

Wirtschaftskriminalität

Vom Mitarbeiter zum Spion

Von *Anne Seith*, Frankfurt am Main

Firmen und Sicherheitsexperten schlagen Alarm: In der Wirtschaftskrise hat Industriespionage Hochkonjunktur. Der Wettbewerbsdruck nimmt zu - und wenn Angestellte um ihren Job bangen, wächst die Bereitschaft, Know-how an einen Konkurrenten zu verscherbeln. Vor allem Mittelständler trifft es hart.

Die Entdeckung war so ungeheuerlich, dass Eginhard Vietz es erst nicht glauben konnte. Die gleiche Produktionshalle, eins zu eins nachgebaut. Nur 85 Kilometer entfernt vom Original, der neuen Fabrik in China, die Vietz mit einem einheimischen Partner errichtet hatte, um die bekannten deutschen Vietz-Maschinen für den Pipeline-Bau endlich auch in Asien zu produzieren. Jeden Morgen, an dem der 68-jährige Unternehmer aus Hannover nicht vor Ort war, fuhr ein VW-Bus hin und her. Arbeiter wurden ausgetauscht. Ein Know-how-Transfer auf Rädern.

Vietz lernte bald, dass die Gefahr nicht nur im fernen Asien lauert. Zweimal wurde sein Hauptrechner in Hannover in den vergangenen Jahren attackiert. Einmal sei es die CIA gewesen, sagt Vietz. Am meisten hat den Unternehmer mit der stattlichen Figur und dem zurückgekämmten weißen Haar aber der jüngste Fall erschüttert. Ein Mitarbeiter, seit Jahren dabei, kündigte und machte ein Konkurrenzunternehmen auf. Das Geschäftsmodell: Der Verkauf einer brandneuen Methode zum Rohrtransport. "Unsere Technologie", sagt Vietz. Der einstige Mitarbeiter habe alles mitgenommen, sagt Vietz: "Sämtliche Zeichnungen, die Kundendatei, Angebote." Bald soll es zum Gerichtsverfahren kommen.

Vietz ist noch immer empört. "Der Mann hat bei uns gelernt, Groß- und Außenhandelskaufmann", erzählt der Unternehmer. "Einmal ist er sogar durch die Prüfung gefallen. Aber wir haben ihn gefördert." Die "menschliche Enttäuschung" sitze tief, dass ausgerechnet so einer betrügt.

Dabei sind es oft langjährige Mitarbeiter, ganz normale Kollegen, die irgendwann ihr Wissen versilbern wollen. Auch ein Maschinenbauer musste jüngst erleben, wie ein Projektleiter sein Wissen dem Konkurrenten verkaufen wollte. Der Mann war mehr als 22 Jahre im Unternehmen. Um möglichst viele Daten unauffällig zusammenzuraffen, fragte er Untergebene nach ihren Zugangsdaten, ohne dass jemand Verdacht schöpfte. Männlich, verheiratet, überdurchschnittlich gebildet und selten vorbestraft - so beschreibt eine Studie den typischen Täter. Die Untersuchung hat die Uni Leipzig für die Unternehmensberatung Rölfspartner erstellt.

In der Krise sinkt die Hemmschwelle

Meist greife ein Angestellter erst zu, wenn er Probleme habe, heißt es darin. Wenn etwa der Jobverlust droht. Industrie- und Handelskammern, Verfassungsschützer und Sicherheitsexperten schlagen deshalb Alarm, mahnen zu mehr Vorsicht. In der Wirtschaftskrise drohe die Zahl der Spionagefälle rasant zu steigen. Und schon 2007 sei der Wirtschaft ein Schaden von geschätzt 20 Milliarden Euro entstanden, warnten etwa die IHK in Potsdam und der brandenburgische Verfassungsschutz jüngst.

Genau beziffern lässt sich die Zahl der Attacken freilich nicht. Betroffene Firmen scheuen die Öffentlichkeit und wenden sich deshalb nur selten an die Polizei. Lieber gehen sie zu Detekteien und privaten Sicherheitsfirmen, die die Vorfälle diskret untersuchen und die Firmen auf Schwachstellen abklopfen. Die Branche hat derzeit Hochkonjunktur. "In den letzten Monaten haben wir einen drastischen Anstieg an geschädigten Unternehmen", sagt Christian Schaaf vom Berater Corporate Trust. Auch die Angst nimmt zu. "Im letzten Jahr hat sich unser Auftragsvolumen bei Präventionskonzepten verdreifacht", sagt etwa der Chef des Münchner Beraters Prevent, Thorsten Mehles.

Oft bündeln die Sicherheitsfirmen Technik und Know-how, von dem viele Polizei-Teams träumen dürften. Der 47-Jährige Mehles etwa war selbst über Jahre hinweg bei der Kriminalpolizei und

beim BND. Zu seinem 45-Mann-Team gehören unter anderem eine Kriminalpsychologin, die früher bei Scotland Yard war, und Elmar Mäder, langjähriger Kommandant der päpstlichen Schweizer Garde.

Auch IT-Forensiker, Buchhalter und Juristen arbeiten mit. Sie durchforsten beim Kunden die Strukturen und die Bücher. Gehen mit schwererer Gerätschaft auf Wanzenjagd, nehmen dafür in Konferenzsälen jede Steckdose auseinander und durchleuchten die Wände mit Wärmebildkameras. Oder sie befragen einfach nur die Mitarbeiter nach ihrem täglichen Verhalten.

