

GEHEIMDIENSTE

Digitale Spionage

Die Online-Durchsuchung von Computern ist so umstritten wie kein zweites Instrument der Sicherheitspolitik. Eine interne Untersuchung des Kanzleramts zeigt, wie häufig der BND in fremde Rechner eindringt. Nun soll der Nachrichtendienst noch stärker kontrolliert werden.



cherheitsbehörde. Mehr als 2500 Mal, heißt es im BND, sei der Dienst mittlerweile in fremde Rechner im Ausland eingedrungen. In den meisten Fällen installierten die Beamten einen „Keylogger“, ein Programm, um Tastatureingaben mitzuverfolgen und so Passwörter zu entwenden. Anschließend öffneten sie das fremde Mailfach und werteten den Briefverkehr aus, oft über viele Monate. Gelegentlich verschickten die Geheimen auch einen Trojaner, mit dem wie bei Abdul Qadir Khan der gesamte Inhalt einer Festplatte heimlich nach Deutschland kopiert wurde.

Die Online-Durchsuchung, das wissen die Pullacher seitdem, ist ein mächtiges Werkzeug. Der Einsatz der Spähtechnik erweitert das klassische Repertoire der Dienste, es ist die Ausweitung der Spionagetechnik ins Internet. Die meisten Geheimdienste weltweit setzen sie ein, allen voran Amerikaner und Israelis. Ihr komme „zur Abwehr von Gefahren des internationalen Terrorismus eine zentrale Rolle zu“, sagt Bundesinnenminister Wolfgang Schäuble (CDU).

Doch der Einsatz ist nicht unproblematisch. In einer wegweisenden Entscheidung im Februar vergangenen Jahres hat das Bundesverfassungsgericht die Hürden für Online-Durchsuchungen hochgelegt. „In einem Rechtsstaat ist Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme und bedarf besonderer Rechtfertigung“, urteilten die Richter mit Blick auf Polizei und Verfassungsschutz. Ohne eine „existenzielle Bedrohungslage“ sei eine so intime staatliche Überwachung „grundsätzlich nicht angemessen“.

Dass der Staat Computer längst in großem Stil durch seinen Auslandsgeheimdienst infiltriert, war den Richtern in Karlsruhe allerdings ebenso unbekannt wie den Parlamentariern in Berlin. Erst seit kurzem kennen einige wenige Bundestagsabgeordnete die Dimension des Themas. Der Geheimdienstkoordinator im Kanzleramt, Klaus-Dieter Fritsche, präsentierte den Mitgliedern des Parlamentarischen Kontrollgremiums die Ergebnisse einer internen Untersuchung, die das Kanzleramt in Auftrag gegeben hatte, nachdem im vergangenen Jahr bekannt geworden war, dass der BND die Korrespondenz zwischen dem afghanischen Minister Amin Farhang und einer SPIE-

Kanzlerin Merkel, BND-Chef Uhrlau: Präsident auf Abruf

Die Diebe kamen, als es in Pakistan Nacht war und die Atomwissenschaftler schliefen. Sie sichteten die Dokumente im Büro des Forschungszentrums in der Nähe von Islamabad, die Buchhaltung, die geheimen Akten und kopierten, was sie konnten. Dann verschwanden sie lautlos. Niemand bemerkte am nächsten Morgen, dass eingebrochen worden war im Allerheiligsten von Abdul Qadir Khan, dem Vater der pakistanischen Atombombe.

Aus dem gestohlenen Material ging hervor, dass Khan in der afrikanischen Wüstenstadt Timbuktu ein kleines Hotel mit einer Handvoll Betten betrieb und sich dort regelmäßig mit einem seiner Wissenschaftler aufhielt. Die Korrespondenz enthielt Kontakte zu diversen Schurkenstaaten und einem Netzwerk skrupelloser Geschäftsleute, die gerade dabei waren, die Baupläne für eine Atombombe zu verkaufen (SPIEGEL 05/2004).

Der Diebstahl von 2003 trug wesentlich zur Aufklärung des internationalen Atomsmugglerings bei, den Khan dirigierte. Und er war ein „signifikanter Durchbruch“, wie ein Teilnehmer voller Stolz lobt, für ein neuartiges Instrument der Sicherheitsbehörden, das es erst seit wenigen Jahren gibt – die Online-Durchsuchung.

