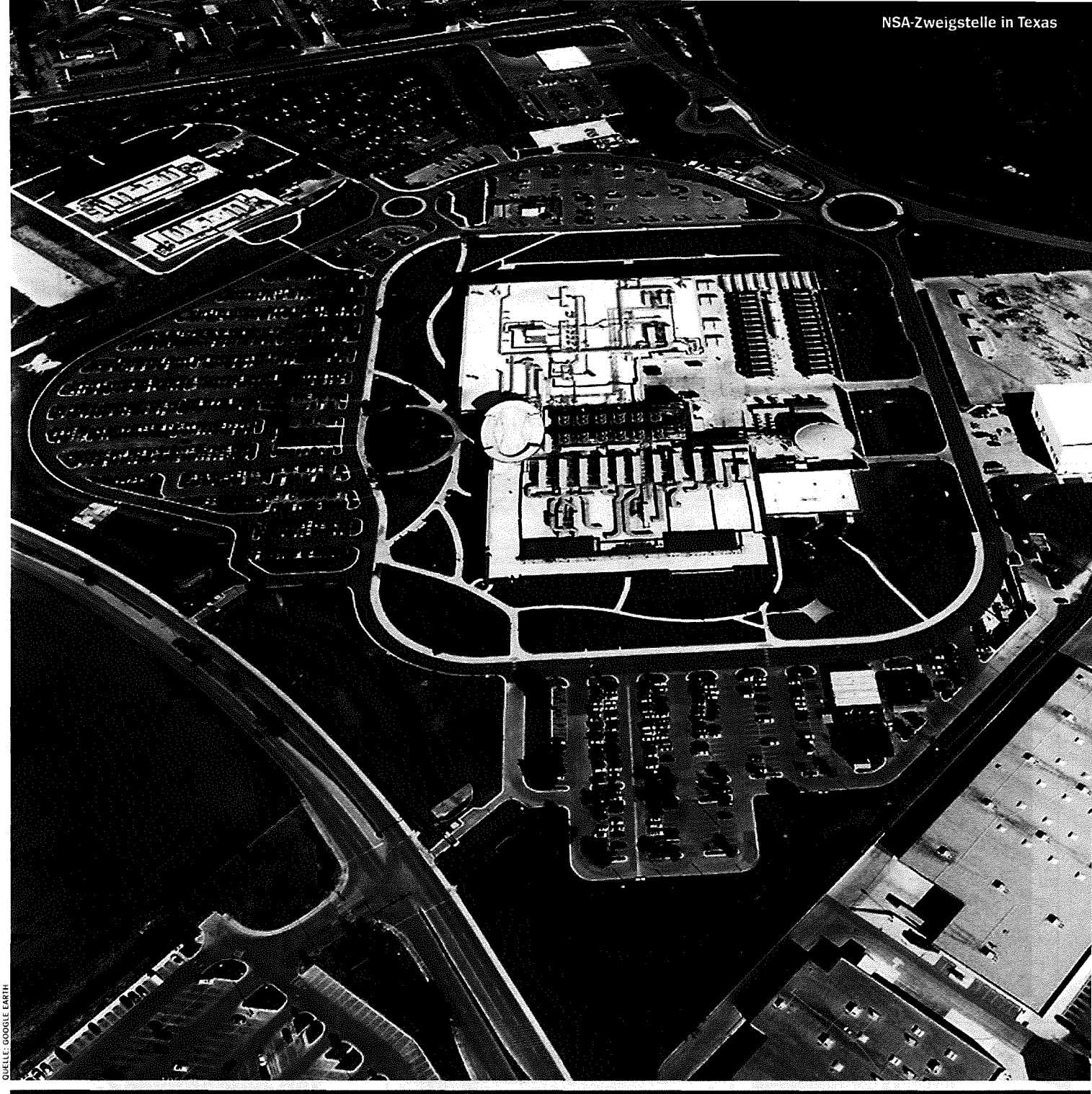


NSA-Zweigstelle in Texas

QUELLE: GOOGLE EARTH

NSA

Die Klempner aus San Antonio

Sie wird gerufen, wenn der normale Zugang versperrt ist: Die Hacker-Einheit TAO gilt als Wunderwaffe der NSA. Sie unterhält ein eigenes Schattennetz, infiltriert Rechner weltweit und fischt sogar Geräte aus der Post, um deren Platinen zu manipulieren.

Es war im Januar vor vier Jahren im texanischen San Antonio: Zahlreiche Hausbesitzer standen da plötzlich in ihren Vorgärten vor verschlossenen Garagen. Sie wollten zur Arbeit oder zum Einkaufen fahren, doch die Fernbedienungen für die Garagentore waren tot. So sehr sie auch auf ihnen herumdrückten, die Tore bewegten sich keinen Millimeter. Betroffen waren vor allem Anwohner im Westen der Stadt, rund um den Military Drive.

