

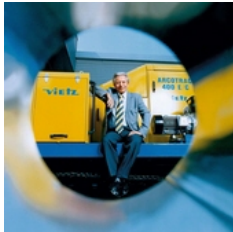
04.03.2009 , 11:37 Uhr

Wirtschaftsspionage

Mittelstand im Visier von Wirtschaftsspionen

von Midia Nuri

Eginhard Vietz hat ziemlich viel erlebt: Die CIA hackte die Computersysteme seines mittelständischen Unternehmens, zwei Mitarbeiter entwendeten Daten, ein chinesisches Staatsunternehmen kuferte eine komplette Vietz-Produktionsanlage samt Produkten ab. Mittelständler sind oft Ziel von Wirtschaftsspionen. Doch Schutz ist möglich.



Unternehmer Eginhard Vietz: Von der CIA, einem chinesischen Partnerbetrieb und eigenen Mitarbeitern ausspioniert.

DÜSSELDORF. Mittelständler sind, Sicherheitsexperten zufolge, leichte Beute für Spione aller Kaliber. "Sie sind oft Weltmarktführer in ihrer Nische", sagt Harald Woll, Leiter der Abteilung für Spionageabwehr, Geheim- und Sabotageschutz des baden-württembergischen Landesamtes für Verfassungsschutz. Weil Deutschlands Mittelständler oft Spitze sind, sind sie attraktiv für Wirtschaftsspione. Beispiel Vietz: Mit dem Know-how seiner Firma lässt sich der Bau von Ölpipelines deutlich schneller vorantreiben.

Zu den beliebtesten Zielen gehören Autozulieferer und Maschinenbauer, die es den Schnüfflern oft leicht machen: Zumal kleine und mittlere Unternehmen ihr wertvolles Wissen erstaunlich schlecht vor unbefugtem Zugriff sichern. "In mindestens 80 Prozent aller Fälle von Wirtschafts- und Industriespionage sind Mittelständler die Opfer", sagt Karl Stefan Schotzko, Geschäftsführer des Verbandes für Sicherheit in der Wirtschaft Baden-Württemberg (VSW-BW). Eine Studie der Münchner Beratungsgesellschaft Corporate Trust bestätigt: 96,1 Prozent der Schäden entfallen auf kleine und mittelständische Unternehmen.

Unternehmer Vietz hatte ein ungutes Gefühl. Dem 67-Jährigen war in seinem Pekinger Werk aufgefallen, dass Mitarbeiter ohne Grund fehlten und Konstruktionszeichnungen offen herumlagen. "Dabei bewahrte unser technischer Leiter die in seinem mit Vorhängeschlössern gesicherten Schreibtisch auf und schwor, er selbst habe sie nicht herumliegen lassen."

Vietz schilderte seine Beobachtungen einem langjährigen Freund im chinesischen Wirtschaftsministerium. Gemeinsam legten sich der Unternehmer und der Ministeriale in einem Kleinwagen vor dem Werkstor auf die Lauer. "Ein VW-Bus fuhr vor", erinnert sich Vietz, "Leute stiegen ein und aus, dann fuhr der Bus weg." Vietz und sein Freund hinterher. In Langfang, 40 Kilometer entfernt, hielt der Bus vor einer Halle. "Die gleiche Halle wie bei uns." Die gleichen Maschinen, die gleichen Produkte - aber viel mehr Leute.

"Vor Entsetzen sind mir die Tränen gekommen", erinnert sich Vietz. Offensichtlich hatte der Joint-Venture-Partner, die staatliche CNPC, es darauf angelegt, Know-how abzugreifen. Vietz ließ sich die Anteile rückübertragen, machte mit neuen Mitarbeitern und strengeren Sicherheitsvorkehrungen weiter. Und fühlte sich sicher.

Dann kam dieser neue Bewerber. Ingenieur, Chinese. Sprach perfekt Englisch. "Er hat uns sehr beeindruckt, weil er unglaublich pffigig und gut war", erinnert sich Vietz. Der Mann bekam den Posten als neuer technischer Leiter. Wenige Monate darauf erwischte Vietz ihn, wie er nachts mit einem - strikt verbotenen - Laptop Daten vom Rechner kopierte. Vietz reichte es. "Ich habe alles liquidiert und per Container nach Hause geschickt", erzählt er. Sein China-Engagement war nach mehr als 20 Jahren beendet.

Mit dem Spionieren war aber immer noch nicht Schluss. Zu Hause in Hannover bot der niedersächsische Verfassungsschutz Vietz an, die Sicherheitssysteme zu prüfen. Die Verfassungsschützer - bundesweit arbeiten sie mit 2 000 Unternehmen zusammen - fanden heraus, dass der US-Geheimdienst CIA schon zweimal die Rechner angegriffen hatte. "Die wollten an unsere neue Lasertechnologie heran", sagt Vietz. "Statt wie zuvor mit 300 Leuten 1,0 bis 1,3 Kilometer Pipeline am Tag zu verlegen, können Sie mit der neuen Technologie fünf Kilometer mit zehn Leuten schaffen."

