hören, was dahinter steckt!

DAS ARD RADIO FEATURE

Der Staat und seine Trojaner

Von Achim Nuhr

hr2 kultur

Besetzung:
Sprecher: Udo Schenk
Zitatorin: Gergana Muskalla
Zitator 1: Aart Veder
Zitator 2: Reinhard von Stolzmann
Zitator 3: Hanns Jörg Krumpholz
Zitator 4: Sascha Nathan
An- und Absage: Helge Heynold
Regie: Helge Heynold
Technische Realisation: André Bouchareb
Redaktion: Dorothee Meyer-Kahrweg

Alle Sendetermine im Überblick: 23. – 28. April 2014

SWR	23.04./22:05/SWR 2
SR	26.04./09:05/SR 2
BR	26.04./13:05/BR
	W: 27.04./21:05/BR 2
RB	27.04./16:05/Nordwestradio
	W: -
NDR	27.04./ 11:05/NDR Info
WDR	27.04./11:05/WDR 5
	W: 28.04./20:05/WDR 5
HR	27.04./18:05/HR 2-Kultur

ARD · BR Bayern 2 · hr2 kultur · NDR Info · nordwest radio · SR2 · SWR2 · WDR 5

Jingle: ARD-radiofeature

ATMO:

Flughafen München

SPRECHER:

Sommer 2009 – in der Ankunft-Halle des Flughafens München eilen Passagiere zum Ausgang. Ein bayerischer Kaufmann wird angehalten: Zöllner nehmen seinen Laptop, verschwinden damit, geben ihm das Gerät aber bald zurück. Dieser scheinbar harmlose Zwischenfall wird später noch große Schlagzeilen machen. Denn die Zöllner haben heimlich eine Spionage-Software auf dem Laptop installiert, wie Hacker, ein Richter sowie der Bundesdatenschutzbeauftragte noch unabhängig voneinander ermitteln werden: einen Staatstrojaner.

ATMO:

in Landshut unterwegs

SPRECHER:

Eine Spionage-Software, mit der der Staat seine Bürger ausspäht? Was ist das für eine Software, was kann sie und wer darf sie in welchem Umfang einsetzen?
Um mehr über solche Staatstrojaner zu erfahren, mache ich mich auf den Weg. Mein erstes Ziel: Landshut, wo ich Patrick Schladt treffe, den Anwalt des Kaufmanns. Der war Monate nach dem Vorfall am Flughafen misstrauisch geworden.

O-TON (Schladt):

Ich habe versucht, aufzuklären, was da eigentlich passiert ist. Was man unter so einem Trojaner versteht. Das geschah letztendlich am Flughafen. Dort wurde der Trojaner im Rahmen einer Kontrolle aufgespielt, bzw. beim Hinflug

zunächst einmal das Modell des Laptops durchgesehen und beim Rückflug wurde das entsprechend aufgespielt.

SPRECHER:

Gegen Schladts Mandanten ermittelt das bayerische Landeskriminalamt: Der Landshuter Kaufmann handelt mit Pharmaprodukten, die bei der Ausfuhr aus Deutschland unter das Betäubungsmittelrecht fallen könnten. Damit wäre dieser Handel illegal gewesen. Eine Routineermittlung, die sich nach Schladts Angaben bis heute hinzieht. Aber die Fahndungsmethode ist neu, hochbrisant und - wie ich später herausfinden werde – rechtswidrig.

O-TON (Schladt):

Das hat sich erst nach einer Weile herauskristallisiert: Die Besonderheit dieses Staatstrojaners. Ein normaler Telefonüberwachungs-Beschluss beinhaltet im Regelfall die Anschlusskennung. Im hiesigen Fall war die Anordnung die Überwachung des Internets. Das ist etwas Atypisches, weil man das in dieser Form noch nicht hatte.

ANSAGE:

Der Staat und seine Trojaner

Ein Feature über amtliche Computerüberwachung in Deutschland

von Achim Nuhr

SPRECHER:

Seit den 1990er Jahren schreiben immer mehr Menschen Emails statt Briefe. Bald telefonieren sie auch über das Internet. Die neuen Kommunikationswege beunruhigen die Polizei: Denn „Internetprotokoll-“ oder kurz: „IP-Telefonate“ werden routinemäßig verschlüsselt, und auch Emails lassen sich leicht chiffrieren. Diese neuen, diskreten Möglichkeiten werden auch von Kriminellen genutzt.

Deshalb wollen Polizisten oder auch die Zollbehörden am liebsten direkt in die Computer und Smartphones von Verdächtigen vordringen: um Daten abzugreifen, bevor sie dort verschlüsselt werden und anschließend auf Reisen gehen. Der Fachbegriff lautet: „Quellen-Telekommunikationsüberwachung“, oder kurz: Quellen-TKÜ. Dabei gibt es allerdings ein Problem: In den Geräten von Verdächtigen stoßen die Fahnder schnell auf den „absolut geschützten Kernbereich privater Lebensgestaltung“, und den schützen die Bundesverfassungsrichter vor jedem behördlichen Zugriff – auch bei Menschen, die Straftaten begangen haben könnten. Wie dringt man in Rechner und Smartphones ein, ohne dabei diese engste Privatsphäre der Bürger zu verletzen?
Viele halten das für nahezu unmöglich, wie zum Beispiel
Ulf Buermeyer. Der Verfassungsrechtler, Publizist und Richter am Landgericht Berlin erklärt mir:

O-TON (Buermeyer):
Es ist vermutlich so, dass der Eingriff in einen Computer inzwischen gravierender ist als eine Hausdurchsuchung. Und zwar einfach deswegen, weil sich in einem Computer im Zweifel wesentlich mehr Daten befinden, die Auskunft geben über das Denken eines Menschen zum einen. Und zum anderen ist es in einem Computer auch wesentlich schwerer zu kontrollieren, was denn eigentlich gespeichert ist. Wenn man sich mal die Komplexität heutiger Rechnersysteme anguckt: dass die sehr viele Informationen in irgendwelchen dunklen Verzeichnissen ablegen, die wir selbst längst vergessen haben. In der Tat weiß man bei der Wohnungsuntersuchung jedenfalls, dass sie stattgefunden hat. Und das ist bei der Online-Durchsuchung eben ein großes Problem: Im Zweifel bekommt man ja zunächst einmal auch gar nicht mit, dass eine solche Maßnahme vorgenommen wurde.

SPRECHER:

Dazu liefert der Landshuter Staatstrojaner eine spannende, haarsträubende Geschichte: Der Weg führt mich hinaus aus der bayerischen Provinz zu den Hackern des Chaos Computer Clubs, zu Politikern, die Cyberpolizisten kontrollieren sollen, aber schon das Internet kaum verstehen, und zum Bundeskriminalamt, das sich von Privatunternehmen potentiell gesetzwidrige Software andrehen lässt. Endstation ist ein privater Trojaner-Produzent, der sowohl an deutsche Kriminalämter als auch an internationale Folterer liefert.

ATMO:

in Landshut unterwegs

SPRECHER:

Von all dem ahnt der Landshuter Rechtsanwalt Patrick Schladt nichts, als er für seinen Mandanten Einsicht in Behördenakten fordert. In den Amtsräumen erlebt Schladt dann die erste Überraschung: Er stößt auf einen digitalen Datenträger mit etwa 60.000 Fotos, die allesamt den Laptop-Bildschirm seines Mandanten zeigen. Die unzähligen „Screenshots“ dokumentieren, was der Landshuter Kaufmann über Monate mit seinem Laptop gemacht hat: also mit dem Gerät, das die Zöllner des Flughafens München kurz in ihren Dienstraum mitgenommen hatten.