Im Auto- und Pendlerland USA war die mysteriöse Garagentorblockade bald ein Thema für die Kommunalpolitik. Der Bezirksverwaltung gelang es schließlich, das Rätsel zu lösen. Für den Fehler mit den Fernbedienungen war ein Nachrichtendienst der Vereinigten Staaten verantwortlich, die National Security Agency (NSA), die in San Antonio einen Standort unterhält. Die NSA musste einräumen, dass eine ihrer Antennen auf derselben Frequenz sendet wie die Fernbedienungen der Garagen. Die Geheimdienstler versprachen Abhilfe, die Tore ließen sich bald wieder öffnen.

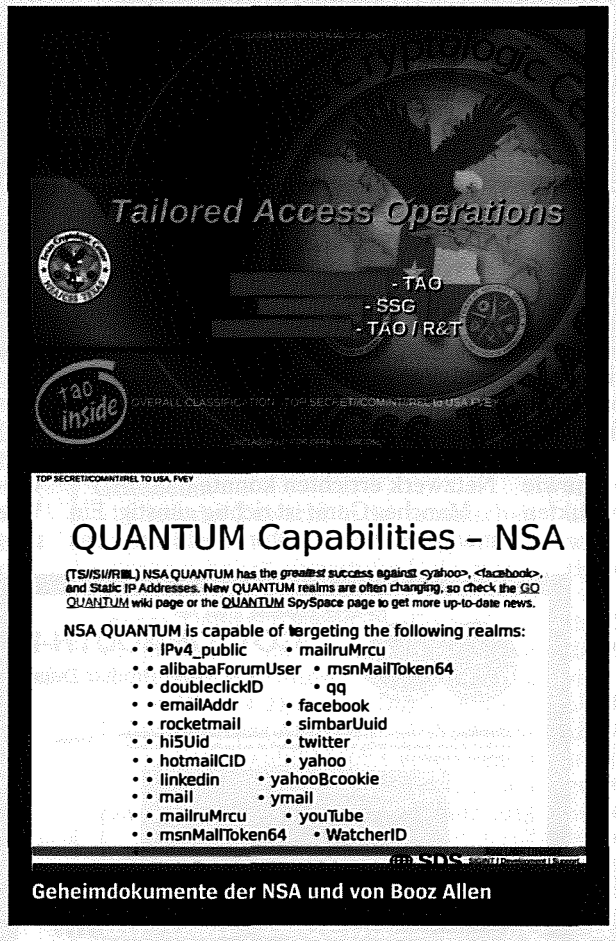
Aber die Episode machte den Texanern bewusst, wie sehr die Arbeit des Geheimdienstes inzwischen in ihren Alltag hineinragt. Auf der Lackland Air Force Base von San Antonio arbeiten schon seit langem rund 2000 NSA-Mitarbeiter. Im Jahr 2005 übernahm der Geheimdienst noch dazu eine stillgelegte Sony-Chipfabrik im Westen der Stadt und investierte 30,5 Millionen Dollar in ihren Ausbau. Auf dem gewaltigen Areal mit zwei rechteckigen Gebäuden, verbunden durch ein metallenes Oval, wurde danach aufwendig umgebaut. Die Übernahme des Gebäudes durch die NSA war Teil jener atemberaubenden Expansion der Behörde, die dem 11. September 2001 folgte.

In einem der beiden Hauptgebäude residiert seither eine Eliteeinheit der NSA, die von diesem Ausbau profitierte und in den vergangenen Jahren so schnell wie kaum eine andere wuchs: das Büro für maßgeschneiderte Operationen, „Office of Tailored Access Operations“, kurz TAO. Es ist die operative Speerspitze der NSA, eine Art Klempnertruppe, die gerufen wird, wenn der normale Zugang zu einem Ziel versperrt ist.

Laut internen NSA-Dokumenten, die der SPIEGEL einsehen konnte, sind die Klempner vom Dienst bei vielen heiklen Operationen der amerikanischen Dienste beteiligt. Das Einsatzgebiet der TAO-Spezialisten reicht vom Anti-Terror-Kampf über Cyberattacken bis hin zur klassischen Spionage. Die Dokumente belegen auch, welch umfangreichen Werkzeugkasten sich die TAO zugelegt hat. Und wie sie mit ihm die technischen Schwächen der IT-Branche – von Microsoft über Cisco und Huawei – für ihre diskreten Zugriffe eiskalt ausnutzt.

Die Einheit sei das „Wunderkind im amerikanischen Geheimdienstverbund“, sagt der NSA-Experte Matthew Aid. „Getting the ungettable“, das Unerreichbare erreichen, so bezeichnet die NSA selbst ihre Aufgabe: Es gehe nicht um Quantität, sondern um Qualität, beschrieb eine frühere TAO-Chefin ihre Arbeit, nachzulesen in einem internen Dokument. Die TAO habe „einige der wichtigsten Erkenntnisse beigesteuert, die unser Land je gesehen hat“. Ihre Einheit nehme „die härtesten Geheimdienstziele“ ins Visier.

Die Ex-TAO-Chefin definierte damals die Zukunft ihrer Abteilung so: Die Truppe müsse neben der Aufklärung „Attacken in Computernetzen als integrierten Teil militärischer Operationen“ ermöglichen. Damit die NSA erfolgreich sei, müsse die TAO das „Fundament legen, um allgegenwärtigen, dauerhaften Zugang zum globalen Netzwerk zu erreichen“. Was letztendlich nichts anderes heißt, als dass sie Hacker mit staatlichem Auftrag sind.



