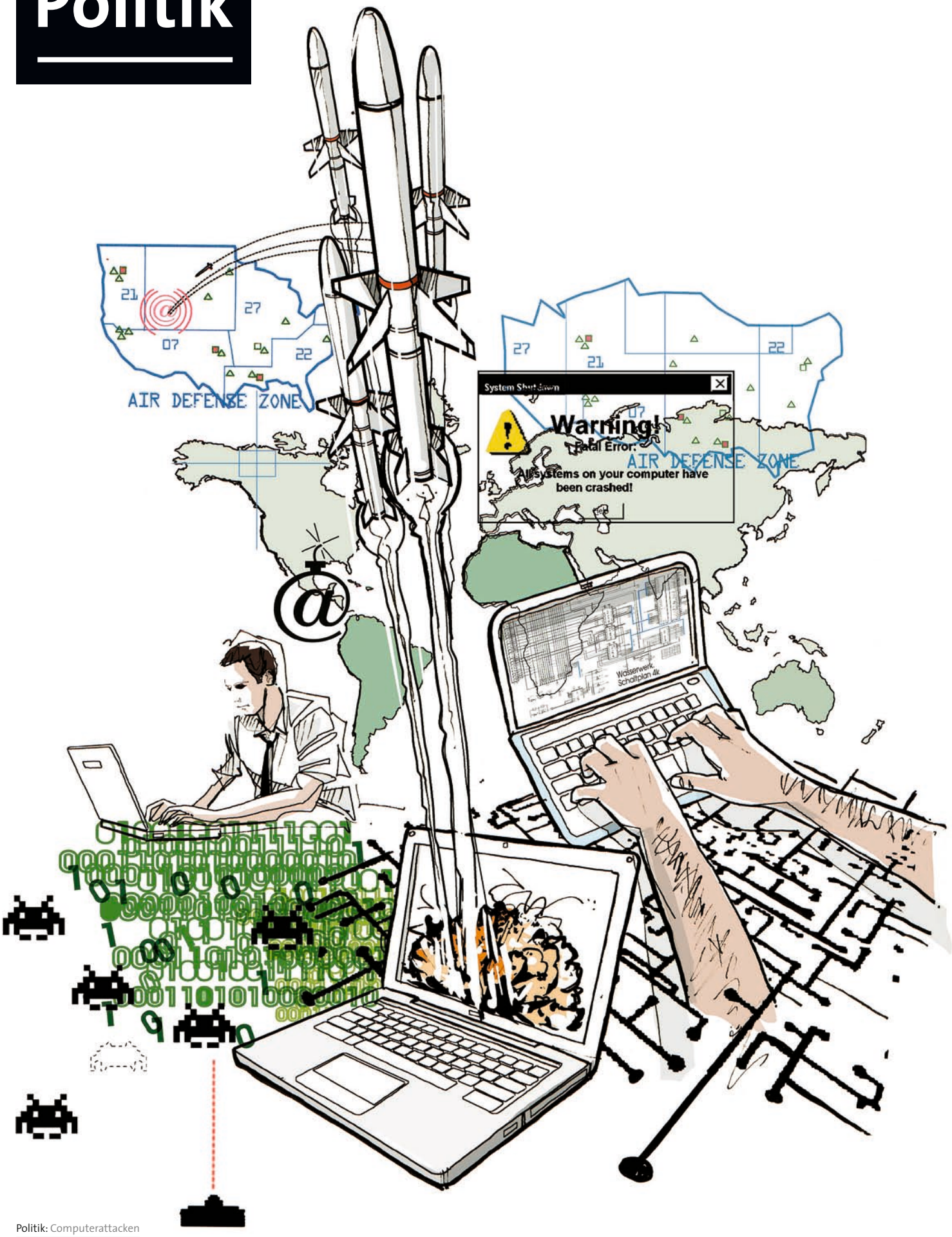
Politik


AIR DEFENSE ZONE
System Shutdown
Warning!
Fatal Error:
All systems on your computer have been crashed!
AIR DEFENSE ZONE
Wasserwerk Schaltplan.dir

