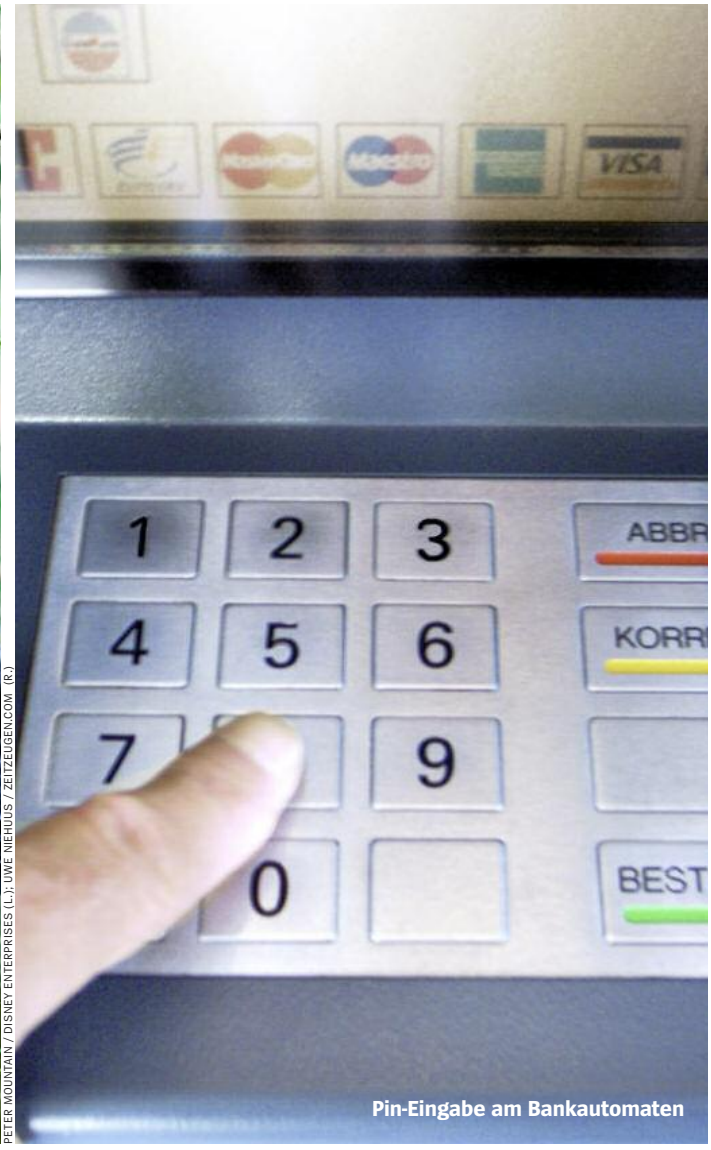
Szene aus „Fluch der Karibik 4“




Pin-Eingabe am Bankautomaten

PETER MOUNTAIN / DISNEY ENTERPRISES (L.); UWE NIEHUUS / ZEITZEUGEN.COM (R.)

## COPYRIGHT-VERSTOSS

Portalbetreiber bieten illegal kopierte Songs oder Kinofilme zum Download oder als Stream an und verdienen dabei Millionen. Auch die Nutzer dieser illegalen Plattformen können sich unter Umständen strafbar machen.

## DATEN-ABGRIFF

Mit Schad-Software infizierte Rechner übermitteln sensible Nutzerdaten wie Passwörter, Pin-Nummern oder Zugangscodes für das Online-Banking an Hacker-Banden.

# Das perfekte Verbrechen

Eine neue Generation von Kriminellen baut sich im Internet eine digitale Unterwelt. Die Gangster bleiben fast immer gesichtslos, ihre Waffen hinterlassen kaum Spuren. Bekannt sind meist nur die Opfer – sie erleiden Schäden in Milliardenhöhe.

Versandzentrum von Amazon

Internetnutzerin im Café

BERNHARD CLASSEN / ACTION PRESS (L.); JOCHEN ZICK / ACTION PRESS (R.)

## WARENBETRUG

Zum Schein angelegte Internetshops verkaufen gegen Vorkasse Waren, die der Käufer nie erhält. Über ein ausgeklügeltes Netz von oft ahnungslosen Finanzagenten verschwindet das Geld in dunkle Kanäle.

## GEKAPERTE RECHNER

Ohne Wissen der Besitzer werden Computer mit Hilfe unbemerkt eingeschleuster Programme Teil von Bot-Netzwerken, die dann mit gezielten simultanen Angriffen auch Websites lahmlegen können.

Der Mann ist Mitte fünfzig und liebt es schnell. Seit mehr als 20 Jahren ist er Taxifahrer in Hamburg, am Wochenende rast er gern mit dem Kite-Buggy über den Sandstrand von St. Peter-Ording.

Die spektakulären Bilder seiner Strandrennen wollte Alp Yücel zu Hause gern hochauflösend sehen und vorzeigen. Er suchte im Internet nach einem billigen Flachbildfernseher. „Das Gerät, das mich interessierte, sollte im Laden 1000 Euro kosten, bei einem Online-Shop gab es das gleiche für 406 Euro“, sagt er.

Bestellt, bezahlt, betrogen: Yücel wartete vergebens auf seinen Fernseher. Er schrieb böse E-Mails an den Verkäufer, aber Sparshopchen24.de reagierte nicht. Dann rief er die Telefonnummer an, die im Impressum stand. Dort wusste man von nichts. Schließlich ging er zur Polizei.

Die sogenannte „Fakeshop-Bande“ hatte wieder zugeschlagen. Yücel wurde offenbar Opfer einer international agierenden, vor kurzem noch unbekannten Cyber-Mafia, die ein florierendes Geschäft mit über 300 Filialen betrieb: virtuelle Shops mit teuren Kameras, die nie verschickt wurden, und iPods, die nie ihren Besteller erreichten. Sogar Goldbarren, Ferienhäuser und Autos boten die falschen Händler ihren Kunden an.

Am 11. Mai war es damit vorbei. Bundesweit rückten über 170 Polizisten aus, sie durchsuchten 29 Büros, Wohnungen und nahmen acht Personen fest, darunter wohl auch die Anführer der mutmaßlichen Verbrecherbande. In Österreich gab es ebenfalls eine Festnahme. Die Ermittlungsakte füllt bereits mehr als 20 000 Seiten und ist noch nicht geschlossen.

Schon jetzt zeichnet sich ab: Die „Fakeshop-Bande“ steht für den bislang wohl größten Betrugsfall im deutschen Online-Handel. Ermittlern zufolge fielen rund 100 000 Kunden, wie Alp Yücel in Hamburg, auf ihre gefälschten Angebote herein. Der Schaden dürfte, so eine erste Schätzung der Polizei, bei über 20 Millionen Euro liegen.

Das Verbrechen bedient sich der digitalen Revolution. Eine neue Generation von Kriminellen baut mit Tatwerkzeugen, die man nicht sehen kann, eine Unterwelt auf, die nur aus elektronischen Impulsen besteht. So bleiben auch die Gangster fast immer gesichtslos, der Tatort lässt sich kaum zurückverfolgen, die Waffen sind Schadprogramme, die durch klassische Spurensicherung kaum zu finden sind.

Sicher ist bislang nur eins: Die Folgen sind alles andere als virtuell. Sie sind real. Schätzungen über den jährlich entstehenden globalen Schaden erreichen teils dreistellige Milliardenbeträge.

Eine ganz besondere New Economy ist so entstanden, sie ist professionell, innovativ und weltweit vernetzt. Und sie führt zu einem Gründerfieber unter Kriminellen: Ständig neue Geschäftsmodelle fluten den Markt, Tausende illegaler Startups versuchen dort ihr Glück.

Die Zuwachsraten sind gewaltig und müssen gewöhnliche Gangster neidisch machen. So zeigt es auch die deutsche Kriminalitätsstatistik: Raub und Erpressung konventioneller Natur sind danach rückläufig, während die Computerkriminalität explodiert.