Die Einbrecher waren nicht in Pakistan, sondern saßen in Pullach, beim Bundesnachrichtendienst (BND). Sie kamen durch die Datenleitungen, zapften mit einem Hilfsprogramm das Computernetzwerk der Khan-Labore an und saugten mehrere Gigabyte ab. Es waren so viele Informationen, dass der BND eigens ein kleines Programm zur Auswertung entwickelte, um in der Datenflut nicht zu ertrinken.

Der Coup gilt als eine der erfolgreichsten Operationen der vergangenen Jahre. Seitdem nutzt der deutsche Auslandsgeheimdienst die Möglichkeiten der modernen Technik wie keine zweite deutsche Si-

AXEL SCHMIDT / ACTION PRESS

GEL-Reporterin mitgelesen hatte (SPIEGEL 18/2008).

Der vertrauliche Bericht aus Pullach wirft eine Reihe schwerwiegender Fragen auf. Wie schrankenlos soll der Geheimdienst operieren? Wer soll und wer kann den BND kontrollieren? Und wie aggressiv dürfen die Geheimen in Zukunft gegen fremde Staaten vorgehen?

„Der BND braucht für die Online-Durchsuchung dringend eine Rechtsgrundlage“, fordert der CDU-Innenexper-

Jahre stießen die Beamten fast automatisch auf die Frage, wie man wohl am besten den Computer des Gegners anzapfen könne. Als ein russischer Wissenschaftler als Informant geworben werden sollte, erinnert sich ein BND-Veteran, wurden die Pullacher auf einen Wiener Internet-Anbieter aufmerksam, der Zugang zu russischen Computern und der Akademie der Wissenschaft in Moskau bot. Wie wäre es, fragte man sich beim BND, wenn man dort heimlich eindringen könnte?

waffen. Wenn es dem Hacker gelänge, sich in die Netzwerke der Mullahs einzuloggen, lockten die Beamten, sei der Lohn fürstlich, Straffreiheit inklusive.

Der junge Mann lehnte ab, andere aber bissen an. Mit klassischer Spionage und Staatssicherheit kannten sich die Technikfreaks nicht aus, wohl aber mit dem Eindringen in fremde Computernetze. Der BND zahlte anständig und gab die Ziele vor. Intern wurden die Hacker als „nachrichtendienstliche Verbindung“ geführt. Bis heute beschäftigt der BND solche „Externen“, unter anderem um sogenannte Trojaner programmieren zu lassen.

Weil das Werkzeug so erfolgreich war, entwickelte sich ein fröhlicher Wildwuchs. Vor allem Firmen, die Rüstungsmaterial schmuggelten, attackierte die Behörde, bevorzugt im Nahen Osten. Infiltriert wurde aber auch das Computernetz des Irak.

Weder August Hanning, bis Dezember 2005 Präsident des BND, noch sein Nachfolger Ernst Uhrlau hatten den genauen Überblick. Oft entschied einer der einflussreichen Referatsleiter. Gleich an drei Stellen im BND wurde die Online-Durchsuchung angewandt: im Referat „Opus“ („Operative Unterstützung und Lauschtechnik“) der Abteilung 2. Daneben waren zwei Referate in der Abteilung 1 aktiv, darunter die Männer von 12 Z.

Dieses Referat war es auch, das den ersten Skandal im Zusammenhang mit den Computer-Razzien produzierte. Es ging um eine Operation im Kongo, die den beteiligten Nachrichtendienstlern erkennbar außer Kontrolle geriet.

Der BND sollte im Kongo der Bundeswehr als „Auge und Ohr“ Informationen liefern. Franz Josef Jung, der deutsche Verteidigungsminister, hatte 2006 rund 800 Soldaten in die Krisenregion entsandt, um friedliche Wahlen abzusichern. Von Pullach aus überwachte der BND unter anderem eines der größten Hotels der kongolesischen Hauptstadt Kinshasa. Es war bekannt dafür, dass sich dort bevorzugt Oppositionelle trafen. Auf einem der wenigen öffentlichen Hotelrechner mit Internet-Zugang installierten die Geheimen einen „Keylogger“. Auf diese Weise konnte der Geheimdienst mitlesen, mit welchen Passwörtern sich die kongolesischen Oppositionspolitiker in ihre E-Mailfächer einwählten. Ab sofort loggte sich auch der BND ein. Es war eine ebenso bequeme wie ertragreiche Form der Spionage.

Sie endet abrupt, nachdem einer der Beamten das geheime Programm kurzerhand für private Zwecke missbrauchte.

