Anlage hatte Shehabi ihr eigenes Smartphone in ein hochgefährliches Überwachungsinstrument verwandelt, das im autoritär regierten Bahrain Menschen in Lebensgefahr bringen kann: Sie hatte unwissentlich Finfisher aktiviert.

O-Ton – Ala'a Shehabi, darüber Übersetzerin:
Eine Woche später bekam ich eine andere Mail, angeblich von einer Reporterin des Senders Al Jazeera. In der Anlage sollte diese Mail Informationen über den Leiter des Bahrainischen Zentrums für Menschenrechte enthalten. Aber diesmal war ich vorsichtiger und klickte nicht auf die Anlage. Zwei Tage später folgte eine weitere dubiose Mail, mit einem angeblichen „News-Report“.

Sprecherin 2:
Ala'a Shehabi wurde misstrauisch.

O-Ton – Ala'a Shehabi, darüber Übersetzerin:
Ich dachte mir, dass die Regierung versuchen könnte, Oppositionelle mit gefälschten Mails reinzulegen. Mit individuell aufgemachten Mails. Deshalb kontaktierte ich unabhängige IT-Experten. Die entdeckten auf meinem Smartphone einen Trojaner und begannen, sein Verhalten zu erforschen. Insgesamt zwei Monate lang. Für mich war die Frage am wichtigsten, an wen all diese Informationen aus meinem Smartphone gesendet worden waren? Die Experten ermittelten, dass sie an einen Server in Bahrain geschickt wurden. Es war zu befürchten, dass das Regime Zugriff auf diesen Server hatte. Das wollten wir dann beweisen.

Sprecher 1:
Die IT-Experten von „Privacy International“ sowie des „Citizen Lab“ der Universität von Toronto isolierten den Trojaner zuerst in einer sicheren Computerumgebung. Als sie ihn dort auspackten und loslaufen ließen, breitete er sich rasend schnell aus. Dabei verwischte er seine Spuren, indem er Namen von Ordnern und Dateien mehrfach änderte. Dann drang er in Systemdateien ein. Schritt für Schritt dokumentierten die Forscher mit Screenshots, wie Finfisher das Betriebssystem des Smartphones zu manipulieren begann: Der Trojaner erklärte vorhandene Systemdateien für gelöscht oder neu beschreibbar und überschrieb sie anschließend mit eigenen Dateien. Am Ende hatte er das Smartphone der Bürgerrechtlerin zu einer Wanze umfunktioniert, die von einem externen Server gesteuert wurde.

Sprecherin 2:
Dessen IP-Adresse fand sich in einem öffentlichen Register und gehörte der „Bahrain Telecommunications Company“, kurz: „Batelco“. Batelco ist bis heute nach eigenen Angaben das größte Telekom-Unternehmen des „Königreichs Bharain“ – „reguliert“ von der dortigen Telekom-Behörde. Zu den Hauptaktionären gehören regierungsnahe Pensionsfonds. Batelco ist laut Unternehmens-Webseite auch auf den europäischen Inseln Jersey, Guernsey und Isle of Man tätig, die als „Kronbesitz“

keiner Regierung, sondern nur der britischen Krone unterstehen und ein beliebter Sitz sind für Firmen, die Steuern sparen wollen. Nach der Spähaktion erwartete die Bürgerrechtlerin Shehabi das Schlimmste:

O-Ton – Ala'a Shehabi, darüber Übersetzerin:
Jeden Tag wartete ich zuhause mit gepackten Sachen, ob die Polizei mich holt. Ich musste davon ausgehen, dass ich auf deren Fahndungsliste stehe. Aber dann wurde stattdessen mein Mann verhaftet. Vielleicht lag das daran, dass er nur Bürger von Bahrain ist, während ich zusätzlich die britische Staatsbürgerschaft besitze. Sie verhafteten und bestraften ihn – für meine Aktivitäten und die meines ebenfalls aktiven Vaters.

Atmo:
Protestrufe

Sprecher 1:
Laut Shehabi ist ihr Mann ein unpolitischer Geschäftsmann. Trotzdem wurde er zehn Monate lang im Gefängnis gefoltert. Seine Freilassung hatte er einem Autorennen zu verdanken, berichtet Shehabi: einem der Formel 1-Events, die bis heute regelmäßig in Bahrain stattfinden. Sie sprach damals den Formel 1-Chef Bernie Ecclestone auf ihren inhaftierten Mann an, und der setzte sich beim Kronprinzen des Königreichs für die Entlassung ein. Und plötzlich öffnete sich nachts eine Zellentür: Shehabis Mann floh aus dem Bahrainer Gefängnis ins Exil nach London.

