

Sie befinden sich hier: [vdi-nachrichten.com](http://vdi-nachrichten.com) » [VDI nachrichten](#) » [Technik & Gesellschaft](#) » [Technik & Gesellschaft](#)

## Industriespionage: Hacker-Angriffe auf Computernetze von Unternehmen sind seltener als die Preisgabe sensibler Daten durch eigene Mitarbeiter



### Wenn Mitarbeiter Wissen preisgeben

VDI nachrichten, Düsseldorf, 5. 9. 08, ciu - Es muss nicht unbedingt Absicht dahinter stecken, wenn Mitarbeiter sensible Informationen weitergeben. Oft reichen unachtsame Momente auf Dienstreisen oder bei Messebesuchen, um zum Spionageopfer zu werden. Der Schaden für die deutsche Wirtschaft ist dabei erheblich.



Geschäftsreisende werden leichter Opfer unbemerkten Diebstahls, als sie es vermuten. Davon geht Christian Schaaf, Geschäftsführer der Risikoberatung Corporate Trust in München, aus. Wie er im Vorfeld des FVW-Kongresses "Forum Business Travel", am 17. September in Köln, gegenüber den VDI nachrichten sagte, seien viele Geschäftsleute nicht ausreichend für die Problematik sensibilisiert. "In der Praxis werden beim Zoll Datenträger teilweise für 30 Minuten und mehr konfisziert, Hotelsafes werden gezielt nach Daten durchforstet oder angenommene teure Gastgeschenke für die spätere Erpressung von Daten genutzt", machte er deutlich.

Längst ist Industriespionage eine ernstzunehmende Bedrohung für die deutsche Wirtschaft, der allein im letzten Jahr ein Schaden in Milliardenhöhe entstand. Eine im Herbst 2007

von der auf Sicherheitsfragen spezialisierten Unternehmensberatung Corporate Trust gemeinsam mit dem Handelsblatt, Düsseldorf, und dem Büro für angewandte Kriminologie, Hamburg, durchgeführten Umfrage beläuft er sich auf mindestens 2,8 Mrd. € pro Jahr. Die Summe wurde aus den Angaben der Befragten auf alle deutsche Unternehmen hochgerechnet.

Andere bewerten die Bedrohung sogar noch höher. Dr. August Hanning z. B., Staatssekretär im Bundesinnenministerium und ehemaliger Leiter des Bundesnachrichtendienstes, schätzte den Schaden auf über 20 Mrd. € pro Jahr. Bei der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW), in der DIHK, Wirtschafts-, Sicherheits- und Branchenverbände vertreten sind, hält man für dieses Jahr eher 30 Mrd. € für wahrscheinlich und sogar bis zu 50 Mrd. € für möglich.

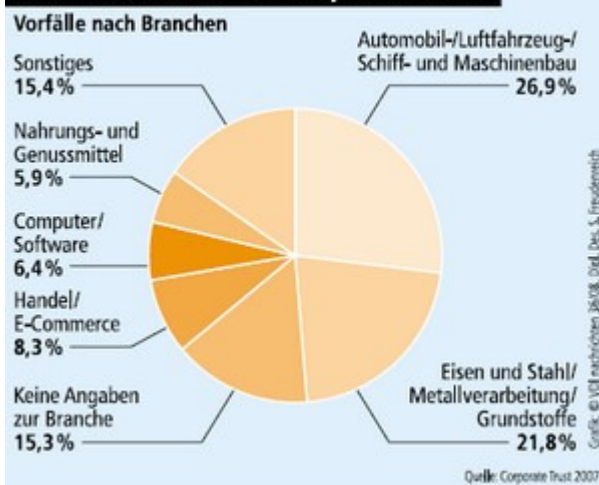
Industriespionage ist nicht mehr nur ein Betätigungsfeld für ausländische Geheimdienste, sondern ein gebräuchliches Mittel konkurrierender Unternehmen. Und sie "gewinnt im Rahmen des globalen Ringens um Marktanteile und Dominanz immer mehr an Bedeutung", heißt es in der Mitte Mai veröffentlichten Fassung des Verfassungsschutzberichts 2007. Während technologisch weniger entwickelte Staaten eher technisches Know-how ausspähen, um Kosten für die eigene Forschung und Entwicklung sowie Lizenzgebühren zu vermeiden, präzisieren die Verfassungsschützer, interessierten sich hochentwickelte Staaten für Produktideen, komplexe Fertigungstechniken sowie Unternehmens- und Marktstrategien.

