Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

Mit Sicherheit erfolgreich

Erfolgsfaktor Know-how-Schutz

Information und Prävention

Inhalt

Grußwort

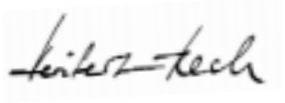
Wirtschaftsspionage hat sich im Laufe der letzten Jahre immer mehr zu einer ernsthaften Bedrohung entwickelt. Im Vordergrund steht die Beschaffung von Informationen, die dem eigenen Wettbewerbsvorteil dienen. Den unmittelbaren Schaden trägt das vom Informationsverlust betroffene Unternehmen. Aber auch die Folgeschäden, wie etwa der Verlust von Arbeitsplätzen oder langfristige Nachteile für die gesamte Volkswirtschaft, können erhebliche Ausmaße annehmen.

Baden-Württemberg mit seiner hohen Dichte an Unternehmen und Forschungseinrichtungen aus dem Bereich der Hochtechnologie ist dabei besonders gefährdet. In den Unternehmen des Landes gibt es viele Bereiche, in denen der Informationsschutz eine große Rolle spielt. Eine gute Idee ist immer auch für andere interessant. Kein Unternehmen sollte sich deshalb in Sicherheit wiegen – der ungewollte Abfluss von Know-how bedroht sämtliche Branchen.

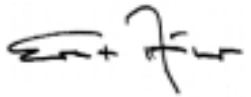
Die Landesregierung von Baden-Württemberg will das Augenmerk auf die Gefahren des Know-how-Verlustes lenken. Gerade in kleineren und mittelständischen Unternehmen ist dieses Bewusstsein noch nicht stark genug ausgeprägt. Wirksame Prävention findet dort leider noch viel zu selten statt. Reagiert wird oft erst, wenn bereits Informationsverluste eingetreten sind.

Mit der vorliegenden Broschüre wird das Gefährdungspotenzial der Konkurrenzausspähung aufgezeigt. Anhand von Beispielsfällen aus der täglichen Praxis wird veranschaulicht, welche Schäden durch mangelnden Informationsschutz entstehen können. Mit den Handlungsempfehlungen erhalten Unternehmen praktische Hinweise, wie sie wirksame Vorkehrungen gegen Wirtschaftsspionage ergreifen können.

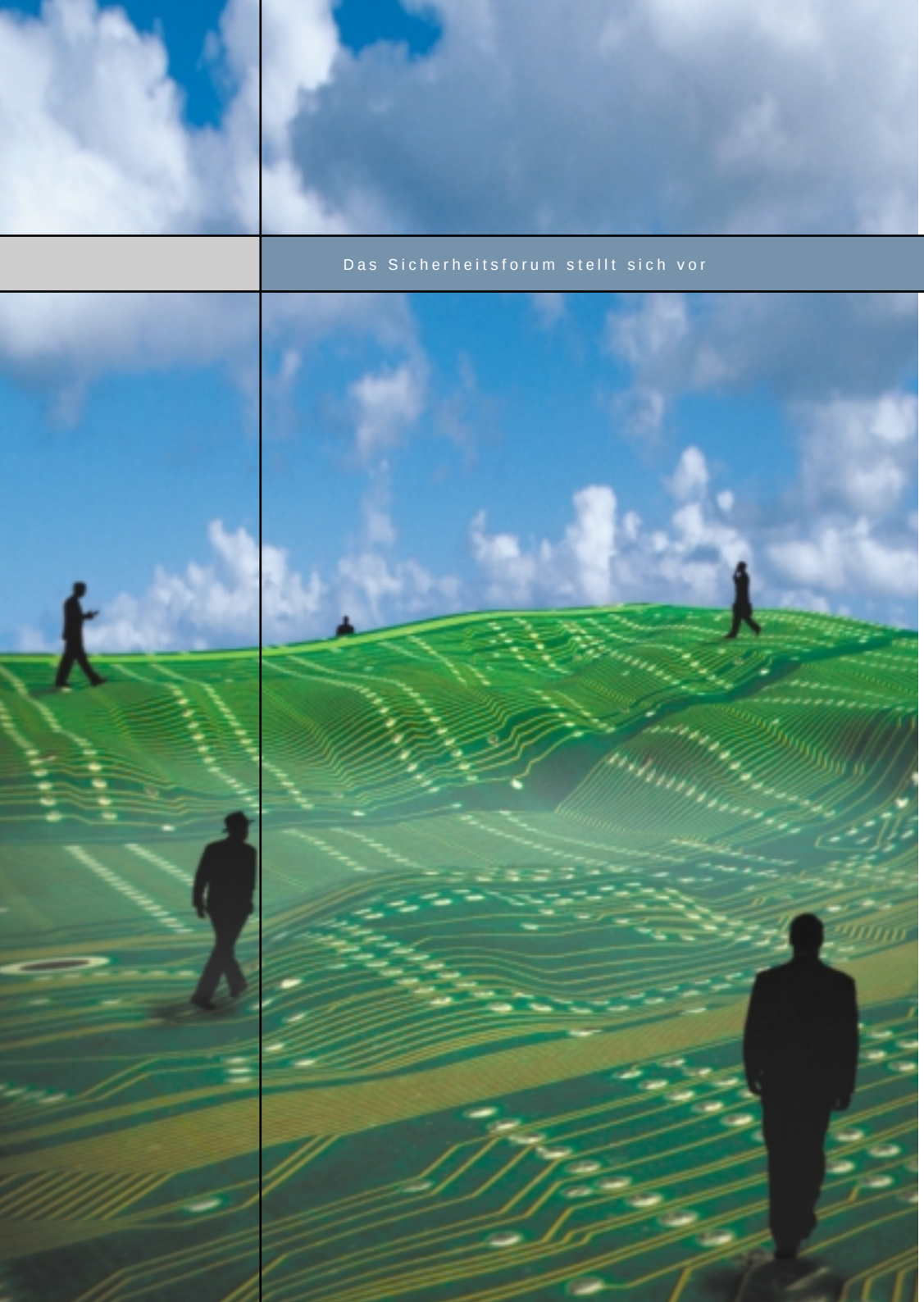
Der Titel der Broschüre gibt die Richtung vor: Nur wer den Erfolgsfaktor Know-how-Schutz ernst nimmt, wird langfristig wirtschaftlich erfolgreich sein können.