Mit alarmierenden Zahlen ging das Bundeskriminalamt (BKA) am Donnerstag an die Öffentlichkeit. In seinem Lagebild „Cybercrime 2010“ geht es von rund 60 000 Internetstraftaten im engeren Sinne aus, zum Beispiel Passwortklau – ein Zuwachs von 19,1 Prozent im Vergleich zum Vorjahr. Der finanzielle Schaden stieg in Deutschland in der gleichen Zeit um zwei Drittel – auf 61,5 Millionen Euro. Insgesamt hat das BKA sogar 247 000 Fälle erfasst, in denen das Internet als Tatmittel eine Rolle spielte.

Ebenfalls am Donnerstag stellte der Hightech-Verband Bitkom neue Umfragen vor. 85 Prozent der Befragten fühlen sich demnach von Internetkriminalität bedroht. Und bei immerhin sieben Millionen Deutschen wurden bereits Zugangsdaten etwa zu E-Mail-Diensten oder Bankkonten ausspioniert: fast doppelt so viel wie 2009.

ANDREAS HERZAU / DER SPIEGEL

**Betrugsopfer Yücel:** *Sparshopchen24.de reagierte nicht*

Nicht nur oft ahnungslose Internetnutzer gehören zu den Geschädigten. Selbst Weltkonzerne sind vor den Angriffen nicht gefeit. Gleich mehrfach traf es in den vergangenen Wochen große Elektronik- und Finanzunternehmen: Erst wurden Sony die Daten von über 100 Millionen Kunden gestohlen, dann meldete die Citigroup mehr als 360 000 geklaute Datensätze, schließlich erwischte es Nintendo.

Auch Google wurde überfallen. Bislang nicht identifizierte Hacker knackten gerade zum wiederholten Mal den von Millionen Menschen genutzten E-Mail-Dienst Gmail und drangen in die Konten von US-Regierungsbeamten und chinesischen Aktivisten ein.

Oft zielten die Raubzüge auf Privatadressen und Kontonummern; wertvolle Informationen, die auf Schwarzmärkten verkauft werden können.

Regierungen in aller Welt sind alarmiert. Es geht um den Schutz der Verbraucher, um die Sicherheit im Netz, um mächtige ökonomische Interessen – und auch um nationale Sicherheit.

Spätestens seit der Computervirus Stuxnet vor einem Jahr das iranische Atomprogramm erfolgreich verzögerte, müssen Staaten mit virtuellen Angriffen auf ihre Infrastruktur rechnen. Cyber-Attacken ab einer bestimmten Größenordnung würden künftig als Kriegserklärung betrachtet und mit militärischen Mitteln beantwortet, warnte das US-Verteidigungsministerium vor wenigen Wochen.

Wer steckt hinter den wirtschaftlichen und politischen Attacken? Kann man die Angreifer zur Verantwortung ziehen? Und womit kann man sich gegen sie schützen?

Die Gegner sind so vielseitig wie ihre Motive. Kriminalität, Spionage, Vandalismus und Krieg im Internet haben in der Regel wenig miteinander zu tun – nur in einem, allerdings entscheidenden, Punkt

## Lexikon der digitalen Halbwelt

**Black Hat**
Bösartiger Hacker, in Abgrenzung zum *„White Hat“* (gutartiger Hacker). Oft sind die Übergänge fließend.

**Finanzagent/Money Mule**
Strohmann, der sein Konto für Finanztransaktionen von Web-Gangstern zur Verfügung stellt. Weiß mitunter nichts von einer Geldwäsche.

**FUD**
„Fully undetected“: Getarnte Angriffssoftware, die nicht von herkömmlichen Anti-Viren-Scannern erkannt wird, weil sie z. B. verschlüsselt ist.

**Keylogger**
Spionageprogramm, das etwa Tastatureingaben (z. B. Pins) mitprotokolliert und die Daten unbemerkt an die Adresse des Angreifers verschickt.

**Phishing** *(sprich: „Fisching“)*
Erbeuten von Nutzerdaten wie etwa Kontonummern zum Missbrauch und Weiterverkauf.

**Proxy**
Ein Netzrechner, der dazu dienen kann, Sperren oder Überwachungen zu umgehen, indem Datenpakete nicht direkt von A nach B geleitet werden, sondern sozusagen „über Bande“.

**Ripper**
Betrüger, die an Schwarzmärkten Geld kassieren, aber dann die Ware nicht liefern.

**Zero Day Exploit**
Von Hackern entdeckte Sicherheitslücke, für die es noch keine Schutzmaßnahmen *(„Patches“)* gibt und die deshalb ausgenutzt werden kann.

DER SPIEGEL

kommen sie zusammen: Die Täter nutzen ähnliche Waffen, häufig decken sie sich auf denselben Märkten ein.

Ermittlungsbehörden vom FBI bis zum BKA haben Sonderkommissionen eingerichtet, es gibt nationale Cyber-Abwehrzentren, die Nato hat eigens einen Cyber-Stützpunkt in Estland eröffnet, der Angriffe aus dem Netz abwehren soll.

Und doch ist das Ausmaß der Gefahr für viele immer noch so überraschend wie für den neuen Bundesinnenminister Hans-Peter Friedrich, 54. Als der CSU-Politiker kürzlich zum Antrittsbesuch ins BKA nach Wiesbaden kam, klärten ihn Spezialisten des Referats SO 43 über Internetverbrecher und ihre Methoden auf. Sie führten ihm zum Beispiel den Einsatz von Erpressersoftware vor und zeigten, wie die ergaunerten Milliardenbeträge in einem Labyrinth von internationalen Finanztransfers verschwinden.

Immer wieder schüttelte der Minister ungläubig den Kopf, der Schrecken schien ihm ins Gesicht geschrieben, als die Beamten ihren Vortrag beendeten. Der Titel ihrer Computerpräsentation: „Willkommen im digitalen Untergrund“.

Wochenlang hat der SPIEGEL in dieser Untergrundökonomie recherchiert, er kommunizierte mit Tätern, Opfern und Ermittlern; Spuren führten zu einem jungen Hacker in Österreich und zu einer digitalen Bürgerwehr in Sachsen-Anhalt, die bei der Gangsterjagd schneller war als die Polizei.

Diese Recherchen ermöglichen nun weitreichende Einblicke in die abgeschottete Welt der Online-Kriminalität. Der Fall der „Fakeshop-Bande“, aber auch andere Beispiele und Ermittlungsergebnisse zeigen, wie sich das Verbrechen gerade neu erfindet.

Da gibt es, ganz wie im legalen Teil des Internets, Software-Genies, die ihre Karriere im Kinderzimmer beginnen. Es gibt globale Netzwerke, in denen Entwickler virtuelle Tatwerkzeuge bauen, als ginge es um eine Facebook-Applikation. Es gibt Marktplätze, auf denen Schadprogramme und Bankdaten gehandelt werden wie anderswo Briefmarken oder Bücher: eine Art Ebay für Kriminelle.

Nur elf Jahre ist es her, dass der „I Love You“-Virus das Internet befiel. Er infizierte Hunderttausende Computer weltweit, Rechner stürzten ab, Firmennetze brachen zusammen – ein Milliardenschaden.

Doch es handelte sich um einen Dumme-Jungen-Streich. Der philippinische Student Onel de Guzman, der den Virus programmiert hatte, wollte nur Aufsehen erregen, er verdiente nichts damit und wurde laufengelassen.

Inzwischen sind die Computerviren mutiert, wie man es aus der Biologie kennt: Sie haben sich angepasst an ihren Lebensraum, sie bringen Rechner nur noch selten zum Absturz, stattdessen nisten sie sich unbemerkt ein.

Seitdem ist das nahezu perfekte Verbrechen möglich, ein Delikt, das scheinbar ohne Täter, Tatort und Waffen auskommt und Schäden verursacht, die meistens viel zu spät und manchmal überhaupt nicht bemerkt werden. Es ist nicht einfach, sich dagegen zu schützen. Wer es versuchen will, muss wissen, mit wem er es zu tun hat, und seine Methoden verstehen.