World Wide War

Computerattacken. Mit immer dreisteren Methoden dringen Hacker im Auftrag von Verbrechersyndikaten oder Staaten in fremde Rechner ein. Um Schäden abzuwenden, heuern Firmen und Regierungen eigenwillige Experten an, die ihre Netze verteidigen sollen: die Cyberkrieger des Guten

Text: Nils Kreimeier
Illustrationen: Tim Möller-Kaya

Charlie Miller braucht nicht viel, um Angst und Schrecken zu verbreiten. Der hagere Mann mit dem spärlichen Haarwuchs verschickt einfach eine E-Mail – nur dass deren Absender nicht Charlie Miller heißt, sondern einen Namen trägt, der dem Empfänger gut bekannt ist.

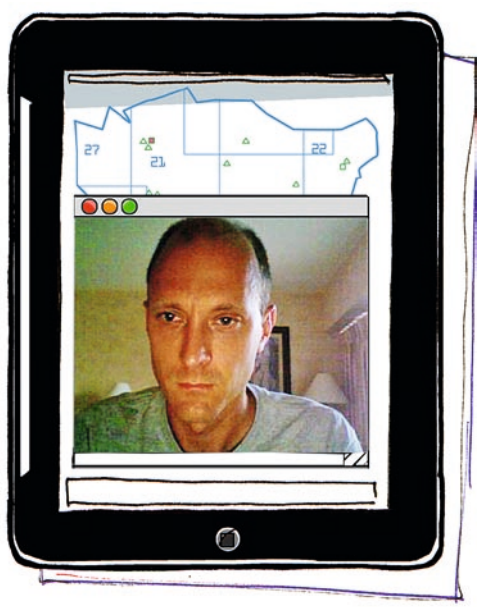
„Hallo Michael", steht dann da, „schau doch mal auf diese Website." Klickt Michael auf den eingefügten Link, geht das Spiel los. Während das Opfer noch surft, dringt Miller in den fremden Computer ein. Er schaut sich dort Dateien an, macht mit der Webcam ein Foto des Benutzers. Und zu guter Letzt verkündet eine Stimme über den Lautsprecher des Rechners: „Ich habe dich gehackt."

Miller findet Softwarelücken und dringt in Netzwerke ein, um zu zeigen, wie anfällig sie sind. In der Welt der Hacker ist er längst zur Legende geworden. Selbst Apple hat er das Fürchten gelehrt: 2007 gelang es Miller als Erstem, das iPhone zu kapern. Das Magazin „Forbes" nennt ihn „den vielleicht berühmtesten Mac-Hacker der Welt". Miller selbst sieht sich als „einen der Guten". Einen, der uns mit seinen Mitstreitern vor Katastrophen bewahren will, von denen wir nicht einmal etwas ahnen.

Die Treffen dieser Szene, etwa die jährlichen Black-Hat- und Defcon-Konferenzen, die zuletzt Ende Juli in Las Vegas stattfanden, sind inzwischen international beachtete Großereignisse. Denn was die Hacker so treiben und herausfinden, plagt längst nicht mehr bloß die Forschungs- und PR-Abteilungen der IT-Branche. Es treibt die Sicherheitsbehörden in aller Welt um.

Mit Tricks wie der gefälschten E-Mail werden Jahr für Jahr Hunderttausende von Rechnern gekapert. Erst vor wenigen Wochen verhaftete die Polizei drei slowenische Informatiker, mit deren Software fast 13 Millionen Computer unter Kontrolle gebracht worden waren. In der Hand krimineller Banden werden solche Netzwerke zu Waffen. Gegen Unternehmen, gegen internationale Organisationen – sogar gegen Staaten.

Für die Insider ist klar, dass im Internet eine neue Front entstanden ist. „Der Cyberkrieg hat begonnen", schreibt Richard Clarke, der als Antiterrorberater und Spezialist für Computersicherheit fast 20 Jahre lang für die US-Regierung gearbeitet hat, zuletzt für die Präsidenten Bill Clinton und George W. Bush. „Die Staaten bereiten sich schon auf die Schlacht vor."