Geheimdokumente der NSA und von Booz Allen

Aggressive Angriffe, so geht es auch aus einer Selbstdarstellung hervor, gehören ausdrücklich zu den Aufgaben der Einheit. Mitte des vergangenen Jahrzehnts hatte sich die Spezialabteilung Zugang zu 258 Zielen in 89 Ländern verschafft – fast rund um den Globus. Im Jahr 2010 liefen demnach weltweit 279 Operationen.

TAO-Spezialisten griffen in der Vergangenheit auf geschützte Netzwerke demokratisch gewählter Staatschefs zu. Sie infiltrierten Netzwerke von Telekommunikationskonzernen in Europa. Und sie knackten die für sicher gehaltenen, verschlüsselten BlackBerry-Mail-Server – eine „längere TAO-Operation“ sei dazu notwendig gewesen, heißt es in den Unterlagen.

Die Einheit ist ein Kind des Internets. 1997, als weltweit noch nicht einmal zwei Prozent aller Menschen über einen Netzzugang verfügten und noch niemand an Facebook, YouTube oder Twitter dachte, wurde sie gegründet. Die ersten TAO-Mitarbeiter bezogen ihre Büros im NSA-Hauptquartier in Fort Meade, Maryland, abgeschottet vom Rest des Geheimdienstes. Rund um die Uhr sollten sie nach Möglichkeiten suchen, sich in den globalen Kommunikationsverkehr zu hacken.

Dafür aber brauchte die NSA einen neuen Typus Mitarbeiter. Die TAO-Angestellten, die in San Antonio Zutrittsberechtigungen für die speziell gesicherte Etage haben, sind meist deutlich jünger als der Durchschnitt der NSA-Belegschaft. Sie sehen aus wie Nerds – und sind es auch. Ihre Mission: das Einbrechen, Manipulieren und Ausbeuten von Computernetzwerken.

Nur logisch, dass die NSA das Personal auf großen US-Hacker-Konferenzen rekrutiert: NSA-Chef Keith Alexander trat dort in den vergangenen Jahren mehrmals auf und warb um Vertrauen und Nachwuchs – manchmal in Jeans und T-Shirt, manchmal im legeren kurzen Uniformhemd. Die Rekrutierungsstrategie ist offenbar erfolgreich, kaum ein anderer Bereich innerhalb der Behörde wächst so schnell wie die TAO. Einheiten der Truppe gibt es mittlerweile auch in Wahiawa auf Hawaii, in Fort Gordon, Georgia, auf dem NSA-Außenposten Buckley Air Force Base bei Denver – und natürlich in San Antonio.

Eine Spur der Hacker führt nach Deutschland: Ausweislich eines Papiers aus dem Jahr 2010, das die „wichtigsten TAO-Kontaktstellen“ im In- und Ausland mit Namen, Mailadressen und „sicheren Telefonnummern“ auflistet, gab es eine solche TAO-Verbindungsstelle in Darm-

Otto-Katalog für Spione

NSA-Papiere belegen: Der Geheimdienst verfügt über Hintertüren für zahlreiche Produkte.

Wenn es um moderne Schutzwälle für Firmennetze geht, spart der zweitgrößte Netzwerkausrüster der Welt nicht mit Eigenlob. Die eigenen Produkte seien „ideal", um Unternehmen und Rechenzentren vor unerwünschten Zugriffen von außen zu schützen, schwärmen die PR-Leute des US-Unternehmens Juniper Networks. Die Leistung der Spezialrechner sei „unerreicht", die Firewalls seien die „besten ihrer Klasse". Vor dem US-Geheimdienst NSA aber schützen sie nicht.

Spezialisten des Dienstes ist es schon vor Jahren gelungen, die digitalen Schutzwälle des Unternehmens zu durchlöchern. Und nicht nur Juniper-Kunden sind betroffen: Eine Art Produktkatalog, den der SPIEGEL einsehen konnte, belegt, dass eine NSA-Abteilung namens ANT auch die Sicherheitsprodukte anderer Branchengrößen ausgehöhlt hat, darunter der amerikanische Weltmarktführer Cisco, sein chinesischer Herausforderer Huawei – sowie die Produzenten von Massenprodukten wie der US-Hersteller Dell.

Im Visier der Spezialisten für geheime Hintertüren sind alle Ebenen unseres digitalen Lebens: von ganzen Rechenzentren über einzelne Computer und Notebooks bis zu Mobiltelefonen. Für fast jedes Schloss findet sich im ANT-Werkzeugkasten ein Schlüssel. Es ist wie in der Fabel vom Hasen und vom Igel. Egal welche Wand die Firmen aufbauen – die NSA-Spezialisten stehen schon dahinter. Dieser Eindruck jedenfalls entsteht, wenn man durch den rund 50-seitigen Otto-Katalog für Agenten blättert, in dem NSA-Mitarbeiter das jeweils Passende zum Abschöpfen ihrer Ziele bei der Abteilung ANT bestellen können. Sogar die Preise der elektronischen Einbruchswerkzeuge sind vermerkt, von 0 bis 250 000 Dollar.