## Täter

Sanft gewellt verlaufen die Weinberge entlang der tschechischen Grenze, hier in Niederösterreich stehen an jeder Ecke Marterln mit Gekreuzigtem, malerische Barock- und Renaissancefassaden schmücken das Städtchen Retz. Bislang war es hauptsächlich für seinen historischen Weinkeller bekannt, den größten des Landes.

In dieser Gegend war bis vor kurzem offenbar eine der vielleicht wichtigsten Anlaufstellen für deutschsprachige Internetkriminelle zu finden: ein Schindelhaus mit Wetterhahn auf dem Dach, zugezogenen Vorhängen und einer Webcam, die das Eingangstor zum dunklen Hof überwacht.

Kein Name steht am Klingelschild, niemand öffnet die Tür.

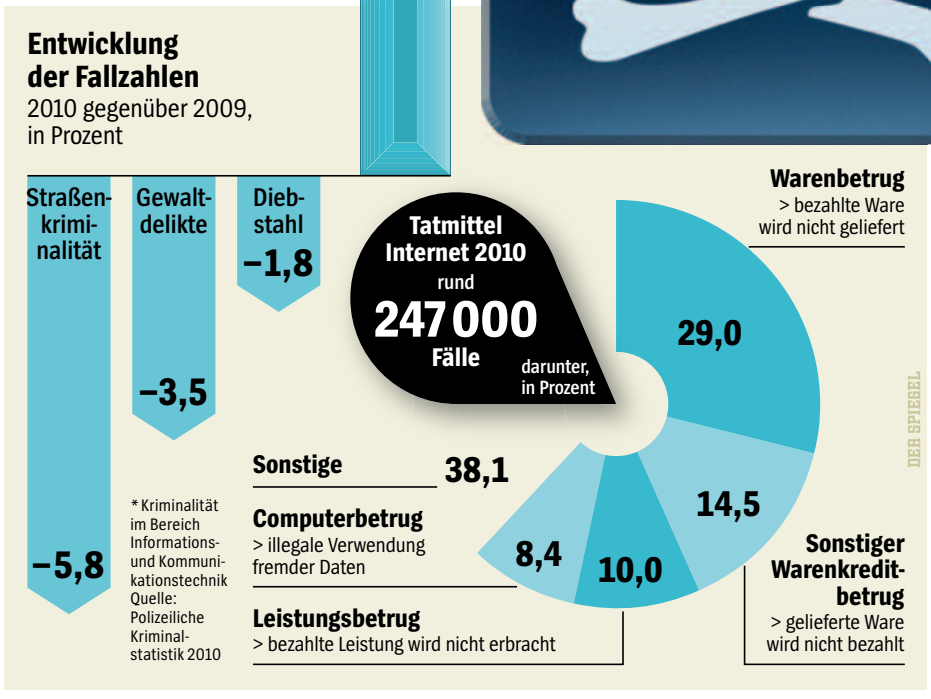
Der Bewohner, im Netz nur als „13speedtest37“ bekannt, ist nicht daheim. Er sitzt in Untersuchungshaft.

Vor ein paar Jahren noch hätte sich ein Kleinkrimineller in der Provinz eher auf das Frisieren von Mopeds spezialisieren können. Heute dagegen bietet der DSL-Anschluss jedem, der will, einen direkten Einstieg in die globalisierte Unterwelt an.

Und „13speedtest37“ – bürgerlicher Name: Dominik B. – ist nach den Erkenntnissen von Ermittlern tief eingestiegen, sehr tief.

Im realen Leben fiel er kaum auf: Ein langhaariger Bursche Anfang 20, von dem Nachbarn und Bekannte sagen, dass er ein ruhiger Typ sei, unauffällig, am öffentlichen Leben in seinem Ort habe er sich praktisch nicht beteiligt.

Umso aktiver und umtriebiger war er im Netz. Seit 2007 kontrollierte Dominik B. vom Weinviertel aus offenkundig das damals wohl wichtigste deutschsprachige Forum im digitalen Untergrund. Er nannte es „1337crew“. Im Slang der Szene,



dem sogenannten Leet-Speak, steht die Ziffernfolge 1337 für „elite“. Und Dominik B. sah sich selbst an deren Spitze.

Unter Rubriken wie „Passwort Cracking“ oder „Online-Betrug“ gab es dort Hacking-Anleitungen und jede Menge illegal erbeuteter Daten. Es erschienen sogar Werbebanner, auf denen andere Anbieter beispielsweise „die geilsten gefälschten Ausweise“ anpriesen. Rund 18 000 Mitglieder zählte die Plattform zuletzt nach eigenen Angaben. Ihr Slogan: „Das beste Hacker-Forum aller Zeiten“.

Dominik B. alias „13speedtest37“ hatte Ermittlern zufolge noch mehr im Angebot: Er soll mit „heihachi.net“ im Geschäft mit sogenannten kugelsicheren Internetpräsenzen mitgemischt haben. Diese bleiben wie Schweizer Nummernkonten anonym und können als Basis für alle möglichen illegalen Aktivitäten genutzt werden.

Dennoch brachten winzige digitale Spuren die Ermittler auf den jungen Mann. 200 Beamte durchsuchten im November 2009 die Wohnungen von B. und rund 50 weiteren Verdächtigen in Deutschland und Österreich; „13speedtest37“ wurde festgenommen, kam nach umfangreichen Aussagen aber wieder frei. Er habe mit der Szene abgeschlossen, schrieb er daraufhin in einer E-Mail, „das war der größte Fehler meines Lebens“.

Lange hielt seine Reue anscheinend nicht. Die Hinweise verdichteten sich, dass B. wieder kriminell aktiv wurde. Am 5. Mai bat ihn der SPIEGEL um ein Hintergrundgespräch. Er antwortete per E-Mail: „Ich denke, ich kann hier nicht behilflich sein.“ Fünf Tage später wurde er erneut verhaftet. Diesmal flog er im Zusammenhang mit den „Fakeshop“-Anbietern auf, die ihre dubiosen Geschäfte mit Kunden wie dem Hamburger Taxifahrer Yücel offenbar über „13speedtest37“ abgewickelt haben. Aktuell wird ihm unter anderem vorgeworfen, für die falschen Online-Händler die Infrastruktur bereitgestellt zu haben.

PAUL HANNA / REUTERS

**Internetaktivisten mit „Anonymous“-Masken:** *„Impulsive, risikofreudige Kinder“*

Die Karriere von Internetkriminellen beginnt früh, viele fangen schon als Teenager an. Im Gegensatz zu Hackern der ersten Generation sind profunde Software-Kenntnisse und eine teure Hardware-Ausstattung heute nicht mehr grundsätzlich erforderlich. Oft reicht ein einfaches Netbook für 250 Euro, der Rest ist in Leitfäden für den Nachwuchs („tutorials“) schnell zu lernen.

Auch das von Forschern und Hollywood-Regisseuren lange gepflegte Image von pickeligen Einzelgängern aus kaputten Mittelklassefamilien, den sogenannten Crackern, ist nicht mehr aktuell.

Die Nachfolger sind bunt gemischte, kontaktfreudige Anhänger der Facebook-Generation. „Es handelt sich meist um impulsive, risikofreudige Kinder“, sagt Thomas Holt von der School of Criminal Justice an der Michigan State University; diese Kinder neigten dazu, „eine Chance schneller zu ergreifen als andere“. Das ideale Profil eines Firmengründers würde sich ähnlich lesen.

Wie in der altmodischen Gangsterwelt gibt es im digitalen Untergrund verschiedene Verbrechertypen. Neben „Multitalenten“ wie Dominik B. durchstreifen auch klassische Diebe das Netz – sowie Erpresser und Gesinnungstäter.

Zwei jungen Hackern aus dem Ruhrgebiet zum Beispiel gelang es, unveröffentlichte Songs von Lady Gaga und anderen zu klauen und dann für rund 15 000 Euro weiterzuverkaufen. Popfans und Internetexperten staunten gleichermaßen über den digitalen Raubzug der beiden.