Mac-Schreck: Charlie Miller knackte das iPhone und brauchte 2008 nur zwei Minuten, um als Erster ein Apple-MacBook zu hacken. Der Ex-Regierungsbeamte ist weltweit gefragter Berater

Charlie Miller

In seinem Buch „Cyber War", das im April erschienen ist, entwirft Clarke ein Szenario, bei dem innerhalb von 15 Minuten ganze Stromnetze in den USA lahmgelegt werden, Raffinerien in Brand geraten, die komplette Flugsicherung des Landes ausfällt und die Datensätze der Notenbank verschwinden – alles durch einen Angriff aus dem Netz.

Eine konkrete Attacke dieses Kalibers, das gibt auch Clarke zu, hat es bisher noch nicht gegeben. Doch eine Reihe von Ereignissen in Europa und den USA hat das Militär aufgeschreckt.

Im Frühjahr 2007 legten Unbekannte in Estland mehrere Tage lang die Websites von Banken und Regierungseinrichtungen lahm. Zuvor hatten sich Estland und Russland über die Verlegung eines Kriegerdenkmals in der estnischen Hauptstadt Tallinn gestritten.

Im März 2009 deckten Experten ein Spionagenetzwerk namens Ghostnet auf, das, vermutlich von chinesischen Servern ausgehend, in die Computer von Regierungen und Organisationen in über 100 Staaten eingedrungen war.

Im Juli 2009 wurden die Websites von Regierung, Medien und Finanzinstituten in den USA und Südkorea zum Opfer koordinierter Cyberattacken.

Für Richard Clarke sind das alles nur erste „Testläufe", die einem größeren, echten Cyberkrieg vorangehen. Ein Land wie Israel schlägt sich heute schon im Alltag mit den Angriffen von Hackern herum. „Jedes Mal, wenn es zu politischen Spannungen kommt, sind wir Ziel von Cyberattacken", sagt Assaf Keren, Direktor für IT-Sicherheit bei der israe- ▶

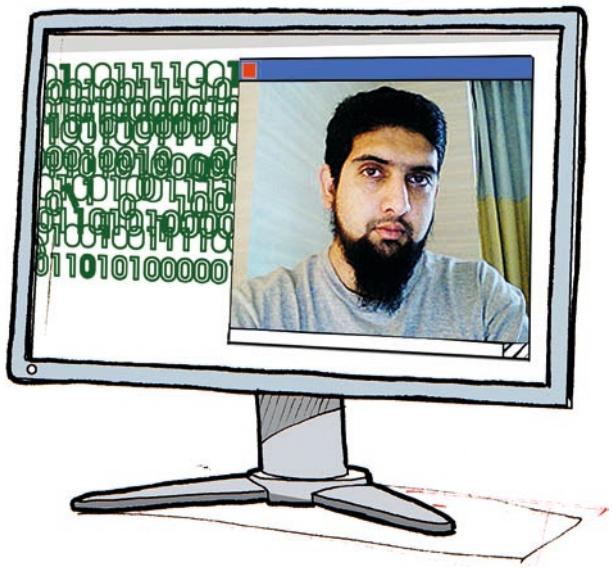
lischen Regierung. In der Krisenregion Nahost heißt das: fast immer.

Wer hinter solchen Angriffen aus dem Netz steckt, lässt sich kaum herausfinden. So schien die Attacke auf Südkorea zunächst aus dem feindlichen Nordkorea zu kommen. Bis sich herausstellte, dass der verantwortliche Rechner offenbar in Miami stand – und von dort aus den Umweg über nordkoreanische Server nahm. Wer die Aktion tatsächlich steuerte, können die Behörden bis heute nicht sagen.