O-TON (Schladt):

Es bedeutet: Jedes Mal, wenn der Betroffene seinen Rechner eingeschaltet hat und dabei entweder das Browser-Fenster oder den E-Mail-Client oder ähnliches geöffnet hat, dann wurde im 30sekündigen Abstand letztendlich abfotografiert und dieses dann an die Ermittlungsbehörden herausgegeben. Zusätzlich dazu eben auch noch die Überwachung des verschlüsselten Verkehrs über Skype und natürlich auch Chat-Überwachung und ähnliche Sachen. Und das ist schon Monitoring. Das ist schon ein sehr stärkeres

Überwachen wie das, was man eigentlich mit einer bloßen E-Mail-Ausleitung hat. Das ist eine Stufe weiter. Was dann dieser Trojaner eigentlich alles kann, das hat sich ja dann erst später letztendlich herausgestellt: als die Experten des CCC diesen dann analysierten.

ATMO:

Landshut, Treppenhaus

SPRECHER:

Schladt wagte einen ungewöhnlichen Schritt: In Absprache mit seinem Mandanten übergab der Rechtsanwalt dessen Laptop an den Chaos Computer Club e.V.. Die renommierten Hacker sollten nach der Spionage-Software suchen, die die Screenshots angefertigt und weiter geleitet haben musste. Aber die Sprecherin des CCC, Constanze Kurz, reagierte zuerst skeptisch.

O-TON (Kurz):

Wir haben eigentlich offen gestanden nicht gedacht, dass wir etwas finden. Weil wir schon dachten, dass die Strafverfolgungsbehörden technisch in der Lage sind, ihre eigene Spionagesoftware sicher zu löschen. Und die Idee, mal im Papierkorb nachzuschauen, im so genannten Papierkorb, war uns erst gar nicht gekommen. Aber so fanden wir auf dieser Festplatte diese Software. (Lacht) Tja. War unerwartet. Also wir hatten schon angenommen, dass die Strafverfolgungsbehörden diese Platte auch von den Überresten dieser Spionage-Software bereinigen würden.
Und dann war eigentlich nach zwei, drei Wochen schon ziemlich klar: Damit werden wir an die Öffentlichkeit gehen.

O-Ton

Tagesschau-Fanfare

(Nachrichtensprecher:) Guten Abend meine Damen und Herren. In Deutschland sorgt der Einsatz eines sogenannten Staatstrojaners für Diskussionen. FDP und Opposition fordern (...) Aufklärung, denn die Software kann möglicherweise mehr Informationen liefern, als das Bundesverfassungsgericht erlaubt.

(im Hintergrund weiterlaufen lassen)

SPRECHER:

Ende 2011 nahm der Fall des Landshuter Staatstrojaners politisch Fahrt auf. Zwei verantwortliche Unions-Politiker stammen selbst aus Bayern: der damalige deutsche Innenminister Hans-Peter Friedrich und der Innenpolitische Sprecher der CDU/CSU-Fraktion, Hans-Peter Uhl. Im Bundestag verteidigte Uhl den Staatstrojaner gegen missliebige Kritiker:

O-TON (Uhl):

Das Land wird von Sicherheitsbehörden geleitet, die sehr kontrolliert, sehr sorgfältig, sehr behutsam mit dem sensiblen Instrument der Quellen-TKÜ umgehen – und so soll es auch sein. Das heißt, es wäre schlimm, wenn unser Land am Schluss regiert werden würde von Piraten und Chaoten äh aus dem Computerclub. Es wird regiert von Sicherheitsbeamten, die dem Recht und dem Gesetz verpflichtet sind.

SPRECHER:

Das Landgericht Landshut wird das Vorgehen später ganz anders beurteilen, nämlich als „rechtswidrig". Und der damalige Datenschutzbeauftragte des Bundes, Peter Schaar, wird sogar eine „Missachtung der Rechtsprechung durch das Bundesverfassungsgericht" erkennen.
Schaar wird insgesamt 40 Fälle untersuchen, in denen Behörden Staatstrojaner einsetzten, und dann den Sicherheitsbehörden des Bundes berichten.

Dies ist zwar eigentlich „VS – also Verschlusssache – nur für den Dienstgebrauch“, doch der Chaos Computer Club bekommt Schaars Bericht später zugespielt und veröffentlicht ihn im Internet, wo man ihn herunterladen kann. Darin hält Deutschlands oberster Datenschützer gleich eingangs amtlich fest:

ZITATOR 1:
Die Durchführung … der Quellen-TKÜ durch das Bundeskriminalamt, den Zollfahndungsdienst und die Bundespolizei konnte nur begrenzt datenschutzrechtlich überprüft werden. … Den genannten Behörden … (lag) der Quellcode … der Software oder eine anderweitige hinreichende Programmdokumentation nicht vor. Belastbare und abschließende Aussagen … sind daher nicht möglich.

SPRECHER:
Der Quellcode oder auch Quelltext ist der in einer Programmiersprache geschriebene Text eines Computerprogramms. Deutsche Behörden setzten also fremde Schnüffel-Software ein, und der Trojaner-Lieferant, Digitask, ein Privatunternehmen, behielt dabei entscheidende Informationen für sich. Dazu bemerkt Digitask in einer Stellungnahme:

ZITATORIN:
Wir haben Herrn Schaar die Einsichtnahme in den Quellcode nicht verwehrt.

SPRECHER:
Allerdings ist im Internet ein Schaar-Bericht an den Innenausschuss des Deutschen Bundestages zu finden, der die Umstände dieser „Nicht-Verwehrung“ erläutert. Schaar schreibt:

ZITATOR 1:

Das Bundeskriminalamt ... teilte mir ...mit, dass die Firma Digitask GmbH die Einsichtnahme in den Quellcode nur unter der Voraussetzung ermöglichen werde, dass der Bundesbeauftragte für den Datenschutz ...eine Geheimhaltungsvereinbarung unterzeichne. Darüber hinaus werde die Firma zum Ausgleich der entstehenden Kosten Ansprüche auf Kostenerstattung geltend machen. Der Tagessatz für "Consulting-Dienstleistungen" betrage 1.200,00 EUR pro Tag und Mitarbeiter zuzüglich der gesetzlichen Mehrwertsteuer. ...Die von mir vorgeschlagenen Termine waren seitens der Digitask GmbH nicht realisierbar."

SPRECHER:

Trotzdem findet Schaar heraus:

ZITATOR 1:

Die ... eingesetzte Software ermöglicht es nicht, die den Kernbereich privater Lebensgestaltung betreffenden Inhalte ausgeleiteter Gespräche gezielt zu löschen. Damit wurde der vom Bundesverfassungsgericht in ständiger Rechtsprechung entwickelte Schutz ... missachtet.

SPRECHER:

Dem Staatstrojaner scheint eine entscheidende Löschfunktion zu fehlen.
Zwar behauptet Digitask später mir gegenüber in einer Stellungnahme, ohne dies näher zu erläutern:

ZITATORIN:

Im Verbund mit unserer Systemtechnik ist die verfassungsrechtlich gebotene Kernbereichsbehandlung berücksichtigt.

SPRECHER:

Doch der Bundes-Datenschutzbeauftragte kommt zu einem anderen Schluss:

ZITATOR 1:

In den ... Verfahren hatten zahlreiche der erfassten Gespräche für das Strafverfahren nicht relevante Kommunikation zum Inhalt.