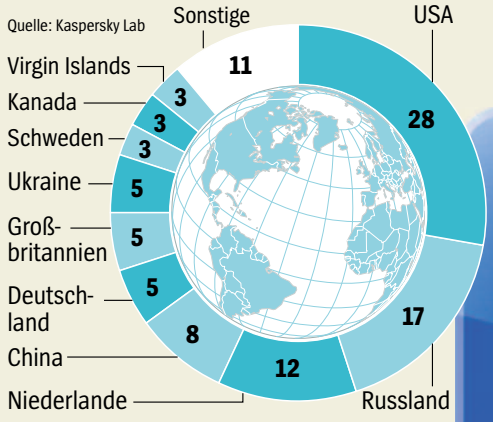
Urheberrechtsverletzungen in viel größerem Ausmaß betrieben offenbar auch die Macher von kino.to, einem Filmportal, auf dem täglich vier Millionen Besucher die neuesten Hollywood-Produktionen online anschauten. Vor wenigen Wochen schlugen Ermittler zu und beschlagnahmten mehrere Luxuswagen und 2,5 Millionen Euro, die im Besitz der Gruppe waren. Ihr mutmaßlicher Anführer, ein Leipziger Bodenleger, sitzt seit Anfang Juni in Untersuchungshaft.

Findige Trickbetrüger setzten auf sogenannte Scareware, die ängstlichen Internetnutzern vorgaukelte, ihr Computer sei mit Viren infiziert. Dann wurden die Opfer aufgefordert, eine Antivirensoftware herunterzuladen und per Kreditkarte bis zu 129 Dollar zu zahlen. Wer drauf reinfiel, hatte gleich dreimal Pech: Der vorher gesunde Computer war nun infiziert, das Geld weg und die Kreditkartennummer in falschen Händen. Drei Jahre lang lief dieser Trick, 960 000 Menschen glaubten den Warnungen der „Scareware“-Bande, die in ihrer

**Aufkommen verschickter Schadprogramme**

Anteil nach Ländern, I. Quartal 2011, in Prozent

Quelle: Kaspersky Lab




**Neue Schadprogramm-varianten**
weltweit, 2010

über 2 Mio.

Quelle: G Data Malware Report 2/2010

DER SPIEGEL

Software offenbar Zeitgeist, Psychologie und kriminelle Energie auf besonders kreative Weise verband.

Zur Erpresserkategorie zählen Fahnder Oliver S., einen arbeitslosen, zeitweise auch obdachlosen Mittzwanziger aus Frankfurt am Main, der sich nach dem Hamburger Freibeuter Klaus Störtebeker benannte. Für 65 Dollar im Monat mietete sich „Störtebeker“ in Russland Rechnerkapazitäten, um Websites lahmzulegen. Dann bedrohte er ein Online-Portal für Pferdewetten und lieferte gleich den Beweis seiner Feuerkraft mit, indem er es fünf Stunden lang blockierte.

„Störtebeker“ verlangte zunächst 2500 Euro; sollte nicht gezahlt werden, drohte er, das Wettportal ausgerechnet während des Derby-Meetings in Hamburg lahmzulegen. Für die Anbieter der Pferdewetten wäre dies eine finanzielle Katastrophe gewesen. Ähnliche Drohungen gingen an sechs weitere Zocker-Seiten.

Oliver S. wurde geschnappt, aber das Erpressungsgeschäft floriert, nicht zuletzt wegen der geringen Anfangsinvestitionen. Viele Unternehmen zeigen zudem Erpressungsversuche nicht an, um Nachahmer nicht zu ermuntern. „Pizzeria 2.0“ nennen Experten des BKA intern diese Form von Internetkriminalität: Online-Erpresser würden wie die klassische Mafia ganz schlicht auf Einschüchterung und Schutzgeldforderungen setzen, sagen sie.

Und dann sind da noch Überzeugungstäter wie „Anonymous“ oder „LulzSec“: lose, politisch motivierte Gruppierungen, die kein Geld wollen, sondern bloß Aufmerksamkeit. Wie „Störtebeker“ legen sie mit Attacken die Websites ihrer Opfer lahm.

In den USA traf es zum Beispiel Visa und PayPal, weil sie es gewagt hatten, Geschäfte mit der Enthüllerplattform WikiLeaks zu beenden. Auch der TV-Sender Fox wurde attackiert – anscheinend weil dessen konservatives Programm der Spaßguerilla von „LulzSec“ missfiel.

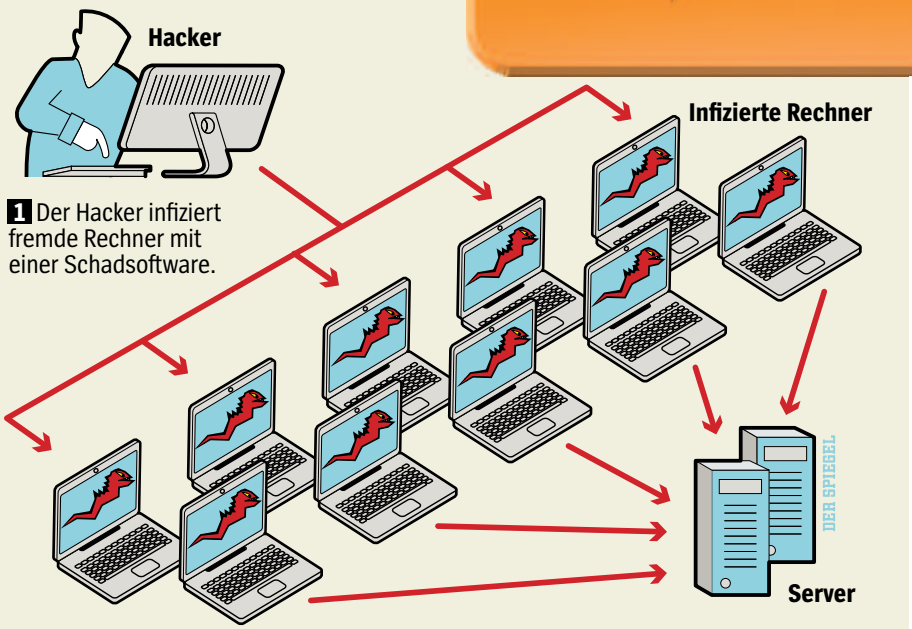
## Tatwaffen

Es braucht nur ein paar Klicks, es reicht, einschlägige Suchbegriffe zu googeln, schon öffnen sich die Türen zu gigantischen Schwarzmärkten, auf denen alles zu finden ist, was derzeit in Mode ist: Angriffssoftware, Viren oder sogenannte Phishing-Programme.

„Verkaufe die Privatversion meines Keyloggers“, preist ein „Viotto“ seine Ware auf einem dieser Basare an, deren Server oft im Pazifikraum stehen, auf Samoa, einem Inselreich, dessen Behörden legendär widerwillig sind, auf Rechtshilfeersuchen zu reagieren.

Keylogger sind Spionageprogramme, die auf fremden Computern installiert werden, um alles zu protokollieren, was ein Nutzer eintippt, zum Beispiel Passwörter oder Kreditkartennummern. Dann werden diese Daten im Hintergrund an den Angreifer verschickt. Das Opfer merkt davon meist erst, wenn auf seinen Kontoauszügen merkwürdige Abbuchungen zu finden sind.

### Wie Hacker ganze Datendienste lahmlegen




**1** Der Hacker infiziert fremde Rechner mit einer Schadsoftware.

**2** Mit einem Befehl von außen kann der Hacker sämtliche infizierte Rechner miteinander koppeln und für seine Zwecke nutzen („Botnet“).

**3** So können etwa mit simultan verschickten Anfragen auf ausgewählte Server diese überlastet, verlangsamt und schließlich arbeitsunfähig gemacht werden („Denial of Service“).

Bei „Viotto“, der sich als ehemaliger Informatikstudent aus Rom ausgibt, sind Keylogger für nur 30 Euro zu haben, inklusive „lebenslang kostenlose Updates“. Eine möglichst kompetente Beratung gehört dabei selbstverständlich dazu, alles findet öffentlich statt.

