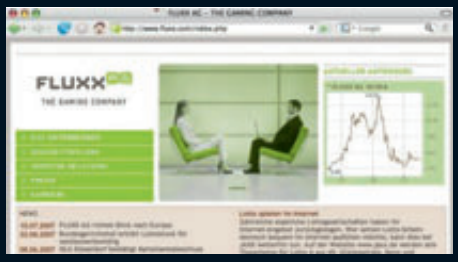

Fluxx-Finanzvorstand Stefan Hänel, Homepage des deutschen Glücksspieleanbieters: Mutmaßlich osteuropäische Hacker forderten 40 000 Euro für die Einstellung der Attacken auf die Fluxx-Web-Seite. Das Geld sollte über Western Union überwiesen werden, Fluxx zahlte nicht.

INTERNET

Angriff der Cyber-Söldner

Für eine Handvoll Dollar attackieren russische Hacker jede Internet-Seite. Sie arbeiten schnell und ohne jeden Skrupel. Ihre Opfer sind Oppositionelle und Kreml-kritische Medien im eigenen Land sowie Unternehmen – auch im Westen.

Der Herr der Zombies ruft seine Sklaven und wartet ungeduldig auf ihre Antwort – auf ein lautloses Echo aus dem Internet, aber eines mit verheerenden Folgen für seine Opfer. Wassilij, vernarrt in Computer seit dem zwölften Lebensjahr, blickt gebannt auf den flimmernden Monitor. Seinen richtigen Namen will der 18-jährige Informatikstudent nicht nennen, er lebt in einer Provinzstadt zwei Zeitzonen östlich von Moskau. Würden Polizisten entdecken, was er tut, käme er ins Gefängnis.

Mit wenigen blitzschnellen Fingerbewegungen über seine Tastatur demonstriert der junge Russe, mit welchen Befehlskombinationen er Web-Seiten irgendwo in weiter Ferne lahmlegt. Heute attackiert er ein großes Baustoffunternehmen. „Ich bombardiere die Seite mit sinnlosen Anfragen von 50 000 Computern gleichzeitig“, sagt er triumphierend. Der Fachbegriff für seine Web-Attacke lautet „Distributed Denial of Service“ (DDoS). Er steht für eine Datenlawine, abgesandt von fremden Computern, die das angegriffene System so lange überlastet, bis es zusammenbricht. „Es erstickt buchstäblich im Müll“, sagt Wassilij und lacht.

Weltweit werden täglich Tausende Unternehmen Opfer von DDoS-Attacken. Längst bedrohen die Hacker nicht nur die Wirtschaft, in Russland beispielsweise sind sie auch in der politischen Auseinandersetzung vor den anstehenden Wahlen zu einem gewichtigen Faktor und zu einer Gefahr für die letzten unabhängigen Medien des Landes geworden. Die DDoS wird gezielt eingesetzt, um die Opposition und unliebsame Medien mundtot zu machen.

Russische Hacker hatten auch ihre Finger im Spiel, als im Frühjahr die IT-Infrastruktur des kleinen Baltenstaates Estland am Boden lag. Estnische Politiker und westliche Medien sprachen von Cyber-Krieg. Wer dahintersteckte, blieb aber unklar.

Die Hacker verdingen sich für eine Handvoll Dollar als moderne Söldner an jedweden Auftraggeber. Wassilij preist in einem Hacker-Forum seinen „qualitativ hochwertigen Service“ für 150 Dollar an. Bei Anbieter DrDDoS gibt es bei zwei Bestellungen „35 Prozent Rabatt“.

Die Cyber-Piraten kapern fremde Rechner und schleusen über E-Mails oder verseuchte Web-Seiten Programme auf die Computer, die ihnen volle Kontrolle verschaffen. So dient Wassilij etwa der Server einer Gynäkologie-Klinik in Frankreich als sogenannter Bot. Experten schätzen, dass weltweit bis zu einem Viertel der mit dem Internet verbundenen Rechner solche Zombies sein könnten.

„Die Besitzer dieser Computer wissen nicht, dass sie für kriminelle Zwecke missbraucht werden“, sagt Peter Stamm, der Leiter des Referats zur Bekämpfung der Computerkriminalität des Bundeskriminalamts (BKA) in Wiesbaden. Das sogenannte Zombiemeter der amerikani-

Diskussion bei Echo Moskau, Homepage des Senders (links): Nach einem Angriff auf die Web-Seite der regierungskritischen Radiostation war Echo Moskau zwar weiterhin auf Sendung, die populären Internet-Seiten aber vier Tage lang nicht mehr online.

Putin-Kritiker Kasparow (am 14. April in Moskau), Homepage seines Bündnisses „Anderes Russland“: Weil der Kreml weite Teile der Medien kontrolliert, ist die Opposition auf das Internet angewiesen, wenn sie ihre Anhänger mobilisieren will. Kasparows Seiten wurden deshalb kurz vor geplanten Demonstrationen mehrfach angegriffen.

