Wirtschafts Woche

Spionage

Der unsichtbare Wirtschaftskrieg

von Jürgen Berke

Mit jedem neuen Handy, Kopiergerät oder Laptop wächst die Gefahr für die Unternehmen, ausgespäht zu werden. Doch die wenigsten wollen wahrhaben, wie einfach sie es allen voran chinesischen und russischen Spionen machen. Der Feind surft schneller durch geheime Datenschätze, als viele Manager denken.

Airbus-Montage
Quelle: Foto: Laif/Peter Rigaud

Die Aktionäre wollten zum gemütlichen Teil der Hauptversammlung übergehen. Der Vorstand war entlastet, die Kürzung der Dividende auf 6,90 Euro pro Aktie beschlossen. Da ruft Wolfgang Kirsch, der Aufsichtsratsvorsitzende der genossenschaftlich organisierten R+V Versicherung, als nächsten Hauptredner einen gewissen Götz Schartner auf.

Ein jugendlich wirkender Mann tritt vor die 200 Anteilseigner, die im Wiesbadener Dorint-Hotel zusammengekommen sind. Er baut vier Laptops auf der Bühne auf und beginnt eine Live-Demonstration, wie sie die Vertreter der Anteilseigner, meist Vorstände von Volks- und Raiffeisenbanken, noch nicht erlebt haben.

Der Mann da vorn, das merken die Zuhörer sofort, ist keiner von ihnen. Er ist, wie sie später erfahren, Geschäftsführer der 8com GmbH & Co. KG aus Ludwigshafen und auf besonderen Wunsch des Vorstands angereist. Denn Schartner besitzt die Lizenz zum Spionieren. Als staatlich autorisierter Hacker gewährt er ganz offiziell, im Auftrag von Unternehmen und Bundesbehörden, Top-Managern und -beamten Einblick in tief Verborgenes: in die neuesten und gefährlichsten Methoden ausländischer Geheimdienste.

Schock für die Bankmanager

Alles geht rasend schnell im Wiesbadener Dorint-Hotel. Für Schartner ist es ein Kinderspiel, mithilfe einer Schnüffelsoftware auf einem seiner Laptops die Zugangskodes der iPhones, Blackberrys und anderer Handys im Raum zu knacken und deren E-Mails auszulesen. Vor aller Augen zieht Schartner die Kontakte aus den elektronischen Telefonbüchern der Anwesenden, fängt E-Mails ab und drückt auf den Auslöser der Handykamera. Der unfreiwillige Fotograf kann sein unfreiwillig geschossenes Bild auf der Leinwand bewundern, auf die Schartner den Monitor seines Laptops projiziert.

Für die meisten der Bankmanager ist das ein Schock. Bis gerade, sagt einer, dachten sie noch: „Wir sind doch sicher, weil wir eine professionelle IT-Abteilung haben, weil wir viel Geld für hochwertige Firewalls ausgeben und unsere Systeme durch Anti-Viren-Programme schützen." Jetzt zeigt ihnen Schartner, dass sie alle einem Trugschluss erlegen sind.

Die spektakuläre Aufklärungsaktion am 6. Mai, sagen Experten, würde wohl bei den meisten deutschen Unternehmen auf ähnliche Reaktionen stoßen. In fast jedem Betrieb finden sich Sicherheitslücken, die Spione und Geheimdienste so leicht wie Schartner als Einfallstor nutzen. Die Folgen können für Unternehmen existenzbedrohend sein. Ohne dass die Betroffenen davon etwas mitbekommen, fließen interne Informationen ab und landen bei der Konkurrenz.

Leichtfertig und arglos

Die meisten Unternehmen ignorieren das Risiko, weil sie sich zu leichtfertig und zu arglos mit vermeintlichen hohen Sicherheitsstandards zufriedengeben, die in der Praxis aber viel zu löchrig sind. „Stellen Sie sich vor: Es werden 100 Schuss aus einer großkalibrigen Waffe abgegeben", sagt Schartner. „Sie kommen zu der Bewertung: 99-mal konnte der Mensch ausweichen, 99-mal hat der Mörder danebengeschossen. Also konnte ich 99 Prozent der Angriffe abwehren." In solchen Fällen gäben fast alle Unternehmen ihren Sicherheitssystemen eine gute Note.