Jeder kann mitlesen, wenn sich ein Kunde bei „Viotto“ beschwert, weil sein neues Spionageprogramm von einer Antivirensoftware blockiert wird: „Wat is problem?“ Wenn dann alle Hürden beseitigt sind, steht einem Raubzug durch fremde Rechner nichts mehr im Weg.

Auch Botnets – das sind Netzwerke, die aus Zigtausenden infizierten Privatrechnern bestehen – sind auf dem Schwarzmarkt leicht anzumieten. Über sie lassen sich beispielsweise massenhaft unerwünschte Werbe-Mails („Spam“) verschicken, die bei Millionen Nutzern die Inbox mit Angeboten etwa für „Penisverlängerungen“ oder „sagenhafte Renditen“ verstopfen.

Doch das ist nur eine der harmloseren Einsatzmöglichkeiten: Wer ein Botnet dirigiert, kann damit Websites lahmlegen, indem er gleichzeitig und wiederholt Zehntausende Privatrechner eine bestimmte Adresse besuchen lässt, bis sie zusammenbricht („Denial of Service“). Mit dieser Methode hatte zum Beispiel „Störtebeker“ Pferdewett-Portale attackiert. Auch Dominik B. soll ein solches Heer von aggressiven Zombierechnern kommandiert haben.

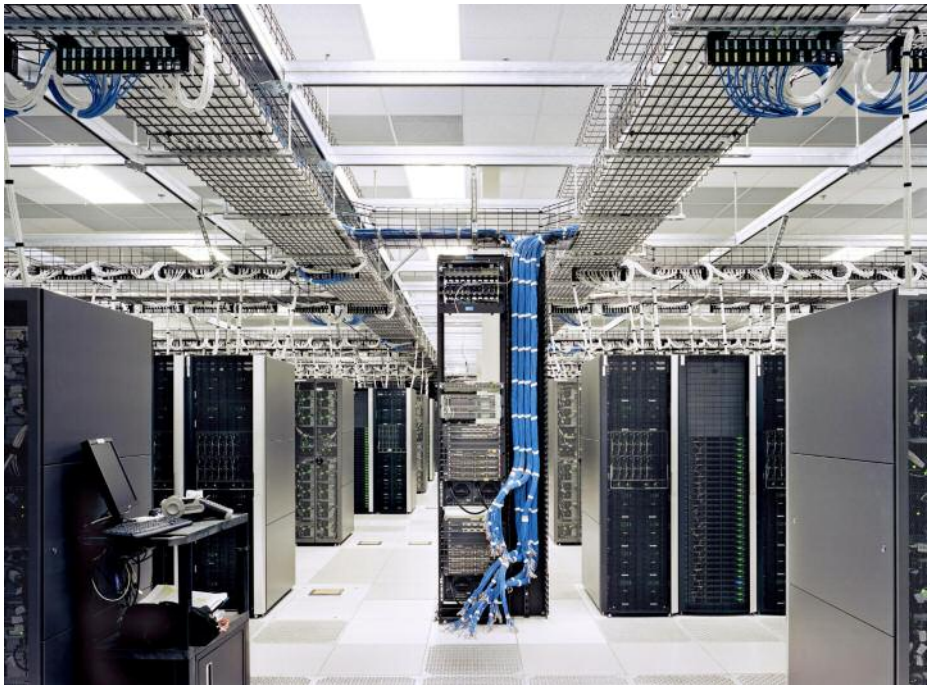
Auf ähnliche Weise lässt sich Werbekunden vorgaukeln, dass ihre Internetbanner von Millionen Nutzern besucht und angeklickt werden – während in Wahrheit ein anonymes Botnet diesen Job erledigt. Fast 19 Prozent aller Klicks auf Werbebanner sind nicht von Menschen gemacht, sondern von ferngesteuerten Botnet-Rechnern, schätzt die Sicherheitsfirma Click Forensics. In der Werbebranche ist dieser Betrug als „Click Fraud“ gefürchtet.

Aus Gangstersicht das Beste an der neuen Technik: Diese Netze lassen sich ganz einfach mieten, für nur wenige Dollar pro Tag. Eine Vielzahl von Anbietern hält große Armeen solcher ferngelenkter Rechner bereit. Allein das „Coreflood“-Netz verursachte mit 800 000 infizierten Rechnern einen Schaden von bis zu 100

Millionen Dollar innerhalb von zehn Jahren. Im April wurde es von US-Behörden abgeschaltet.

Die neueste, leistungsstärkste Generation von Botnets („TDL 4“) umfasst laut Experten mindestens 4,5 Millionen Rechner und gilt in der Branche vorläufig als „unzerstörbar“. Dass die Besitzer der missbrauchten Computer von solchen Innovationen und Eingriffen nichts mitbekommen, versteht sich in der Szene von allein.

„Selbst technikferne Anfänger klicken sich die von Profis angebotene Software für ihre illegalen Geschäftsideen zusammen“, sagt Thomas Holt, der Dozent aus Michigan, der auch das Täterprofil von Internetkriminellen untersucht hat. Er beherrscht den Slang der digitalen Schwarzmärkte und hält über ein Pseudonym Kontakt zu den dort agierenden Kriminellen.



SIMON NORFOLK / AGENTUR FOCUS

**Amerikanischer Serverraum:** *Selbst Hightech-Konzerne sind vor Angriffen nicht gefeit*

Holt ist fasziniert, wie prächtig die Märkte funktionieren, angesichts der Tatsache, dass jede Transaktion anonym abläuft und illegal ist. „Der Kundenservice ist oft gut, die Anbieter sind teils rund um die Uhr erreichbar“, sagt er.

Wenn zum Beispiel gestohlene Kreditkartennummern gesperrt sind, bieten viele Hehler umgehend Ersatz an. Andere melden sich freundlich bei ihren kriminellen Kunden ab, wenn sie verreisen. „Ich fahre in den Urlaub, daher bin ich nicht immer erreichbar“, heißt das dann etwa bei einem Hehler, der sich „Ca$$$$hboi“ nennt.

Gangsterehre ist in der virtuellen Szene offenkundig noch viel wichtiger als im realen Leben, gerade weil man sich nicht persönlich kennt. Wie bei Ebay vergeben Schwarzmarktforen deshalb Qualitätsnoten wie „Verified Seller“. Nur wer erprobte, funktionierende Ware verkauft, bekommt das begehrte Gütesiegel.

Wer trickst oder schlechte Software vertickt, wird an den Pranger des Netzes gestellt und bestenfalls als Stümper verlacht – oder gleich als Abzocker beschimpft und gesperrt.

So hat sich eine seltsame Moral herausgebildet, denn selbst Schwarzmärkte blühen nur auf der Basis von Vertrauen. Nirgendwo ist dies so wichtig wie beim Kreditkartenklau. Das sogenannte Carding ist die Königsdisziplin, hier kommen alle Branchen der Untergrundökonomie zusammen.

Die komplizierte Transaktion beginnt mit einer Spam-Mail zum Beispiel aus Russland, die einem Empfänger in Deutschland vortäuscht, dass mit seiner Kreditkarte etwas nicht stimmt. Am Ende, nach Einsatz diverser Phishing- oder Keylogger-Instrumente, hat das Opfer oder das Geldinstitut oft viele tausend Euro verloren.

Fehler dürfen bei solchen Raubzügen nicht passieren. „Wir spielen hier ein gefährliches Spiel, und daher müssen Verkäufer ehrlich sein“, mahnt ein Kreditkartenhehler, „ich brauche absolute Ehrlichkeit über das Zeug, das ich kaufe.“

## Handlanger und Hintermänner

Betrug, Erpressung, Rufmord und Abzocke im Netz, all das ist relativ einfach: Die Software lässt sich billig mieten. Die Server stehen im Ausland, die Kommunikation läuft verschlüsselt, die Anonymität der Täter lässt sich auf vielerlei Weise schützen.