Im Fall von Juniper heißt einer der digitalen Dietriche „Feedtrough", Futtertrog. Diese Spionagesoftware nistet sich in Juniper-Firewalls ein und sorgt dafür, dass weitere NSA-Programme in den Großrechner geschmuggelt werden, die dank Feedtrough selbst „Neustarts und Software-Upgrades" überstehen können. So sichern sich die US-Spione eine dauerhafte Präsenz in fremden Netzwerken. Die Software, so heißt es im Katalog, „ist bereits auf zahlreichen Zielplattformen im Einsatz".

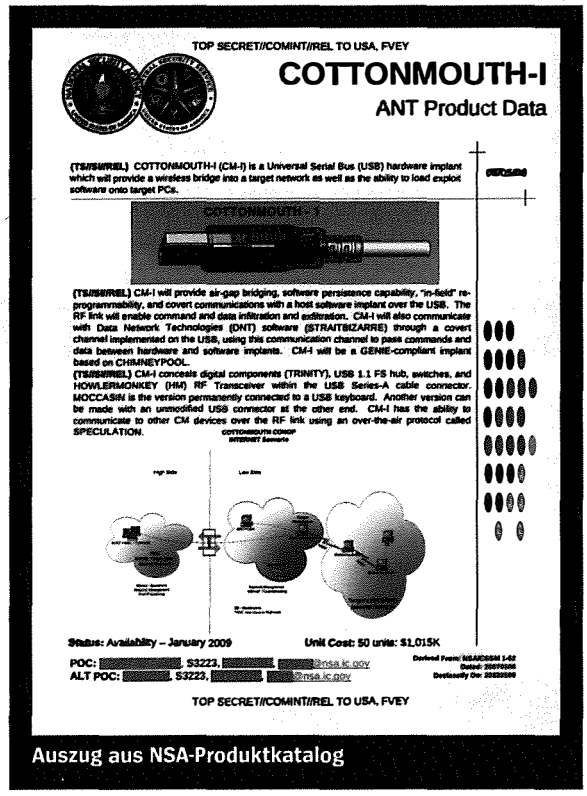
Die Spezialisten von ANT – die Buchstaben stehen vermutlich für „Advanced" oder „Access Network Technology" – sind die hochbegabten Handwerksmeister der NSA-Abteilung für maßgeschneiderte Operationen, Tailored Access Operations (TAO). Wo deren herkömmliche Einbruchs- und Abschöpfmethoden nicht ausreichen, stehen die ANT-Leute mit ihren Spezialwerkzeugen parat. Sie können damit in Netzwerkausrüstungen eindringen, Handys und Computer überwachen, Daten ausleiten oder gar verändern. Derlei „Implantate" (NSA-Jargon) sind maßgeblich daran beteiligt, dass der US-Geheimdienst ein globales Schatten-Netzwerk errichten konnte.

Manches Gerät ist richtig günstig: Ein manipuliertes Monitorkabel etwa, das es „TAO-Personal erlaubt zu sehen, was auf dem anvisierten Monitor angezeigt wird", gibt es schon für 30 Dollar. Eine „aktive GSM-Basisstation", also ein Werkzeug, das es ermöglicht, sich als Handy-Funkmast auszugeben, um so Mobiltelefone zu überwachen, kostet dagegen 40 000 Dollar. Computerwanzen, als normale USB-Stecker getarnt, die unbemerkt über Funk Daten senden und empfangen, gibt es im Fünfzigerpack für mehr als eine Million Dollar.

Doch die Abteilung ANT stellt nicht nur Spionage-Hardware her, sie entwickelt eben auch Software für Spezialaufgaben. Besonders gern versuchen die ANT-Entwickler offenbar, ihren Schadcode im sogenannten BIOS zu platzieren, einer Software, die direkt auf der Hauptplatine eines PC sitzt und beim Einschalten als Erstes geladen wird.

Das hat eine Reihe unschätzbarer Vorteile: Ein so infizierter PC oder Server scheint normal zu funktionieren, für Virenschutz- oder andere Sicherheitsprogramme bleibt die Infektion unsichtbar. Mehr noch: Selbst wenn die Festplatte eines so infizierten Rechners komplett gelöscht und ein neues Betriebssystem aufgespielt wird, funktionieren die ANT-Schadprogramme weiter und sorgen dafür, dass später erneut Späh- und Schnüffelsoftware auf den vermeintlich gesäuberten Rechner nachgeladen wird. „Persistence" nennen die ANT-Entwickler das – sie haben damit dauerhaft Zugriff.