Atmo:
Raumatmo, tippen

Sprecherin 2:
Auf Shehabis Smartphone waren die IT-Experten zuletzt in dessen „Gedächtnis“ vorgestoßen: das „memory dump“. In dem Datenwust war wiederholt eine bestimmte Signatur aufgetaucht: „Finspy“, also: Fin-Spion. Ein ziemlich nachlässiger Fehler des Trojaner-Produzenten: Während die Spionage-Software vielerlei Spuren verwischte, führte deren Signatur auf direktem Weg zum damaligen Anbieter: dem Unternehmen „Gamma International“, das sich inzwischen „Gamma Group“ nennt und bis heute für den Verkauf von „Überwachungssystemen“ in seinen Niederlassungen in Europa, Asien, dem Mittleren Osten und Afrika wirbt.

Sprecher 1:
Heute meidet Gamma jeden offiziellen Hinweis auf das heikle Produkt „Finspy“ bzw. „Finfisher“. Deshalb besuchte ein ARD-Reporter die Messe „Security & Policing“ der britischen Regierung, um am Stand der „Gammagroup“ nach dem Produkt zu fragen.

O-Ton – Autor im Gespräch mit Gamma, darüber Übersetzer:
Autor: Pardon, Sie arbeiten für Gamma?
Gamma (männl.): Nehmen Sie mich gerade auf?
Autor: Wenn Sie es erlauben.
Gamma: Sind Sie von der Presse?
Autor: Dem öffentlich-rechtlichen Deutschen Radio, ARD.

Sprecher 1:
Der Standleiter war überrascht, auf einen Reporter zu treffen, denn Journalisten haben auf dieser „Sicherheits“-Messe normalerweise keinen Zutritt.

O-Ton – Autor im Gespräch mit Gamma, darüber Übersetzer:
Autor: In Deutschland hat die Bundespolizei eine Software namens „Finfisher“ gekauft, die Handys überwacht. –
Gamma: Darüber habe ich keine Informationen. Da müssen Sie das Unternehmen fragen, das „Finfisher“ herstellt. –
Autor: Welches Unternehmen, wenn nicht Sie? –
Gamma: Es heißt „Finfisher GmbH“. Ein komplett neues Unternehmen. „Gamma“ hat keine Beteiligung mehr an „Finfisher“. Gar keine. –
Autor: Aber „Gamma“ war früher beteiligt. –
Gamma: Ja, wir haben das Projekt ursprünglich entwickelt und dann später entschieden, uns davon zu (Pause) distanzieren. –
Autor: Und was war Ihr Grund, sich zu distanzieren? –
Gamma: Ich wollte nicht mehr, weil die Medien und die Presse in unser Geschäftsleben und unser Privatleben eindrangen. –
Autor: Was war das für ein Eindringen? –
Gamma: Na, so wie Sie das gerade machen. –
Autor: Aber vielleicht fühlen andere Leute, dass „Finfisher“ in ihr Leben eingedrungen ist. –
Gamma: Wollen Sie, dass ich den Sicherheitsdienst hole? Ich mach‘ das! –
Autor: Die Aufsicht? –
Gamma: Ich fordere Sie auf, zu gehen und nicht mehr länger mit mir zu sprechen. Bitte. Liegt bei Ihnen./Ihre Entscheidung.

Sprecher 1:
In München wirbt heute die FinFisher GmbH für ihre, Zitat: „erstklassigen Cyber-Lösungen für erfolgreiche Operationen gegen das organisierte Verbrechen“. *A*llerdings fehlt der Gesellschaft mit beschränkter Haftung jegliche Hoheitsfunktion über das Produkt, wenn es einmal verkauft ist: Behörden wie die des Unrechtsstaates Bahrain können Finfisher zuerst kaufen und dann nach eigenem Belieben einsetzen: zum Beispiel, um Regimekritiker zu überwachen, zu verhaften und zu foltern. Zu diesen und anderen Gefahren äußert sich die FinFisher GmbH nicht: Von 2013 bis heute blieben zahlreiche journalistische Anfragen unbeantwortet.

