Die Sprache der Destruktion: der Code des Stuxnet-Wurms, der 2010 den iranischen Atomreaktor in Buschehr sabotierte

Angriff aus dem Netz

Das Internet ist ein Segen. Und ein Fluch zugleich. Die digitale Welt bietet Schlupfwinkel für Diebe, Hehler, Spione und TERRORISTEN. Nie war der Mensch gläserner – und damit auch bedrohter

+++ Zürich im Spätherbst +++

Ein unscheinbares Mehrfamilienhaus, ein kleines Büro darin und Computer, Kabel, Festplatten, Stühle. Hier arbeitet Max, der mit richtigem Namen nicht genannt werden darf, weil er in geheimer Mission unterwegs ist. Max, schwarzes Strubbelhaar, wache Augen hinter Hornbrille, ist privater Internetfahnder. Firmen engagieren ihn, um Sicherheitslücken zu identifizieren. Sein Tagessatz beträgt 2000 Euro, aber das ist nichts im Vergleich zu dem, was seine Kunden durch Cyberkriminalität verlieren.

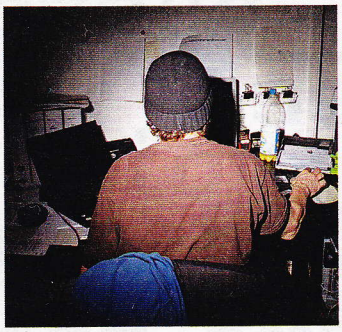
Max hat sich für die gute Seite des Netzes entschieden, aber seine Arbeit spielt in weiten Teilen auf der anderen Seite, auf der dunklen Seite, der Seite der Cybergangster.

Das Dunkle steht längst neben dem Schönen im Internet. Systematisch verseucht der Mensch auch die digitale Welt. Die gute Seite existiert natürlich noch und glitzert zum Beispiel in der Sonne des arabischen Frühlings, aber das Dunkle breitet sich aus. Im Netz verstecken sich Diebe, Hehler, Spione und Krieger und Terroristen. Es ist eine Welt der Pseudonyme und Aliasse, der Codenamen und Verschlüsselungen, der Viren und Würmer. Und offenbar rechnen die Mächtigen mit dem Schlimmsten: Regierungen schließen sich zusammen und halten Internetmanöver ab, die „Cyber Atlantic 2011" oder „Cyber Storm" heißen. Sie proben für den Krieg im Netz.

Die Menschen in der realen Welt haben ein Gespür dafür, dass Fluch und Segen im Netz Zwillinge sind. 85 Prozent der deutschen User fühlen sich von Netzkriminalität bedroht. Jeder fünfte Internetnutzer hierzulande hat schon üble Erfahrungen mit Viren und anderen schädlichen Programmen gemacht.

Und exakt an der Schnittstelle zwischen Gut und Böse sitzt Max.

Er bekämpft seine Gegner mit deren eigenen Waffen, mit den Waffen des „Social Engineering". Max sammelt zunächst sämtliche Informationen, die über eine Zielperson im Internet kursieren. Dann nimmt er Kontakt auf und nutzt sein Wissen über den anderen, um dessen Vertrauen zu gewinnen. Max verwendet „Social Engineering", man könnte sagen, Überredungskünste an der Tastatur, um die Identität von Web-Straftätern zu enttarnen.



Der Privatfahnder: Aus seinem Büro in Zürich spürt Max im Auftrag von Firmen Dealer und Hehler auf. Für 2000 Euro am Tag

Der Schaden durch Cybercrime beträgt nach konservativen Schätzungen 200 Milliarden Dollar pro Jahr. Und nach progressiven eine Billion

An einem regnerischen Tag im Herbst 2011 empfängt Max in seinem Büro. Er zeigt, wie leicht es ist, an Trojaner zu kommen, mit denen sich Computer ausspähen lassen. Oder an Listen mit gestohlenen Mailadressen. Oder an gehackte Server, die für groß angelegte Netzangriffe taugen. Oder an Kreditkarten-Dateien. Alles da im Web, ein virtueller Supermarkt aus Gigabytes. 2009 kursierten im Netz rund 162 Millionen Datensätze für Kreditkarten.