Für Schartner ist dies jedoch eine grundsätzlich falsche Bewertung: „Das heißt doch, eine Kugel kommt durch und tötet“, sagt er und schlussfolgert: „Also gibt es eine nicht tolerierbare Schwachstelle.“ Übersetzt auf die Situation im Unternehmen heißt das: Schon nach wenigen Minuten Dauerangriff können Firmengeheimnisse auf einem Rechner der Konkurrenz liegen – und dem Unternehmen der mühsam erarbeitete Know-how-Vorsprung verlorengehen.

Der 39-jährige Sicherheitsprediger aus der Pfalz trifft mit Aufklärungsaktionen wie diesen wohl einen der sensibelsten Punkte der deutschen Unternehmen. So sehr das Bundesamt für Verfassungsschutz (BfV) auch Sensibilisierungsgespräche mit Managern und Forschungseinrichtungen führt, die Spitzentechnologien entwickeln, so unterentwickelt scheint das Bewusstsein für die Gefahren selbst im banalen Alltag.

Emissionshandelsstelle in Berlin
Quelle: Quelle: Umweltbundesamt

Denn auch wenn das offiziell kein Politiker je sagen würde: Deutsche Unternehmen stehen unter Dauerbeschuss allen voran russischer und chinesischer Geheimdienste. Und Zielobjekte sind längst nicht mehr nur Konzerne und High-Tech-Schmieden. Zunehmend ins Fadenkreuz geraten auch Banken, die interessante Datensammlungen über die Finanzkraft von Unternehmen und Staaten besitzen. Ein Grund, weshalb die R+V Versicherung in Wiesbaden ihre Anteilseigner aus den Volks- und Raiffeisenbanken auf der Hauptversammlung so schockte.

Längst vorbei sind nämlich die Zeiten, in denen ausländische Gegner jahrelang Spione aufbauten, sie mit Kamera oder Nachschlüssel auf Jagd schickten oder sie Abhörwanzen an unzugänglichen Stellen einrichten ließen. Stattdessen droht heute die größte Gefahr aus dem Rechner, im Extremfall sitzt der Spion Tausende Kilometer entfernt.

„Spionage, insbesondere via Computer, wird oftmals gar nicht oder erst zu spät bemerkt“, sagt Burkhard Even, Abteilungsleiter Spionageabwehr beim Bundesamt für Verfassungsschutz in Köln. Und wenn ein Unternehmen einem Spionagefall auf die Spur gekommen ist, schaltet es in der Regel nicht die Sicherheitsbehörden ein. „Die Betroffenen fürchten vor allem den Imageschaden.“

Die Tricks der Cyberkrieger

Wie leicht Unbefugte an Unternehmensdaten kommen, zeigen erschreckende Beispiele aus der Praxis.

Wer will, kann es selbst versuchen. Jeder, auch ohne die geringste Ahnung in Spionagetechniken, kann zum Hacker werden, der sich in Unternehmen einschleicht. Zu den ersten Fingerübungen zählt: Man gebe in das Suchfenster bei Google „intitle: live view / - axis“ ein – und schon liefert die Suchmaschine Web-Kameras, die frei über das Internet anwählbar sind.

Und das sind ganz schön viele. Kein Problem, um mit ein paar Klicks in die Überwachungskamera am Swimmingpool eines Hotels in Dubai oder einer Verkehrskreuzung in Köln einzudringen. Mehr noch. Vom eigenen PC aus lässt sich die Kamera nach links und rechts steuern. Auch das Zoomen, also das Heranfahren an besonders interessante Objekte, ist häufig kein Problem. Profi-Hacker schaffen es auch, den Aufpasser in der Leitstelle zu ärgern, indem sie das gesamte Bild mit ein paar Dutzend x durchkreuzen – und sich dann in eine andere Web-Cam einwählen.