Fast zeitgleich stellte sich heraus, dass auch ein ehemaliger langjähriger Mitarbeiter Know-how abgegriffen hatte. Der Mann hatte Vietz bei der Kündigung erzählt, er ziehe aus privaten Gründen nach Wuppertal und arbeite bei einem Lebensmittelhersteller. "Stattdessen war er bei einem unserer Zulieferer eingestiegen und hatte die Kundendatei und alle Zeichnungen dorthin mitgenommen", berichtet Vietz.

Der niedersächsische Unternehmer ist nur eines von vielen Opfern. "Die Dunkelziffer ist sehr hoch", sagt Verfassungsschutz Woll. 325 Fälle von Konkurrenzspionage registrierte das Bundeskriminalamt (BKA) 2008 - in Fünftel mehr als vor fünf Jahren. "Bei der Produktpiraterie stieg die Zahl um das Zehnfache auf 32 000 Fälle im vergangenen Jahr", sagt Jörg Ziercke, Präsident des Bundeskriminalamtes (BKA). Die oberste Polizeibehörde beobachtet, dass die Geheimdienste Russlands und Chinas zunehmend die Computer deutscher Unternehmen vorzugsweise mit Trojanern ausspionieren - schädlichen Programmen, die sie von außen einschleusen und die ihnen Zugriff auf die befahrenen Computer oder Server verschaffen.

Wie hoch der Schaden ist, lässt sich nur schätzen. Die Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC) beziffert in einer Studie den Schaden europäischer Unternehmen-Konzernen wie Mittelständlern - durch Spionage für die Jahre 2005 und 2006 auf durchschnittlich 1,6 Millionen Euro.

Der Volkswirtschaft kommen dadurch Jobs und Innovationsvorsprung abhanden. Auf 80 Milliarden Euro bundesweit schätzt Frank Hülsberg den Gesamtschaden. Hülsberg leitet bei den Wirtschaftsprüfern von KPMG die Abteilung Forensik, die Computerdaten auf Spuren krimineller Handlungen durchsucht. Zwei Drittel aller Spionagefälle kommen durch Zufall ans Licht, beobachtet Steffen Salvenmoser, der die Forensik bei PwC verantwortet.

Viele Attacken ließen sich relativ einfach verhindern. "Gerade Mittelständler sind oft viel zu vertrauensvoll", sagt KPMG-Experte Hülsberg. "Es gibt keine gefährlicheren Täter als die von innen", so Verbandsgeschäftsführer Schotzko. Auch Fremdfirmen sollten die Unternehmer im Auge behalten. "Zum Teil werden die mit Werksausweisen durchgewinkt." Überprüft werden sie ebenso selten wie Praktikanten, Diplomanden oder Aushilfen.

"Unzufriedene Mitarbeiter gibt es überall", sagt Schotzko. "Die Finanzkrise und die mit ihr einhergehenden Umstrukturierungen und Stellenstreichungen erhöhen die Gefahr für Wirtschaftsspionage noch zusätzlich", sagt Klaus-Dieter Matschke, Gründer und Inhaber der Frankfurter Sicherheitsberatung KDM.

Verfassungsschützer wissen: In einem von fünf Fällen bringen Profi-Agenten Unternehmensmitarbeiter erfolgreich dazu, ihnen vertrauliche Informationen zu überlassen. "Sie haben es hier mit bestens ausgebildeten Leuten zu tun, die jede Schwachstelle systematisch in Erfahrung bringen und dann gnadenlos ausnutzen", warnt Sicherheitsberater Matschke.

Geheimdienstlich geschulte Mitarbeiter finden leicht heraus, ob einer Schulden hat oder erpressbar ist. "Eine beliebte Methode ist, sich auf Kontaktanzeigen von Sekretärinnen zu melden oder den technischen Leiter auf Messebesuch im Ausland von einer als Prostituierten getarnten Spionin aushorchen zu lassen", so Matschke. Kontakt lasse sich auch über private Hobbys herstellen. Erfolgversprechend ist auch, auf Messen als vermeintliche Kollegen mit Entwicklungsingenieuren zu fachsimpeln. Die Fachleute freuen sich oft über den informellen Austausch. "Irgendwo bekommen Sie fast jeden Menschen zu fassen", so der ehemalige Kriminaloberrat.

Gelegentlich dreht Matschke den Spieß um - zum Wohle seiner Klienten. Um einen Forschungsingenieur zu überführen, der die Technologie eines schwäbischen Maschinenbauers an einen französischen Konkurrenten verraten hatte, gründete Matschke eigens eine Tarnfirma: "Wir haben ihm Headhunter geschickt und uns interessiert gegeben, an seinem Wissen und Können teilzuhaben." Matschke ließ den Mann umschmeicheln - und brachte ihn schließlich dazu, die Technologie ein weiteres Mal auf eigene Rechnung zu verkaufen. Zur Vertragsunterzeichnung lud der vermeintliche neue Arbeitgeber den

Produktentwickler ins Pariser Hotel Ritz ein - wo der sich seinem Ex-Chef gegenüber sah. Das französische Unternehmen warf den Spion hinaus und zahlte Matschkes Auftraggeber eine Millionen-Entscheidung.