Max loggt sich ein auf den Chatkanal „UnderNet", das Ladenlokal der digitalen Unterwelt. Er sagt: „Sie nennen sich verified seller, also lizenzierte Verkäufer, aber ihre Ware eignet sich nicht für Ebay." Es ist Hehlerware. Man kommuniziert über den Chat von Skype, ICQ oder Jabber, in Echtzeit. Max kontaktiert „no name". Der bietet „dumps without pin" an, Szenejargon für gestohlene oder kopierte Kreditkarten. Mit ihnen lässt sich online einkaufen – ohne PIN-Code. Max bekundet zum Schein Interesse an fünf Karten aus Deutschland. Sekunden später postet „no name", er wolle fünf für 100 Euro pro Stück liefern. Er geht sogar in Vorleistung: Zwei Datensätze versende er sofort, zur Probe, die restlichen drei nach Zahlungseingang. Die Überweisung soll über eine Bank in Costa Rica laufen. Max' Finger rasen über die Tastatur, dann weiß er: „Unser Freund ohne Namen nutzt für seine Geschäfte einen Provider in Bulgarien."

Die deutschen Behörden könnten nun ein Rechtshilfeersuchen an ihre osteuropäischen Kollegen stellen. Das ist kompliziert, zeitaufwendig und in der Regel erfolglos. Deshalb gibt es Privatdetektive wie Max. Sie übernehmen gewissermaßen die Arbeit der Polizei. Sie sind schnell, effizient und unsichtbar. Im Auftrag ihrer Klienten ermitteln sie die Klarnamen der Täter und wo sie zu fassen sind. Ihr Job ist krisensicher, weil das Netz wächst und wächst und wächst. Und linear wachsen auch Missbrauch, Abzocke, Spionage. Alle zwei Sekunden entsteht ein neues Schadprogramm, pro Tag werden 21 000 Webseiten infiziert. Der Schaden durch Cybercrime und -Spionage beträgt nach konservativen Schätzungen bis zu 200 Milliarden Dollar pro Jahr und nach progressiven eine Billion.

Betroffen sind normale PC-Nutzer. Betroffen sind kleine Firmen. Betroffen sind Global Player wie Google und Sony. Und betroffen sind Staaten. Russische Hacker legten 2007 zeitweise das estnische Netz lahm und ein Jahr später das georgische.

Die Marketender im Netz prahlen und feilschen wie auf dem Viktualienmarkt. Max zeigt auf ein Angebot von „Krabum1", vermutlich ein Mazedonier, der bietet Kreditkarten an, als verkaufe er Äpfel: „Alles frisch, aus USA, England, Deutschland, Italien, Kanada. 80 Prozent Gold oder Premium." Nie war der Mensch gläserner. Und damit angreifbarer. Es kann jeden treffen, überall. Auch auf Facebook.

+++ Die Koobface-Bande +++

Sie könnten stolz sein, sie könnten ruhig ein wenig angeben mit ihrem Gespür, ihrer Akribie und der monatelangen Arbeit, abends nach dem Job. Aber das Staunen überlassen die Hamburger Jan Drömer, 32, und Dirk Kollberg, 38, den anderen. Den großen Zeitungen, der „New York Times" oder dem „Guardian". Sie werden dort gefeiert als IT-Helden, die es schafften, eine der berüchtigtsten Cyber-Banden der Gegenwart zu enttarnen, die Koobface-Gang.

Koobface ist ein Anagramm von Facebook. Die Bande, fünf Männer aus St. Petersburg, nutzte das soziale Netzwerk für ihre Beutezüge und verdiente Millionen. Bis zum 17. Januar. An diesem Tag wurden die Klar- →

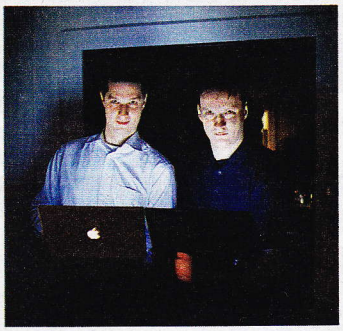
FOTO: THOMAS RABSCH

namen der Russen öffentlich. Mit diesem Tag endeten die Angriffe auf Facebook.

Drömer und Kollberg sitzen in einem Steakhouse im Hamburger Norden, und sie machen fast den Eindruck, als wäre ihnen der Scoop gar nicht so recht. Als wäre es nur ein kleiner Sieg. Irgendwie stimmt das auch. Drömer, im Hauptberuf EDV-Koordinator für die Flugzeug-Betankungsfirma AFS, sagt: „Es ist ja nicht mal klar, ob gegen die fünf jemals Anklage erhoben wird." Kollberg, im Hauptberuf Antivirenspezialist für die Internet-Sicherheitsfirma Sophos, sagt: „Unser Material liegt ja schon seit fast zwei Jahren beim FBI und bei Facebook." Sie wundern sich, warum die russischen Behörden derart träge reagierten und Stanislav A., Svyatoslav P., Anton K., Roman K. und Alexander K. zwar nun bekannt sind, aber eben nicht verhaftet. Das ist eine andere Geschichte, eine von Bürokratie, mangelnder Kooperation und womöglich von Korruption.

