

"Gefahrenbarometer 2010"

Mittelständler fürchten sich vor Spionage

Von Claudia Tödtmann

29.03.2009 4,5 (2) **Legende**

Mehr als jede zweite mittelständische Firma in Deutschland hält nach den Ergebnissen einer Exklusiv-Studie Spionage- und Informationsdiebstahl für das größte Risiko ihres Unternehmens. Die Furcht ist berechtigt. Denn gegen Wirtschaftskriminalität sind die wenigsten Mittelständler ausreichend gewappnet.



Datendiebstahl kann schwere Folgen für ein Unternehmen haben. Quelle: dpa handelsblatt.com

DÜSSELDORF. Der Chef des niedersächsischen Unternehmens für Spezialchemie war arglos, bis ihn sein neuer Hausjustiziar auf etwas aufmerksam machte. Wo sich denn die - für die Firma überlebenswichtigen - Konstruktionszeichnungen so befänden? Ein Satz davon lag beispielsweise bei der Umweltbehörde - dort wähnte der Chef sie sicher. "Dass es heute Einsichtsrechte für derlei Firmenunterlagen bei Behörden gibt - und zwar für jedermann und auch ohne jedes konkrete Anliegen -, das war dem Chef nicht klar", erzählt Alexander Haudan, Anwalt bei der Topkanzlei Taylor Wessing in Düsseldorf.

Der Firmenchef handelte direkt. Er fuhr persönlich zur Behörde, stempelte die Konstruktionszeichnungen als "geheim" - damit jeder Sachbearbeiter gewarnt war - und versiegelte sie im Umschlag. Das war gerade noch rechtzeitig. Zwei Tage später tauchten zwei Ex-Mitarbeiter dieser Chemiefirma bei der Behörde auf, die genau in diese Zeichnungen Einblick nehmen wollten. "Mit der Haltung des Firmenchefs `Meine Leute machen so etwas nicht' war es dann vorbei", so Haudan.

So wie er denkt heute bereits die Mehrzahl der Mittelständler: 53 Prozent von ihnen glauben, dass Spionage und Informationsdiebstahl oder-verlust in Zukunft die größten Risiken für ihr Unternehmen hierzulande darstellen. 50 Prozent befürchten Hackerangriffe, und 29 Prozent denken, dass Korruption für sie ein hohes Risiko ist. Das zeigt die Umfrage "Gefahrenbarometer 2010" vom Sicherheitsunternehmen Corporate Trust zusammen mit dem Handelsblatt, das Sicherheitsrisiken des deutschen Mittelstands auslotet.

Befragt wurden 5 154 Geschäftsführer, Vorstände, Sicherheitsverantwortliche, IT- und Personalleiter in mittelständischen Unternehmen aus allen Branchen (Antwortquote: neun Prozent). Zudem erfolgten 30 Tiefeninterviews mit Weltmarktführern, also Hidden Champions.

Nur 20 Prozent haben Compliance-Richtlinien

Ein weiteres bemerkenswertes Ergebnis der Umfrage: Große Mittelständler werden öfter Opfer krimineller Delikte wie Untreue, Unterschlagung, Betrug, Korruption oder Industriespionage als kleinere Mittelständler. Die meisten Schäden - 37 Prozent - entstanden bei den größeren Mittelständlern mit 50 bis 250 Millionen Euro Umsatz und 250 bis 1 000 Mitarbeitern. Die

Unternehmen mit 250 Millionen bis eine Milliarde Euro Umsatz waren in 24 Prozent der Fälle die Geschädigten. 21 Prozent der Schäden entfielen auf Unternehmen mit zehn bis 50 Millionen Euro Umsatz. Wer über eine Milliarde Umsatz hat, verzeichnet 18 Prozent der Schäden. Generell gilt: Großunternehmen sind weniger gefährdet.

"Fast alle Konzerne haben die Sicherheitsabteilung als Schutzschild, zum Teil Abteilungen mit mehreren Hundert Mann", weiß Sicherheitsprofi Christian Schaaf, Chef der Sicherheitsberatung Corporate Trust in München. "Mittelständler zeigen an der Stelle dagegen häufig eine offene Flanke." Das zeigt auch die Studie: Gegen Wirtschaftskriminalität sind die wenigsten Mittelständler ausreichend gewappnet. Compliance-Richtlinien haben nur 20 Prozent von ihnen, ihre Revision zu Fachseminaren schicken nur sechs Prozent, und Whistle-Blowing-Systeme haben nur fünf Prozent installiert.

Drohen Risiken von innen, also von den eigenen Leuten, so muss dies nicht einmal einen kriminellen Hintergrund wie Racheakte entlassener Mitarbeiter oder Geldgier haben. Mal werden Interna leichtsinnig auf dem Flughafen ausposaunt oder am Telefon allzu bereitwillig Firmeninterna ausgeplaudert. Oder Mitarbeiter merken einfach nicht, welche Intention der Anrufer mit den vielen Fragen tatsächlich hat und dass sie gerade ein Opfer von Industriespionage werden. Eine brisante Rolle spielen dabei heute Laptops: Verliert ein Mitarbeiter sein Gerät oder wird es ihm gar gestohlen, ist es eine wahre Fundgrube für Konkurrenten - und es kann sich zu einem großen Problem auswachsen, wenn Kundendateien oder Konstruktionspläne darauf waren und in die falschen Hände fallen.

