MARKT UND MITTELSTAND

DAS UNTERNEHMERMAGAZIN

MARKT UND MITTELSTAND

02
4 394129 309509

STEUERBRIEF: Diese Urteile sind bares Geld wert S. 104

FIRMENKILLER

INDUSTRIE-SPIONAGE

So schützen Sie Ihre Betriebsgeheimnisse S. 30

WUNDERWAFFE

Wie Sie mit Offenheit noch mehr Rendite machen S. 36

MOGELPACKUNG

Warum Schröders Web-Initiative dem Mittelstand nicht hilft S. 80

Gewinnen Sie eine Pulsmessuhr

KAMPF MIT ALLEN MITTELN

Industriespionage verursacht bei mittelständischen Firmen jährlich Schäden in Milliardenhöhe und gefährdet Existenzen. Oft stecken kriminelle Mitarbeiter dahinter. Schon einfache Maßnahmen senken das Risiko des Know-how-Abflusses drastisch.

„Eine sorgfältige Personalauswahl ist der beste Schutz vor Sicherheitsverstößen."
ASW-Geschäftsführer Klaus-Gert Hartmann

Rät Firmenchefs, Bewerbungsunterlagen kritisch auf Echtheit zu prüfen: Sicherheitsexperte KLAUS-GERT HARTMANN

» Es gibt ein Thema, bei dem wird selbst der redseligste Unternehmer plötzlich sehr einsilbig, um schon nach kurzer Zeit völlig in Schweigen zu verfallen: Industriespionage. Hat ein Firmenchef den Verdacht, dass wertvolles Wissen aus seinem Betrieb abfließt, führt der Weg meist schnell zu einem Privatermittler wie Günter Lehmann. Der 40-Jährige ist Chef der alteingesessenen Detektei Grützmacher in Berlin-Wilmersdorf. Im Idealfall gelingt es einem seiner 15 Mitarbeiter, den Spion zu überführen, bevor dieser sein Wissen verkaufen kann. Deutlich unbefriedigender ist es, den Know-how-Dieb zwar dingfest zu machen, jedoch erst, nachdem er sein illegales Geschäft abgewickelt hat.

Glück im Unglück hatte der Chef eines mittelständischen Bedachungsunternehmens aus dem Großraum Berlin, der Lehmann unmittelbar nach dem Besuch einer Fachmesse aufsuchte. „Auf dieser Veranstaltung hörte der Unternehmer, dass einer seiner Mitarbeiter versucht, Rezepturen von Spezialkunststoffen an einen norddeutschen Wettbewerber zu verkaufen", erinnert sich Lehmann. Verdächtig war ein Werkmeister, der Zugang zu den strategisch wichtigen Informationen hatte. Jahrelang arbeitete dieser Mitarbeiter unauffällig für den Betrieb, bis ihn der Firmenchef wegen Diebstahls anzeigte und beurlaubte. Der Werkmeister hatte Material für seinen privaten Hausbau abgezweigt.

Um den Verdacht des Unternehmers zu bestätigen, folgte ein Grützmacher-Detektiv dem Mitarbeiter mit dem Wagen von Berlin nach Hamburg. Dort traf sich der Werkmeister mit einem Vertreter des Konkurrenzunternehmens zu Verkaufsverhandlungen in einem Hotel. Während die beiden beim Mittagessen über die Geschäftsabwicklung sprachen, dokumentierte der Detektiv das konspirative Treffen vom Nachbartisch aus mit einer verdeckten Videokamera.

Noch bevor der Deal über die Bühne gehen konnte, informierte Lehmanns Auftraggeber den norddeutschen Kaufinteressenten, dass er von dem geplanten kriminellen Know-how-Transfer wisse und auf Schadenersatz klagen werde, sollte es der Konkurrent wagen, die Kunststoffrezepturen zu kaufen. Der Berliner Unternehmer schätzt, dass ihm durch diesen Fall von Konkurrenzspionage ein Schaden von etwa 30 Millionen Mark entstanden wäre. Bei derartigen Schadenssummen führt der Weg eines bestohlenen Mittelständlers schnell zum Insolvenzrichter. Für Detektiv Lehmann sind die Beweggründe des diebischen Werkmeisters klar: „Zum einen war es Gewinnsucht, zum anderen waren es die Differenzen mit seinem Arbeitgeber; da werden selbst langjährige Mitarbeiter schwach."