Drömers und Kollbergs Geschichte begann im September 2009. Die Koobface-Gang war da schon ein Jahr lang unterwegs – und gefürchtet. Die Russen, die sich selbst den sinnigen Namen „Ali Baba &4" gaben, verbreiteten einen Computerwurm, Koobface eben, der sich von Rechner zu Rechner fortpflanzte. Das Prinzip war simpel, genial und kriminell: Der Wurm streute Links auf Facebook-Profilseiten, in denen auf „funny" oder „sexy" Videos verwiesen wurde. Die Russen setzten auf die Neugier, und sie lagen richtig. Angeklickt, erschien eine Botschaft, der User möge bitte die Flash-Software für die Videofunktion aktualisieren. Jeder kennt solche Nachrichten. Aber mit dem nächsten Klick begann der Download des Schadprogramms ohne Wissen der arglosen Betrachter, die die Filmchen weiter und weiter schickten an Freunde und Bekannte – und die Seuche weiter verbreiteten.

Zur Hoch-Zeit von Koobface im Jahr 2010 waren zwischen 400 000 und 800 000 Rechner infiziert und bildeten ein sogenanntes Bot-Netz, einen Zusammenschluss von vielen Computern. Der Command-Server kann durchaus Tausende Kilometer entfernt stehen und die Rechner wie Drohnen für sich arbeiten lassen, ohne dass die Besitzer auch nur die leiseste Ahnung vom Eigenleben ihrer Festplatten haben.



Die Enthüller: Jan Drömer (links) und Dirk Kollberg enttarnten gemeinsam mit dem FBI die berüchtigte Koobface-Bande aus St. Petersburg

Koobface war ein Superwurm. Er infizierte bis zu 800 000 Computer – die meisten über Facebook. Die Besitzer ahnten vom Eigenleben ihrer Rechner nichts

Koobface ist ein Superwurm. Er kann eigene Konten bei sozialen Netzwerken bilden. Er kann auch Scareware aktivieren, schädliche Software, die dem Benutzer vorgaukelt, sein Computer sei infiziert und benötige sofort ein neues Antivirenprogramm. Viele fielen darauf herein und bestellten die vermeintliche Antivirensoftware, die aber nur eine Attrappe war, ein virtuelles Potemkin'sches Dorf, und rein gar nichts bewirkte. Ali Baba und seine Leute waren nur Zwischenhändler für den Schrott und wurden an den Verkäufen beteiligt. Sie hätten mit ihrem Know-how größeren Schaden anrichten und mehr Geld verdienen können.

Jan Drömer war fasziniert von Koobface. Er sagt: „Ich wollte einfach wissen, wer dahintersteckt." Also setzte er sich abends nach der Arbeit an den Computer und durchforstete IP-Adressen, Domains und Profile und bat alsbald seinen Freund Kollberg um Beistand. Sie tüftelten und setzten Mosaiksteinchen für Mosaiksteinchen zusammen. Die Russen machten erstaunliche Fehler, sie hinterließen Spuren im Netz, auf Seiten der Social Networks, auf Youtube und Flickr zum Beispiel. Diesen Spuren folgten die beiden Hamburger, und nach einigen Wochen hatten sie Zugang zum „Mutterschiff", wie sie es nennen, einem Server in Prag, der Schatzkammer von Ali Baba.

Vier Monate puzzelten sie weiter, bis sie die Pseudonyme geknackt hatten und die Klarnamen wussten. Sie kannten die Handynummern, den Namen der Firma mit dem sibyllinischen Titel Mob-Soft, die Firmenadressen in Prag und St. Petersburg und als Zugabe noch Megabytes von Fotos und Videos der Tatverdächtigen. Es wurde klar: Die Herrschaften mochten's heiß. Sie reisten nach Mallorca, Monaco, Bali und in die Türkei. Sie umgaben sich mit Frauen, sie spielten im Kasino. Sie fotografierten sich und drehten Filmchen. Einer von ihnen twitterte sogar. „Die Kriminellen", sagt Dirk Kollberg, „sind ungeheuer gut in dem, was sie können. Aber sie sind eben keine Sicherheitsexperten."