Im Angebot ist auch ein Programm, das sich in der Firmware von Festplatten der Hersteller Western Digital, Seagate und Samsung einnistet – die beiden erstgenannten Unternehmen stammen aus den USA. In diesen Fällen kompromittiert der US-Geheimdienst also US-Technik. Andere ANT-Programme zielen auf Internet-Router für den professionellen Einsatz oder auf Hardware-Firewalls, die etwa Unternehmensnetze vor Angriffen aus dem Internet schützen sollen. Viele der digitalen Angriffswaffen lassen sich „per Fernzu-


TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" reprogrammability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

Status: Availability – January 2009 Unit Cost: 50 units: $1,015K

POC: [redacted], S3223, [redacted]@nsa.ic.gov

ALT POC: [redacted], S3223, [redacted]@nsa.ic.gov

TOP SECRET//COMINT//REL TO USA, FVEY

Auszug aus NSA-Produktkatalog

MARK WILSON / GETTY IMAGES

Vertreter großer Computerunternehmen, Präsident Obama im Weißen Haus am 17. Dezember: *Ziel ist es, „Endgeräte zu kapern"*

griff" installieren, also über das Internet. Andere erfordern das physische Abfangen von Endgeräten, um diese mit Schadsoftware oder Wanzen zu bestücken.

Aus den eingesehenen Unterlagen ergibt sich nicht, dass die erwähnten Unternehmen die NSA unterstützt oder Kenntnis von den Überwachungslösungen hätten. „Cisco arbeitet mit keiner Regierung zusammen, um eigene Produkte zu verändern oder sogenannte Sicherheitshintertüren in unseren Produkten zu installieren", so eine Stellungnahme des Konzerns. Bei Western Digital, Juniper Networks und Huawei hieß es, man wisse nichts von derlei Modifizierungen. Dell beteuerte generell, sich an die Gesetze aller Länder zu halten, in denen die Firma tätig sei.

Viele der im Katalog angebotenen Softwarelösungen stammen aus dem Jahr 2008, manche betreffen Server, die heute nicht mehr verkauft werden. Doch die staatlichen Hacker entwickeln ihr Arsenal permanent weiter. Auf manchen Seiten des Katalogs werden neuere Systeme aufgeführt, gegen die 2008 noch keine Angriffswaffen zur Verfügung standen. Aber, so versprechen die Autoren, man arbeite bereits an Wegen, um auch diese Systeme „bald zu unterstützen". JACOB APPELBAUM, JUDITH HORCHERT, CHRISTIAN STÖCKER

stadt – im „European Security Operations Center" des „Dagger Complexe" bei Griesheim.

Allein der Zuwachs in der texanischen Dependance ist beeindruckend, wie als „streng geheim" eingestufte Dokumente belegen, die der SPIEGEL auswerten konnte. Demnach waren im „Texas Cryptologic Center" im Jahr 2008 nicht einmal 60 TAO-Spezialisten beschäftigt. Bis 2015 sollen es 270 sein. Dazu gehören 85 Fachleute der Abteilung „Anforderungen & Zielauswahl", 2008 waren es noch 13. Die Zahl der Softwareentwickler soll von 3 im Jahr 2008 auf 38 im Jahr 2015 steigen. Von San Antonio aus werden Ziele im Nahen Osten, auf Kuba, in Venezuela und Kolumbien angegriffen – und im 200 Kilometer entfernten Mexiko, dessen Regierung die Hacker im Visier hatten.

Der Erfindungsreichtum der NSA erinnert an den legendären „Q" aus James Bond.

Das mexikanische Sekretariat für öffentliche Sicherheit, das Anfang 2013 in der Nationalen Sicherheitskommission aufging, war damals zuständig für die Polizei, die Terrorabwehr, das Gefängnissystem und den Grenzschutz. Die meisten der rund 20 000 Mitarbeiter arbeiteten im Hauptquartier an der Avenida Constituyentes, einer vielbefahrenen Straße in Mexico City. Von hier aus werden die meisten mexikanischen Sicherheitsbehörden beaufsichtigt, die zum Hoheitsbereich des Sekretariats zählten. Wer etwas über den Sicherheitsapparat des Landes wissen möchte, ist hier also an der richtigen Adresse.

Insofern war es nur naheliegend, dass die TAO, die Abteilung für maßgeschneiderte Operationen, den Auftrag bekam, sich das Sekretariat vorzunehmen. Das US-Heimatschutzministerium und die Geheimdienste, so hieß es in dem Auftrag, müssten schließlich alles über Drogenhandel, Menschenschmuggel und die Sicherheit der mexikanisch-amerikanischen Grenze wissen. Das Sekretariat sei eine „potentielle Goldmine" für die Auswerter. Als Ziel nahmen sich die TAO-Leute die Systemadministratoren und Telekommunikationsingenieure der Behörde vor. Operation „Whitetamale" lief an, benannt nach den in Mexiko beliebten Maistaschen.

Das NSA-Büro für die Zielerfassung, das 2002 auch Angela Merkel ins Visier genommen hatte, schickte den TAO-Leuten eine Liste mit Funktionären des Sekretariats, die als Ziele interessant seien. Zuerst drang die TAO in deren Postfächer ein, das war vergleichsweise einfach. Dann infiltrierten die Spezialisten das ge-

samte Netzwerk und schnitten den Datenverkehr mit.

Bald kannten die NSA-Spione die Server der Behörde, die dazugehörigen IP-Adressen, die Rechner für den Mailverkehr und die Adressen diverser Mitarbeiter. Und sie beschafften Diagramme über die Struktur der Sicherheitsbehörde, inklusive Videoüberwachung. Die Operation lief offenbar über Jahre, bis der SPIEGEL darüber im Oktober erstmals berichtete (SPIEGEL 43/2013).