SPRECHER:

Schaars Bericht dokumentiert zahlreiche weitere Gesetzesverstöße: wie „unzureichende Verschlüsselung ... der ausgeleiteten Daten“ und die „mangelnde Authentisierung ... der an den (Quellen-TKÜs) beteiligten Personen“. Aber seit Dezember 2013 müssen die Behörden den strengen Datenschützer nicht mehr fürchten: Denn da schied Schaar aus dem Amt. Seine Nachfolgerin ist Andrea Voßhoff von der CDU, die zuvor als Mitglied des Deutschen Bundestags die von Schaar kritisierten Überwachungsmaßnahmen befürwortet hatte. Anfang 2014, kurz nach Schaars Abgang, werden die Macher einer Website namens netzpolitik.org ein Dokument des Generalbundesanwalts erhalten und ins Internet stellen. Laut Stempel „nur für die Handakten“ bestimmt, reagierte der Generalbundesanwalt bereits im Herbst 2010 auf eine „Anregung“ des Bundeskriminalamtes in einem Ermittlungsverfahren mit den Worten:

ZITATOR 2:

Ein Antrag auf Anordnung einer sogenannten Quellen-Telekommunikationsüberwachung kommt aus Rechtsgründen nicht in Betracht. Es fehlt an der erforderlichen Rechtsgrundlage für einen Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

SPRECHER:

Doch diese Stellungnahme des Generalbundesanwalts stört das Bundeskriminalamt anscheinend nicht: Wie ich noch sehen werde, kaufen die Bundespolizisten noch nach 2010 eine teure Software zur Quellen-TKÜ aus einer trüben Quelle. Und wenn so ein Überwachungssystem einmal

vorhanden ist, dann wird es auch gern eingesetzt, weiß der Verfassungsrechtler Ulf Buermeyer. Er kennt die polizeiliche Praxis aus seiner Arbeit als Richter beim Landgericht Berlin.

O-TON (Buermeyer):
Der Hintergrund ist, dass Polizeibeamte in Ihrer täglichen Arbeit sehr häufig sehr schnell entscheiden müssen, wie sie vorgehen. Wie sie ermittlungstaktisch vorgehen, welche Maßnahmen sie einleiten. Man muss sich dann vor Augen halten, dass die allermeisten Polizeibeamten keine ausgebildeten Juristen sind. Aus meiner Alltagsarbeit im Gericht kann ich sagen, dass die allermeisten Polizeibeamten versuchen, in der Tat nach Recht und Gesetz zu handeln. Viele sind natürlich sehr engagiert in den Ermittlungen und loten die absoluten Grenzen dessen, was sie dürfen, aus. Manchmal gehen sie auch darüber hinaus.

SPRECHER:
Seit langem werden analoge Telefone abgehört, um nach Kriminellen zu fahnden: über einen festgelegten Zeitraum, gemäß richterlichem Beschluss. Kaum jemand zweifelt diese Praxis an. Aber bei der Überwachung von Computer-Telefonaten gibt es einen wichtigen Unterschied:
Computer und ihre kleinen Verwandten, die Smartphones, können sehr viel mehr als alte Kabel-Telefone – und daher ist auf Festplatten auch sehr viel mehr zu finden als in alten Fernsprechern.
Deshalb schufen die Karlsruher Verfassungsrichter bereits im Jahr 2008 ein neues Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“. Dort heißt es:

ZITATORIN:
Die heimliche Infiltration eines informationstechnischen Systems ... ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.

Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

SPRECHER:

Im Fall des Landshuter Kaufmanns gehen die Ermittler keineswegs von Schwerstkriminalität aus. Von einer Bedrohung der Bundesrepublik Deutschland oder einer Gefährdung der Menschheit kann erst recht nicht die Rede sein.
Die Karlsruher Verfassungsrichter haben den Polizisten aber ein Hintertürchen offen gelassen:
Für das bloße Abhören von IP-Telefonaten sind die Hürden wesentlich geringer als für eine umfassende Online-Durchsuchung eines ganzen Computers. Zitat:

ZITATORIN:

(Für) eine staatliche Maßnahme ..., durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben ... werden, ist der Eingriff an Art. 10 Abs. 1 GG (Grundgesetz) zu messen.

SPRECHER:

Im Artikel 10 des Grundgesetzes geht es um das gute, alte „Post- und Fernmeldegeheimnis“. Den Bundesverfassungsrichtern ist es also juristisch egal, mit welchen Geräten die abgehörten Telefonate geführt werden: ob von einem alten Telefon mit Wählscheibe oder einem Computer mit einer Terabyte-Festplatte. Kein Wunder: Die Karlsruher Richter sind schließlich Juristen, keine Informatiker. Dass man aber in einen Computer zuerst einmal technisch einbrechen muss, um dort die „laufende Telekommunikation“ zu überwachen, kümmert sie nicht.
In Deutschland werden jährlich etwa 25.000 Abhörmaßnahmen richterlich genehmigt, wie mir der Verfassungsrechtler Ulf Buermeyer berichtet. Und

immer mehr Menschen führen ihre Gespräche mit Hilfe des Computers. Wie viele Quellen-TKÜ-Maßnahmen bisher insgesamt realisiert wurden, wird laut dem zuständigen Bundesamt für Justiz statistisch nicht erfasst. Buermeyer:

O-TON (Buermeyer):
Technisch betrachtet wird sowohl bei Online-Durchsuchung als bei der Quellen-TKÜ der Computer der Zielperson mit einem staatlichen Trojaner infiziert. D.h. also, der technische Vorgang ist genau derselbe. Die Quellen-TKÜ ist aber eine Online-Durchsuchung, die hinten ´rum ein wenig kastriert worden ist. Hinten ´rum deswegen, weil die Behörden nur bestimmte Daten tatsächlich verwenden dürfen. Diese Hintertür macht große Probleme aus rechtsstaatlicher Sicht: Die Ermittlungsbehörden halten sich, ich will gar nicht mal sagen mit böser Absicht, halten sich in der Praxis schlicht und ergreifend nicht an die Grenzen einer Quellen-TKÜ. Jedenfalls allzu oft.

SPRECHER:
Vielleicht hätte der Gesetzgeber diese Grenzen zuerst genauer definieren sollen, bevor überhaupt mit den Quellen-TKÜs begonnen wurde? Stattdessen scheint selbst aus Regierungssicht eine präzise Rechtsgrundlage bis heute zu fehlen. Oder wie ist die folgende Passage im aktuellen Koalitionsvertrag der Großen Koalition zu verstehen?

ZITATORIN:
Die Vorschriften über die Quellen-Telekommunikationsüberwachung werden wir rechtsstaatlich präzisieren, um unter anderem das Bundeskriminalamt bei seiner Aufgabenerfüllung zu unterstützen.