Im Februar 2010 übergaben Drömer und Kollberg das fertige Mosaik an Facebook und das FBI. Fast zwei Jahre vergingen. Denn den Amerikanern waren die Hände gebunden. St. Petersburg ist Russland. Und die russischen Kollegen unternahmen nichts. Mitte Januar tauchte der Klarname von Ali Baba schließlich in einem obskuren bulgarischen Blog auf, und also bestand plötzlich die Gefahr, dass die Bande abtaucht. Drömer und Kollberg, das FBI und Facebook berieten sich. Und sie beschlossen entgegen der ursprünglichen Planung: „We go public", wir gehen an die Öffentlichkeit. Seitdem sind Ali Baba und die Räuber bloßgestellt, blamiert. Aber immer noch frei.

Jan Drömer und Dirk Kollberg wollten keine Belohnung, sie wollten nur mehr wissen und dieses Wissen teilen. Sie hatten neben dem FBI auch das Bundeskriminalamt in Wiesbaden kontaktiert. Vom BKA kam keine Antwort. „Wahrscheinlich", sagt Jan Drömer, „haben die genug mit der deutschen Szene zu tun."

+++ Wiesbaden, BKA +++

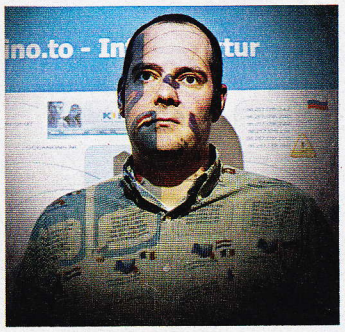
Schreibtische, aufgeschraubte Hardware und lose Kabel, die wie leblose Schlangen auf dem Boden liegen. Mirko Manske, ein stämmiger Typ mit raspelkurzen Haaren, ist eine Art Internet-Profiler des BKA. Er wusste natürlich von der Koobface-Gang und den laufenden Ermittlungen. Facebook ist ein amerikanischer Konzern, dafür sind die US-Kollegen zuständig. Sein Beritt ist Deutschland, und was er über seine Klientel sagt, klingt nach verdammt viel Arbeit: „Die Täter sind →

FOTO: THOMAS RABSCH

heute wesentlich breiter aufgestellt. Sie greifen vom E-Mail-Postfach, Ebay, Amazon bis zu Paypal die komplette digitale Ausprägung der Menschen im Netz an."

Im ersten Halbjahr 2011 verzeichneten die BKA-Ermittler 125 Prozent mehr Straftaten als im Vorjahr, das schlimmste Jahr, das es bis dahin gab – mit 246 000 Fällen von Netzkriminalität oder, wie es im sperrigen Fachterminus heißt, „mit dem Tatmittel Internet".

Die Kriminellen, sagt Manske, wachsen an ihren Aufgaben. Er erzählt von digitaler Schutzgelderpressung, auch bei Seiten mit hohen Klickzahlen. Werden deren Server beispielsweise mit Spam-Mails zugemüllt und deshalb langsamer, sinken die Klicks, sinken die Werbeeinnahmen, leidet der Umsatz. Und irgendwann meldet sich die Netz-Mafia: „Sollten wir nicht mal darüber nachdenken, was wir dagegen tun können? Gegen einen kleinen Obolus von ein paar Tausend Euro?"



Der Ermittler: Mirko Manske vom Bundeskriminalamt warnt vor Tätern, die „die komplette digitale Ausprägung der Menschen" angreifen

Der Kampf gegen die Kriminellen im Netz erinnert ein bisschen an den Kampf gegen das Doping in der realen Welt. Kaum wird eine neue Substanz entdeckt, kursiert bereits eine hochwertigere Variante. Es gibt Experten, die glauben nicht mehr an den Sieg des Guten. Sie fürchten, dass es in fünf Jahren keinen sauberen Rechner mehr gibt. Noch, und das ist ein eher schwacher Trost, überlappen sich analoge und digitale Welt des Verbrechens. Zumindest manchmal.

+++ Berlin im Oktober +++

Die Polizei ließ in einer groß angelegten Aktion eine Hackerbande hochgehen. Es ist ein besonders gut dokumentierter Fall. Er zeigt exemplarisch, wie die organisierte Bandenkriminalität ins Netz abgebogen ist.

Kopf dieser Gang war Stanislav A., ein heute 33 Jahre alter israelischer Staatsbürger. A. beauftragte irgendwann Ende 2009 einen Hacker, sich Zugang zu fremden Konten zu verschaffen. Der Mann benutzte dafür eine Software, die sich aktiviert, sobald sich die Opfer zum Onlinebanking einloggen. Die Methode heißt Phishing, der Gleichklang mit „fishing" kommt nicht von ungefähr. Es ist das Angeln nach Passwörtern und Zugangscodes.