Der Fachbegriff für diese Form der Ausspähung lautet „Computer Network Exploitation" – Ausbeutung von Computernetzwerken. Ziel sei es, „Endgeräte zu kapern", heißt es in einer NSA-Präsentation. Aufgezählt werden darin alle Geräte, die unseren digitalen Alltag bestimmen: „Server, Workstations, Firewalls, Router, Telefone und Telefon-Schaltanlagen". Hinzu kommen Scada-Systeme, Steuermodule für Industrieanlagen, die in Fabriken und Kraftwerken eingesetzt werden. Wer sie unter Kontrolle bringt, kann Teile der kritischen Infrastruktur eines Landes aushebeln.

Das berüchtigtste Beispiel für einen derartigen Angriff ist Stuxnet, ein Superwurm, der im Juni 2010 entdeckt wurde. Er war von den Amerikanern und israelischen Geheimdiensten entwickelt worden, um das iranische Atomprogramm zu sabotieren – mit Erfolg: Es wurde um Jahre zurückgeworfen, nachdem Stuxnet die Scada-Steuerungstechnik, die die Iraner in der Uran-Anreicherungsanlage von Natans einsetzen, manipuliert und bis zu 1000 Zentrifugen unbrauchbar gemacht hatte.

Neue Techniken entwickelt und testet die Sonderabteilung der NSA in einem eigenen Entwicklungsbereich. Dort sitzen die eigentlichen Tüftler – und ihr Erfindungsreichtum, in fremde Netze, Rechner oder Smartphones einzudringen, erinnert an eine zeitgemäßere Version des legendären „Q" aus den James-Bond-Filmen. Wie kreativ die Truppe vorgeht, zeigt sich bei einer Einbruchsmethode, die auf die Fehleranfälligkeit des Microsoft-Betriebssystems Windows setzt.

Windows-Nutzer kennen das Fenster, das auf ihrem Bildschirm aufploppt, wenn das System einen Fehler erkannt hat. Mit einem Standardtext werden die Kunden aufgefordert, einen Fehlerbericht an den Hersteller zu schicken und das Programm neu zu starten. Für die TAO-Spezialisten bieten diese „Crash Reports" eine willkommene Gelegenheit zum Ausspähen des Computers.

Denn wenn die Spezialeinheit einen Rechner irgendwo auf der Welt zu ihrem Ziel erklärt und in eine entsprechende Datenbank aufgenommen hat, werden die Geheimdienstler benachrichtigt, sobald das Betriebssystem des Computers kollabiert und der Nutzer der Bitte nachkommt, den Hersteller Microsoft zu benachrichtigen. Offenbar werden diese Crash-Benachrichtigungen mit dem NSA-Spionagewerkzeug XKeyscore aus dem allgemeinen Internetverkehr herausgefischt.

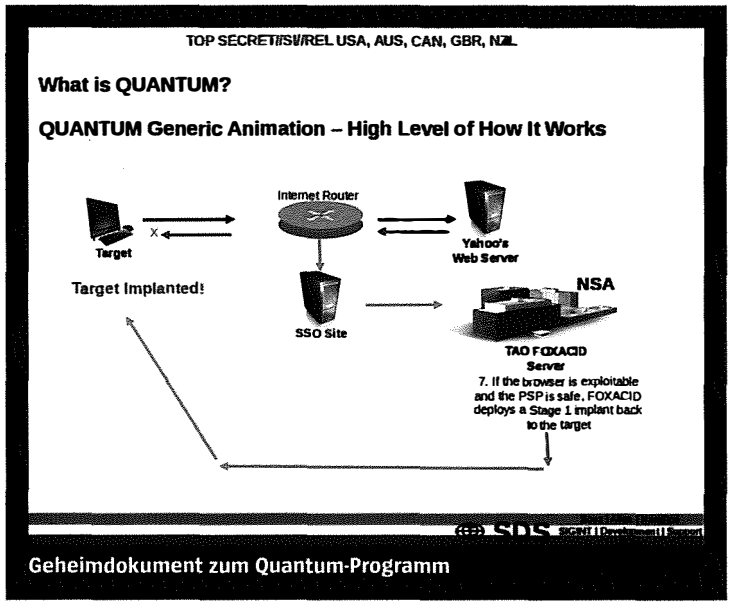
Die automatisierten Crash-Meldungen seien eine „hübsche Methode", um sich „passiven Zugriff" auf einen Rechner zu verschaffen, heißt es in einer internen Präsentation. Zunächst werden dabei nur Daten erfasst, die vom betroffenen Computer aus ins Internet wandern. Veränderungen auf dem Rechner selbst werden noch nicht durchgeführt. Aber die Fehlermeldungen legen wertvolle Informationen frei. Etwa darüber, was mit dem Rechner der jeweiligen Zielperson nicht stimmt. Also auch, welche Sicherheitslücken sich ausnutzen lassen, um dem ahnungslosen Opfer Schad- und Spähsoftware unterzujubeln. Obwohl die Methode in der Praxis kaum Bedeutung haben soll, haben die Agenten der NSA ihren Spaß damit, denn sie lieben Scherze auf Kosten des Software-Riesen aus Seattle.