"Langfristig ist ein gutes Betriebsklima der wirkungsvollste Schutz vor Know-how-Abfluss", glaubt Matschke. Das BKA hält Unzufriedenheit für eines der wichtigsten Motive in der Wirtschaftskriminalität. Matschke rät Unternehmern dazu, wichtige Mitarbeiter auch mal über die Maßen zu loben - und sie ruhig auch mal mit einer bezahlten Reise zu belohnen. Aber auch im angenehmsten Betriebsklima müssen Mittelständler den Zugang zu Informationen kontrollieren. "Wenn das Risiko, erwischt zu werden, gegen null geht, darf man sich nicht wundern, wenn etwas passiert", warnt Schotzko.

Mittelständler Eginhard Vietz hat seine Lektion gelernt. Wo zuvor alle nichtgewerblichen Mitarbeiter in sämtliche Räume gelangen konnten, zeichnen heute Kartenlesegeräte auf, welcher Mitarbeiter sich Zutritt verschafft. "Wenn unsere Mitarbeiter Konstruktionszeichnungen einsehen, müssen sie unterschreiben, dass sie keine Kopien ziehen. Das muss auch jeder Kunde, bevor er technische Daten bekommt. Bei Verstoß drohen millionenschwere Strafen. "Wer nicht unterschreibt, bekommt kein Angebot", so Vietz.

"Mittelständler können und sollten vieles auch über vertragliche Vereinbarungen regeln, beispielsweise indem sie Zulieferern untersagen, ihre Maschinen vorzuzeigen", rät Patentanwalt Wolfram Schiweck, der für die Münchner Kanzlei Viering, Jentschura & Partner das Büro in Singapur leitet. Patentschutz helfe zwar, meint Schiweck, sei aber nicht immer sinnvoll: "Wenn sich ein Produkt nicht ohne Weiteres nachbauen lässt, ist es besser, kein Patent anzumelden", sagt der Patentanwalt, "denn das Patent macht die Technologie ja öffentlich."

"Ein sehr bewusster Umgang mit Informationen und ihrem Schutz ist immer wichtig - besonders, wenn Unternehmen in China Geschäfte machen", ist Thomas Pattloch überzeugt. Der Rechtsanwalt hat jahrelang für eine Wirtschaftskanzlei deutsche Mittelständler in China vertreten, vor allem in Fällen von Produktpiraterie. Nun arbeitet er als Experte für geistiges Eigentum, kurz IP (vom englischen "Intellectual Property") für die EU-Delegation in Peking.

Vor allem die "gigantische Informationsgier" der Behörden macht Pattloch für den Informationsabfluss verantwortlich. 2003 führte die chinesische Regierung die Kennzeichnungspflicht mit dem Gütesiegel CCC ein. Betroffen sind Hersteller von Aufzügen ebenso wie Handyzubehörlieferanten oder Möbelproduzenten. "Von den Unternehmen, mit denen wir sprechen, betrifft das Siegel im Zweifel alle", sagt Pattloch.

Im CCC-Prüfverfahren zwingen die chinesischen Behörden Unternehmen dazu, etliche technische Daten offenzulegen. "Auch wenn der Staat den Missbrauch dieser unzähligen Informationen nicht erlaubt - es ist für ihn fast unmöglich, ihn zu unterbinden", urteilt Pattloch. Zum Prüfverfahren gehört auch eine Besichtigung des Stammwerks. "Dabei dürfen Mittelständler sich keineswegs so verhalten, als hätten sie einen europäischen Kunden oder Zulieferer zu Besuch", warnt Pattloch.

Alles, was sie für die Erteilung des Gütesiegels nicht unbedingt zeigen müssen, sollte weggeschlossen sein, rät der Experte. Bei einem Verdacht sollten sich Unternehmer an den IP-Helpdesk der EU in China - die Anlaufstelle für Unternehmen mit Fragen oder Problemen in Sachen Schutz des geistigen Eigentums - wenden. Oder in schweren Verdachtsfällen gleich an die Kommission. "Wenn ein Inspektionsmitglied sein Handy zum Fotografieren zückt, sollten Mittelständler das freundlich, aber bestimmt unterbinden", rät Pattloch. Und darauf achten, dass die Gruppe zusammenbleibt; keiner darf verlorengehen.

"Mitarbeiter zu schulen, gehört zur langfristigen Prävention", sagt KPMG-Mann Hülsberg. Geschulte Mitarbeiter sprechen eher fremde Personen an, die allein die Unternehmensflur entlangschlendern, und sie passen besser auf, was sie selbst außerhalb der Firma tun und sagen.

Fast jeder Experte weiß davon zu berichten, wie sich Techniker oder Manager eines Unternehmens im Bahnabteil über Kunden unterhalten haben. PwC-Forensiker Salvenmoser konnte einmal im Zug die aktuellen Finanzdaten eines börsennotierten Unternehmens mitlesen. "Ich habe den Mann dezent darauf angesprochen"

Link zum Artikel: <http://www.handelsblatt.com/unternehmen/nachrichten-trends/mittelstand-im-visier-von-wirtschaftsspionen;2161179>