"Datensammler, die alle Informationen mitnehmen"

Schließlich sind Unternehmen oft an unzähligen Stellen gleichzeitig verletzbar. Vor allem Mittelständler. Große Konzerne haben riesige Sicherheitsabteilungen, die das Werksgelände und die IT hermetisch abriegeln. Kleine und mittlere Unternehmen unterschätzen das Problem häufig. Sie lassen Lieferanten frei über das Werksgelände laufen oder Handwerker und Reinigungsfirmen ohne Bedenken stundenlang allein im Büro. Selbst nachts. Dabei dauert es nur noch Sekunden, eine Wanze zu installieren. Oder einen Keylogger zwischen Tastatur und PC zu stecken, der alle Eingaben an dem Gerät speichert oder direkt einem fremden Empfänger sendet.

Eine der größten Gefahren ist Sicherheitsexperten zufolge allerdings immer noch der Mitarbeiter. Oft aus reiner Unachtsamkeit heraus. Er benutzt USB-Sticks, die ihm als Werbegeschenk in die Hand gedrückt wurden und lädt sich so unbemerkt Spionage-Software auf den PC. Er telefoniert lautstark am Flughafen oder packt im Zug den Laptop aus, arbeitet sorglos an vertraulichen Dokumenten. Dabei kann nicht nur der Nachbar mitlesen, auch aus 100 Metern Entfernung können Daten auf dem Bildschirm noch mühelos auf ein anderes Gerät gespiegelt werden. Ähnlich problemlos lassen sich Handys, Palms und Blackberrys anzapfen.

"Es gibt Datensammler, die gezielt auf öffentliche Plätze gehen und alle Informationen mitnehmen, die sie bekommen", sagt Corporate-Trust-Chef Christian Schaaf. "Wie Staubsauger." Schaaf zufolge stehen die Täter am Flughafen oder ziehen am Montagmorgen durch ICEs, die auf typischen Business-Strecken fahren. Berlin-Frankfurt etwa. Manchmal sind es Kriminelle, die Firmen erpressen wollen. Manchmal sind es Geheimdienstler. "In vielen Ländern gehört es zu ihrem gesetzlichen Auftrag, Wirtschaftsspionage zu betreiben."

Mini-Sender, die in Feuerzeuge passen

Praktisch allen Spionen, Laien und Profis, steht dabei ein breites Angebot an Hightech zur Verfügung, das nicht schwer zu organisieren ist. Das meiste gibt's im Internet. Winzige Videokameras, stecknadelgroße Wanzen und Mini-Sender etwa, die in Feuerzeuge passen. Im bayerischen Kolbermoor wurde kürzlich der Geschäftsführer einer chinesischen Betonbaufirma festgenommen. Er hatte bei einer Werksbesichtigung Ton- und Bildaufnahmen gemacht - das Mini-Gerät war mit einem Clip am Hosengürtel befestigt.

Oft reicht auch schlichte Dreistigkeit. Anrufer stellen sich als Mitarbeiter einer "US-Research-Firma" vor und wollen Firmeninterna wissen. Oder sie fragen die Sekretärin nach dem Geburtstag des Chefs, nach seiner Familie, etwa mit dem Vorwand, ein passendes Geschenk zu suchen. Tatsächlich setzen sich viele Passwörter aus diesen schlichten Daten zusammen.

Allerdings nicht bei Pipeline-Experte Vietz. Er hat sich gerüstet, sein Unternehmen so weit es geht spionagefest gemacht. Kein Mitarbeiter kann mehr allein auf alle Daten zugreifen. Stattdessen lädt ein externer EDV-Spezialist regelmäßig die einzelnen Pakete auf einen Hauptrechner. "Er ist vom Verfassungsschutz überprüft", sagt Vietz. Aus der Konstruktionsabteilung können zudem keine E-Mails verschickt werden und es herrscht dort striktes Handy-Verbot.

Und in China produziert Vietz gar nicht mehr.

URL:

<http://www.spiegel.de/wirtschaft/unternehmen/0,1518,648933,00.html>

FORUM:

Industriespionage - wie groß ist die Gefahr?

<http://forum.spiegel.de/showthread.php?t=8604&goto=newpost>

ZUM THEMA AUF SPIEGEL ONLINE:

Verfassungsschutz: Immer mehr Internet-Spionage gegen deutsche Firmen und Behörden (18.05.2009)

<http://www.spiegel.de/netzwelt/web/0,1518,625588,00.html>

Terrorbekämpfung: "Verfassungsschutz braucht Online-Durchsuchung" (01.04.2009)

<http://www.spiegel.de/politik/deutschland/0,1518,616767,00.html>

Headhunter-Abwehr: "Es gibt böse Buben, verdammt böse Buben" (06.02.2009)

<http://www.spiegel.de/unispiegel/jobundberuf/0,1518,604689,00.html>

Konzernsicherheit: Wie deutsche Unternehmen ihre Mitarbeiter überwachen (26.05.2008)

<http://www.spiegel.de/wirtschaft/0,1518,555503,00.html>

ZUM THEMA IM INTERNET:

Tagesticker: Rekordarbeitslosigkeit in den OECD-Staaten (manager-magazin.de)

<http://www.manager-magazin.de/koepfe/artikel/0,2828,649289,00.html>

SPIEGEL ONLINE ist nicht verantwortlich für die Inhalte externer Internet-Seiten.

© SPIEGEL ONLINE 2009

Alle Rechte vorbehalten

Vervielfältigung nur mit Genehmigung der SPIEGELnet GmbH