SPRECHER:
Die Hacker des Chaos Computer Clubs hatten den Landshuter Staatstrojaner enttarnt. Sie forderten interessierte Whistleblower auf, dem CCC weitere verdächtige Geräte zu schicken. Mit Erfolg: Bald kamen per Post erste

Festplatten an, andere wurden direkt in CCC-Büros übergeben. Prompt entdeckten die Hacker weitere Staatstrojaner. Mehr noch: Nach eigener Aussage fanden sie nun sogar in der Trojaner-Malware Aktenzeichen ermittelnder Behörden – und veröffentlichten erneut ihre Ergebnisse. Club-Sprecherin Constanze Kurz:

O-TON (Kurz):
Wir wollten also natürlich verhindern, dass gerade im Einsatz befindliche Trojaner der Öffentlichkeit bekannt werden. Wir haben vor der Veröffentlichung sozusagen durch einen befreundeten, freiheitsliebenden Politiker - das war Burkhard Hirsch - eine Vorwarnung rausgegeben. Wir haben gesagt: Naja, da kommt jetzt sozusagen am Sonntag was in der Zeitung und wäre vielleicht gut jetzt, diesen Server abzustellen, um damit die laufenden Verfahren, die mit derselben Software laufen, zu schützen. Aber das ist natürlich auch nicht erfolgt. Wir konnten also noch sehr lange Kontakt zu diesem Server aufbauen. Das heißt, die Behörden haben sich nicht in der Lage gesehen, innerhalb von zwei, drei Tagen Ihre Überwachungsinfrastruktur runterzufahren. Naja, peinlich. Peinlich wie vieles in diesem Staatstrojaner-Skandal.

ATMO:
Pförtnerin am Empfang des Reichstages, durch Kontrolle, hallige Atmo, Schritte

SPRECHER:
Der Innenpolitiker Hans-Peter Uhl von der CSU hat Staatstrojaner im Bundestag verteidigt. Im Dezember 2013 war er bereit, mir ein Interview zu geben. In der „Frankfurter Allgemeinen“ Zeitung hatte er im Sommer zuvor in einem Interview zum NSA-Skandal, also der weltweiten Ausspähung von Kommunikationsdaten durch US-Dienste, noch große Wissenslücken offenbart.

ZITATOR 1:

+ FAZ: Herr Uhl, der Bundesinnenminister und Sie haben die Bürger dazu aufgerufen, ihre elektronische Kommunikation zu verschlüsseln. Die Bürger dürften nicht auf den Schutz des Staats hoffen. Ist das eine Bankrotterklärung der Politik?

ZITATOR 2:

+ Uhl: Wir haben heute vom Bundesnachrichtendienst erfahren, wie Kommunikation durch Glasfaserkabel verläuft, wie die E-Mails geleitet werden. Es geht nicht um den kürzesten Weg, sondern allein nach finanziellen Gesichtspunkten. Wenn Sie innerhalb Deutschlands eine E-Mail verschicken, ist es durchaus denkbar, dass diese über die Vereinigten Staaten und wieder zurück läuft.

ZITATOR 1

+ FAZ: Das konnte man auch schon in der Zeitung lesen.

ZITATOR 2

+ Uhl: Für mich war das neu.

7 ATMO:

Geplauder, Abgang ins Restaurant des Bundestages

SPRECHER:

Wie kann Uhl an präziseren Gesetzen zur Quellen-Telekommunikationsüberwachung arbeiten, wenn ihm bereits dieses Basiswissen über Emails fehlt? Im Internet ist dazu leicht Unterrichtsmaterial für Schulen zu finden, auch für die Unterstufe. Trotzdem sah sich Uhl im vergangenen Dezember mir gegenüber noch unverdrossen in der Rolle eines Experten:

O-TON (Uhl):

So ins Detail brauchen wir ja gar nicht gehen. Der Hörer versteht diese Feinheiten ja doch nicht. Wie detailliert hätten Sie es denn gerne?

SPRECHER:

Uhl sitzt seit 1998 im Bundestag, ein gestandener Politiker und Jurist. Als Jahrgang 1944 gehört er allerdings nicht zu den Digital Natives, die mit Computern und Internet aufgewachsen sind. Von mir angesprochen auf seine Brandrede im Bundestag, in der er Deutschland vor den „Chaoten aus dem Computerclub“ warnte, sagte er.

O-TON (Uhl):

Wenn man frei formuliert, kann sowas mal passieren. Ich habe sagen wollen, dass in diesem Rechtsstaat Deutschland nicht Chaoten und Piraten regieren, sondern Beamte, die sich an Gesetz und Recht halten, aber eben nicht regieren. Und das habe ich etwas verunglückt formuliert und dann korrigiert. Darum geht es mir. Also wir sollten diese Schreckensmeldungen des Chaos Computer Clubs nicht alle für bare Münze nehmen.

SPRECHER:

Die „Schreckensmeldungen“ des Chaos Computer Clubs: Das sind vor allem deren „Staatstrojaner-Reporte“, in denen die Hacker penibel auflisten, was sie jeweils gefunden haben. Wie dachte Uhl rückblickend über den Landshuter Staatstrojaner?

O-TON (Uhl):

Es ging damals um die sehr interessante Frage: Wenn man den Quellcode einer zuarbeitenden Firma nicht kennt, muss man sich ja darauf verlassen, dass das, was sie sagen, stimmt. Weil man es ja nicht überprüfen kann. Nämlich sie sagen: Wir tun nur das, was wir dürfen, obwohl wir vielleicht mehr könnten. Und dann sind wir im Glaubensbereich. Das ist nicht gut.

SPRECHER:

Diesem unguten Glauben der verantwortlichen Politiker hatte der Chaos Computer Club seine Analysen entgegengesetzt. Die Hacker hatten auch die angesprochene „zuarbeitende Firma“ ermittelt: die Digitask GmbH aus Hessen, die den Staatstrojaner entwickelt und dann an deutsche Behörden verkauft hatte. Ein Interview zu ihrem Trojaner lehnt Digitask allerdings ab.

ZITATORIN:

„Bitte haben Sie Verständnis, dass wir ... keine Möglichkeit für ein Hörfunk-Interview sehen“

SPRECHER:

Der Innenausschuss des Deutschen Bundestages lud 2011 den Präsidenten des Bundeskriminalamtes ein: Jörg Ziercke sollte erzählen, was seine Staatstrojaner so alles leisten können. In dessen Bericht hieß es:

ZITATOR 1:

Die durch den Chaos Computer Club analysierte Quellen-TKÜ-Software bezieht sich ... auf eine ca. drei Jahre alte Version der Software, die das BKA nicht eingesetzt hat.

SPRECHER:

Und weiter :

ZITATOR 1:

Seit der Veröffentlichung der Signatur der Verschlüsselung durch den CCC könnten noch laufende Maßnahmen entdeckt werden. Das BKA hat daher in einem aktuellen Verfahren der organisierten Rauschgiftkriminalität die Maßnahme sofort abgebrochen und dies der Staatsanwaltschaft und dem anordnenden Gericht mitgeteilt.

SPRECHER:

All dies wegen einer drei Jahre alten Software, die das BKA angeblich gar „nicht eingesetzt hat“? Zierckes Bericht gipfelt in einer klaren Aussage über den eingesetzten Staatstrojaner:

ZITATOR 1:

Dritte können nicht widerrechtlich eindringen und durch eine Hintertür evtl. eigene Dateninhalte platzieren.

ATMO:

Der CCC analysiert den Staatstrojaner (Chaos Computer Club) – liegt vor

SPRECHER:

Dabei hatte der CCC zu diesem Zeitpunkt bereits einen Videoclip im Internet veröffentlicht – laut „Youtube“ bereits zehn Tage vor Zierckes Vortrag: In dem bis heute frei zugänglichen Clip dokumentieren die Hacker in einzelnen Schritten, wie sie den Staatstrojaner des BKA schrittweise übernommen hatten – also einen klaren „Zugriff Dritter“. Ein Hacker sitzt mit dem Rücken zur Kamera und klickt munter vor sich hin.