Für Unternehmen ist das eine sehr ernste Gefahr. Manchmal reicht schon das Eindringen in einen einzigen Firmenrechner aus, um in den inzwischen völlig vernetzten Unternehmen unbehelligt umherzustreifen. Nicht nur der Computer, auch Telefonanlagen und viele andere Maschinen besitzen inzwischen einen Internet-Anschluss mit einem vom Werk voreingestellten und öffentlich bekannten Zugangskode. Mehr als leichtsinnig sind all die Unternehmen, die vergessen, dieses Standard-Passwort abzuändern.

Gut durchorganisierter Coup

Gelingt es einem Angreifer, auf diese oder ähnliche Art in einen Rechner vorzustoßen, verfolgt er meist nur ein Ziel: Er muss eine schädliche Software, etwa einen Trojaner, auf dem Rechner eines Mitarbeiters platzieren. Geheimdienstler nehmen dazu gern den falschen Namen eines Freundes oder alten Bekannten des PC-Benutzers an, den sie leicht in Kontaktlisten der sozialen Netzwerke finden. Dann schicken sie dem PC-Benutzer eine E-Mail mit Anhang, in der etwa ein Trojaner versteckt ist. Wird der Anhang auf einem PC geöffnet, der unzureichend durch Schutzprogramme abgesichert ist, breitet sich der Trojaner sofort aus. Mit seiner Hilfe kann der Spion dann im schlimmsten Fall in das gesamte Datennetz eines Unternehmens vordringen.

Misslingt der Angriff aus der Ferne, bleibt manchmal nur die Attacke aus der Nähe. So berichten Verfassungsschützer von Spionen, die auf Messen getarnt als Kunden oder Verkäufer Kontakt mit ihren Opfern aufnehmen und ihnen einen USB-Stick schenken, auf der eine Spionagesoftware versteckt ist. Der Rechner infiziert sich, sobald das Opfer den Stick in einen ungeschützten Computer schiebt.

Selbst normalerweise gut abgesicherte Institutionen sind gegen solche Angriffe nicht immun. Im Februar und März dieses Jahres drangen Computerbetrüger in die Emissionshandelsstelle des Umweltbundesamtes ein, nachdem sie durch fingierte E-Mails die Passwörter einiger Großkunden abgefangen hatten. Innerhalb kurzer Zeit hatten die Betrüger mit den Daten der Geschädigten rund 250.000 CO2-Zertifikate gestohlen und zum Börsenwert von zwölf Euro an andere Händler weiterverkauft. Bei dem gut durchorganisierten Coup konnten die Betrüger eine Beute von rund drei Millionen Euro machen.

Der Raubzug konnte nur gelingen, weil die Emissionshandelsstelle nicht an das besonders abgeschottete Regierungsnetz, dem sogenannten Informationsverbund Bonn-Berlin, angeschlossen ist. Dort werden schädliche E-Mails aller Art automatisch herausgefiltert.

Universitätsbibliothek der TU Ilmenau
Quelle: dpa

Solche Attacken zeigen, wie sehr Unternehmen nach wie vor das Internet unterschätzen. Viele Vorstände wissen zwar, dass es das zentrale Nervensystem in jedem Unternehmen ist, das alle Bereiche miteinander verbindet. Viele Chefs verdrängen aber, dass fast alle Maschinen inzwischen einen Anschluss mit Internet-Adresse, kurz: IP, besitzen und damit ein potenzielles Einfallstor für Spione sind.

Ein beliebtes Angriffsziel sind die neuen Multifunktionsgeräte, die traditionelle Drucker, Kopierer und Fax-Maschinen auf jeder Büroetage verdrängen. Dank ihrer IP-Adresse stellen viele dieser Tausendsassas auch Verbindungen zu den mitunter leicht zugänglichen Prozessoren und Speichern her. Dort werden kopierte und gefaxte Vorlagen zwischengespeichert – eine Fundgrube für Spione.