Sprecherin 2:
Ausspionieren ist ein lukratives Geschäft. Staatstrojaner haben sich zu einem Verkaufsschlager entwickelt. Seit etwa fünf Jahren breiten sie sich immer weiter aus: Finfisher ist der bekannteste, aber keinesfalls der Einzige.

Sprecher 1:
Die renommierte Nichtregierungsorganisation Privacy International in London veröffentlichte bereits vor zwei Jahren einen „Index der Überwachungsindustrie“ mit 528 Unternehmen. Die meisten von ihnen haben ihren Sitz in den USA, England, Frankreich, Israel und Deutschland.

Sprecherin 2:
Die Hersteller von Antiviren-Softwares merken bei ihrer täglichen Arbeit, dass immer mehr hochentwickelte Trojaner durch das Internet wandern. Sie versuchen, sie möglichst schnell zu entdecken und zu blockieren, um ihre Kunden zu schützen. Candid Wüest von Symantec aus Zürich:

O-Ton – Candid Wüest:
Es gibt verschiedene Merkmale, wie wir diese verdächtigen Softwarepakete enttarnen können. Das einfachste ist: Wir überwachen die Verhaltensmuster. Wenn das unbekannte Programm jetzt plötzlich anfängt, Ihre Webkamera einzuschalten, mit dem Mikrofon noch etwas mitzuschneiden und die Tastaturanschläge zu protokollieren, dann ist das schon sehr, sehr verdächtig. Und letztendlich blockieren wir es, wenn wir sagen: Jetzt ist zu viel Verdächtiges gemacht worden. Und deshalb, bevor der Schaden entsteht, wird dann blockiert.

Atmo:
Büroflur

Sprecher 1:
Doch die Finfisher GmbH und die andere Trojaner-Anbieter entwickeln ebenfalls immer neue Tricks und setzen auf immer neue Varianten ihrer Software.

Sprecherin 2:
Inzwischen erhalten Zielpersonen zuerst per Mail oder als Update mehrere Datenpakete, die jeweils unverdächtig erscheinen. Erst auf der Festplatte fügen sich die einzelnen Pakete dann zu einem gefährlichen Trojaner zusammen.

Sprecher 1:
Am besten lassen sich die wendigen Trojaner beim Export ihrer Beute ertappen: Denn die gestohlenen Daten müssen den Computer verlassen, um an die auswärtigen Schnüffler zu gelangen.

O-Ton – Candid Wüest:
Die Überwachungs-Software wird meistens irgendeinen zentralen Rechner haben, wo sie sich anmeldet und sagt: Ich habe erfolgreich mein Ziel kompromittiert – welche Befehle soll ich ausführen? Was soll ich denn wirklich genau stehlen? Wenn wir wissen, welche Server hier benutzt werden, dann können wir den Benutzer aktivieren und sagen: Dein Rechner macht gerade eine Verbindung auf zu diesem Rechner im Internet. Und da wissen wir: Der wird eigentlich nur für solche Überwachungs-Software eingesetzt. Das heißt im Umkehrschluss: Dein Rechner ist sehr wahrscheinlich infiziert.

Sprecherin 2:
Oft bleibt allerdings unklar, wer den Angriff ausführte, wann er begann und was gestohlen wurde. So erging es Anfang 2018 sogar der deutschen Bundesregierung mit ihrem eigentlich speziell geschützten Regierungsnetz:

Atmo – Tagesschau 1.3.18, 22.15 Uhr:
„Wenn es um digitale Sicherheit geht, sollten wir uns alles andere als zu sicher wähnen. 1.23 Während der Vorfall offenbar noch andauert, stellt sich die Frage: Haben wir überhaupt die richtigen, die modernsten Möglichkeiten in einem globalen Cyberkampf? Oder schützen wir uns nur mit veralteter Technologie?“

Sprecherin 2:
Nach jüngsten Meldungen drang bereits 2016 ein Trojaner ins deutsche Regierungsnetz ein. Erst ein Jahr später wurde er von außen aktiviert und infizierte Computer des Auswärtigen Amtes. Wer die Angreifer waren, welcher Trojaner zum Einsatz kam und welche Dokumente gestohlen wurden, bleibt bis heute letztlich unklar. Den Virenforscher Wüest überrascht das nicht:

