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“.

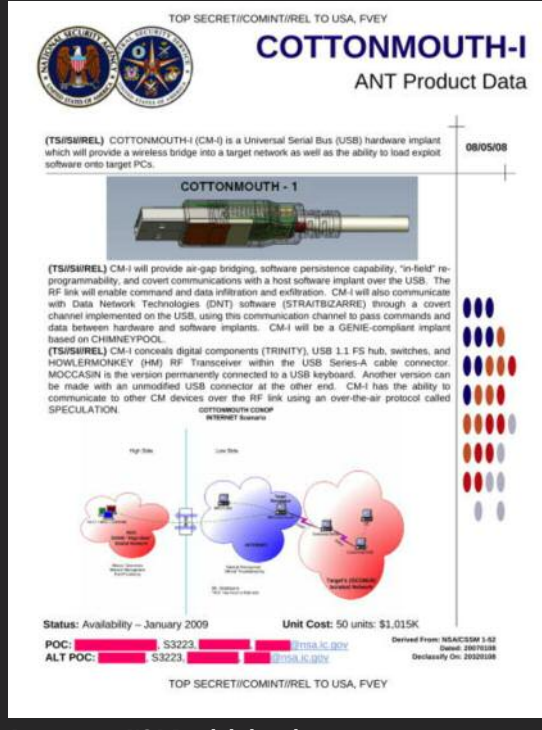
Die Spezialisten von ANT – die Buchstaben stehen vermutlich für „Advanced“ oder „Access Network Technology“ – sind die hochbegabten Handwerksmeister der NSA-Abteilung für maßgeschneiderte Operationen, Tailored Access Operations (TAO). Wo deren herkömmliche Einbruchs- und Abschöpfmethoden nicht ausreichen, 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

08/05/08

COTTONMOUTH - 1

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

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-