Offenbar werden immer mehr Angestellte weich und die Konkurrenten durch den zunehmenden Wettbewerbsdruck immer interessierter. Seit Jahren verzeichnet die Polizeiliche Kriminalstatistik (PKS) des Bundes-

Um wertvolles Know-how vor den Blicken neugieriger Konkurrenten zu schützen, müssen Unternehmer im Betrieb gut vorsorgen

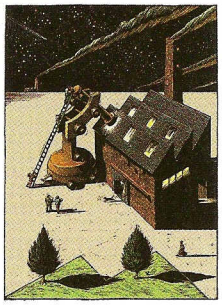
Warnt mittelständische Firmenchefs vor dem Irrglauben, ihr Unternehmen sei für Industriespione wegen seiner geringen Größe uninteressant: KDM-Geschäftsführer KLAUS-DIETER MATSCHKE

innenministeriums eine stetige Zunahme bei den Wirtschaftsdelikten. ***Im Jahr 1999 erfassten die Behörden etwa 110 000 Fälle*** – rund 26 Prozent mehr als noch im Vorjahr. Darunter sind mehr als 14 000 Wettbewerbsvergehen. Wie viele davon der Industrie- oder Konkurrenzspionage zuzuordnen sind, darüber lässt sich nur spekulieren.

Zusätzlich rechnen Spezialisten des Bayerischen Landeskriminalamts in München beim Tatbestand Industriespionage mit einer Dunkelziffer von gut 90 Prozent. Meist regeln Unternehmer diese Delikte unter Ausschluss der Öffentlichkeit. *„Firmenchefs wollen solche Straftaten nicht an die große Glocke hängen“*, berichtet DIHT-Wirtschaftsschutzexperte Stephan Kuhnert. Sie fürchteten als Begleiterscheinung von Prozessen vor allem den zusätzlichen Imageverlust sowie den Zwang, betriebliche Interna offen zu legen.

Experten der Frankfurter Wirtschaftsprüfungsgesellschaft KPMG schätzen den Schaden in Betrieben durch Spionage vorsichtig auf rund 15 Milliarden Mark jährlich. In ihrer Umfrage in den 1000 größten deutschen Unternehmen ermittelten sie 1999, dass zwei von drei Befragten in den vergangenen fünf Jahren Opfer wirtschaftskrimineller Handlungen wurden. Im Mittelstand dürfte die Situation kaum besser sein.

Im Visier der Industriespione stehen besonders Unternehmen aus den Branchen Elektronik, Pharma, Chemie, Luft- und Raumfahrt sowie Maschinen- und Fahrzeugbau. Grundsätzlich gilt jedoch: „Jedes Unternehmen, das über einen Wettbewerbsvorteil verfügt, kann Ziel von Angriffen werden.“ So die Warnung von Klaus-Dieter Matschke. Der ehemalige Kriminaloberrat leitet die KDM Gesellschaft für Sicherheitsberatung mbH in Frankfurt am Main. Bei einer erfolgreichen Spionagemission sparen die Auftraggeber oft eigene F&E-Ausgaben in Millionenhöhe. ***Diebe haben es nicht nur auf Forschungsergebnisse und neue Entwicklungen abgesehen.*** „Auch Lieferanten- und Kundenkarteien, Aus-



SPIONAGEVERDACHT

Diese Anzeichen sollten Sie skeptisch machen

Konkurrenzkampf: Ein Mitbewerber bietet vergleichbare Produkte zu einem Verkaufspreis an, der bislang nicht möglich erschien. Stutzig werden sollten Sie auch, wenn ein Konkurrent plötzlich ein ungewöhnlich aggressives Wettbewerbsverhalten an den Tag legt, das direkt auf Sie zu zielen scheint.