O-TON (Chaos Computer Club):

(Video) ... Auch zu dem Anfertigen von Bildschirmfotos. Schlimmer noch: Der Trojaner kann sogar beliebige Software auf den infizierten PC hochladen und dort ausführen. Hier wird gezeigt, wie mit einem selbst programmierten Steuerprogramm über den Trojaner jede Webbrowser-Seite mit gelesen werden kann. Mikrofon und Kamera des infizierten Rechners können beispielsweise durch ein nachträglich hoch geladenes Programm für einen großen Lauschangriff gestartet werden.

(Video im Hintergrund weiter laufen lassen)

SPRECHER:

Die Club-Hacker haben dem Staatstrojaner einen eigenen Server übergestülpt: also eine Software, die mit der Staatstrojaner-Software kommunizieren kann. In dem Videoclip nutzen sie den Trojaner nun nach eigenem Gutdünken. Constanze Kurz ist bis heute stolz auf die selbst gebastelte Kommandozentrale.

O-TON (Kurz):

Ziel dieser ganzen Analyse war natürlich auch, einen eigenen so genannten command and controll-Server zu bauen. Also selbst sozusagen die Befehle an diese Software zu geben. Und damit auch zu prüfen, ob Dritte, nämlich wir oder auch andere Dritte, Befehle an diese Software senden können. Also das hat ungefähr einen Tag gedauert, bis wir selbst so einen command and controll-Server bauen konnten.

SPRECHER:

Als ich das Bundeskriminalamt um eine Stellungnahme bitte, räumt die Pressestelle ein, dass „das Aussetzen von Quellen-TKÜ-Maßnahmen ... im Zusammenhang (steht) mit den Veröffentlichungen des CCC“.

ATMO:

Mit dem Zug unterwegs in Berlin

SPRECHER:

Noch in Berlin erhalte ich von Dritten ein Dokument mit dem Stempel „VS – nur für den Dienstgebrauch“. Darin informiert das Bundes-Innenministerium einen Bundestags-Ausschuss über die Bemühungen des Bundeskriminalamtes, einen hauseigenen Staatstrojaner zu entwickeln. Dazu ist laut diesem Bericht seit Sommer 2012 ein „Kompetenzzentrum Informationstechnische Überwachung“, kurz ITÜ, eingerichtet worden. In dem Dokument über das ITÜ wird auch die ...

ZITATORIN:

... Marktsichtung von kommerziellen Quellen-TKÜ-Lösungen ... für die Durchführung von Maßnahmen für den Zeitraum bis zur Bereitstellung der BKA-Eigenentwicklung...

SPRECHER:

... angesprochen. Auf Deutsch: Bevor der BKA-eigene Trojaner endlich fertig wird, wollte das Bundeskriminalamt nach dem Digitask-Desaster einen besseren Privat-Trojaner einkaufen und gegebenenfalls auch einsetzen. Bei der Suche nach diesem Produkt half eine „Standardisierte Leistungsbeschreibung“:

ZITATORIN:

Hersteller und Anbieter von Software zur Quellen-TKÜ sind sorgfältig im Hinblick auf ihre Fachkompetenz und Vertrauenswürdigkeit auszuwählen.

SPRECHER:

Am Ende heißt es in dem Dokument des Bundesinnenministeriums, dass bereits ein Trojaner-Produzent gefunden worden sei:

ZITATORIN:

Das BKA hat für den Fall eines erforderlichen Einsatzes ein kommerzielles Produkt der Firma Elaman/Gamma beschafft.

SPRECHER:

Ein Reporter-Déjà-vu. Die Firma Elaman/Gamma und deren Überwachungs-Software kenne ich bereits von einer anderen Recherche: Dabei ging es um die vom Staat angeordnete Überwachung missliebiger Oppositioneller in Bahrain - einem arabischen „Königreich“, dessen Herrschern seit langem Menschenrechtsverletzungen vorgeworfen werden.

ATMO:

in der Londoner U-Bahn, Stimmengewirr

SPRECHER:

2013 war ich deswegen nach England gereist, um Oppositionelle aus Bahrain zu treffen. Sie waren nach eigenen Angaben von arabischen Geheimpolizisten erst ausspioniert, dann einige von ihnen auch entführt und gefoltert worden. Die Geheimdienste hatten dabei offensichtlich ebenfalls einen Trojaner der Firma Elaman/Gamma benutzt. Eines der bahrainischen Opfer hatte sein Handy an die Nichtregierungsorganisation „Privacy International" in London übergeben. Deren Head of Research, Eric King, hatte den Mini-Computer untersucht und anscheinend einen Trojaner der Firma Elaman/Gamma gefunden:

O-TON (King):

Trojan that hacks their computer ... every single night.

ZITATOR 3:

Der Trojaner kann Emails lesen, den Kalender anschauen, aber noch viel mehr: zum Beispiel die getippten Tasten protokollieren und auf diese Weise verschlüsselte Passwörter ermitteln. Der Trojaner kann auch sämtliche Sicherheits-Software umgehen, deine Kamera anschalten, Fotos und Videos aufnehmen. Aus der Ferne kann das Telefon-Mikro angeschaltet werden. Dann trägst du ahnungslos eine Abhör-Wanze mit dir herum und lädst deren Akku auch noch jede Nacht selbst neu auf.

SPRECHER:

Die Gamma Group sitzt hundert Kilometer westlich von London, deren deutsche Partnergesellschaft, die Elaman GmbH, in München. Das Duo Elaman/Gamma nannte seine Staatstrojaner-Software „Finfisher", manchmal auch „Finspy". Heute wird „Finfisher" auf einer eigenen Website

als Software zur „offensiven IT-Intrusion“ beworben, also als Software für den „offensiven Einbruch in Informationstechnik“. Angeblich wird Finfisher aber nur an seriöse „Strafverfolgungsbehörden und Geheimdienste“ geliefert, um „Schwerverbrecher zu identifizieren, zu finden und zu verurteilen“, wie es auf der Website heißt. Doch damit scheinen die Verkäufer auch zum Beispiel die Behörden und Dienste in Bahrain zu meinen, die bedenkenlos schwere Waffen gegen Demonstranten einsetzen.

ATMO:

Unruhen in Bahrain

SPRECHER:

Privacy International und das renommierte Citizenlab der Universität von Toronto waren wochenlang beschäftigt gewesen, den Trojaner im Smartphone der Bahrainer Aktivistin zu knacken. Dortige Dienste hatten Betroffenen zuerst eine Mail mit Anhang gesendet – mit einer Absender-Kennung, die auf einen bekannten Oppositionellen hinzuweisen schien. Die Aktivistin öffnete den Anhang und verlor damit unbemerkt die Kontrolle über ihr Smartphone:
Im Labor stießen King und seine Kollegen im „Gedächtnis“ des Smartphones, dem „memory dump“, auf die Signatur von Elaman/Gamma, den Begriff „Finspy“ sowie die Internet-Domain gamma-international.de.
Diese Domain gehörte damals laut dem internationalen Standardverzeichnis für Webseiten, DomainTools, einer Münchener „Organisation“ namens Gamma International GmbH und einer Person namens „Martin Muench“, auf die ich später noch einmal stoßen werde. Im fernen Bahrain war mittlerweile nach Angaben der Aktivistin deren Ehemann gekidnappt und zehn Monate lang in einem Gefängnis gefoltert worden.

Die Häscher hatten sich auf Erkenntnisse aus Smartphones berufen, dank Gamma und Finfisher.