Meist lässt sich nicht einmal klären, ob es feindliche Staaten oder Verbrechersyndikate sind, die sich einschleichen. Viele Regierungen haben eigene Abteilungen für den Krieg im Netz eingerichtet. Daneben gibt es kriminelle Organisationen, die als Auftragshacker arbeiten. Für gutes Geld können Staaten oder Terrorgruppen ihre Dienste einkaufen.

Die Cybergangster kontrollieren oft Hunderttausende von Rechnern, die in sogenannten Botnets zusammengeschlossen sind und auf Bestellung in den Angriff geschickt werden. Eine beliebte Methode sind „Distributed Denial of Service"-Attacken, bei denen Server mit Anfragen überflutet und so zum Stillstand gebracht werden.

Als Spezialist für dieses Verfahren gilt das harmlos klingende Russian Business Network, der Onlinezweig der russischen Mafia. Dieses Netzwerk hat vom Kreditkartendiebstahl bis zur großflächigen Attacke die komplette Palette der Internetkriminalität im Angebot. Es steckt angeblich auch hinter den Onlineangriffen, denen georgische Regierungsserver im Krieg vom August 2008 gegen Russland ausgesetzt waren.



Was Sie schon immer über digitale Kriegskunst wissen wollten: Der Profihacker Haroon Meer aus Südafrika berät nicht nur Unternehmen, sondern auch Offiziere der Nato

Wer noch keine solche Organisation hat, kann geeignete Leute heute relativ leicht anheuern. „Wenn man mich fragen würde, ob ich für ein paar Hunderttausend Dollar eine Truppe aufstellen kann, die sich so gut wie überall reinhacken kann, wäre meine Antwort: Ja", sagt Haroon Meer, der als Profihacker vor allem die Sicherheitslücken von Unternehmensnetzwerken aufzeigt.

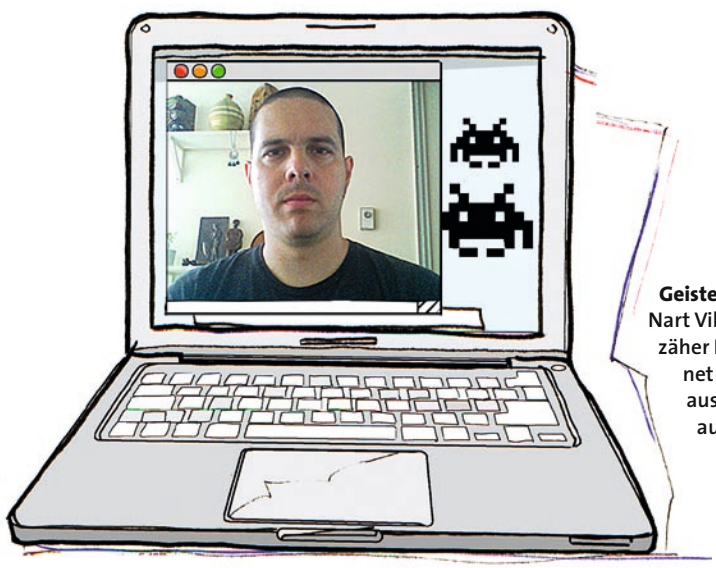
Gefährliche Geisternetze

Auch Meer ist „einer von den Guten". Wie so viele der Kämpfer im Cyberkrieg ist er nur schwer als solcher zu erkennen. Der freundliche Südafrikaner trägt bei offiziellen Anlässen gern gelbe T-Shirts mit den Umrissen seines Kontinents darauf und sieht ansonsten so aus, wie sich Lieschen Müller einen Taliban vorstellt. Doch wenn Meer über die Gefahren des Internets referiert, dann hören auch uniformierte Nato-Offiziere aufmerksam zu. Ebenso wie bei Nart Villeneuve, einem schüchtern wirkenden Kanadier, der dem Publikum schon mal als „Meisterhacker" vorgestellt wird. Was ihm selbst eher unangenehm ist.