Produktgleichheit: Plötzlich überrascht ein Mitbewerber mit Produkten, die in Machart und Äußerem stark von seiner bisherigen Linie abweichen und stattdessen Ihre Handschrift tragen.

Mitarbeiterverhalten: Unerklärlicher Leistungsabfall oder Übereifer bei einem Mitarbeiter. Skeptisch werden sollten Sie auch, wenn ein Angestellter offensichtlich über seine Verhältnisse lebt.

Hinweise: Achten Sie auch auf anonyme Hinweise aus dem eigenen Betrieb oder von Kunden, wonach ein Mitarbeiter versucht, Material aus dem Unternehmen zu verkaufen.

Fotos: Charly Kurz (1)

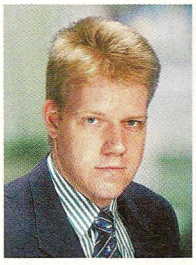
schreibungsunterlagen, Einkaufspreise, Marketingstrategien oder Angebotskalkulationen sind für Konkurrenten interessant", ergänzt Klaus-Gert Hartmann, Geschäftsführer der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) in Bonn. Damit lassen sich den ausgespähten Unternehmen leicht Kunden und Aufträge abjagen.

Prominentestes Beispiel: der ehemalige VW-Manager José Ignacio López. Als López im Jahre 1993 von General Motors (GM) zu VW wechselte, nahmen er und sein Team nach Überzeugung der Staatsanwaltschaft Darmstadt säckeweise vertrauliche Unterlagen mit. Sie klagte López und drei seiner engsten Mitarbeiter drei Jahre später wegen Unterschlagung von GM-Geschäftsunterlagen nach § 246 des Strafgesetzbuches (StGB) und wegen Geheimnisverrats nach § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) an. ***Gleichzeitig lief ein Straf- und Zivilverfahren in den USA.*** Anfang 1997 stimmte das VW-Management zu, 100 Millionen Dollar an GM/Opel zu zahlen und darüber hinaus von dort Autoteile im Wert von einer Milliarde Dollar zu beziehen. Nach der außergerichtlichen Einigung von GM/Opel und VW verhängte die Darmstädter Staatsanwaltschaft gegen die vier Manager hohe Geldbußen und stellte das Verfahren ein.

Wie der Fall López zeigt, sind selbst Konzerne trotz Sicherheitsabteilungen und Schutzkonzepten gegen Angriffe nicht gefeit. Noch niedriger sind die Hürden für Industriespione in mittelständischen Unternehmen. „Gerade innovative Mittelständler sind die Opfer", berichtet KDM-Chef Matschke. Häufig verfügten sie zwar über Spitzentechnologien, unterschätzten jedoch die Bedrohung und vernachlässigten deshalb die betriebliche Sicherheit sträflich.

Eine Studie des Sicherheitsforums Baden-Württemberg bestätigt diese Einschätzung. Das Sicherheitsforum ist ein unabhängiges Gremium aus Unternehmen, Verbänden, Forschungseinrichtungen sowie aus Kammern und Behörden. Zwei Drittel der am Innovationsstandort Baden-Württemberg befragten Führungskräfte bewerten das Risiko, ausspioniert zu werden, als gering. Entsprechend lax sind die Sicherheitsvorkehrungen: Derzeit schützen sich etwa drei bis vier Prozent der Unternehmen vor Spionage, beispielsweise mit technischen Maßnahmen wie der Verschlüsselung ihrer Daten.