So heißt es in einer internen Grafik anstelle des Microsoft-Originaltextes hämisch: „Diese Meldung kann von einem ausländischen Sigint-System abgefangen werden, um detaillierte Informationen zu sammeln und Ihren Computer besser anzuzapfen." Sigint steht für technische Aufklärung.

Das Infiltrieren von Zielrechnern mit sogenannten Implantaten oder Trojanern ist eine der Kernaufgaben der Hacker, die ihren Spähwaffen Namen wie „Wütender Nachbar", „Brüllaffe" oder „Wasserhexe" geben. Aber was putzig klingt, ist so aggressiv wie effektiv. Laut dem Etatplan für die US-Geheimdienste sollen bis Ende 2013 weltweit rund 85 000 Computer von den NSA-Spezialisten infiltriert sein. Die mit Abstand meisten dieser Infektionen erledigen die TAO-Teams über das Internet.

Bis vor wenigen Jahren agierten die NSA-Agenten wie Cyberkriminelle und verschickten Spam-E-Mails mit Links, die auf virenverseuchte Websites führten. Kennt man die Sicherheitslücken eines Internet-Browsers, kann es ausreichen, dass die Zielperson eine manipulierte Website aufruft, um ihren Rechner mit Spähsoftware zu infiltrieren. Besonders populär ist bei den NSA-Hackern Microsofts Internet Explorer. Doch die Spam-Methode funktionierte viel zu selten.

Mittlerweile hat die Abteilung TAO ihren Werkzeugkasten aufgerüstet. Sie verfügt über ein ausgefeiltes Arsenal, das unter dem Oberbegriff „Quantumtheory" geführt wird. „Bestimmte Quantum-Missionen haben eine Erfolgsquote von bis zu 80 Prozent, während Spam bei weniger als einem Prozent liegt", heißt es in einer NSA-internen Präsentation.



Geheimdokument zum Quantum-Programm

Ein ausführliches Dokument mit dem Titel „Quantum-Fähigkeiten", das der SPIEGEL einsehen konnte, enthält als Zielobjekte viele populäre Dienstanbieter wie Facebook, Yahoo, Twitter und YouTube. „NSA Quantum funktioniert am besten gegen Yahoo, Facebook und statische IP-Adressen", heißt es da. Nutzer von Google-Diensten dagegen könne die NSA mit dieser Methode nicht ins Visier nehmen – das könne nur der britische Geheimdienst GCHQ, der den Quantum-Werkzeugkasten von der NSA übernommen hat.

Besonders beliebt ist bei den Staats-Hackern die Methode „Quantum Insert". Damit hat das GCHQ Mitarbeiter des halbstaatlichen Telekommunikationsanbieters Belgacom angegriffen, um über deren Rechner in das firmeneigene Netzwerk vorzudringen (SPIEGEL 46/2013). Die NSA nahm so Verantwortliche der Organisation erdölexportierender Länder in der Wiener Zentrale ins Visier. In beiden Fällen verschaffte sich das Spionagekonsortium Zugang zu wertvollen Wirtschaftsdaten.

Die Insert-Methode beruht wie andere Quantum-Varianten darauf, dass die NSA neben dem Internet ein Schattennetz betreibt, mit einer eigenen, gut versteckten Infrastruktur, „schwarzen" Routern und Servern. Zum Teil werden in das Schattennetz der NSA offenbar auch Router

ARMIN KÜBELBECK

NSA-Niederlassung in Griesheim bei Darmstadt: *Eine Spur führt nach Deutschland*

und Server aus fremden Rechenzentren in aller Welt eingemeindet, indem sie von den Staatshackern per „Implant" verseucht und anschließend aus der Ferne kontrolliert werden (siehe Kasten Seite 102)

Der Geheimdienst versucht auf diese Weise, seine Ziele anhand ihrer digitalen Lebenszeichen zu erkennen und zu verfolgen. Das kann eine bestimmte Mailadresse sein oder das Cookie einer Website. Cookies sind kleine Dateien, die Websites auf den Computern ihrer Besucher anlegen, um diese später wiederzuerkennen. Ein Cookie allein identifiziert dabei nicht die Person, die vor dem Rechner sitzt. Hat man jedoch weitere Informationen, etwa die Mailadresse, mit der sich der Nutzer eindeutig erkennen lässt, ist ein Cookie wie ein Fingerabdruck im Netz.

Haben die TAO-Teams die Gewohnheiten ihrer Ziele ausspioniert, können sie zum Angriff übergehen. Von nun an arbeitet das Quantum-System weitgehend automatisch: Taucht in einem Datenpaket, das durch die überwachten Kabel und Router fließt, die Mailadresse oder das Cookie auf, schlägt das System Alarm. Es ermittelt, welche Website die Zielperson gerade aufrufen möchte, und aktiviert einen der „schwarzen" Server des Geheimdienstes, die den Codenamen „Foxacid" tragen. Dieser NSA-Server versucht, sich blitzschnell zwischen den Rechner der Zielperson und die von ihr angeforderte Website zu schieben. Ein Taschenspielertrick fürs Internet. Im Fall der Belgacom-Ingenieure bekamen diese statt ihrer angeforderten persönlichen LinkedIn-Seite eine perfekte Kopie vom NSA-Server. Huckepack und unsichtbar für den Nutzer transportiert die manipulierte Seite Spähsoftware, die auf die Sicherheitslücken im Rechner der Zielperson abgestimmt ist.