Einen genaueren Einblick liefert die Corporate-Trust-Studie, an der sich sich 741 Unternehmen aus unterschiedlichen Industriebereichen beteiligten. Nahezu jedes Fünfte davon ist danach bereits Opfer eines "ungewollten Informationsabflusses" geworden: 18,9 % der befragten Unternehmen gaben an, mindestens einmal ausspioniert worden zu sein. Tatsächlich dürften es wesentlich mehr sein, denn immerhin 35,1 % der Firmen äußerten den Verdacht, ausspäht worden zu sein. Die Dunkelziffer ist hoch, die Angst vor einem Imageschaden ebenfalls und die Bereitschaft, den Fall publik zu machen, dementsprechend schwach ausgeprägt. Von den betroffenen Unternehmen hatte sich nur jedes Vierte an die Behörden gewandt. In 40 % der Fälle suchte man Hilfe bei externen Spezialisten.

Ziel der Spionageattacken waren meistens technische Innovationen bzw. Wissen über Produktionsabläufe. In Gefahr ausspioniert zu werden, sind der Studie zufolge zu vor allem kleine Unternehmen (10 Mio. € bis 50 Mio. € Umsatz oder 10 bis 50 Mitarbeiter) und mittelständische Unternehmen (50 Mio. € bis 500 Mio. €

Umsatz oder 50 bis 250 Mitarbeiter). Sie machten 38,5 % bzw. 57,6 % der Fälle aus. Konzerne, mit mehr als 500 Mio. € Umsatz oder mehr als 500 Mitarbeitern, waren nur in 3,9 % der aufgedeckten Schäden und Verdachtsfälle betroffen.

### Wo in deutschen Firmen spioniert wird



Besonders viele der geschädigten Unternehmen finden sich in den Branchen Automobil-, Luftfahrzeug-, Schiff- und Maschinenbau (26,9 %) sowie Eisen und Stahl/Metallverarbeitung/Grundstoffe (21,8 %). "In diesem Zusammenhang fällt auf", heißt es in der Studie, "dass die Branchen Chemie/ Pharma/ Biotechnologie und Banken/ Finanzdienstleistungen/ Versicherungen gar keine Angaben zu Schäden machten." Corporate-Trust-Geschäftsführer Christian Schaaf bezweifelt, dass es in diesen Bereichen nicht zu unerwünschtem Wissenstransfer gekommen ist. "Gerade die Finanzbranche ist bekannt dafür, jedes Jahr hohe Beträge für die Sicherheit ihrer Systeme auszugeben. Und die Chemie-, Pharma- und Biotechnologiebranche hat vermutlich einen der höchsten Forschungsetats aller Branchen."

### Aufgedeckte Spionagetätigkeit in deutschen Unternehmen

Konkret festgestellte Handlungen, Mehrfachnennungen möglich



**Menschliche Schwächen:** Viel häufiger als durch Hackerangriffe auf Kommunikationsnetze von Unternehmen werden sensible Informationen von den eigenen Mitarbeitern an wissbegierige Dritte weitergegeben.

Hackerangriffe und in die IT-Systeme eingeschleuste Spionageprogramme waren mit 14,9 % der gemeldeten Fälle allerdings lediglich die zweithäufigste Form der illegalen Attacken auf Unternehmen. In fast 25 % der aufgedeckten Spionagefälle waren die eigenen Mitarbeiter Ursache für den unerwünschten Know-how-Transfer. "Bemerkenswert ist", so heißt es in der Studie, "dass nicht Forschung und Entwicklung (FuE), sondern der Vertrieb der am stärksten durch Spionage betroffene Unternehmensbereich ist." Dort ereigneten sich 20 % der Fälle.