Diese Sorglosigkeit der Unternehmensleitungen vermittelt Spitzeln das Gefühl, dass ihr Risiko, entdeckt zu werden, sehr gering ist. Wie einfach sensible Betriebsinformationen nach außen gelangen können, erfuhr die Geschäftsleitung eines Telekommunikationsunternehmens aus dem schwäbischen Backnang auf schmerzliche Weise. Ein mit einem Zeitvertrag angestellter Mitarbeiter kundschaftete die dort hergestellte Übermittlungstechnik bei Schalt- und Schnittstellen aus. ***Per E-Mail schickte er 900 Seiten vertraulicher Informationen an ein US-Unternehmen*** sowie an einen Universitätsprofessor. Zwar gelang es wenigstens, den Spion vor seiner Ab-



Weiß, dass Firmenchefs Fälle von Industriespionage gern ohne Gerichte klären: DIHT-Experte STEPHAN KUHNERT

PERSONALPOLITIK

So senken Sie das Spionagerisiko

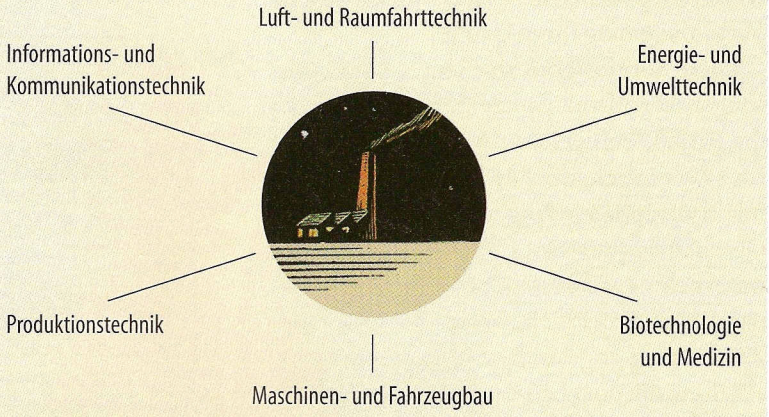
Nutzen Sie alle Möglichkeiten, sich über den beruflichen Werdegang eines Bewerbers zu informieren. Denken Sie daran: Papier ist geduldig.
Prüfen Sie die Bewerbungsunterlagen eines potenziellen neuen Mitarbeiters auf Echtheit, Lückenlosigkeit und Schlüssigkeit – besonders wenn er künftig Zugang zu sensiblen Daten hat.
Nehmen Sie in den Arbeitsvertrag unbedingt einen Passus auf, wonach der Angestellte über sämtliche Betriebsinterna auch nach seinem Ausscheiden zu schweigen hat.
Verpflichten Sie den Mitarbeiter schriftlich dazu, bei seinem Ausscheiden aus dem Unternehmen sämtliche Unterlagen zurückzugeben.
Vermeiden Sie es, Angestellten auf Zeit (wie Leiharbeitern, Diplomanden, Doktoranden) den Zugang zu sensiblen Unternehmensbereichen zu gewähren. Ist dies unumgänglich, sollte es nur unter Aufsicht geschehen.
Sensibilisieren Sie sämtliche Mitarbeiter für die Gefahren durch Industriespionage, und zeigen Sie die konkreten Folgen für die Arbeitsplätze auf. Geben Sie Tipps, welche Themen gegenüber Externen tabu sind.
Schaffen Sie ein Klima des Vertrauens und der Offenheit. Dies senkt das Risiko, dass ein frustrierter Mitarbeiter wichtige Betriebsinterna verkauft.
Sichern Sie zu, Hinweise auf undichte Stellen im Unternehmen vertraulich zu behandeln.

Quelle: KDM Gesellschaft für Sicherheitsberatung/eigene Recherchen

„Gerade innovative Mittelständler sind häufig die Opfer von Spionen."
Klaus-Dieter Matschke, Sicherheitsberater

OPFER

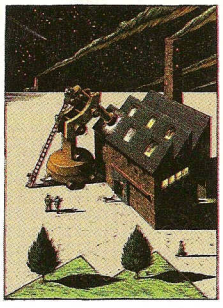
Diese Branchen interessieren Spitzel am stärksten



Quelle: Landesamt für Verfassungsschutz Baden-Württemberg

„Unternehmer sind noch immer viel zu blauäugig und leichtsinnig."

Privatdetektiv Günter Lehmann



reise in die USA festzunehmen, doch waren die Daten trotzdem für immer verloren.