Bei der Internet-Recherche fällt jetzt auf: Inzwischen gibt es eine eigene Website einer „Finfisher GmbH“, mit angeblich „über 40 Angestellten“ und Firmensitz in München. Die Finfisher GmbH sei heute „unabhängig“ organisiert und „eigenständig finanziert“, heißt es dort. Offensichtlich wurde das Produkt Finfisher in ein neu geschaffenes Unternehmen ausgegliedert. Gamma und Elaman reagieren ebenso wenig auf meine schriftlichen Interviewanfragen wie die inzwischen eigenständige Finfisher GmbH. Das war schon damals nach meiner Recherche in London so gewesen: Schon seit Juni 2013 hatten der Westdeutsche Rundfunk und ich mehrfach um Stellungnahmen und Interviews gebeten. Nun fahre ich also noch einmal nach Großbritannien. Denn in Farnborough nahe London findet Mitte März 2014 die Messe „Security & Policing“ für Sicherheits-Technologien statt, die vom britischen Innenministerium veranstaltet wird. Ich besuche den Stand der Gammagroup, um die Mitarbeiter auf Finfisher anzusprechen.

O-TON (Autor/Gamma):

Excuse me, are you with gamma? – Are you recording me? – Iif you allow so. – are you press, media? – Public German radio, ARD – ok – So what kind of tools you concentrate on? –I am trying to find the guy who does – (employee:) I can brief here. The digital forensic is for retrieving information from damaged hard drives. So it is mainly for industries which have had problems with their service and such. So it is for the retrieval of just damaged areas of companies' hard drives.

Sprecher: Entschuldigung, Sie arbeiten für Gamma?

Zitator 1 (männl.): Nehmen Sie mich gerade auf?

Sprecher: Wenn Sie es erlauben. –

Zitator 1: Sind Sie von der Presse?

Sprecher: Dem öffentlichen Deutschen Radio, ARD.

Zitator 1: OK.

Sprecher: Welche Produkte bieten Sie hauptsächlich an? –

Zitator 1:
Ich suche mal meinen Angestellten ... -

Zitator 2:
Ich kann Sie briefen: Bei der digitalen Forensik werden Informationen von beschädigten Festplatten wiederhergestellt. Da geht es vor allem um Industrien, die deswegen Probleme beim Service hatten. Es geht also nur um die Wiederherstellung beschädigter Teile von Unternehmens-Festplatten.

SPRECHER:
Gamma - ein oller Reparaturbetrieb für kaputte Festplatten? Doch ich habe ja selbst im Internet festgestellt, dass für Finfisher anscheinend eine eigene GmbH in München gegründet worden ist.

O-TON (Autor/Gamma):
In Germany the federal police and the state police they bought a software called Finfisher which is related to supervising mobile phones. – No, I do not have any information about that at all. You have to ask the company that manufactures Finfisher. – What company is it? – It is called Finfisher gmbh. It is a completely new company. Gamma has no involvement in Finfisher at all. None. - But it has had connections to Finfisher. – Yes, we developed the project originally and then we decided to (pause) distance ourselves from it. – That was when? – October last year! – October last year? - But what was the main reason for distancing yourself from Finfisher? – I don't want an

involvement basically because of media- and press intrusion into our business and our personal lives. – So what kind of intrusion was this? – Much like what you are doing right now. – But probably some other people may feel intruded by Finfisher. – oh no, I would not think so. I would not think so at all. – Last time I have been to London I met a Bahraini activist, a woman. – Oh I am not interested in your conversations. –Wikileaks published some brochures with offers from gamma to the turkmenistan government and public telecom company. – Your information is incorrect. - But generally do you sometimes understand that people themselves feel intruded without being criminals. – No, I don't. You want me to go and get the authorities? Because I will! – You will get the authorities? – I ask you to leave and stop talking to me. Please. Up to you. – I will think it´s over. –

Sprecher:
In Deutschland haben die Bundespolizei und Landeskriminalämter eine Software namens Finfisher gekauft, die Handys überwacht.

Zitator 2:
Darüber habe ich keine Informationen. Da müssen Sie das Unternehmen fragen, dass Finfisher herstellt.

Sprecher:
Welches Unternehmen ist das?

Zitator 2:
Es heißt Finfisher GmbH. Ein komplett neues Unternehmen. Gamma hat keine Beteiligung an Finfisher. Gar keine.

Sprecher:
Aber Gamma war früher beteiligt.

Zitator 2:

Ja, wir haben das Projekt ursprünglich entwickelt und dann später entschieden, uns davon zu (Pause) distanzieren.

Sprecher:

Wann war das?

Zitator 2:

Letztes Jahr im Oktober.

Sprecher:

Und was war Ihr Grund, sich zu distanzieren?

Zitator 2:

Ich wollte nicht mehr, weil die Medien und die Presse in unser Geschäftsleben und unser Privatleben eindrangen.

Sprecher:

Was war das für ein Eindringen?

Zitator 2:

Na so wie Sie das gerade machen.

Sprecher:

Aber vielleicht fühlen andere Leute, dass Finfisher in ihr Leben eingedrungen ist.

Zitator 2:

Oh nein, das denke ich aber gar nicht.

Sprecher:

Als ich das letzte Mal in London war, traf ich eine Aktivistin aus Bahrain ...

Zitator 2:

Mich interessiert nicht, was Sie sagen.

Sprecher:

Wikileaks hat Unterlagen veröffentlicht, in denen Gamma der turkmenischen öffentlichen Telekom-Gesellschaft Angebote machte ...

Zitator 2:

Ihre Informationen sind inkorrekt.

Sprecher:

Aber verstehen Sie generell, dass sich Leute von Finfisher bedrängt fühlen, die keine Kriminellen sind?

Zitator 2:

Nein, tu ich nicht. Wollen Sie, dass ich die Aufsicht hole? Ich mach‘ das!

Sprecher:

Die Aufsicht?

Zitator 2:

Ich fordere Sie auf, zu gehen und nicht mehr länger mit mir zu sprechen. Bitte. Liegt an Ihnen.

SPRECHER:

Als ich mich etwas zurückziehe, alarmiert der Gamma-Mann den Veranstalter: das britische Innenministerium. Zügig erscheinen zwei

stämmige Herren in Warnwesten und eine elegant gekleidete Dame vom „Home Office“.

ATMO:

I got an accreditation 3 weeks ago. – no, no, I understand, yes. –ich: any problem? – We sort it out for you, Sir. Ich: maybe it is related to this gentleman over there? – I do not know sir! you are not recording, are you?

ATMO:

Messelärm, v.a. Stimmengewirr

SPRECHER:

Ich sei der einzige Journalist, dem jemals zu dieser jährlichen Messe Zutritt gewährt worden wäre, meint die Dame – und dass dies ein Versehen gewesen sei. Und nun wolle ich das Innenministerium doch bestimmt nicht in Verlegenheit bringen, vermutet Lynne Head – so steht es auf ihrem Namensschild. Wir könnten mein Interview mit Gamma doch mal gemeinsam anhören, und ich es solle es keinesfalls ohne Abstimmung veröffentlichen. Derweil schaut der Gamma-Mann aus fünf Metern Abstand böse herüber und die beiden stämmigen Herren starren auf mein Aufnahmegerät. Erst nach einer Stunde Verhör kann ich gehen – mein Material habe ich nicht herausgerückt.