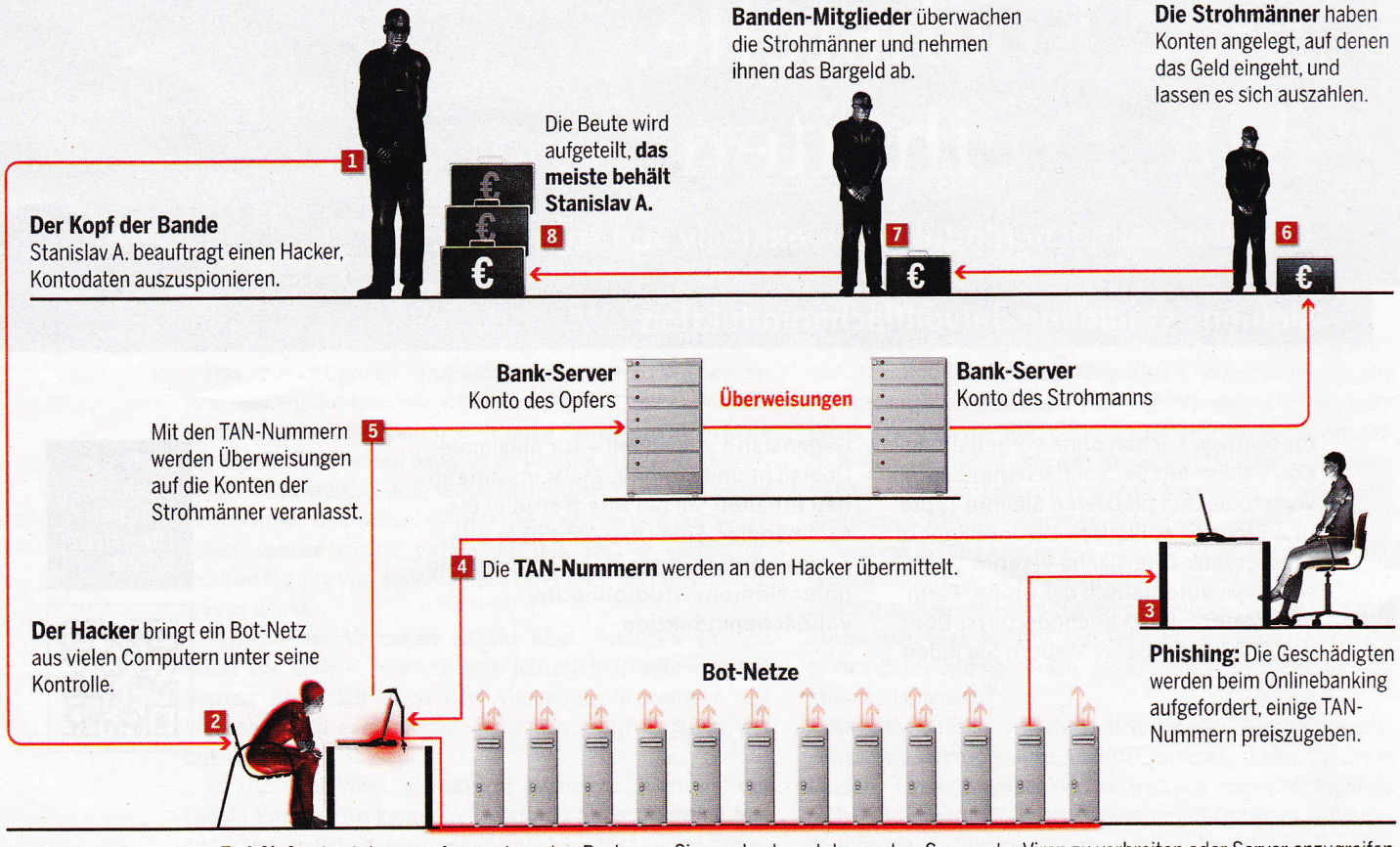
Der Hacker phishte auch bei Sabine P., einer Verkäuferin aus der Nähe von Erfurt. Der fielen Anfang Juni 2010 Merkwürdigkeiten auf. Ein kleines Fenster poppte auf und der Satz: „Um Online-Banking noch sicherer zu machen, bitte einmalig die TAN-Nummern eingeben."

Das tat sie, und danach fehlten ihr 990 Euro. 1085 andere taten es auch. Gesamtschaden: 1,24 Millionen Euro. →

FOTO: THOMAS RABSCH

Die Berliner Phishing-Bande

So erbeuteten Kriminelle rund 1,24 Millionen Euro mithilfe eines Bot-Netzes



infografik

Bot-Netze bestehen aus ferngesteuerten Rechnern. Sie werden benutzt, um etwa Spam oder Viren zu verbreiten oder Server anzugreifen.