O-Ton – Candid Wüest:
Falsche Fährten sind sehr beliebt bei den Angreifern. Wenn also ein Staat, nehmen wir rein hypothetisch Russland, die Deutschen angreifen möchte, könnte es natürlich auch sein, dass die sagen: Wir möchten nicht, dass das so eindeutig zurückzuverfolgen ist. Und deshalb nehmen wir dann auch den schon bekannten und auch schon im Internet diskutierten Schadcode zum Beispiel von China oder Amerika, und legen den absichtlich auf den Computer. So dass jeder, der die Analyse macht, dann eben merkt: Den Schadcode habe ich schon mal gesehen – der gehört den Chinesen – und dann eher da anfängt zu suchen und eben nicht die eigentliche Fährte findet.

Sprecherin 2:
Im deutschen Regierungsnetz soll das Bundesamt für Sicherheit in der Informationstechnik den Trojaner erst Anfang 2018 entdeckt und dann „kontrolliert beobachtet“ haben, um Angreifer und Motive zu ermitteln.

O-Ton – Candid Wüest:
Man kann nicht immer eindeutig sagen, was genau passiert. Es kann wirklich sein, dass eine dritte Partei auch auf dem gleichen Rechner ist. Weil: Wenn die erste Partei Interesse hat, an Informationen zu kommen, dann ist‘s wahrscheinlich eine interessante Person. Dann kann es sein, dass vielleicht zwei, zum Teil drei verschiedene Angreifer drauf sind. Wir haben auch schon gesehen, dass die zum Teil unbewusst miteinander spielen: Der eine lässt den anderen die Arbeit machen, mitlesen ist dann die kleinere Anstrengung. – Autor: Ist denn immer die Grenze klar, dass nur ein Trojaner aufgespielt wurde und nicht vielleicht auch Dateien? – Die Grenze ist definitiv nicht immer klar. Das Katz-und-Maus-Spiel von Angreifer und Verteidiger ist klassisch und wird sich auch in Zukunft noch weiter austragen.

Sprecher 1:
Gegen die Ausfuhr von Trojanern wie Finfisher in Diktaturen stimmte Anfang 2018 das Europäische Parlament: Sie soll durch striktere Exportkontrollen behördlich gesteuert und Missbrauch so verhindert werden. Bis dahin scheint es noch ein langer Weg zu sein: Denn wenige Monate zuvor musste die Bundesregierung noch einräumen, dass nach jüngsten Zahlen in den Jahren 2014 bis 2016 der Export von „Überwachungsausrüstungen“ und „Netzwerk-Überwachungssystemen“ in Länder

wie Äthiopien, Iran, Saudi-Arabien und Turkmenistan offiziell genehmigt worden war. Der Bundestags-Abgeordnete Konstantin von Notz von den Grünen gehörte zu denen, die kritische Fragen stellten:

O-Ton – Konstantin von Notz:
Diese Technologie kann in Einzelfällen sogar problematischer sein als eine Waffenlieferung. Sie ermöglicht eine Überwachung, wie man sie vor dieser Technik überhaupt nicht kannte. Und damit eben in den Händen von nicht demokratischen Herrschern eine Unterdrückungsmöglichkeit, wie man sie bisher nicht kannte. Ich glaube, es muss da einen glasklaren rechtsstaatlichen Kompass geben. Solche Technik hat in Unrechtsstaaten nichts verloren, denn sie wird dort nur dafür eingesetzt, Leute auszufinden, auszukundschaften und zu überwachen, sie dann in die Folterkeller zu führen. Und insofern muss man sagen: Das Kriterium muss Rechtsstaatlichkeit sein. Sonst darf man solche Technik dorthin nicht exportieren.

Sprecher 1:
Ein einmal gehackter Computer steht offen und ist auch von außen manipulierbar: Deshalb können auch gesetzestreue Strafverfolgungsbehörden oft nicht mehr feststellen, wer dort belastendes Material abgelegt hat. Deshalb mag man auch fragen, warum das deutsche Bundeskriminalamt zu den Kunden der Finfisher GmbH zählt: Bereits 2011 investierte das BKA stolze 150.000 Euro in eine frühe Finfisher-Lizenz, obwohl dieser Trojaner lange Zeit gar nicht eingesetzt werden durfte: weil er mehr kann, als der deutschen Polizei erlaubt ist.