Villeneuve hat sich eigentlich darauf spezialisiert, Zensur im Internet aufzudecken und anzuprangern. Der größte Coup gelang ihm und anderen Mitarbeitern des Information Warfare Monitor aber, als sie im vergangenen Jahr das offenbar von China angelegte Ghostnet enthüllten. Allmachtsfantasien sind diesen Cyberkämpfern, die sich um die Nervensysteme der modernen Zivilisation sorgen, völlig fremd. Wer mit Haroon Meer, Nart Villeneuve oder Charlie Miller spricht, der versteht rasch, wie schwierig die Aufgabe ist, Angriffe aus dem Netz abzuwehren.

„Es ist ziemlich klar, dass die Kriminellen den guten Jungs bisher immer einen Schritt voraus sind", sagt Meer. „Und selbst wenn wir uns der Gefahr bewusst werden, könnte es sein, dass wir ihr nur schwer begegnen können." Der schlimmste Albtraum vieler Sicherheitsexperten ist inzwischen, dass Terroristen sich die Waffe Internet noch stärker zunutze machen könnten.

Die US-Bundespolizei FBI gab im November 2009 bekannt, Verbindungsleute des Terrornetzwerks al-Kaida bemühten sich, ihre Computer- und Hackerkenntnisse entscheidend zu verbessern, und suchten daher nach Rat und Tat von außen. Dunkle Geschäfte lassen sich leicht aufziehen: Das Internet bringt Käufer und Verkäufer von Viren und Malware auf ganz unkomplizierte Weise zusam-



Geisterstunden: Der Kanadier Nart Villeneuve deckte 2009 in zäher Puzzlearbeit das Ghostnet auf, mit dem von China aus Computer in aller Welt ausspioniert worden sind

Haroon Meer; Nart Villeneuve

men; schädliche Standardprogramme gibt es schon für ein Taschengeld. Das IT-Sicherheitsunternehmen Symantec schätzt in einer unlängst veröffentlichten Studie, dass eine Grundausrüstung für Computerattacken höchstens 120 Dollar pro Monat kostet. Die Schlacht im Netz findet damit oft zwischen David und Goliath statt. „Hacken ist ziemlich billig", sagt der Südafrikaner Meer. „Und zudem ist Angreifen billiger als Verteidigen."

Doch die Verteidiger rüsten auf. Zum Beispiel im estnischen Tallinn: In ein paar unscheinbaren, aber gut gesicherten Militärgebäuden ist hier seit Mai 2008 ein Exzellenzzentrum zur Cyberabwehr untergebracht. Sieben Nato-Staaten, darunter auch Deutschland, haben Experten entsandt, die mögliche Gefahren aus dem Netz simulieren und Abwehrstrategien entwerfen sollen.

Im Mai dieses Jahres ließ das Zentrum in einer Übung zwei Gruppen gegeneinander antreten: Sechs getrennte Teams spielten jeweils einen Stromkonzern und mussten ihre branchentypischen Netzwerke gegen eine Mannschaft feindlicher Computerhacker verteidigen. Nach Ablauf von zwei Tagen hatten die Angreifer einen Großteil der beteiligten Computer infiltriert, verfolgten die interne Kommunikation der Gegenseite und schafften es in einem Fall sogar, ein virtuelles Kraftwerk in Brand zu setzen.

Der Feind in der Hosentasche

Für die Organisatoren war das Ergebnis alles andere als beruhigend. „Wir müssen uns auf etwas vorbereiten, auf das man sich eigentlich gar nicht vorbereiten kann", sagt Ilmar Tamm, Leiter des Exzellenzzentrums.

Die größte Sorge gilt nicht der militärischen Infrastruktur, die oft auch online besser gesichert ist als der zivile Bereich. Besonders verwundbar sind die Energieversorger, die komplette Volkswirtschaften am Laufen halten. Aber auch die Telekommunikation, deren Geschäftsmodell auf zunehmender Vernetzung beruht, ist eine Achillesferse. Haroon Meer malt aus, welche Folgen es haben kann, wenn die Rechner eines großen Mobilfunkunternehmens von außen gekapert werden: Die Bewegungen von Soldaten, die ihre Handys bei sich tragen, könnten von einem feindlichen Beobachter exakt verfolgt werden. Eine bessere Feindbeobachtung lässt sich kaum denken – und die Gegenseite muss dafür nicht einmal ein eigenes militärisches Risiko eingehen.