Gewiefte Hacker kontrollieren die Gebäudetechnik

Auch moderne Kommunikationssysteme in Konferenzräumen, etwa die Konferenzspinne oder die Videokamera, besitzen eine IP-Adresse und lassen sich mit denselben Tricks wie bei der Web-Cam-Einwahl fernsteuern und als Wanze einsetzen. Wer einmal die Firewalls zum Intranet überwunden hat, kann auch diese Geräte aktivieren und Diskussionen hinter verschlossenen Türen live verfolgen, ohne dass irgendjemand Verdacht schöpft.

Gewiefte Spione können sogar bis in die technische Leitstelle vordringen und damit die Kontrolle über die gesamte Gebäudetechnik und die daran angeschlossenen Heizungen, Klimaanlagen, Aufzüge und Zugangskontrollen eines Unternehmens übernehmen. „Wir haben bisher bei jeder unserer Sicherheitsüberprüfungen zahlreiche Schwachstellen gefunden“, sagt Spionagespezialist Karl Pausch, Geschäftsführer der Fink Secure Communication GmbH in Coburg in Oberfranken. Firmengründer Manfred Fink ist zurzeit der einzige öffentlich bestellte und vereidigte Sachverständige für Abhörsicherheit in Deutschland, nachdem sich die Deutsche Telekom aus dem Geschäft mit der Spionageabwehr zurückgezogen hat.

Besonders riskant für Unternehmen ist der Einzug der Telefonie über das Internet, der sogenannten IP-Telefonie. Immer mehr Betriebe schalten ihre klassischen Nebenstellenanlagen ab und rüsten ihre internen Computernetze für IP-Telefonie um.

Telefon als Wanze

Der Nachteil: Mit dem Anschluss ans Internet lassen sich auch Bürotelefone als Wanze scharf schalten. Über den Wartungskanal des Herstellers aktivieren Geheimdienste heimlich die Freisprecheinrichtung und lauschen so allen Gesprächen im Raum. Genauso leicht einrichtbar ist eine Konferenzschaltung. Das heißt: Ein unbekannter Dritter hört mit, was zwei Manager am Telefon besprechen.

Umso erstaunlicher ist, wie fahrlässig sich sogar Top-Manager über interne Sicherheitsvorkehrungen hinwegsetzen. Immer öfter findet Experte Pausch unter den Schreibtischen „Accesspoints“, die Mitarbeiter und Manager ohne Zustimmung ihres Arbeitgebers installiert haben. So nennt der Abhör-Sachverständige Funksysteme (im IT-Jargon: WLAN-Hotspots), über den sich ein Laptop ins Firmennetz einklinkt. Oft sind solche Hotspots so leistungsstark, dass sich die Signale auch noch in einem Kilometer Entfernung auffangen lassen und sich Schnüffler über diesen Weg ins Firmennetz einwählen. „Solche Accesspoints bergen ein nahezu unkalkulierbares Risiko“, sagt Pausch.

Genauso gefährlich handeln Manager, die ihre alte PC-Tastatur wegwerfen und sie durch eine schicke drahtlose ersetzen. Kaum jemand ahnt, dass auch diese Signale in einer Entfernung von bis zu 300 Meter empfangbar sind und damit Passwörter weit außerhalb des Firmengeländes im Klartext gelesen können.

Europäisches Patentamt in München
Quelle: AP

Der Spion tarnte sich als hochrangiger Besucher. Und Wolfgang Rieder, Geschäftsführer der Rieder Faserbeton-Elemente GmbH im bayrischen Kolbenmoor, ertappte ihn auf frischer Tat.