Es ist wie ein Wettrennen der Server. Im Spionage-Slang eines der Dokumente liest sich das so: „Warte auf einen Seitenaufruf! Schieße! Hoffe!" Manchmal seien die Spionagewerkzeuge aus dem schwarzen Netz „zu langsam, um das Rennen zu gewinnen". Häufig genug aber seien sie erfolgreich. Insbesondere bei LinkedIn klappe das Infiltrieren mit Quantum Insert inzwischen in mehr als 50 Prozent aller Versuche.

Die NSA hat dabei nicht nur Einzelpersonen im Visier. Im Gegenteil: Besonders interessant sind ganze Netze und Netzbetreiber – zum Beispiel die Glasfaserkabel, die einen großen Teil des weltweiten Internetverkehrs über den Grund der Weltmeere leiten. In einem Dokument mit der Einstufung „streng geheim" und „nicht für Ausländer" wird zum Beispiel ein Erfolg bei der Erkundung des sogenannten Sea-Me-We-4-Kabelsystems beschrieben.

Dieser Unterwasser-Kabelstrang verbindet Europa mit Nordafrika und den Golfstaaten und erstreckt sich von dort aus weiter über Pakistan und Indien bis nach Malaysia und Thailand. Seinen Ausgangspunkt nimmt das Kabelsystem in Südfrankreich, bei Marseille. Zu den Betreibern gehören France Télécom, heute bekannt als Orange, und Telecom Italia Sparkle. Orange gehört bis heute teilweise dem französischen Staat.

Am 13. Februar 2013, so wird in dem Papier stolz verkündet, sei es der TAO gelungen, „Informationen über das Netzwerkmanagement des Sea-Me-We-4-Unterwasser-Kabelsystems zu erlangen". Mit Hilfe einer „Website-Maskerade-Aktion" habe man sich Informationen über „die Verschaltung bedeutsamer Teile des Netzwerks" verschafft – offenbar waren die Hacker hier wieder mit der Quantum-Insert-Methode erfolgreich.

Wenn nötig, stellt das FBI auch einen behördeneigenen Jet zur Verfügung.

Das TAO-Team hackte demnach eine interne Website des Betreiberkonsortiums und kopierte Unterlagen über die technische Infrastruktur. Doch das war nur ein erster Schritt. „Weitere Operationen sind für die Zukunft geplant, um zusätzliche Informationen über dieses und andere Kabelsysteme zu erlangen."

Was die Abteilung innerhalb der NSA so besonders macht, sind nicht nur Erfolgsmeldungen wie diese. Ungewöhnlich ist, dass sie anders als die meisten NSA-Operationen häufig physischen Zugang zu ihren Zielen braucht, etwa um eine zentrale Mobilfunkstation zu manipulieren.

Dafür kooperiert die NSA mit anderen Geheimdiensten wie der CIA oder dem FBI und deren Informanten vor Ort, die bereit sind, bei der Mission zu helfen. Auf diese Weise kann die TAO auch Netzwerke angreifen, die nicht ans Internet angeschlossen sind. Wenn nötig, stellt das FBI auch einen behördeneigenen Jet zur Verfügung, damit die Klempner rechtzeitig zum Ziel gelangen, dort eine halbe Stunde lang an einem Server schrauben und unerkannt wieder verschwinden.

Die Abteilung TAO sei ein einzigartiges Instrument der USA, heißt es in einer Stellungnahme der NSA. Sie versetze den Dienst in die Lage, „die Nation und ihre Verbündeten an vorderster Front zu verteidigen. Sie konzentriert sich dabei auf die Informationsbeschaffung im Ausland durch die Ausbeutung von Computernetzen." Zu Einzelheiten über die Aufgaben der TAO äußere sich die NSA nicht.

Manchmal jedoch arbeiten auch die modernsten Spione der Welt sehr konventionell und fangen einfach nur die Post ab. Bestellt eine Zielperson, eine Behörde oder ein Unternehmen einen neuen Rechner oder Zubehör, dann leitet die TAO die Postlieferung in eine geheime Werkstatt um. Dort wird das Paket vorsichtig geöffnet, um an sogenannten „Ladestationen" Schadsoftware aufzuspielen oder mittels Hardware-Einbauten Hintertüren für den Geheimdienst zu schaffen. Der Rest kann dann wieder bequem vom Rechner aus erledigt werden.

Diese kleinen Unterbrechungen in der Lieferkette gehörten zu den „produktivsten Operationen" der Elite-Hacker, heißt es in einem Geheimdokument. Mit ihrer Hilfe erlange man Zugänge zu Netzen „überall auf der Welt". Ein wenig altes Handwerk überlebt also auch noch im Internetzeitalter.

JACOB APPELBAUM, LAURA POITRAS, MARCEL ROSENBACH, JÖRG SCHINDLER, HOLGER STARK, CHRISTIAN STÖCKER