Das Grundproblem liegt in der Anfälligkeit der weltweit verwendeten Software. Bislang war noch jede neue Version einer gängigen Büroanwendung umfangreicher als ihr Vorgänger. Je mehr Zeilen an Programmiercode aber geschrieben werden, desto eher unterlaufen Fehler, die selbst bei mehrfacher Prüfung nicht ausgeputzt werden.

Solche Programmierfehler sind für Könner ein gefundenes Fressen und können genutzt werden, um eine Software zu manipulieren. Betroffen sind ▶

Netzkrieg Wenn Hacker die Weltpolitik bewegen

Es fällt kein Schuss, es rollt kein Panzer – Onlineattacken sind nur schwer aufzudecken, und über die Auftraggeber kann meist nur spekuliert werden. In mehreren Fällen waren Cyberkrieger an internationalen Konflikten beteiligt

Syrien 2007 Anfang September bombardierten israelische Kampfjets eine Nuklearanlage im syrischen al-Kibar, in der ein Kernreaktor nordkoreanischer Bauart installiert gewesen sein soll. Schon bald nach dem Angriff kam die Frage auf, wie die Jagdbomber vom Typ F-15 und F-16 in den syrischen Luftraum eindringen konnten, ohne dass die dortige Luftabwehr reagierte und Alarm schlug. In Presseberichten wurden dazu anonyme amerikanische und israelische Geheimdienstler zitiert, nach deren Aussage die Israelis zuvor das syrische Radarsystem gehackt und de facto die Kontrolle über die Bildschirme des Gegners übernommen haben sollen: Anstelle der Kampfjets war nur ein leerer Luftraum zu sehen.
Welche Technik dabei genau zum Einsatz kam, ist unbekannt. Einer Theorie zufolge hatte ein Israel-treuer Programmierer in das Luftabwehrsystem russischer Herkunft eine Falltür eingebaut: Dabei zeigt der Radarbildschirm nach dem Empfang eines bestimmten Signals für einen bestimmten Zeitraum nichts an.

Georgien 2008 Die Onlineattacken gegen georgische Regierungsstellen begannen bereits zwei Wochen vor Ausbruch des militärischen Konflikts mit Russland. Mitte Juli wurde die Website des georgischen Präsidenten mit einer Flut von Anfragen eine Zeit lang lahmgelegt. Die eigentliche Welle rollte ab dem 8. August und damit zeitgleich mit dem russischen Einmarsch in Georgien.
Innerhalb weniger Stunden wurden die Websites des Präsidenten Michail Saakaschwili, des Außen- und des Verteidigungsministeriums attackiert und deren Inhalte zum Teil verändert. Ziel des Angriffs waren zudem die größte kommerzielle Bank Georgiens, die Zentralbank und zahlreiche Medien.
Die georgische Führung machte Russlands Regierung verantwortlich, doch dieser Vorwurf lässt sich nur schwer untermauern. Als sicher gilt, dass an dem Angriff mehrere weltweite Botnets beteiligt waren, von denen mindestens eines offenbar unter Kontrolle des Russian Business Network stand, einer russischen Organisation von Onlinekriminellen. Zudem bezeichneten unabhängige Beobachter die Aktion als ausgesprochen koordiniert. Die russische Führung hat stets zurückgewiesen, an dem Cyberangriff beteiligt gewesen zu sein.