Doch es gibt in fast allen Bereichen der Internetkriminalität einen Moment der Wahrheit. Irgendwann müssen online ergaunerte Waren oder Euro zu den Tätern gelangen.

Wie kam zum Beispiel die „Fakeshop-Bande“ an das Geld ihrer gutgläubigen Kunden? Was passierte mit den 406 Euro, die in Hamburg Alp Yücel für einen Flachbildfernseher an „sparshopchen24.de“ überwiesen hatte?

Die Gangster konnten dafür schließlich nicht ihre eigenen Konten verwenden, dann wären sie sofort aufgeflogen. Deshalb baten sie offenbar fremde Menschen, ihnen ihr Konto für diesen Zweck „auszuleihen“, gegen eine Mietgebühr von 400 oder 600 Euro pro Monat.

„Ich war arbeitslos und brauchte Geld“, sagt Felix H. aus einem kleinen Ort bei Chemnitz. Eigentlich wollte der Endzwanziger sich selbständig machen mit seiner Musik, er spielt Gitarre und singt, er liebt Pavarotti und Mozart. Auf einer Web-Seite hatte er ein Jobangebot gesehen, das ein Nebeneinkommen von 600 Euro im Monat versprach. Er meldete sich. Ein gewisser Silvio T. aus Gela in Italien schickte ihm per E-Mail einen „Vertrag über ein Deutsches Giro Konto“.

Der Sänger aus Sachsen eröffnete ein Postbank-Konto und schickte die Zugangscodes an den Fremden in Italien. So wurde er zum Handlanger der „Fakeshop-Bande“, ohne so ganz genau zu wissen, mit wem er es zu tun hatte und was mit seiner neuen Bankverbindung geschehen sollte.

Im Februar 2010 landeten die ersten 1000 Euro auf dem Konto. Dann kamen die nächsten Tranchen, insgesamt rund 20 000 Euro. Wann immer Beträge eingingen, wurden sie schnell wieder abgebucht von dem Fremden. Bis die Postbank das Konto sperrte.

Das Geld kam von Kunden wie Yücel. Sie stellten Überweisungen auf sein Konto aus und glaubten, bald die bezahlten Produkte zugeschickt zu bekommen.

Felix H. war nicht der einzige Geldesel der „Fakeshop-Bande“. Etwa tausend solcher Handlanger – Ermittler sprechen von „Finanzagenten“ – warben die Gangster an.

Der Sänger ist jetzt wegen Geldwäsche angeklagt und soll für die Schäden haften. „Mir tun die armen Leute leid, die da beschissen worden sind“, sagt Felix H. Allerdings sieht er sich auch selbst als Opfer der Bande, er hält sich für unschuldig und hat Anzeige gegen unbekannt erstattet.

Die Anwerbemethoden der „Fakeshop“-Betrüger waren nicht einmal besonders ausgefeilt. Andere Gruppierungen gehen weitaus professioneller vor, sie verlangen ausführliche Bewerbungsschreiben von den Leuten, die sie benutzen wollen.

„Der Arbeitsvertrag, auf den ich reingefallen bin, war richtig gut gemacht, ich kenne mich mit so etwas aus“, sagt etwa

Günter M., Mitte 50, ein Diplom-Kaufmann aus dem Schwarzwald.

Er bewarb sich als „Repräsentant und Handelsagent“ bei einer Firma, die angeblich im amerikanischen Richmond sitzt. Er bekam einen „Arbeitsvertrag über eine geringfügige Beschäftigung“ zugeschickt, in dem ihm eine Provision von fünf Prozent in Aussicht gestellt wurde – für alle Beträge, die über sein Konto laufen. Im März traf die erste Zahlung ein: 1940 Euro.

M. hob das Geld ab und ging zu einer Tankstelle. Dort kaufte er im gleichen Wert anonyme Gutscheine der Firma Ukash. Diese Gutscheine sind mit 19-stelligen Transaktionsnummern versehen. M. musste jetzt nur noch diese Zahlenkolonnen an seine Partner mailen, und schon war die Geldwäsche perfekt: Die Dunkelmänner konnten den Betrag nun weltweit an Ukash-Standpunkten zu Bargeld machen oder für Internetkäufe nutzen.

Doch schon drei Tage danach wurde M.s Konto gesperrt, die Bank forderte das Geld zurück. Einen Monat später flatterte ihm ein Strafbefehl ins Haus, im Juli 2010 wurde der Diplom-Kaufmann wegen „leichtfertiger Geldwäsche“ zu einer Gesamtstrafe von 500 Euro verurteilt.

Ohne Handlanger wie M. und Felix H. würde das globale Cyber-Crime kaum funktionieren. Sie sind meist die Ersten, die erwischt und verurteilt werden. Und wenn die Ermittler Glück haben, werden sie auf ein paar merkwürdige Überweisungen aufmerksam – und schon sind sie bei Gangs wie der „Fakeshop-Bande“. Dann fliegt auch mal ein ganzes Netzwerk auf.

STEPHAN SAHM / DER SPIEGEL

**Ermittlerin Nagel:** *„Das waren Profis“*

Die Hintermänner dagegen werden nur selten gefasst. Es handelt sich um Geldgeber, die sich manchmal ähnlich wie Investoren im Silicon Valley verhalten und – wie sogenannte Business Angels – besonders innovative Gründer aus der Hacker-Szene finanzieren. Auch kann es vorkommen, dass sie bei Bandenkriegen die Strippen ziehen oder die feindliche Übernahme gegnerischer Foren betreiben. Die passenden Stichworte aus der Geschäftswelt heißen „unfriendly takeover“ oder „mergers & acquisitions“.

Allerdings stehen dahinter nicht klassische Venture-Capital-Firmen.

In seinem Buch „Fatal System Error“ beschreibt der US-Autor Joseph Menn, wie britische und amerikanische Ermittler nach einem millionenschweren Betrug von Citibank-Kunden die Spur des Geldes bis in die obersten Etagen der Kriminellen-Organisation verfolgten. Und dann in der russischen Republik Dagestan an ihre Grenzen stießen. Dort lebt Artur G., in einschlägigen Online-Kreisen auch als „King Arthur“ bekannt; nach Überzeugung der Fahnder ist er einer der wichtigsten Hintermänner im digitalen Untergrund. Doch die russischen Behörden verweigerten die Zusammenarbeit, „King Arthur“ hat anscheinend gute Verbindungen in die Politik.

Geld, Schutz, beste politische Kontakte: Die Hintermänner von Cyber-Verbrechen stammen häufig aus der Mafia, sagt Menn. Russische und italienische Paten, chinesische Triaden, japanische Yakuza oder südamerikanische Drogenkartelle reagieren offenbar besonders gewandt auf neue Business-Chancen im Internet.

## Verfolger

Verbrecher und ihre Verfolger liefern sich dabei einen Wettlauf um die modernste Technik, die besten Ressourcen und die raffinierteste Tarnung. Nicht immer sind es Ermittlungsbehörden, denen dabei die schnellsten Erfolge gelingen.

„Schau mal, dieser Shop hier kommt mir verdächtig vor“, sagt die schlanke, langhaarige Frau, die sich im Netz „Eclipse“ nennt – Sonnenfinsternis. „Ja, den sollten wir mal etwas genauer beobachten“, sagt der Teenager neben ihr. Er kommt gerade aus der Schule, sie von der Arbeit. Sie sitzen bei Kaffee und Kakao in einem Internetcafé irgendwo in Sachsen-Anhalt und beugen sich über ein Notebook. Immer wieder schauen sie sich nervös um, ob sie beobachtet werden. Ihre Namen im „RL“, dem „Real Life“, wollen sie nicht veröffentlicht sehen. Sie sind Mutter und Sohn, und sie fürchten Vergeltung. Drohungen gab es schon.