All die geschilderten Fälle haben eines gemeinsam: Die Industriespione griffen nicht von außen das Unternehmen an. Wie Experten vom Landesamt für Verfassungsschutz Baden-Württemberg ermittelt haben, stellen Innentäter die größte Gefahr dar für die Sicherheit eines Betriebes. Nach Angaben der IHK Magdeburg stecken hinter rund 75 Prozent der von in Unternehmen verübten Wirtschaftsdelikte die eigenen Mitarbeiter.

Angesichts dieser erschreckenden Einschätzungen empfehlen Sicherheitsexperten wie ASW-Chef Hartmann Hilfe suchenden Firmenchefs: ***„Sorgfältige Personalauswahl ist der beste Schutz vor Sicherheitsverstößen."*** So müssten sie sich angewöhnen, Bewerbungsunterlagen auf ihre Echtheit, Lückenlosigkeit und Schlüssigkeit zu prüfen. Der kritische Einstellungs-Check ist jedoch nur eine von mehreren personellen Maßnahmen, die Unternehmer ergreifen müssen. Dazu zählt auch, einen Sicherheitsbeauftragten zu ernennen und zu qualifizieren, Mitarbeiter in sensiblen Unternehmensbereichen regelmäßig zu überprüfen oder die Belegschaft auf die Spionagegefahr aufmerksam zu machen. Vorsicht geboten ist auch auf Messen und Tagungen. Unabsichtlich verraten stolze Entwicklungsingenieure oder Führungskräfte im Gespräch am Rande schnell mehr, als ein externer Industriespion je ermitteln könnte.

Eine wichtige Rolle spielt das Betriebsklima. Ist es gut, sinkt die Gefahr, dass ein frustrierter Mitarbeiter Firmeninterna an die Konkurrenz weiterleitet. Auch eine geplatzte Beförderung, mangelnde Anerkennung oder ein geplanter Personalabbau schwächen die Loyalität gegenüber dem Arbeitgeber.

Ebenfalls das Ausspähen erschweren sollen organisatorische Maßnahmen wie der geregelte Zugang zu strategisch wichtigen Daten. So sollten sich Mitarbeiter beim Betreten eines sensiblen Unternehmensbereiches ausweisen müssen, ihre Anwesenheit sollte dokumentiert werden, sie dürfen nur ohne Aktenkoffer kommen und gehen und auch nur zu bestimmten Zeiten auf vertrauliche Daten zugreifen. Obwohl diese vergleichsweise einfachen Maßnahmen kriminelle Mitarbeiter abschrecken, setzen sie noch immer viel zu wenige Firmenchefs um. Dazu Privatermittler Lehmann: „Unternehmer haben in den letzten Jahren zwar einiges zur Spionagevorbeugung getan, doch sind sie immer noch viel zu blauäugig und leichtsinnig." «

ORGANISATION

Welche Maßnahmen einem Spion die Arbeit erschweren

Schwachstellenanalyse: Beauftragen Sie einen Sicherheitsexperten mit einer Schwachstellenanalyse, und verändern Sie danach die Organisationsstruktur.

Sicherheitsverantwortlicher: Benennen und qualifizieren Sie einen Sicherheitsverantwortlichen. Er untersteht Ihnen direkt!

Konzentration: Versuchen Sie nicht, alles zu schützen. Sinnvoller ist es, weniger, das jedoch effektiv zu schützen. Halten Sie den Kreis der Geheimnisträger klein.

Zugangsberechtigung: Legen Sie fest, wer wann wo zu welchen Bedingungen in sensiblen Unternehmensbereichen arbeiten darf.

Kontrolle: Überprüfen Sie regelmäßig, ob sich alle Beschäftigten an Ihre Sicherheitsanweisungen halten, und sanktionieren Sie Verstöße umgehend.

Sonstiges: Installieren Sie ein zuverlässiges Besucher- und Schlüsselmanagement sowie eine funktionierende Stellvertreterregelung.

Weitere Informationen unter **www.asw-online.de** und unter **www.baden-wuerttemberg.de/verfassungsschutz**