Heribert Rech MdL
Innenminister



Ernst Pfister MdL
Wirtschaftsminister



1. Das Sicherheitsforum stellt sich vor

In dem 1999 gegründeten Sicherheitsforum Baden-Württemberg haben sich Vertreter aus Unternehmen, Kammern, Verbänden, Forschungseinrichtungen und Behörden des Landes Baden-Württemberg zusammengeschlossen. So unterschiedlich sie in ihrem Wirken auch sein mögen, haben doch alle erkannt, dass die Säulen unseres Wohlstandes, die hier ansässigen Unternehmen und Forschungseinrichtungen, durch ungewollte Wissensverluste gefährdet sind.

Vor dem Hintergrund erheblicher wirtschaftlicher Schäden, die durch ungewollten Know-how-Abfluss entstehen, will das Sicherheitsforum Baden-Württemberg insbesondere kleine und mittelständische Unternehmen beim Schutz ihres Wissens und ihrer Innovationen unterstützen. Durch Aufzeigen von Risiken sollen sie für die Bildung einer Sicherheitskultur im Unternehmen sensibilisiert werden. Auch wenn dabei bislang die Informationsabschöpfung auf elektronischem Weg im Vordergrund steht, bezieht das Sicherheitsforum Baden-Württemberg auch sonstige Sicherheitsaspekte wie baulich-technische Maßnahmen, Integrität und Zuverlässigkeit der Mitarbeiter, Schutz des geistigen Eigentums oder den Schutz vor Korruption in seine Arbeit ein.

Das Sicherheitsforum Baden-Württemberg will nicht in Konkurrenz zu gewerblichen Anbietern auftreten; es verfolgt insbesondere keine wirtschaftlichen Interessen und ist politisch nicht gebunden.

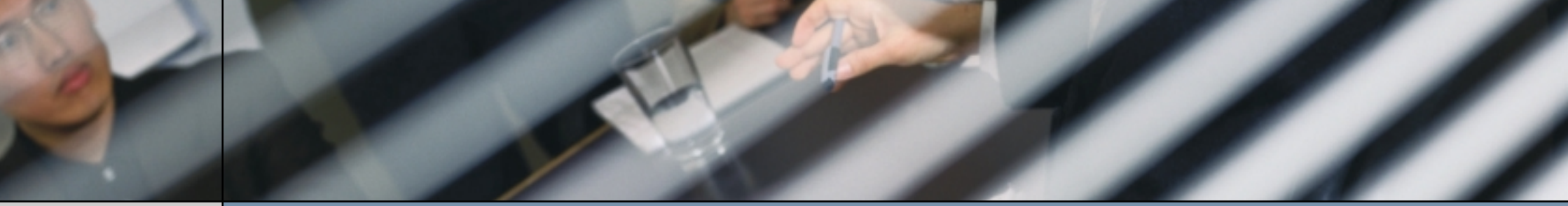
2. Mittelständische Wirtschaft in Baden-Württemberg

Große Schäden durch Spionage

Wirtschaftspionage durch Nachrichtendienste und Konkurrenzausspähung werden für die baden-württembergische Wirtschaft immer mehr zum Problem und bedeuten eine existenzielle Gefahr für die Unternehmen. Das Gefährdungspotenzial für Produktideen und Produktions-Know-how sowie die tatsächlich schon eingetretenen Schäden sind immens. Das ist das Ergebnis einer vom Sicherheitsforum Baden-Württemberg an die Universität Lüneburg vergebenen Studie. Die bisherigen Schätzungen hierzu waren zu ungenau und spekulativ, um darauf tragfähige Aussagen aufbauen zu können. Durch die vorgelegte Analyse wird eine wesentliche Lücke im Kenntnisstand über die Bedeutung und das Zustandekommen von Informationsverlusten in Unternehmen geschlossen.