Vor dem Abflug gehe ich in London noch einmal zu Privacy International. Haben die Bürgerrechtler herausgefunden, warum Gamma seinen Verkaufsschlager Finfisher ausgegliedert hat? Dort berichtet Eric King, dass mittlerweile die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, OECD, zu Finfisher ermittelt: wegen möglicher Verstöße gegen internationale Menschenrechtsstandards und damit gegen OECD-Leitsätze. Eric King:

O-TON (King):

The complaint we filed with the OECD was accepted in which they said that there were grounds to look into this further and to investigate it. We have been in mediation with gamma for the last 4, 5 month. These are confidential so I am afraid there is nothing that I can really say within that process. Other then that we expect a decision to be made by the national contact point within the OECD within the next few months.

ZITATOR 3:

Die OECD hat unsere Beschwerde angenommen und gesagt, dass es Gründe für eine weitere Untersuchung gäbe. Seit vier, fünf Monaten sind wir in einem Mediationsverfahren mit Gamma – ein vertraulicher Prozess, zu dem ich nichts sagen kann, solange er andauert. Außer, dass wir in den kommenden Monaten eine Entscheidung der OECD erwarten.

SPRECHER:

Also gliederte die Gammagroup ihr Produkt Finfisher im selben Zeitraum aus, in dem das Unternehmen auf Druck der OECD das Mediationsverfahren mit Privacy International beginnen musste.

O-TON (King):

I believe that Finfisher has now been found in 35 countries around the world. In Malaysia it was used in the run up to elections. In Indonesia it was used to target some human rights defenders and in Ethiopia it was sent out as part of a mailing to a number of people who were part of the political opposition.

ZITATOR 3:

Ich gehe davon aus, dass Finfisher mittlerweile in 35 Ländern gefunden wurde: unter anderem in Malaysia vor den letzten Wahlen, in Indonesien gegen Menschenrechts-Aktivisten und in Äthiopien gegen die politische Opposition.

ATMO:

am Hbf in Berlin

SPRECHER:

Wer entwickelt solche Software, die auch in autoritären Staaten eingesetzt wird, um Oppositionelle auszuspionieren? Wieder zurück in Deutschland erinnere ich mich an ein Video-Interview mit der CCC-Sprecherin Constanze Kurz bei Golem.de, einem Dienst für IT-Nachrichten. Dort sagte sie:

O-TON (Kurz):

Wir haben auch durchaus Interesse zum Beispiel an ehemaligen Programmierern solcher Schadsoftware für den behördlichen Bereich: da durchaus auch mal in ein Gespräch zu kommen.

SPRECHER:

Hat sich da vielleicht zwischenzeitlich etwas getan? Hat der Chaos Computer Club nun auch einen Trojaner-Programmierer geknackt? Constanze Kurz klingt aufgeschlossen, als ich sie darauf anspreche:

O-TON (Kurz):

Es gibt natürlich auch Aussteiger aus dieser Szene, klar. Oder die sich irgendwann unwohl fühlen mit den Tools, die sie bauen. Oder vielleicht wo die Käufer sich verändern: Vielleicht findet man es ja als Programmierer noch OK, so etwas für den deutschen Staat zu bauen. Aber vielleicht nicht für syrische Folterkeller.

ATMO:

ins Steakhaus

SPRECHER:

Nun hat die CCC-Sprecherin ein Treffen zu Dritt arrangiert: Sie will einen Programmierer vorstellen, der Finfisher mit entwickelt haben soll.
In einem Steakhaus am Berliner S-Bahnhof Friedrichstraße stellt mir Constanze Kurz den Informatiker vor, dessen Programmierkünste sogar sie selbst zu beeindrucken scheinen.

ATMO:

Fortsetzung

SPRECHER:

Es ist ein junger Mann in Szene-Klamotten: schwarze Jeans, schwarzes Sweat-Shirt, schwarze, lange Haarlocken, mit einer Nerd-Figur, die auf ausgedehnte Computer-Sitzungen hinzuweisen scheint. Der Mann wirkt wie ausgeschnitten aus einem Foto von einem der berühmten CCC-Kongresse – obwohl sich dort doch eigentlich die Gegner von Staatstrojanern versammeln.

ATMO:

in Berlin unterwegs

SPRECHER:

Ich soll ihn „Simon“ nennen. Für das Interview verlassen wir unseren Treffpunkt und gehen in Richtung der Berliner Filiale des Chaos Computer Clubs.

ATMO:

im CCC-Lokal

SPRECHER:

Dort angekommen, öffnet Simon mit einem eigenen Schlüssel die Eingangstür des CCC-Treffs, und wir betreten gemeinsam den leeren Raum. Der Finfisher-Programmierer Simon sieht sich durchaus in der Tradition der CCC-Hackerszene und damit hier zu Hause. Weil er bei seinen damaligen Auftraggebern Verschwiegenheitsklauseln unterschreiben musste, kann Simon nur anonymisiert berichten. Deshalb werden seine Statements hier wortgenau von einem Schauspieler nachgesprochen. Inzwischen ist er IT-Berater in Sachen Sicherheitslücken. Ein gutes Geschäft, versichert Simon:

O-TON / ZITATOR 4:

Ein typischer Fall ist halt, dass eine Firma ankommt und sagt: Wir haben hier einen Server im Internet stehen oder wir haben ein ganzes Netzwerk, was ans Internet angebunden ist. Und Sie tun jetzt einmal so, als wenn Sie ein bösartiger Hacker sind. Können Sie in diese Systeme eindringen? Dabei gibt es natürlich auch einen Dual Use-Aspekt.

SPRECHER:

Deswegen prüft Simon mittlerweile ganz genau, ob seine Auftraggeber auch wirklich die Betreiber eines schützenswerten Servers sind - und nicht in Wirklichkeit die Bösewichte, die genau diesen Server hacken möchten. Denn damit hat Simon in der Vergangenheit schlechte Erfahrungen gemacht.

O-TON / ZITATOR 4

Naja, es hat ja niemand verlangt, die Seite zu wechseln. Das ist ja das Gemeine an der ganzen Geschichte: dass es sich eben um einen alten Bekannten handelt aus einem Freundeskreis der vergangenen Jahre: Martin Münch - derjenige, der diese Gamma Deutschland quasi mit gegründet hat. Die Firma Gamma Deutschland hat halt zu dieser Zeit niemand mit irgendwelchen bösen oder schädlichen Sachen in Verbindung gebracht. Der fragte halt nach, ob wir nicht Lust hätten, an einer

Machbarkeitsanalyse mitzuarbeiten. So rutschte man im Endeffekt in so ein Projekt hinein, was anfangs sehr harmlos klang.

SPRECHER:

Noch im vergangenen Jahr war Martin Münch der Gamma-Chef in Deutschland. Als ihn Journalisten am Münchner Gamma-Firmensitz besuchten, verglich er Finfisher mit der Fernsehsendung „Deutschland sucht den Superstar“:
Beides fänden zwar viele Menschen „Scheiße“, aber beides sei deshalb noch lange nicht verboten. Über Gammas Kunden wollte Münch nicht sprechen.
Als ich bei meiner jetzigen Recherche noch einmal bei der neuen Finfisher GmbH in München anrufe, erklärt mir eine Mitarbeiterin, dass Martin Münch „gar nicht mehr im Hause“ sei. Als er noch bei Gamma arbeitete, hatte Simon noch für Münch einen virtuellen Allzweck-Dietrich programmiert, und das laut eigener Aussage unwissentlich.