Rieder ist Spezialist für anspruchsvolle Bauteile. Seine 13 Millimeter dünnen Faserbetonplatten stecken zum Beispiel in der spektakulären Fassade des neuen Soccer-City-Stadions im südafrikanischen Johannesburg. In der Arena wird am 11. Juli das Finale der Fußball-Weltmeisterschaft angepfiffen. Der Unternehmer suchte einen Kooperationspartner für ein 20-Millionen-Dollar-Bauprojekt in China. Als Erster meldete sich Yihe M., ein Geschäftsmann aus China, der sich bei seinem Besuch auch die Werkshallen anschauen wollte.

Rieder willigte ein – unter der Voraussetzung absoluter Geheimhaltung. Als der Rundgang startete, fiel einem Mitarbeiter eine Mini-Kamera auf, die Yihe M. am Hosengürtel befestigt hatte und mit der er heimlich die Produktionsabläufe filmte. Rieder zeigte den Geschäftsmann sofort an. Das Landgericht München verurteilte den Chinesen, der ein Geständnis ablegte, zu einer Bewährungsstrafe von eineinhalb Jahren und zur Zahlung einer Entschädigung in Höhe von 80.000 Euro.

Gefährliche Werkstudenten

Der vermeintliche Geschäftsmann aus dem Reich der Mitte repräsentiert nur einen von vielen Vertretern, die in Deutschland auf Datenklau gehen. Genauso gezielt versuchen chinesische Geheimdienste Werkstudenten und Praktikanten in deutsche Unternehmen einzuschleusen. Nur selten gelingt es dem Verfassungsschutz, solche Agenten zu enttarnen. Beim Europäischen Patentamt in München gelang das quasi in letzter Sekunde.

Die Behörde hatte vier Werkstudenten aus China als Praktikanten eingestellt. In wenigen Tagen sollten sie ihren Dienst antreten. „Auf den letzten Drücker“, sagt ein Informant des Verfassungsschutzes, konnten die Beamten verhindern, dass die

Chinesen genau die Schaltstelle besetzen, an die Unternehmen aus ganz Europa die Ergebnisse ihrer Forschungs- und Entwicklungsarbeiten zum Patent anmelden. Dort liegen nicht selten mehrere Monate teilweise mit detaillierten technischen Zeichnungen und Formeln angereicherte Anmeldungen zur Begutachtung, bevor sie im Register veröffentlicht werden. Da können Praktikanten viel lernen.

Selbst wenn die Werkstudenten von sensiblen Datenbanken ferngehalten werden, droht ihren Arbeitgebern Gefahr. Erst kürzlich meldete der europäische Flugzeugbauer Airbus den Diebstahl von zwei Laptops aus der Zentrale im französischen Toulouse. Auf den Geräten sollen sich unter anderem die geheimen Baupläne der Flugzeugmodelle A330, A340 und A350 befunden haben. Nach Informationen der französischen Zeitung „Le Parisien“ hat Airbus den französischen Inlandsgeheimdienst DCRI eingeschaltet. Airbus spielt den Fall herunter. Es hätten sich keine wirklich sensiblen Pläne auf den Geräten befunden.

Scanner im Aktenvernichter

Die stetig steigende Zahl solcher Spionagefälle führen Experten auch auf den Abbau der Stammbelegschaften in vielen Unternehmen zurück. „Wie hoch kann das Verantwortungsgefühl eines Zeitarbeiters sein, der Zugriff auf sensible Informationen hat und nächsten Monat bei einem anderen Unternehmen zum Einsatz kommt?“, fragt Professor Alexander Huber, Sicherheitsexperte an der Beuth Hochschule für Technik in Berlin. „Welche Verlässlichkeit können wir von einer Putzfrau erwarten, die trotz ihres 45-Stunden-Jobs mit 1100 Euro brutto für ihre Familie sorgen muss?“