Ghostnet 2009 Im März vergangenen Jahres deckten kanadische Wissenschaftler ein Onlinespionagenetz auf, das über 1000 Computer in mehr als 100 Staaten unter seine Kontrolle gebracht hatte. Das Netzwerk, das bald den Namen Ghostnet erhielt, erstreckte sich auf zahlreiche Botschaften, Außenministerien, Rechner von Nato-Einrichtungen sowie auf Exilzentren des Dalai Lama. Es nutzte die infizierten Rechner unter anderem zur Raumüberwachung mithilfe von Webcams und Mikrofonen.
Ausgangspunkt des für die Aktion benutzten Spionage-Trojaners (Ghostrat) waren angeblich ausschließlich chinesische Server. Die chinesische Regierung hat jegliche Verwicklung in den Fall weit von sich gewiesen.

nicht nur die gängigen Browser, Textdarstellungsprogramme und E-Mail-Funktionen – auch wenn für sie schon wegen der hohen Nutzerzahl besonders viele Viren und Malware geschrieben werden. Im Prinzip hat jede Software Lücken, die Hacker ausnutzen können. „Eine sichere Software gibt es nicht“, sagt Miller. „Es gibt nur Programme, deren Fehler noch nicht gefunden worden sind.“

Letztlich ist die Verwundbarkeit nicht nur eine Frage der Technik. Auch Juristen zerbrechen sich mittlerweile den Kopf darüber, wie man mit den neuen Bedrohungen umgehen kann. „Ein Staat hat praktisch keine rechtlichen Möglichkeiten, wenn ein Angriff nicht zurechenbar ist. Das ist ein großes Problem“, sagt Wolff Heintschel von Heinegg, Völkerrechtler an der Europa-Universität Viadrina in Frankfurt/Oder.

Notschalter fürs Internet

Als Estland 2007 zum Opfer von Netzattacken wurde, standen die am Angriff beteiligten Computer in mehreren Dutzend Staaten, sie waren zuvor von Kriminellen gekapert worden. Auch wenn die estnische Regierung davon ausging, dass russische Hacker und vielleicht sogar der Kreml hinter der Sache steckten, ließ sich das nicht nachweisen – und schon gar nicht ließ sich daraus ein Angriffsfall nach Nato-Definition konstruieren.

Von Heinegg arbeitet mit mehreren Kollegen an einem Handbuch, das es künftig erleichtern soll, Cyberangriffe juristisch einzuordnen und dagegen vorzugehen. Ein Ergebnis könnte sein, dass Staaten dazu verpflichtet werden, Computer vom Netz zu nehmen, die von ihrem Territorium aus an einer Attacke beteiligt sind. Dies wäre schon auf Basis des bestehenden Völkerrechts möglich.

In den USA, deren internetbegeisterter Präsident Barack Obama als besonders sensibel für das Thema gilt, geht die Debatte schon weiter. Senator Joe Lieberman, ehemals Demokrat, jetzt parteiunabhängig, hat kürzlich den Entwurf für ein Gesetz vorgelegt, das es dem Präsidenten erlauben würde, in Notfällen die Kontrolle über das heimische Netz zu übernehmen. Telekomanbieter könnten dann gezwungen werden, ihren Kunden den Zugang zu sperren, wenn die USA einem Cyberangriff ausgesetzt sind.

Der US-Nachrichtendienst NSA baut derzeit in Utah an einem Zentrum für Cybersicherheit, dessen Aufgabe es unter anderem sein soll, die „Infrastruktur des Landes besser zu schützen“. Gegen solche Tendenzen regt sich allerdings nicht nur der harte Widerstand von Bürgerrechtlern. Auch Internetfirmen warnen davor, die Freiheiten im Netz zu beschränken.

Doch das Gefühl der Verwundbarkeit im Cyberspace hat gerade in den USA enorm zugenommen. Die IT-Wirtschaft, die in ihren Anfängen einmal eine ganz überwiegend amerikanische Veranstaltung war, globalisiert sich immer weiter, die USA verlieren alte Wissensvorsprünge. Die Produktion von Software und Hardware ist in Länder ausgelagert worden, von denen einige als mögliche Angreifer in einem Cyberkrieg gegen den Westen gelten. Wer verhindert, dass diese Konkurrenten absichtlich Sicherheitslücken in die Programmiercodes oder Chips einbauen, die dann später als Einfallstore für Hackerattacken dienen?