O-TON / ZITATOR 4:

Da geht es also um den Zugriff auf den Speicher von Computern über externe Schnittstellen wie FireWire. FireWire ist ja eine recht gängige Schnittstelle, an die man Festplatten, Kameras usw. anschließen kann. Diese Schnittstelle hat einen architekturbedingten Nachteil: dass man nämlich über diese Schnittstelle auf sehr sensible Bereiche in einem Computer zugreifen kann. Über FireWire kann man zugreifen, wenn der Computer zum Beispiel gesperrt ist.
D.h., wenn der Screensaver an ist und man sich eigentlich (noch) nicht mit einem Benutzernamen und einem Passwort anmelden muss. Dieses Werkzeug ist so etwas wie ein Generalschlüssel für alle Türen. D.h., wir haben einen Generalschlüssel gebaut für die meisten Computer, wie sie halt so herum getragen werden und herumstehen.

SPRECHER:

Mit diesem „Generalschlüssel“ wurde auch der weltweit führende Staatstrojaner Finfisher ausgestattet, sagt Simon. Das Unternehmen schweigt dazu.
Dabei hatte Simon gemeint, für eine gute Sache zu arbeiten: dass er hilft, Abwehrmechanismen gegen Eindringlinge zu entwickeln. Aber dann veröffentlicht ab dem Jahr 2011 die Enthüllungsplattform Wikileaks immer mehr interne Firmen-Unterlagen der Finfisher-Anbieter.
Projekt-Angebote richteten sich auch an Geschäftspartner wie die Telekom-Gesellschaft von Turkmenistan – laut Human Rights Watch eines der repressivsten Länder der Welt.
Simon überlegte noch, wie er auf diese Enthüllungen reagieren sollte – da wurde er aus heiterem Himmel von der Defense Advanced Research Projects Agency auf eine Mitarbeit angesprochen: Die DARPA entwickelt neue Waffentechnologien für das US-Militär und sah ihn offensichtlich als geeigneten Mitarbeiter an. Simon rekapitulierte die Fakten und erkannte, was er angerichtet hatte: dass er keineswegs Verfolgten geholfen hatte, sondern den Verfolgern. Er stieg aus, ging zum Chaos Computer Club und kehrte damit zu seinen Wurzeln zurück. Heute berät er freiberuflich zivile Unternehmen, wie sie sich gegen Trojaner aller Art schützen können.

Zu den Finfisher-Kunden gehört jetzt auch das deutsche Bundeskriminalamt, das den eingekauften Trojaner sicher gerne benutzen würde. Dazu muss er aber der eigenen „Standardisierten Leistungsbeschreibung“ entsprechen.
Dabei hatte das Bundes-Innenministerium in seiner geleakten Verschlusssache bereits dem Deutschen Bundestag beichten müssen:

ZITATORIN:

Die Prüfung des Quellcodes auf Übereinstimmung mit den Vorgaben der Standardisierten Leistungsbeschreibung und grundsätzlicher Aspekte der IT-

Sicherheit kann ... nicht geleistet werden. Deswegen wurde die Quellcodeprüfung an ... (die) CSC Deutschland Solutions GmbH vergeben.

SPRECHER:

Nun prüft also, stellvertretend für die Bundespolizei, die eine private GmbH den bei einer anderen privaten GmbH eingekauften Staatstrojaner. Die prüfende CSC GmbH und ihre Tochtergesellschaften haben allerdings mittlerweile noch ganz andere Schlagzeilen gemacht: Denn der nach eigenen Angaben „weltweit führende Anbieter für IT-gestützte Businesslösungen und Dienstleistungen“ charterte Flugzeuge für den amerikanischen Geheimdienst CIA.
Damit flog die CIA Menschen zwischen Folter-Gefängnissen hin und her.
Eines der Opfer: der Deutsche Khaled al Masri. Dazu verweigert das Bundeskriminalamt explizit ein Interview und schickt stattdessen eine Stellungnahme. Darin heißt es:

ZITATORIN:

Die Vorwürfe gegen die CSC Deutschland Solutions GmbH sind dem BKA bekannt. ... Des Weiteren lagen der Bundesregierung weder Anhaltspunkte dafür vor, dass die CSC Deutschland Solutions GmbH in irgendeiner Weise gegen Sicherheits- oder Vertraulichkeitsauflagen verstoßen hat, noch für Unzuverlässigkeiten im vergaberechtlichen Sinne. Zu Vertragsinhalten äußern wir uns nicht. ...Bis zur Verfügbarkeit einer den verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts genügenden Software führt das BKA keine Quellen-TKÜ-Maßnahmen durch. Es wurde ein Zwischenprodukt der Firma (Elaman)/Gamma beschafft ...

SPRECHER:

Immerhin dokumentieren die BKA-Angaben, dass Finfisher also zumindest bis heute nicht den verfassungsrechtlichen Vorgaben in Deutschland genügt.

Allerdings hat das Amt für Finfisher bereits mindestens 150.000 Euro an die Hersteller eben dieser Software bezahlt, und das nur „für zwölf Monate mit der Option zur Verlängerung um weitere zwölf Monate“, wie der Bundes-Parlamentarier Peter Danckert in einer erst vertraulichen, dann aber freigegebenen Anfrage an das Bundesinnenministerium erfuhr.
Ist den deutschen Kriminalbeamten die Gesellschaft der anderen Finfisher-Kunden genehm? Wird es dem BKA irgendwann gelingen, einen eigenen Staatstrojaner zu entwickeln? Werden die Bundespolizisten dann auf legale Weise in Computer und Smartphones von Verdächtigen eindringen? Mit Hilfe eines „präziseren“ Gesetzes, falls der Bundestag bis dahin eines verabschiedet haben sollte? Aber selbst wenn dies alles erreicht werden kann, bleibt ein grundsätzliches Problem. Auf das hatte mich der Verfassungsrechtler Ulf Buermeyer schon bei der Recherche zur Überwachung des Landshuter Kaufmanns angesprochen:

O-TON (Buermeyer):
So sehr sich die meisten Beamten darum bemühen, nach Recht und Gesetz zu handeln: Mitunter geht aber auch der Jagdtrieb mit ihnen durch und der Landshuter Fall ist, finde ich, ein sehr eindrucksvolles Beispiel dafür, wie die Grenzen des Grundgesetzes dann im Eifer des Gefechts schnell mal aus dem Blick geraten.

SPRECHER:
Und „Simon“, der Finfisher-Programmierer wider Willen, meint zum Abschied:

O-TON / ZITATOR 4:
Ein häufiges Argument ist: Naja, die Polizei hat ja auch Schusswaffen. Aber sie rennt nicht herum und erschießt einfach irgendwelche Leute. Der Unterschied ist aber: Wenn ein Polizeibeamter seine Waffe abgibt, dann fällt es auf, wenn eine Kugel fehlt. Wenn man aber solch eine digitale Waffe

einsetzt, dann fehlt da nicht am Ende irgendwo ein Bit. So dass es nicht wirklich sinnvoll möglich ist, die Überwacher zu überwachen.

Absage:

Der Staat und seine Trojaner

Feature von Achim Nuhr

Es sprachen: Udo Schenk, Hanns Jörg Krumpholz, Gergana Muskalla, Sascha Nathan, Reinhard von Stolzmann, Aart Veder.

Technische Realisation: André Bouchareb

Regie: Helge Heynold

Redaktion: Dorothee Meyer-Kahrweg

Eine Produktion des Hessischen Rundfunks für das ARD radiofeature 2014.