Beim Einsatz der Staatstechnik war einem BND-Auswerter aufgefallen, dass in dem Hotel auch deutsche Soldaten der Bundeswehr abstiegen. Sie nutzten, wie die Kongolesen, den infiltrierten Internet-Rechner. Einer der Deutschen loggte sich unter „Psyops“ ein, um seine Mails abzurufen. Der Vorgang wurde in Pullach mit-

Spionageziele des BND



Abdul Qadir Khan



Bundeswehrgesoldaten im Kongo



Amin Farhang

te Wolfgang Bosbach, und der Liberale Max Stadler will „den rechtsstaatlichen Standard neu per Gesetz definieren“. Eine Generalvollmacht, auf die sich der BND berufe, entspreche „nicht mehr dem Stand der Debatte seit der Entscheidung des Verfassungsgerichts“.

Anders als Verfassungsschutz und Polizei soll der BND im Ausland operieren. Er unterliegt dabei kaum Einschränkungen, im Gesetz sind seine Aufgaben bewusst schwammig formuliert: „Der BND sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus.“ Eine Art Blankoscheck also.

Das wissen auch die BND-Angehörigen, die sich mit Überwachungstechnologie auseinandersetzen. Früher als andere Behörden erkannten die Pullacher das Potential der digitalen Spionage. Ende der neunziger

Die Überlegungen wurden konkreter, als die Pullacher zum ersten Mal mit der neuen Technik experimentierten. Während in der Öffentlichkeit kaum jemand etwas mit dem Begriff „Online-Durchsuchung“ anfangen konnte, hatte innerhalb der Behörde längst ein Wettlauf begonnen. Die Techniker in der für Aufklärung zuständigen Abteilung 1 bastelten an einer eigenen Software, und die Kollegen vom Referat 12 Z, die sich um internationalen Waffenschmuggel kümmerten, sprachen einige Hacker an, darunter einen technisch versierten Studenten aus Berlin.

Eine Oldenburger Firma bat den damals 23-Jährigen zu einem Treffen in einem Hotel am Bahnhof Zoo. Benötigt würden Informationen über Iran, angeblich für einen Investor. Doch die Fragen betrafen keine Wirtschaftsthemen. Es ging um iranische Ministerien, eine iranische Bodenstation für den Empfang von Satellitendaten und angebliche Massenvernichtungs-

USMAN KHAN / AFP (L.); THOMAS GRABKA / LATIF (O.); KNUT MÜLLER (U.)

verfolgt, der Sachbearbeiter war neugierig, er fischte das Passwort von „Psyops“ aus den Daten heraus und las dessen Post. Der Mann verschickte offenbar amouröse Post an die Frau eines BND-Mannes. In Pullach wurde die kompromittierende Mail kopiert und anonym an knapp ein Dutzend Bundeswehroldaten geschickt.

Weil einer der Soldaten die Staatsanwaltschaft einschaltete, flog der Spähangriff auf. Es ist illegal, die BND-Technik zu missbrauchen, und es ist auch illegal, einen deutschen Staatsbürger im Ausland ohne schweren Verdacht auszuspähen.

Der Fall „Kongo“ zeigt, wie machtvoll, aber auch wie heikel das Werkzeug sein kann. Er führte im Sommer 2007 zu einem Krisengipfel im Kanzleramt. An einem Augstag musste Ernst Uhlrau, der BND-Präsident, versprechen, auch die zuständigen Abteilungsleiter waren anwesend.

richtet, und wie im Kongo fanden die Aufklärer in Pullach durch die Online-Durchsuchung das Passwort. Sie konnten jetzt mitlesen, was Farhang schrieb.

Später rechtfertigten sich die Geheimen, Farhang habe nicht zu den Personen gehört, denen der Angriff gegolten habe. Aber nachdem er einmal ins Fadenkreuz geraten war, nutzten die Pullacher die Chance. Sie lasen auch mit, was Farhang und Koelbl sich schrieben. Das war illegal, weil es das grundgesetzlich geschützte Persönlichkeitsrecht der Journalistin und die Pressefreiheit verletzte. Zudem war es politisch heikel, weil es eine offiziell befreundete Regierung betraf. Beides war für die Geheimdienstleute letztlich kein Hinderungsgrund.

BND-Präsident Uhlrau erreichte der Fall erst kurz vor Weihnachten 2007, die Fachleute hatten ihn verschwiegen, als sie im

runge einen Geheimdienst leisten, der sich selbständig macht und immer wieder Skandale produziert, vor allem dann nicht, wenn andere Regierungen betroffen sind. So etwas dürfe sich „nie wiederholen“, verlangte der afghanische Außenminister Rangin Dadfar Spanta, nachdem der Angriff auf Farhang bekannt wurde.