Die beiden sind Mitorganisatoren eines Webforums namens autosec4u.info, das sich als digitale Bürgerwehr der Jagd auf Internetbetrüger verschrieben hat. Manch-

## Wie bewegt man sich sicher im Internet?

Wer seinen Computer mit dem Internet verbindet, läuft Gefahr, ausgespäht und abgezockt zu werden. Auch Antivirensoftware und Firewalls schützen nur bedingt.

**Virenschutzprogramme**

lohnen schon aus juristischen Gründen. Denn sollte das Konto geplündert werden, verlangen Banken oft den Beweis, dass man sich geschützt hat.

**Passwörter**

sollten einmal monatlich geändert werden, mindestens zehn Zeichen lang sein, Sonderzeichen und Zahlen umfassen und nicht auf dem Rechner gespeichert sein.

**Transaktionsnummer (Tan)**

Banküberweisungen sollten wenn möglich mit modernen Verfahren wie Chip-Tan oder SMS-Tan autorisiert werden. Die Ära der Tan-Liste auf Papier geht zu Ende.

**Persönliche Daten**

Phishing und Scareware-Botschaften gaukeln oft vor, dass der Computer infiziert ist, dass ein Bankkonto gesperrt wurde und man daher schnell persönliche Daten eingeben soll. Diese Botschaften wirken auf den ersten Blick seriös und protzen oft mit Autorität, offiziellen Logos, Dringlichkeit und setzen auf Angst und Gier. Auf den zweiten Blick fallen oft Rechtschreibfehler und Freemail-Adressen auf.

DER SPIEGEL

**Online-Shopping**

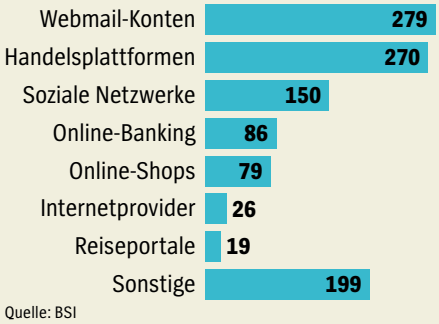
Beim Online-Einkaufen bieten große Portale oft auch größere Sicherheit. Bei kleineren Anbietern lohnt sich ein genauer Blick ins Impressum und ein Testanruf. Ist der angebotene Preis absurd niedrig? Überweisungen per Vorkasse sind leichtsinnig.

## Gestohlene Daten ...

... werden durch Schadprogramme auf von den Tätern kontrollierte Server im Internet („Dropzones“) übertragen. In Deutschland konnten im Jahr 2010 Datensätze aus etwa 200 Dropzones analysiert werden.

insgesamt rund **1,1 Mio.** Datensätze

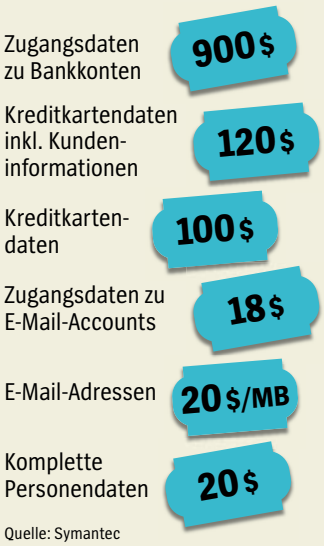
**Herkunft der Datensätze**
in tausend




Quelle: BSI

## ... und ihr Marktwert

Maximale Preise für gestohlene Daten auf dem Schwarzmarkt




Quelle: Symantec

DER SPIEGEL

mal dauert es nur wenige Stunden, bis sich Opfer neuer Abzocker-Websites hier zu Wort melden. Dann beginnen die Forumsmitglieder zu recherchieren.

In diesem Frühjahr feierten sie mit ihren Mitstreitern, die sie nur über das Netz kennen, ihren bislang größten Erfolg. Sie warnten bereits vor der sogenannten „Fakeshop-Bande“, bevor die Kriminalpolizei mit ihren Ermittlungen begann.

Angefangen hat ihr Engagement im April 2009 mit dem Thermomix „TM 31“, einer Küchenmaschine der Firma Vorwerk. Eine Mitstreiterin mit dem Pseudonym „Asterix“ hatte damals begonnen, in einem anderen Forum die Namen der vermeintlichen Anbieter zu veröffentlichen. Ihre Motivation: Die Betrüger hatten ihren Vater reingelegt. Er machte mit seiner Küchenmaschine die gleiche Erfahrung wie der Hamburger Yücel mit seinem Flachbildfernseher. Die Ware wurde zum halben Preis angeboten, per Vorkasse bezahlt, aber nie geliefert.

Die Digitaldetektive merkten schnell, dass sie etwas Größerem auf der Spur waren, immer häufiger gab es in ihrem Forum frische Einträge über neue Abzock-Seiten. Und immer, wenn eine aufflog und geschlossen wurde, entstanden dafür ein paar neue.

Irgendwann kontaktierten sie die Polizei in Düren bei Köln, weil dort einer der Online-Shops gemeldet war. Der Polizist war dankbar und freundlich, konnte aber nicht helfen. Das Impressum war falsch, andere Spuren gab es vorerst nicht.

Deshalb perfektionierten „Asterix“ und ihre Mitstreiter ihr System. Gezielt googelten sie nach Produkten, welche die „Fakeshop-Bande“ in ihren Läden anbot. Sie stellten fest: Häufig tauchten diese Produkte in bezahlten Google-Anzeigen neben den Suchergebnissen auf.

Wer zum Beispiel nach der Vorwerk-Küchenmaschine suchte, konnte schnell auf Anzeigen für das Produkt stoßen, die zum jeweils neuesten „Fakeshop“ führten. Die Verbrecher betrieben offenbar gezieltes Marketing. Und Google verdiente mit.

Fortan konnten die Aktivisten vor neuen Websites der Serientäter warnen, bevor sich die ersten Opfer meldeten. Sie veröffentlichten jetzt Screenshots der gefährlichen Seiten.

Natürlich blieb dies den Abzockern nicht verborgen. Die Netzbürgerwehr hatte ihr Geschäftsmodell nicht nur durchschaut, sie störte es jetzt auch empfindlich. Prompt setzten die Betrüger die Website von autosec4u.info unter Dauerbeschuss, um das Forum zu blockieren; doch ohne Erfolg.

Als Nächstes versuchten sie es mit Drohungen an die Betreiber. „nette wohnung hast du da in einem mehrfamilenwohnungsanlage aus neben einer kaputten schule. Hundewiese kleidercountainer und kamera überwacht. Hoffe du hast es gemütlich oben in 4. stock“, hieß es in Hass-Mails, die unter dem Pseudonym Silvio T. verschickt wurden.

Sie bedrohten einzelne Forenmitglieder persönlich, die Mails waren trotz orthografischer Defizite unmissverständlich: „Du hast mich eine menge geld gekostet daher habe ich richtig investiert um dich zu finden. Seid tagen sind mehrere Leute von einer sogenannten Berliner Libanische mafia in deiner gegend die nur auf mein Kommando warten um dich zu bekommen.“

Der Gauner meldete sich immer wieder, nun unter dem Pseudonym „derhaha“. Für jeden geschlossenen Shop mache er fünf neue auf, hieß es in einer Botschaft. Mal prahlte er mit seinen Einnahmen („habe dicke Sache am laufen jeden tag kommen 80 000 Euro“), mal versprach er, ein Bild seines neuen Porsche zu schicken. Erwischen könne man ihn ohnehin nicht: „Ich bin in einem Asien Land und wechsel die Internetcafes nach 1-2 Stunden. Macht Euch um meine Sicherheit keine Sorgen.“

Doch dann machte er einen Fehler, nur einen einzigen, aber der reichte. „Ich war gerade in einem anderen Netzforum unterwegs, als sich ‚derhaha‘ dort einloggte“, erzählt Hobbydetektivin „Eclipse“. Sie prüfte, mit welcher Rechnerkennung er unterwegs war – und war wie elektrisiert. Zum ersten Mal hatte ihr Gegenspieler offenbar vergessen, seine Identität zu schützen, zum ersten Mal war seine IP-Adresse für sie sichtbar.