Die Gefahr wird von vielen Unternehmen unterschätzt. Das normale Halbwissen eines technischen Laien reicht aus, um an Firmen-Interna heranzukommen und sie systematisch abzuzweigen. Jede Putzkraft kann den Auftrag ausführen, abends, beim Säubern der Büros, an der Rückseite der Rechner einen unscheinbaren Keylogger anzubringen. Keylogger sind elektronische Winzlinge, die alle Tastaturanschläge aufzeichnen. Sie werden am nächsten Abend durch einen neuen ausgetauscht. Die Konkurrenz ist also immer auf dem neuesten Stand. Ähnlich unkompliziert ist es, für Externe die Speicherkarte im Fotokopierer auszutauschen und so alle Kopien auszulesen. Vor allem neuere Modelle speichern Kopiervorlagen zuerst ab, bevor sie vervielfältigt werden – eine sehr effiziente Methode, um an wichtige Papiere zu kommen.

Ohne dass die Firmenchefs etwas von dem Angriff mitbekommen, können Fremde auch den Aktenvernichter unter ihre Kontrolle bringen. Sie müssen nur nachträglich Scanner an der Öffnung des Reißwolfs anbringen, die jede Seite vor ihrer Zerstörung sorgfältig kopieren und als E-Mail über das Mobilfunknetz an eine Adresse im Ausland schicken. „Das nenne ich effiziente Datenbeschaffung, fokussiert auf das Wesentliche“, ätzt Sicherheitsprofessor Huber. Selbst zerhackte Papierschnipsel holen Geheimdienste wieder aus dem Aktenvernichter heraus und setzen sie zusammen. Eine neu entwickelte Software übernimmt die sonst so aussichtslose Puzzlearbeit.

Für Holger Baum war es eine Hiobsbotschaft. Vor einer Woche teilte die WirtschaftsWoche dem Chef des Rechenzentrums der Technischen Universität Ilmenau mit, dass es einem Hacker zeitweise gelungen war, über spezielle Suchmaschinen im Internet Rechnungen, Kostenkalkulationen, Projektskizzen sowie Briefe an den Rektor Peter Scharff einzusehen, herunterzuladen und auszudrucken. Daraufhin startete die thüringische Hochschule eine intensive Recherche.

Daimler-Zentrale in Stuttgart
Quelle: AP

Eigentlich sollten die Dateien auf einem mit Passwort geschützten externen Rechner liegen. Doch einige Bereiche waren ohne Wissen der Universitätsleitung – zum Teil auch nur vorübergehend – ohne Zugriffsschutz abrufbar. Dadurch konnten Außenstehende mithilfe der speziellen Suchmaschine Auszüge aus dem Schriftverkehr mit E.On, NokiaSiemensNetworks und DaimlerChrysler Bank einsehen. Die Suchmaschine heißt Napalm FTP Indexer und wird vor allem in Hackerkreisen genutzt. Relativ leicht lassen sich aus den Datensammlungen der Internet-Rechner Dateien herausfischen, die eigentlich nur für den internen Gebrauch gedacht sind und gar nichts im World Wide Web zu suchen haben.

Die Panne liefert einen Vorgeschmack, was Unternehmen, Behörden und Forschungseinrichtungen in der Wolke passieren kann, wenn sie sich Computerprogrammen auf Großrechnern von IT-Dienstleistern bedienen, statt die Software auf den eigenen Rechnern zu installieren. The Cloud, die Wolke, nennen IT-Verantwortliche diesen jüngsten Trend, Rechnerkapazitäten auszulagern. Dabei vertrauen sich Unternehmen Web-Dienstleistern an, die Datenpakete über das Internet auf unausgelastete Rechner in aller Welt verteilen.

Auf diesem Wege müssen auch die kompletten Auftragsdaten über die Ausstattungsmerkmale und den Verkaufsort aller Mercedes-Fahrzeuge von einer internen Datenbank der Daimler AG nach Moskau gelangt sein. Jahrelang konnte jeder auf einer Web-Seite des russischen Mercedes-Benz-Clubs nach Belieben Fahrgestellnummern eingeben und bekam umgehend alle Details über den Fahrzeugtyp, die Farbe, das Verkaufsdatum und die bei der Bestellung berücksichtigten Sonderausstattungen angezeigt.