Sprecherin 2:
Anfang 2018 meldeten dann WDR, NDR und die Süddeutsche Zeitung, dass das Bundesinnenministerium Finfisher zum Einsatz freigegeben habe. Vor allem die Nutzung verschlüsselter Messenger-Dienste solle damit zukünftig bei verdächtigen Personen überwacht werden dürfen. Warum Finfisher plötzlich deutschen Gesetzen entsprechen soll – dazu verweigert das BKA bis heute jeglichen Kommentar.

Constanze Kurz ist Informatikerin und Datenschützerin beim Chaos Computer Club, einer unabhängigen Hackervereinigung, die sich mit Computersicherheit und Datenschutz beschäftigt. Sie geht davon aus, dass die politisch und polizeilich Verantwortlichen bis heute nicht mal den Quellcode, also den in Programmiersprache geschriebenen Text des Programmes von Finfisher kennen, und dessen Eigenschaften deshalb gar nicht lückenlos einschätzen können.

O-Ton – Constanze Kurz:
Es gibt keine Anhaltspunkte dafür, dass das Innenministerium oder die Benutzer dieser Software, namentlich das BKA, Einblick haben in den Quellcode dieser Software. Ich gehe nicht davon aus, dass die diese Firmen in besonderer Weise kontrollieren. Es mag schon sein, dass die mal Fragen stellen. Aber es gibt keine Anhaltspunkte dafür, jedenfalls keine öffentlichen, dass Finfisher diese Fragen beantwortet. Da, scheint mir, drückt die Bundesregierung und insbesondere das Innenministerium immer gern ein Auge zu, wenn es darum geht, über diese Firmen zu sprechen: Wo holen die zum Beispiel die Schwachstellen her, diese sogenannten zero day exploits?

Sprecherin 2:
„Exploits“ sind die Brechstangen der virtuellen Einbrecher: Sobald ein Software-Hersteller ein Sicherheits-Update bereitstellt, analysieren Hacker die Schwachstelle, die durch das Update geschlossen werden soll. Gelingt das schnell – am besten noch am selben Tag, dem „zero day“ – fehlt vielen Usern noch das Update, und der Hacker kann diese Schwachstelle ausnutzen.

O-Ton – Constanze Kurz:
Bei wem kaufen die eigentlich diese zero day exploits ein, mit wem sind die noch im Bett? Wir diskutieren in Deutschland ja letztlich seit über zehn Jahren über den Staats-Trojaner. Und immer, wenn man an diese Punkte kommt: Was sind das eigentlich für kommerzielle Firmen, mit denen da gehandelt wird, sieht man so ein Ducken – da wird ungern drüber gesprochen.

Sprecherin 2:
Finfisher ist aktuell vermutlich der gefährlichste Trojaner weltweit. Aber die Konkurrenz schläft nicht: Auf „Sicherheits“-Messen sammelten die Bürgerrechtler von Privacy International in den letzten Jahren über 1.500 Verkaufsbroschüren für Überwachungstechnologien ein. Diese Messen, die in Westeuropa, Südafrika, dem Nahen Osten und Südostasien stattfanden, boten zahllose „Lösungen“ für individuell zugeschnittene Überwachungen an.

Sprecher 1:
In George Orwells Roman „1984“ wurden die Menschen noch mit fest stationierten Kameras und Mikrofonen überwacht. Sie wussten davon und versuchten, in tote Winkel zu flüchten. Die Kunden der Überwachungsindustrien – Politiker, Polizisten, Regimes, Folterknechte – könnten darüber heute nur lachen. Constanze Kurz vom Chaos Computer Club sieht hier Probleme, die Staatsorgane, Datenschützer und natürlich auch die Bürgerinnen und Bürger noch länger beschäftigen werden:

O-Ton – Constanze Kurz:
Der Spagat, dass der Staat Geld ausgibt für Sicherheitslücken, aber auf der anderen Seite auch versucht, seine Bürger, seine Unternehmen, seine eigenen Behörden zu schützen – der war schon immer da. Ich glaube, dadurch, indem auch demokratische Staaten beginnen, diesen Markt zu finanzieren und Geld auszugeben, öffnen sie den Markt ja noch weiter. Und aus meiner Sicht ist das natürlich der falsche Weg.

*****

Service:

SWR2 Wissen können Sie auch als Live-Stream hören im **SWR2 Webradio** unter www.swr2.de oder als **Podcast** nachhören: http://www1.swr.de/podcast/xml/swr2/wissen.xml