Gar nicht erstaunlich findet das der Vertriebsleiter eines mittelständischen Anlagenbauunternehmens, der nicht namentlich genannt werden möchte: "Vertrieb ist diejenige Abteilung, die am meisten außerhalb des Unternehmens unterwegs ist - und das mit vielen Daten." Viel mehr erstaunt ihn, "was in Werbebroschüren alles drin steht und wie viel Detailwissen in den Messeprospekten preisgegeben wird", aber auch, "wie leichtfertig Konstruktionszeichnungen aus der Hand gegeben werden." Es fehle das Bewusstsein für die Bedeutung des eigenen Know-hows: "Wer sein geistiges Eigentum gar nicht als

wertvoll erkennt, hat ja auch keinen Grund, es zu schützen."

"Es gibt immer noch Firmen, deren Mitarbeiter laufen mit völlig ungeschützten Laptops durch die Gegend", wundert sich der Vertriebsmann. In seinem Unternehmen seien inzwischen alle Laptops "gecryptet" und kommuniziert werde über VPN. Auch im eignen Unternehmen sei das Problembewusstsein nicht sonderlich ausgeprägt gewesen. Geändert habe sich das erst, nachdem die Datenleitung zum chinesischen Tochterunternehmen angezapft wurde und versucht wurde, die Festplatte zu duplizieren.

Dass die Gefahr, Opfer von Industriespionage zu werden, in den Unternehmen deutlich unterschätzt wird, belegt auch die Corporate-Trust-Studie. Danach glauben mehr als 80 % der Befragten, dass das Risiko für Industriespionage weltweit ansteigen wird, aber nur 33,7 %, dass auch das eigene Unternehmen gefährdet ist. Speziell kleine Unternehmen halten sich häufig für gar nicht wichtig genug, um ausgespäht zu werden.

Aber bereits im "Bericht zur Sicherheitslage 2004/2005" der ASW wird aus einer von der Universität Lüneburg im Auftrag des Sicherheitsforums Baden-Württemberg durchgeführten Untersuchung zitiert, der zufolge Gefahr besonders besteht für "kleine, innovative Unternehmen mit einem hohen Wettbewerbsvorteil, insbesondere wenn sie eine Kleinserienfertigung mit neuen Produkten und zukunftsweisenden Produktionsverfahren haben, international agieren und nur mit wenigen Wettbewerbern konkurrieren."

Ähnlich präzise definierten die Verfassungsschützer die aktuell für Spione besonders interessanten Bereiche. Danach stehen im Fokus der Ausspähungsaktivitäten insbesondere Automobilbau, erneuerbare und saubere Energien, Chemie, Kommunikationstechnologie, Optoelektronik, Röntgentechnologie, Rüstungstechnologie, Werkzeugmaschinen, Verbundwerkstoffe und Materialforschung. ANNE SCHNELLER

Weitere Informationen finden Sie hier:

#### **Was US-Behörden beschlagnahmen**

Geschäftsreisen

VDI nachrichten, London, 5. 9. 08, ciu -

Seit mehreren Jahren beschlagnahmen die amerikanischen Einwanderungsbeamten Laptops und Mobiltelefone von ausländischen Reisenden, um sie auf ihren Inhalt zu untersuchen. Bislang war das ein W...

[mehr](#)

Anzeige



#### **Schiffsinvestment**

Exklusivplatzierung MS "Asian Pioneer" +++ Gesamtauszahlungen ca. 285% +++  
Nahezu steuerfrei



#### **+470,3% in 5 Jahren**

470,3% in 5 Jahren und 2x Rating-Bestnote - Jetzt Rohstoffboom nutzen! 50% auf die Provision.



#### **15% Auszahlung p.a.**

König&Cie. >>Britische Leben III<<: Bis zu 15% Auszahlung p.a. und hohe Steuer-Freibeträge!