Enge Verbindung zu Geheimdiensten

Auf die Anfrage der WirtschaftsWoche, wie diese Daten ins Internet gelangen konnten, ordnete die Daimler-Zentrale in Stuttgart das sofortige Abschalten des sogenannten Fahrgestellnummern-Dekoders an, der die zu jedem Fahrzeug vorliegende Datensammlung im Internet sichtbar macht. „Der Dienst ist vorübergehend nicht verfügbar“, heißt es in einer Fußnote auf der Web-Seite.

Offenbar hatte sich der russische Mercedes-Fanclub den Zugriff auf technische Auftragsdaten verschafft, die sonst nur „Händler, Werkstätten und Gutachter einsehen können“, räumt Daimler in einer offiziellen Stellungnahme ein. Ein Verstoß gegen den Datenschutz liege aber nicht vor, weil keine Rückschlüsse auf die persönlichen Daten der Käufer möglich gewesen seien. Dem Fanclub in Moskau war aber offenbar klar, dass die Installation des Dekoders bei Daimler auf wenig Gegenliebe stößt: „Sie sollten unseren Service nicht nutzen, wenn Sie Angst vor der russischen Mafia haben und unter Verfolgungswahn leiden“,

sticheln die Mercedes-Freunde auf ihrer Web-Seite.

Vor allem in Russland und China leben unzählige gut ausgebildete Cyber-Krieger, die in der Grauzone zwischen Wirtschaftskriminalität und Wirtschaftsspionage leben und enge Verbindungen zu den Geheimdiensten pflegen.

Erst kürzlich konnten Forscher das bislang größte computergesteuerte Spionagenetzwerk in Chengdu im Südwesten Chinas lokalisieren. In mühevoller Kleinarbeit enttarnten Wissenschaftler aus dem in Toronto ansässigen Munk Centre for International Studies die Urheber eines Angriffs auf die Büros der Vereinten Nationen (UNO) und die tibetische Exilregierung des Dalai Lama.

Spektakulärer Spionageangriff aus China

Acht Monate verfolgten die Experten die Spuren der Spione, die über kostenlos verfügbare soziale Netzwerke wie Twitter, Google Groups, Baidu Blogs, blog.com und Yahoo Mail unter anderem 1500 E-Mails des Dalai Lama ausspähten. „Es gibt eine dunkle Unterwelt im Cyberspace“, warnt der Web-Forscher Ron Deibert von der Universität Toronto. „Länder brauchen nicht mehr Milliarden in die Satelliten-Aufklärung stecken, über das Web geht das viel einfacher.“

Ganz gezielt hatte der Spionagering nach Begriffen wie „confidential“ und „restricted“ gesucht und war dabei fündig geworden. Unter anderem kamen sie so in den Besitz vertraulicher Daten aus Visa-Anträgen von Bürgern aus 16 Ländern, darunter auch Deutschland.

Ohnmächtige Mittelständler wie Eginhard Vietz haben längst die Lust auf Geschäfte mit den Chinesen verloren. Bereits vor sechs Jahren, mitten in der China-Euphorie, zog sich der 69-jährige Gründer und Geschäftsführer der Vietz GmbH in Hannover wieder aus dem Reich der Mitte zurück.

Die Reißleine zog Vietz nach einem spektakulären Spionageangriff. Chinesische Partnerfirmen hatten Mitarbeiter in einem Joint Venture installiert, das nur ein Ziel verfolgte: möglichst viel Know-how abzuziehen. Als auch noch der Bereichsleiter mit einem Laptop mit geheimen Baupläne verschwand, bereitete Vietz dem Spuk ein Ende. „Alle, die in China komplette Maschinen bauen, haben die gleichen Erfahrungen gemacht. Doch keiner traut sich, darüber zu sprechen.“