Sie griff zum Telefon und informierte die Polizei. Endlich hatten die Beamten des bereits ermittelnden Bayerischen Landeskriminalamts einen konkreten Ansatz und konnten mit herkömmlichen Ermittlungsmethoden dem Verdächtigen nachstellen: Telefonüberwachung, Observation, Kontenabfragen.

Viele Spuren der „Fakeshop-Bande“ führten schließlich nach Essen zu dem Deutsch-Iraker Karwan M. und einem befreundeten Deutsch-Türken. Sogar einen Porsche fanden die Fahnder in ihrem Umfeld – zumindest in diesem Punkt hatte „derhaha“ offenbar nicht getäuscht.

„Das waren Profis, die haben das wie eine multinationale Firma betrieben“, sagt Sabine Nagel vom Bayerischen Landeskriminalamt fast anerkennend. Eine Abteilung der „Fakeshop-Bande“ habe sich um die Technik gekümmert, andere um das Web-Design und um die Finanzströme. Sogar Marktforschung habe die Bande betrieben: Rechtzeitig zum Goldhype an den Rohstoffmärkten hatte sie im Netz mehrere fiktive Goldshops online gestellt.

„Asterix“ und ihre Verbündeten in der digitalen Bürgerwehr freuen sich über den Erfolg. Ohne ihre Arbeit wäre die

„Fakeshop-Bande“ womöglich heute noch aktiv. „Eigentlich müssten die Warnungen vor Betrügern und falschen Konten von den Banken und der Polizei gemacht werden, nicht von uns“, sagt Forumsmitglied „Eclipse“. Die Frau aus Sachsen-Anhalt macht sich keine Illusionen: „Für jede Betrüger-Website, die auffliegt, entstehen unter anderen Namen zehn neue Shops.“

## Was tun?

Solche Erkenntnisse führten in den USA bereits vor Jahren zu Konsequenzen. Geheimdienste, Polizei, Hightech-Konzerne, Banken und Universitäten arbeiten eng zusammen. Schon 1997 gründeten sie die „National Cyber-Forensics & Training Alliance“, einen Zusammenschluss von heute 15 Behörden und 40 Unternehmen.

Wer virtuelle Verbrechen melden will, kann das bequem durch ein paar Klicks auf ihrer Web-Seite erledigen. Unternehmen und Behörden tauschen, wenn der Verdacht stichhaltig ist, zügig ihre Erkenntnisse aus, um Spuren zu verfolgen, solange sie noch frisch sind.

Vor allem das FBI setzt dabei auf unkonventionelle Methoden. Rund ein Viertel aller Hacker in den USA seien Informanten des FBI, vermutet das Szenemagazin „2600“. Etliche Online-Schwarzmärkte sind offenbar von „Special Agents“ des Bureaus unterwandert.

So kommt es immer wieder zu spektakulären Fahndungserfolgen. Dem Betreiber der illegalen Kreditkartenbörse cardersmarket.com, auf der sich zeitweise bis zu 6000 Online-Kriminelle mit geklauten Visa- oder Mastercard-Nummern versorgten, machte das FBI 2007 den Laden dicht.

Ein anderes Forum namens Darkmarket.ws wurde sogar direkt von einem Regierungsagenten geführt, der unter dem Pseudonym „Master Splynter“ auftrat und zwei Jahre lang die Mitglieder seines Forums ausspähen konnte. Und erst vor knapp zwei Wochen kam es zu einer weltweiten Razzia (Operation „Trident Tribunal“), in der das FBI mit Ermittlern aus elf Ländern, darunter auch der Bundesrepublik, 40 Computer und etliche Bankkonten eines mutmaßlichen Erpresserrings beschlagnahmte. Die Bande soll einen Schaden von 74 Millionen Dollar verursacht haben.

In Deutschland suchen die Behörden noch nach einer angemessenen Antwort auf die Bedrohung. Erst im Juni eröffnete Bundesinnenminister Friedrich offiziell ein neues „Nationales Cyber-Abwehrzentrum“ in Bonn. Es soll mögliche Angriffe auf staatliche Einrichtungen verhindern helfen, aber auch schwere Fälle von Internetkriminalität analysieren.

Der Begriff klingt nach Science-Fiction, nach einer hochmodernen Kommandobrücke mit Hunderten Flachbildschirmen und einer schlagkräftigen, kompaniestarken Einsatztruppe. Tatsächlich schritt Friedrich an wenigen Mitarbeitern vorbei durch ein paar Behördenbüros, an denen große Papierkarten wie aus dem Erdkundeunterricht an die Wände drapiert waren; auf den Karten sind die deutschen Elektrizitäts- und Gasnetze zu erkennen. Der Minister sprach dann auch eher kleinlaut von einem ersten Schritt.

**Hobbydetektivin „Eclipse“ mit Sohn:** *Verdächtiger Shop*

Deutschland ist bei Cyber-Kriminellen sehr beliebt, besonders bei Botnet-Betreibern, weil das Netz hier leistungsstark ist und viele Nutzer Flatrates haben – das heißt, sie sind oft und lange online. Ein ideales Zielobjekt für jeden Nachfolger der „Fakeshop-Bande“.

Nach einer aktuellen Studie der internationalen Virenschutz-Firma Symantec liegt Deutschland in puncto verseuchter Computer im europäischen Spitzenfeld. Rund 22 Prozent aller Internetnutzer in Deutschland hatten binnen eines Jahres mit bösartigen Computerinfektionen zu kämpfen, so eine Studie des europäischen Statistikamtes Eurostat. Demnach wären mehrere 100 000 Rechner der gut sechs Millionen SPIEGEL-Leser derzeit infiziert, die damit möglicherweise zu ahnungslosen Mittätern im digitalen Untergrund werden.

Mirko Manske arbeitet im Referat SO 43 des Bundeskriminalamts. Er war es, der Friedrich bei seinem Antrittsbesuch in Wiesbaden mit einer Präsentation im „digitalen Untergrund“ willkommen hieß.

Der Kommissar ist einer von Deutschlands führenden Cyber-Cops, in seinem Büro flimmern acht Bildschirme, auf denen er und ein Kollege Spuren der Gangster verfolgen. Manske war in den vergangenen Jahren mit allen größeren Fällen von Internetkriminalität befasst. Bei seinem Streifendienst am Rechner trägt er gern Jeans und ein Polohemd mit FBI-Logo – ein Geschenk seiner US-Kollegen, mit denen er eng zusammenarbeitet.

Vor kurzem sprach Manske an einem heißen Frühsommertag auf dem „Deutschen Präventionstag“ in Oldenburg. Gerade mal 23 Zuhörer waren erschienen, um seinen Vortrag über die „aktuelle Bedrohungslage“ im Internet zu hören.

Vielleicht war es das heiße Wetter, vielleicht das spärlich besetzte Auditorium, Manske jedenfalls sprach Klartext. „Keiner weiß genau, wie es weitergehen soll“, sagte er. Unglaublich schnell würden Cyber-Gangster beispielsweise neue Sicherheitsinstrumente im Online-Banking knacken. Dann schilderte er die kreativen Ideen der Szene für den Missbrauch neuer Smartphones und Tabletcomputer wie das iPad. „Die Bad Guys haben auch dafür schon eine Lösung.“

BUNDESKRIMINALAMT

**BKA-Fahnder Manske:** *Streifendienst am Rechner*

Nach dem Vortrag war es still in der Halle 2 der Weser-Ems-Halle. Das sei ja nun alles ziemlich einschüchternd gewesen, sagte schließlich ein Zuhörer. Man sei doch auf dem Präventionstag, was Manske denn empfehle, als Profi, „so präventiv“.

Manske dachte nach. Er selbst sei schon Opfer von Online-Kriminellen geworden, sagte er, 12 000 Dollar habe er verloren.

Seither gebe es bei ihm zu Hause zwei Rechner. Einen nutzt er zum Surfen im Internet. Der andere ist ausschließlich für Bank- und Kaufgeschäfte reserviert.

Marcel Rosenbach, Hilmar Schmundt