Oder USB-Sticks: So bekam kürzlich ein deutscher Pharma-Vorstand von einem potenziellen chinesischen Geschäftspartner einen sehr edlen USB-Stick mit Goldeinfassung geschenkt - der aber leider ein Spionageprogramm enthielt. "Hätte er ihn eingesetzt, wäre der komplette Inhalt seines Laptops nach China gemailt worden", berichtet Sicherheitsexperte Schaaf. Nur durch einen Zufall hatte ein hauseigener IT-Experte den auffälligen Stick bei dem Topmanager entdeckt und vorsichtshalber überprüft, bevor der ihn einsetzen konnte.

Kein Wunder, dass 53 Prozent der Befragten in den nächsten zwei Jahren planen, ihre Mitarbeiter schulen zu lassen, damit sie für solche Situationen sensibilisiert werden. Und 29 Prozent wollen in dem Zeitraum in IT-Sicherheit investieren. Oft machen es die Unternehmen den Tätern auch zu leicht: In 60 Prozent der Unternehmen kann die EDV noch mit USB-Sticks angezapft werden. Manche Firmen dagegen haben nur IT ohne sogenannte USB-Ports. Dieselbe Zahl von Firmen eröffnet, so die Studie, unvorsichtigerweise allen Mitarbeitern offenen Zugang ins Internet - ohne eine Policy für die Mitarbeiter zu haben. Somit hat das Unternehmen später dann auch keine Kontrollmöglichkeit mehr.

Die Angst vor Imageschäden ist groß

Ein weiteres Beispiel: Über die Hälfte der Unternehmen macht ihren Mitarbeitern oder Geschäftspartnern keine klaren Vorgaben, wie sie mit vertraulichen Informationen umgehen sollen. 58 Prozent glauben, dass es die größte Bedrohung für IT und Telekommunikation ist, dass die Mitarbeiter leichtfertig mit Sicherheitsstandards umgehen.

Zudem: Viele Fälle von Wirtschaftskriminalität und Industriespionage werden gar nicht erst aufgedeckt und sogar von den Unternehmen totgeschwiegen, weiß Schaaf. Denn die Angst vor

Imageschäden ist groß. Ein Motiv, warum manche Unternehmen doch Strafanzeige erstatten, ist: dass sie den finanziellen Schaden bei einer Versicherung geltend machen möchten.

Interessant ist dieses Phänomen: "Viele Unternehmen räumen ein, dass sie nur geringe Kenntnisse über wirtschaftskriminelle Handlungsmuster haben. Und genau deshalb unterschätzen sie das Risiko, selbst Opfer von Wirtschaftskriminalität zu werden und investieren zu wenig in Präventionsmaßnahmen", kritisiert Jörg Ziercke, Präsident des Bundeskriminalamts. Obwohl die Schadenssumme schon 2007 vier Milliarden Euro betragen habe - die Dunkelziffer nicht mit eingerechnet.

Die Studie im Detail: Auch die Sicherheit in den Firmen selbst ist nicht überall gewährleistet. 33 Prozent der Mittelständler können nicht sagen, wer gerade in ihrem Unternehmen ist. Nur 43 Prozent stellen sicher, dass Besucher stets in Begleitung eines Mitarbeiters sind. 38 Prozent haben ein Zutrittskontrollsystem, und 34 Prozent notieren am Empfang jeden Besuchernamen.

Gefahren liegen auch in der Internationalität. 72 Prozent der Befragten sind auch im Ausland tätig. Die größten Bedrohungen sehen sie durch Korruption (66 Prozent), Produktpiraterie und Informationsabfluss (48 Prozent), organisierte Kriminalität (41 Prozent) oder Diebstähle und Unterschlagungen (40 Prozent).

Referenzen als Schutz

Eins der erstaunlichsten Ergebnisse der Studie ist: 28 Prozent der Unternehmer sichern sich im Voraus überhaupt nicht ab, wenn sie mit ausländischen Geschäftspartnern zu tun haben. Nur 20 Prozent der Unternehmen machen einen intensiven Background-Check eines neuen Geschäftspartners. Compliance-Richtlinien sind immerhin bei 35 Prozent Vertragsbestandteil, eine Bonitätsprüfung vollziehen wenigstens 41 Prozent. Doch das, was gerade im Ausland am zweckmäßigsten ist, tun nur 38 Prozent: Sie holen Referenzen über ihren künftigen Geschäftspartner ein - bei anderen Unternehmen, die mit ihm schon länger zusammenarbeiten.

Heikel ist es auch für Unternehmen, wenn sie einer ausländischen Behörde - etwa in China - Produktbeschreibungen einreichen müssen, bevor sie in das jeweilige Land liefern dürfen. Schaaf: "Sind die verlangten Informationen überlebenswichtig für die Firma, sollte man das Kernthema nur umschreiben - ohne spezifische Detailangaben. Genügt das der Behörde nicht, sollte man es im Zweifel lieber ganz lassen." Diesem Rat ist so mancher Unternehmer - in Anbetracht des Risikos - gefolgt.

Wer blauäugig ist, dem kann es z.B. so ergehen: Einem Unternehmer, der einen Kooperationspartner für den Bau eines Steuerungsgeräts suchte, wurden in China aus dem Hotelsafe seine Produktionsbeschreibungen gestohlen. Das ereignete sich kurz vor seiner Entscheidung, welche von vier Firmen er beauftragen wollte. Jetzt wartet er darauf, wo sein Konkurrenzprodukt auftaucht. Billiger - dank gesparter Entwicklungskosten.