Das Geld überwies der Hacker auf die Konten von insgesamt mehr als 30 Strohmännern. Einer dieser Männer war der Pole Mariusz K. Er war im Oktober 2009 am Bahnhof Zoo von zwei Litauern angesprochen worden, die ihm eine Arbeit auf dem Bau versprachen. Die Methode der Gangster ähnelte der von Schleppern. Die Männer und Frauen, die sie köderten, stammten aus Polen, Lettland oder Estland. Sie wurden in Kleinbussen nach Deutschland gekarrt, wohnten in Pensionen oder kleinen Wohnungen. Sie waren lediglich dazu da, Konten einzurichten und Geld abzuheben. Sie waren Opfer und Täter zugleich. Der Großteil der im Netz erbeuteten Summe floss an Stanislav A.

Mariusz K., der Pole, spürte alsbald, wie gefährlich seine neuen Bekannten waren. Einmal fuhr er mit einem der Litauer, der sich als „Wito" vorstellte, zur Commerzbank-Filiale im Europa-Center und ließ sich 4800 Euro auszahlen, die ihm Wito aus der Hand riss. Im Auto drohte Wito: Wenn er zur Polizei ginge, würden sie ihn köpfen.

Im Oktober vergangenen Jahres, nach monatelangen Recherchen, schlug die Polizei zu. Und die Wucht der Ermittlungen zeigt, wie wichtig die Behörden die Cyberbetrüger inzwischen nehmen: 115 Beamte durchsuchten elf Wohnungen in Berlin, sie nahmen am Ende sechs Verdächtige fest, unter ihnen auch Mariusz K. Sie sitzen im Knast von Moabit, streng getrennt.

Nur der Hacker blieb verschollen. Die Behörden vermuten ihn in Russland oder einer der ehemaligen Sowjetrepubliken. Und sie gehen davon aus, dass die Bande, genau wie die Koobface-Gang, mit einem Bot-Netz arbeitete.

Diese Bot-Netze sind die Geißel der virtuellen Welt. Das berühmteste hieß „GhostNet"; es kontrollierte mehr als tausend Computer an den sensiblen geografischen Zipfeln der Erde: Südkorea, Taiwan, Iran. Kanadischen IT-Experten gelang es, seinen Ursprung zurückzuverfolgen: China.

Der Pionier: Gong Wei (rechts, mit seinem Schüler Li Qi) gründete 1997 die legendäre „Green Army", die erste Hackergruppe

Chinas Aufstieg zur Supermacht findet seine Entsprechung im Netz. Geschätzte 300 000 Hacker leben dort und sind in ihrer Heimat beliebt wie Popstars

+++ Die schwarzen Gäste +++

Chinas Aufstieg zur Supermacht findet seine Entsprechung im Internet. 1996 begann „China Telecom" damit, die Haushalte flächendeckend mit Internetanschlüssen zu versorgen, das war die Initialzündung. Geschätzte 300 000 Hacker leben heute in China, sie sind in ihrer Heimat beliebt wie Popstars. Es gibt Magazine und Filme und Onlineserien über sie. Sie nennen sich „Heike", das bedeutet „schwarzer Gast". Sie sind jung, gebildet, gut. Und deshalb so bedrohlich.

Chinesen knackten im US-Wahlkampf 2008 die Mobiltelefone von Barack Obama und John McCain. Sie griffen taiwanesische Seiten an und indonesische, sie knackten die Mails des Dalai Lama, sie knackten auch Google und drangen bis zu den Kronjuwelen des Konzerns vor: Entwicklungsabteilung und Passwortsystem des Mail-Programms. Sie infiltrierten das amerikanische Handelsministerium und das Pentagon. Sie kopierten Datensätze für das geplante Kampfflugzeug F 35 Lightning II. Sie drangen in Netze amerikanischer Ölkonzerne ein. Sie belagerten EU-Kommission und Nato-Hauptquartier, aber auch Kanzleramt und Auswärtiges Amt.

Man kann es auch so sehen: Chinesische Hacker sind immer dann aktiv, wenn sie die Interessen der Volksrepublik in Gefahr sehen. Und sie tun das nicht zwangsläufig unter der Regie der Staatsmacht. Der amerikanische IT-Experte Scott Henderson schreibt in seinem Buch „The Dark Visitor": „Ihre Triebfedern sind Nationalismus, Technikinteresse, Ruhm und Geld." Der Volkskongress erließ 2009 offiziell sogar ein Anti-Hacker-Gesetz, die schwarzen Gäste kamen auf die schwarze Liste. Aber in den beiden Jahren zuvor hatte das Ministerium für öffentliche Sicherheit noch Jobangebote in den Hackerforen EvilOctal.com und XFocus.net gepostet.