SEBASTIAN WIDMANN / PICTURE-ALLIANCE/ DPA (L.); MIKHAIL METZEL / AP (M.); JUSTIN JIN / AGENTUR FOCUS (R.)

schen Internet-Sicherheitsfirma Ciphertrust machte allein für diesen Monat mehr als 300 000 neue Bots in Deutschland aus.

„Smertsch“, Windhose, nennt sich das Programm, mit dem Wassilij seine Bots kommandiert. Er tippt die Adresse des Anschlagsziels ein und die Dauer der Attacke. Dann steckt er sich eine Zigarette an, vertritt sich an der frischen Abendluft die Beine. Nach fünf Minuten melden sich seine Cyber-Zombies gefechtsbereit. Mit einem Tastendruck gibt er das Kommando zum Losschlagen.

Die meisten Opfer schweigen. Sie fürchten, das Vertrauen ihrer Kunden zu verlieren, wenn sie die Attacken öffentlich machen. Alexej Bachtiarow allerdings lädt gern in die Büros seiner Firma Infobox in St. Petersburg. Niemals wird er vergessen, wie Hacker am 30. Mai um 11.30 Uhr die Computersysteme seiner Firma ins Visier nahmen. „Die Webpages von mehr als 10 000 Kunden waren für Millionen Besucher nicht mehr zugänglich“, klagt er. Infobox, einer der größten Provider Russlands, betreibt Internet-Seiten für Privatleute, Firmen und Behörden, darunter für den Kreml und die St. Petersburger Stadtverwaltung. „Unsere Reputation hat schwer gelitten“, seufzt Bachtiarow.

Russland gilt als Hochburg der Hacker. General Boris Miroschnikow von einer Spezialeinheit des Innenministeriums hält sie für die besten der Welt.

In einer speckigen Moskauer Wohnung verleiht Ilja Wassiljew, 33, besonders guten Schülern seiner „Bürgerlichen Hackerschule“ seelenruhig einen schwarzen Armreif – so wie es beim Judo für die wahren Meister einen schwarzen Gürtel gibt. Er ist stolz auf seine Jungs. „Sogar aus Deutschland nehmen Leute an meinen Fernkursen teil“, prahlt er.

Eine Zeitschrift mit dem Namen „Chacker“ veröffentlichte jüngst ungestraft eine exakte Anleitung, wie in Web-Seiten ausländischer Regierungen eingedrungen werden kann.

Der Chefredakteur des Blattes, Sergej Pokrowski, bekennt sich dazu, 1999 Natofeindliche Losungen in Nato-Computer in Washington und Brüssel gepflanzt zu haben. Damals hatte das westliche Verteidigungsbündnis den jugoslawischen Diktator Slobodan Milošević, einen Freund Moskaus, mit Bombenangriffen bei seinen ethnischen Säuberungen im Kosovo gestoppt. „Mich haben einfach die Gefühle überwältigt“, sagt der Chefredakteur. „Wir wussten, dass wir dafür nicht bestraft werden.“

YEVGENY KONDAKOV

Hacker-Lehrmeister Wassiljew, Schüler
Die Besten der Welt

In Russland sind DDoS-Attacken zu einer gängigen Praxis geworden. Hetzten dubiose Geschäftsleute in den wilden neunziger Jahren ihren Konkurrenten noch Schlägertrupps oder Auftragsmörder auf den Hals, beauftragen sie heute zunehmend Cyber-Vandalen. Vor allem Firmen wie Infobox, die ihr Geld unmittelbar über oder mit dem Internet verdienen, geraten in das Fadenkreuz der Hacker. So legten Angreifer im Juni die Systeme der Moskauer Firma OSMP für fünf Stunden lahm. Der Schaden für den Anbieter von Online-Zahlungssystemen belief sich auf 150 000 Dollar.

„Es ist einfacher, einen Wettbewerber mit DDoS aus dem Verkehr zu ziehen, als selbst viel Geld in das eigene Marketing zu investieren“, erklärt Paul Sop von der amerikanischen IT-Sicherheitsfirma Prolexic. Sop schätzt die Zahl der täglichen weltweiten Attacken auf rund 10 000.

Das mag übertrieben sein, denn Prolexic verdient gut an der Angst vor Hackern: Die Kunden der Firma zahlen 7000 bis 25 000 Dollar im Monat, dafür können sie, wenn ihre Web-Seiten attackiert werden, auf die großen Hardware-Kapazitäten von Prolexic ausweichen.

„Das Netz ist perfekt für Kriminelle. Das Risiko, geschnappt zu werden, tendiert gegen null“, klagt Sop. „Das sind Zustände wie im Wilden Westen.“

Eher wie im Wilden Osten. Denn es sind insbesondere russischsprachige Hacker, die

im Netz ihre kriminellen Dienste für Geld anbieten und die auch Firmen im Westen bedrohen. Bereits Mitte der neunziger Jahre drang Wladimir Lewin, ein Mathematiker aus St. Petersburg, in den Zentralcomputer des US-Bankriesen Citibank ein und leitete rund zehn Millionen Dollar auf Konten seiner Freunde um.