Für den BND ist es eine Gratwanderung. In den kommenden Wochen wird das Kanzleramt eine Dienstvorschrift erlassen, die die Online-Durchsuchung neu regelt. Ein einziger Bereich, der aus vier Referaten besteht, soll im BND künftig für die Durchführung zuständig sein. Es muss Operationspläne geben, die genau darlegen, was geschieht, und Beamte mit Richterbefähigung sollen den Einsatz kontrollieren. Jede Online-Durchsuchung muss vom Präsidenten persönlich genehmigt werden, es gilt der „Grundsatz der Ver-



> Mehr drin für Sie: Das comdirect Girokonto, das zahlt statt kostet.

- Kostenloses Girokonto ab einem mtl. Geldeingang von 1.250 Euro
- 1 Euro Auszahlung jeden Monat
- Kostenlose ec-/Maestro- und VISA-Karte
- Weltweit kostenlos Bargeld abheben¹
- Inklusive kostenlosem Tagesgeld PLUS-Konto

¹ Im Ausland an Geldautomaten mit der VISA-Karte, im Inland mit der ec-/Maestro-Karte an über 7.000 Geldautomaten der Cash Group.

www.comdirect.de
oder **01803 - 44 45**
(0,09 Euro/Min. aus dem Festnetz der Dt. Telekom)

.comdirect
Ihr Geld kann mehr

„Hat es ähnliche Fälle gegeben?“, wollten Merkels Geheimdienstkoordinator Fritzsche und Uhlrau wissen. „Nein“, versicherten die Fachleute – eine fahrlässige Falschauskunft, denn tatsächlich hatte der BND Mails einer weiteren Deutschen abgefangen: der SPIEGEL-Journalistin Susanne Koelbl.

Im Juni 2006 starteten die „Opus“-Leute eine ebenso kühne wie umfangreiche Operation in Afghanistan. Dazu gehörten auch Spähprogramme, die via Internet auf Rechner am Hindukusch geschleust wurden, um möglichst viele Informationen über ein undurchsichtiges Geflecht aus Aufständischen, Drogenbaronen und gewöhnlichen Kriminellen zu erlangen.

Einer der Rechner gehörte dem afghanischen Handelsministerium, auch der Minister Amin Farhang persönlich nutzte ihn. Er hatte sich ein Postfach bei Yahoo einge-

August 2007 beim Krisengipfel im Kanzleramt berichten sollten. Die erneute Online-Affäre kostete Uhlrau fast das Amt, die Kanzlerin ließ erklären, das Vertrauen sei gestört, aber nicht zerstört. Bis heute ist er ein Präsident auf Bewährung.

Ohne die Spähaktion gegen die SPIEGEL-Journalistin wäre die Dimension der Online-Durchsuchung noch immer unbekannt. Aber Fritzsche, erschrocken von dem Eigenleben des Dienstes und bestärkt von der Kanzlerin, ordnete eine umfassende Aufklärung an.

Grundsätzlich soll der BND mit riskanten, aber ertragreichen Mitteln wie der Online-Durchsuchung agieren, die digitale Spionage im Ausland ist ausdrücklich erwünscht. Das Kanzleramt will deshalb kein eigenes Gesetz, die Wirkungsmacht des Dienstes soll nicht zu sehr beschnitten werden. Gleichzeitig kann sich keine Regie-

hältnismäßigkeit“, der verhindern soll, dass der Einsatz ausufert. E-Mailadressen mit der Endung „.de“ werden automatisch von der Überwachung ausgenommen, damit keine Deutschen betroffen sind. Die Regeln bedeuten das Ende der Anarchie, der Dienst wird diszipliniert. Uhlrau spricht davon, der BND habe seine „Lektion gelernt“ und nehme die Problematik „ernst“. „Ein Vorgang wie die unbeabsichtigte Erfassung von Frau Koelbl kann sich nicht wiederholen.“

Für einige der Beteiligten kommt das allerdings zu spät. Drei Mitarbeiter, die an der Operation gegen Farhang beteiligt waren, wurden strafversetzt, der Abteilungsleiter 2, Dieter U., scheidet wohl demnächst aus. Und BND-Präsident Uhlrau droht nach der Wahl die Ablösung. Die technische Revolution frisst ihre Väter.

HOLGER STARK