Die chinesischen Hacktivisten sind ziemlich genau das Gegenteil der westlichen Nerds, denen Staaten und Regierungen vor allem suspekt sind. Wer diese sonderbare Welt verstehen will, muss dort hin, wo die Szene ihre Wurzeln hat. Wo alles begann, 1997, als sich die erste Hackergruppe formierte: die in der Szene legendäre „Green Army" aus Shanghai.

+++ Shanghai im November +++

„Goodwell" und „liwrml" werden in einem blauen Audi vor einen schäbigen Starbucks-Verschnitt gefahren. Zwei Männer warten draußen wie in einem schlechten Agentenfilm. „Goodwell" ist 36 Jahre alt und heißt mit echtem Namen Gong Wei. Er hat die „Green Army" gegründet. Kurze Haare, starrer Gesichtsausdruck. Sein Schüler Li Qi mit dem kryptischen Alias „liwrml" kommt wie sein Boss in gebügeltem Hemd unter V-Pullover daher. Sie sehen nicht aus wie Cyberkrieger, eher wie Netzwerkadministratoren.

Li Qi hat eine Powerpoint-Präsentation auf seinem Macbook vorbereitet: Er führt Sicherheitslücken auf Servern der US-Armee vor und demonstriert, wie eine der vielen Anonymous-Gruppen Zehntausende Mails der Navy stehlen konnte. Eine Kleinigkeit in ihren Augen. Die beiden kennen sich überhaupt verdammt gut aus mit dem amerikanischen Militär. Sie behaupten, dass chinesische Hacker von der bevorstehenden Tötung Osama bin Ladens schon wussten, als der Al-Qaida-Chef noch lebte.

Gong Wei und Li Qi sind zu diesem Treffen nur erschienen, um ein paar Dinge geradezurücken, die die Menschen im Westen nicht kapieren würden. „Alles begann einst als Protestbewegung", sagt Gong Wei. Ihn prägten, wie viele aus seiner Generation, die Gewaltexzesse gegen die chinesische Minderheit in Indonesien im Jahre 1998. Die Gräueltaten entwickelten sich zum zündenden Momentum für den ersten großen Hackerangriff aufs Ausland.

Die „Grüne Armee" bombardierte seinerzeit indonesische Regierungsseiten mit Mails und →

FOTO: DAVID HOGSHOLT

koordinierten Serveranfragen, bis die Server unter der Last des elektronischen Massenabwurfs zusammenkrachten. Federführend bei der Attacke: Gong Wei.

Im Jahre 2000 wandelte er ziemlich überraschend die „Army" in eine Unternehmensberatung für Netzwerksicherheit um. Und im vergangenen September berief Gong Wei eine Konferenz in Shanghai ein und verpasste der Hacker-Community einen neuen Kodex: weg vom Zerstören, hin zum Gestalten. So steht es im Manifest.

Gong Wei und Li Qi sind wie eine menschliche Firewall, kritische Fragen prallen an ihnen ab. Wer steckt hinter dem Hackerangriff auf den Dalai Lama? „Können wir nicht sagen", sagt Li Qi. Wer attackierte Google? „Keine Ahnung", sagt Gong Wei. Sie haben sich derart konsequent der guten Seite verschrieben, dass sie über die andere nicht mehr reden wollen. Nicht mal darüber, wie heterogen und zerstritten die chinesische Szene ist. Da sind die Grünen und die Roten, die Blackhats und Whitehats, die Cracker und Honker. Sie mögen einander nicht. Lediglich in einem Punkt stimmen sie überein: Was im Westen dunkel scheint, sieht aus fernöstlichem Blickwinkel viel heller aus.

Und umgekehrt. Die Bösen sind die Amerikaner, die Japaner, der Westen. Das ist ihr Koordinatensystem. Simpel und zielführend. Unter chinesischen Schulkindern ist Hacker ein beliebter Berufswunsch. Und die Talentiertesten studieren später in der Hochburg der Hacker: in Chengdu.

+++ Chengdu, Campus der Universität +++

Die University of Electronic Science and Technology liegt in der Nähe eines IT-Industrieparks außerhalb der Fünf-Millionen-Metropole. Wiesen und kleine Wälder umsäumen graue fünfstöckige Betonklötze. Auf den betonierten Straßen patrouillieren Uniformierte auf Elektrorollern. Das Hauptgebäude sieht so aus, als hätte der Hausarchitekt Stalins das Weiße Haus neu entworfen. In Chengdu sitzt auch eine große

Die Hacker-Hochburg: An der technologischen Universität von Chengdu sind rund 29 000 Studenten eingeschrieben

Der elektronische Dschihad könnte auch Deutschland erreichen. Verfassungsschützer fingen einen Aufruf zum Cyberangriff „auf herausragende Vertreter des Unglaubens" ab

IT-Einheit der Volksarmee. Alles fügt sich in Chengdu.