Vom deutschen Glücksspieleanbieter Fluxx verlangten mutmaßlich osteuropäische Hacker 40 000 Euro, zu überweisen über Western Union, damit sie die DDoS-Attacken gegen das Unternehmen im August 2005 einstellten. Die Deutschen zahlten nicht. Britische sowie andere Online-Casinos und Wettbüros jedoch ließen sich von einer Bande russischer Hacker insgesamt vier Millionen Dollar abpressen.

Auch in der Politik mischen die Cyber-Krieger kräftig mit. Im Frühjahr nahmen sie Seiten der Bewegung „Anderes Russland“ des ehemaligen Schachweltmeisters Garri Kasparow unter Feuer, jeweils kurz vor geplanten Anti-Putin-Demonstrationen. Für die Opposition war das ein schwerer Schlag. Weil der Kreml das Fernsehen und weite Teile der Presse kontrolliert, ist sie auf das Internet angewiesen, wenn sie ihre Anhänger mobilisieren will.

Auch die wenigen unabhängigen Medien haben mit DDoS-Anschlägen zu kämpfen, beispielsweise die regierungskritische Radiostation Echo Moskau. Anfang Mai brach die Web-Seite des Senders unter einem mächtigen Hacker-Angriff zusammen. Vier Tage lang war Echo Moskau zwar weiter auf Sendung, die populären Internet-Seiten aber nicht mehr online.

„Die Attacke war groß, gut geplant und offensichtlich bestellt“, glaubt Chefredakteur Alexej Wenediktow, der den Sender zu einem der profiliertesten Medien Russlands gemacht hat. Er sieht in den Angriffen „ein neues Mittel im Kampf mit aufsässigen Redaktionen. Das war ein Probelauf für die kommenden Wahlen“.

Im Dezember wird ein neues Parlament gewählt, im März das Präsidentenamt vergeben. „Zu meinen Auftraggebern“, brüstet sich ein Hacker namens Sergej, „gehören auch politische Strukturen.“

Ein Angriff etwa auf die Seite von Echo Moskau koste pro Tag nicht mehr als 400 Dollar, verrät er. 400 Dollar – und im Internet verstummt die profilierteste Stimme der Kreml-Kritiker. „Ich kann alles“, prahlt Sergej, „aber alles hat seinen Preis.“

Ende April aber zog Sergej ohne entsprechenden Sold in die Schlacht. Als der Konflikt zwischen Russland und Estland um die Verlegung eines sowjetischen Kriegerdenkmals eskalierte, ließ er seine Cyber-Zombies das Nachbarland angreifen. Wie viele stramm chauvinistisch gesinnte russische Hacker fühlte er sich durch die Esten gekränkt. „Klar habe ich mitgemacht“, sagt Sergej, „aus Idealismus.“ Oder besser gesagt: aus Nationalismus.

Benjamin Bidder

DOKUMENTATIONEN

Jäger und Gejagte

Was geschah wirklich in jener Nacht, als Diana starb? In einer umstrittenen TV-Dokumentation erinnern sich Augenzeugen an die Todesfahrt der Prinzessin.

Die Beute versteckte sich im Hotel Ritz in Paris, die Meute wartete vor der Tür. Ein Routinevorgang, für beide Parteien: Diana, geborene Spencer, geschiedene Princess of Wales, und ihr neuer Lover, der ägyptische Playboy Dodi Al-Fayed, hatten sich schließlich schon den ganzen Sommer über den Fotografen gezeigt. Und deshalb würden die Bilderjäger, die seit Stunden am Hoteleingang herumlungerten, auch diesmal zu ihren Aufnahmen kommen. Das Motiv: Ein Promi-Pärchen steigt, umringt von vielen Schaulustigen, in ein Auto. Eine ganze Branche lebt von solchen Fotos.

Es ist kurz nach Mitternacht am 31. August 1997, einem Sonntag, als Di und Dodi das Hotel verlassen. Wenige Minuten später verunglückt ihr Wagen, auf der Flucht

WTN / TELEPRESS / PANDIS

Fahrer Paul, Liebespaar Diana, Dodi in Paris*
Tod im Tunnel

vor einer Horde Paparazzi, wie bald gemeldet wird. „Ich habe immer damit gerechnet, dass die Presse sie irgendwann umbringen würde“, behauptet Dianas Bruder Charles Spencer, als er am folgenden Morgen den Tod der „Prinzessin des Volkes“ (O-Ton Tony Blair) kommentiert.

Doch was passierte damals wirklich im Autotunnel am Pont de l’Alma, als der schwarze Mercedes 280 S von Di und Dodi um 25 Minuten nach Mitternacht gegen einen Pfeiler krachte? Waren die Fotografen

* Am 31. August 1997, 0.19 Uhr, beim Verlassen des Hotel Ritz (Aufnahme einer Hotel-Überwachungskamera).