Noch unter Obama-Vorgänger George W. Bush ist eine Richtlinie verabschiedet worden, die sichere Produktionsketten fordert. Das aber ist leichter hingeschrieben als getan. „Es wird der US-Regierung schwerfallen, nur Software und Hardware zu kaufen, die unter sicheren Bedingungen in den USA hergestellt wurden“, schreibt Clarke. „Derzeit würde sie wohl überhaupt keine finden.“

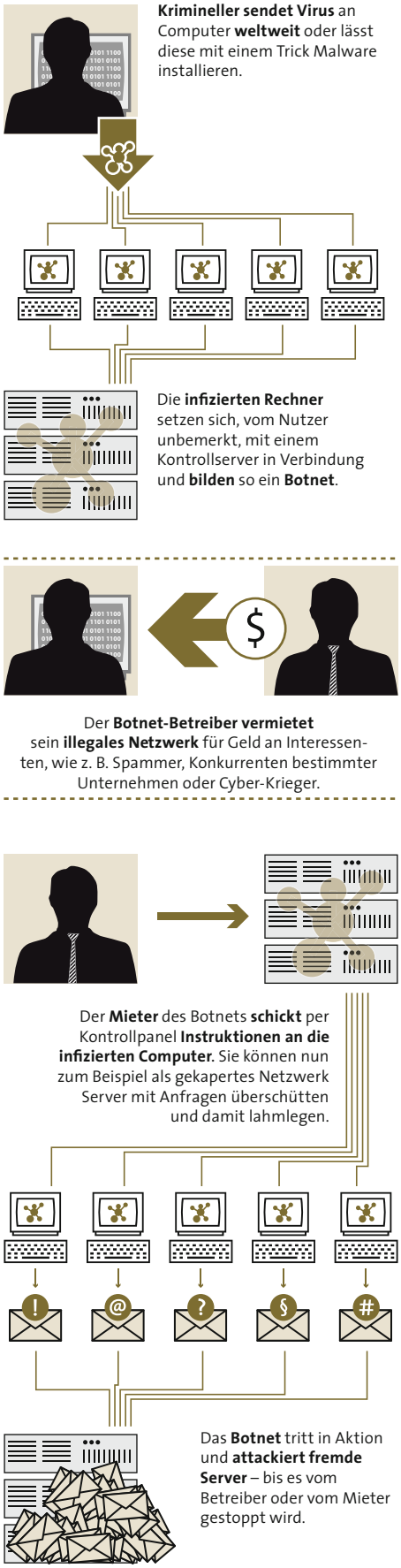
Eines mögen sich allerdings auch die fantasievollsten Cyberexperten auf gar keinen Fall vorstellen: dass die neue Gefahr womöglich dazu führen könnte, dass die Welt künftig wieder entnetzt wird. Zu abhängig ist die moderne Wirtschaft, sind wir alle, von der blitzschnellen Kommunikation – und von der höheren Produktivität und dem höheren Wohlstand, den sie ermöglicht.

Das kleine Estland, das 2007 immerhin eines der ersten Opfer eines größer angelegten Cyberangriffs wurde, hat es zu seinem Markenzeichen gemacht, einen Großteil des gesellschaftlichen Lebens übers Internet abzuwickeln. Die Esten können online wählen, ihre Polizeiakten einsehen, so gut wie jeden Behördengang erledigen und natürlich alle Arten von Bankgeschäften tätigen.

Auch die Hacker des Guten, die täglich tief in die Abgründe der vernetzten Welt schauen, können nur schmunzeln, wenn man sie fragt, ob es nicht sinnvoll wäre, die digitale Revolution aus Sicherheitsgründen ein wenig rückgängig zu machen. „Dieser Geist ist aus der Flasche“, sagt Charlie Miller. „Das lässt sich nicht mehr zurückdrehen.“ ■

Wie ein Botnet funktioniert

Von der E-Mail bis zum Großangriff



Grafik: Alexander Weber