29 000 Studenten sind an der Uni eingeschrieben, rund 700 für das Fach Netzwerksicherheit. Einer von ihnen ist ein Brillenträger im Trenchcoat, Chu Xun, 21. Das ist nicht sein richtiger Name, aber er bekäme sonst Probleme. Er spricht nämlich ungeschminkt darüber, wie einige seiner Kommilitonen nach Unterrichtsschluss in den Computerräumen mit Viren experimentieren und in Server einbrechen. Die Dozenten haben ein Verbot erlassen – wer es dennoch tut, sollte schweigen.

Chu Xun schweigt nicht. Er erzählt, wie eine typische Hackerkarriere verläuft: „Anfänger probieren sich an einfachen Viren aus, infizieren damit Pornowebseiten. Es kommt vor, dass Studenten als Übung Klausurunterlagen von den Computern der Dozenten klauen." In andere Computer einbrechen zu können mache süchtig, bedeute Freiheit und Macht für die Hacker. Selbstredend spricht sich auf dem Campus herum, wenn wieder ein US-Server geknackt wurde. „Wir anderen Studenten bewundern das."

Die besten Absolventen haben glänzende Zukunftsaussichten. Internationale Unternehmen wie IBM und Microsoft rekrutieren hier ihr chinesisches Personal. Einmal im Jahr kommen auch Leute vom nationalen Sicherheitsapparat und fragen Dozenten nach den größten Talenten, sie veranstalten „recruiting sessions" und locken mit Jobs für Computerspionage. Man kann davon ausgehen, dass einige der Hackerangriffe auf deutsche Behörden in Chengdu ausgeheckt wurden.

Im Jahr 2010 verzeichneten die deutschen Staatsschützer 2108 Netzattacken, das waren lediglich die entdeckten Viren, tatsächlich dürften es deutlich mehr gewesen sein. Die meisten gelten dem Auswärtigen Amt – und dort jenen Mitarbeitern mit dem Fachbereich China. Es folgen Kanzleramt, Wirtschafts- und Finanzministerium. Die abgefischten Trojaner-Mails werden vom Verfassungsschutz archiviert und das vermutete Herkunftsland vermerkt. In den meisten Fällen steht dort: China.

+++ Der Heilige Krieg +++

In einem schmucklosen Büro in der noch schmuckloseren Zentrale des Bundesamts für Verfassungsschutz am Stadtrand von Köln sitzen Beamte und sprechen vom Krieg im Netz. Sie sprechen, genauer, vom „elektronischen Dschihad", der längst Realität ist in Israel und im Nahen Osten. Und nun auch Deutschland erreichen könnte. Vergangenen Juni fingen die Verfassungsschützer einen Rekrutierungsaufruf in einem islamistischen Forum ab. Ziel war das Anwerben von Personen mit technischen Fähigkeiten für einen Cyberangriff auf „herausragende Vertreter des Unglaubens". Die Islamisten suchten explizit nach Experten mit exzellenten Sprachkenntnissen von „Russisch bis Chinesisch". Und sie suchten explizit Cybersoldaten mit Wissen über Scada-Systeme, jene komplexen Programme, die Gas- und Wassernetze, Flughäfen und auch Atomkraftwerke steuern. Nach *stern*-Informationen meldeten sich unmittelbar 109 Bewerber auf den Aufruf. Fünf von ihnen erfüllten die meisten Kriterien, zwei hatten sogar Erfahrung mit Scada. Danach flüchteten sie in ein Chat-Forum im Netz-Nirwana.

Sicherheitsexperten nehmen solche Drohungen sehr ernst. Besorgt registrieren sie, dass viele islamische Extremisten an deutschen Universitäten naturwissenschaftliche Fächer studieren. Die Islamisten können modern. Und natürlich können sie Computer.

Mohammed Atta war auch so ein Nerd. ✶

Michael Streck; Christina Elmer, Kiki Fu, Johannes Gunst, Dirk Liedtke, Oliver Schröm, Xifan Yang

MEHR INFORMATIONEN

www.stern.de/investigativ
Interview mit Bundesinnenminister Hans-Peter Friedrich sowie ein Making-of zur Recherche in China

FOTO: DAVID HOGSHOLT