Die Untersuchung wurde vom Institut für Betriebswirtschaftslehre der Universität Lüneburg durchgeführt. Sie befasst sich als erste deutsche Universität fachrichtungsübergreifend mit Fragen des Security-Managements und widmet sich in Forschung und Lehre zentralen Sicherheitsproblemen der Wirtschaft.

In die Analyse wurden 400 technologieorientierte Unternehmen eines repräsentativen Branchen-Querschnitts einbezogen. Sie erwirtschaften ein Volumen von rund 29 Mrd. Euro Umsatz/Jahr, dies entspricht ca. 10 % des Bruttoinlandsproduktes von Baden-Württemberg. Ihre durch Interviews und Fragebogenauswertung zusammengeführten Erfahrungen belegen einen hohen Handlungsbedarf:



- Der Wert des Wettbewerbsvorsprungs, d. h. die gefährdete Substanz, beträgt für die befragten Unternehmen fast 700 Mio. Euro. Bezogen auf Baden-Württemberg beträgt dieses Gefährdungspotenzial ca. 7 Mrd. Euro pro Jahr. Der verursachte Schaden belief sich auf 52 Mio. Euro. Die auf dieser Basis hochgerechneten Schäden für Baden-Württemberg betragen ca. 1 Mrd. Euro.

- Mehr als zwei Drittel aller Unternehmen war schon Opfer eines „unfreundlichen Informationsabflusses“. Dennoch sind die Aufwendungen für Informationssicherheit im Vergleich zum Gefährdungspotenzial zu gering: zwei Drittel der Unternehmen geben weniger als 50.000 Euro pro Jahr aus, im Schnitt weniger als 5 % der Gefährdungssumme.

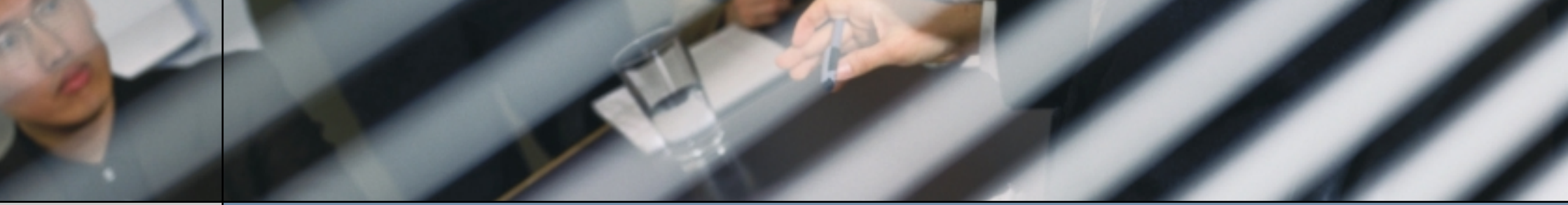
- Kleine, innovative Unternehmen mit einem großen Wettbewerbsvorteil erweisen sich als überproportional gefährdet. Insbesondere, wenn sie Kleinserienfertigung mit neuen Produkten und zukunftsweisenden Produktionsverfahren betreiben, nur mit wenigen Wettbewerbern konkurrieren und international agieren. Die Aufwendungen für Sicherheitsmaßnahmen betragen dort nur ca. 0,1 % des Umsatzes und entsprechen damit nur einem Drittel der aufgetretenen Schäden.

- Bei nur rund 5 % der befragten Unternehmen gibt es bislang einen Sicherheitsverantwortlichen.

- In fast 50 % der Schadensfälle wurden durch das geschädigte Unternehmen keine Anstrengungen unternommen, dem Sicherheitsvorkommnis nachzugehen und die Ursachen zu verifizieren: Nur in 8 % der Fälle schalteten die geschädigten Unternehmen Sicherheitsbehörden oder externe Sicherheitsberater ein.

- Trotz des Gefährdungspotenzials und erlittener wirtschaftlicher Schäden ist nur der Hälfte der Unternehmen die Aufgabenstellung und damit die Möglichkeit der Unterstützung durch Sicherheitsbehörden bekannt. Nur 10 % der Unternehmen kennen die dortigen Ansprechpartner. Nur 5 % der Unternehmen halten regelmäßig Informations- und Arbeitskontakte mit diesen Stellen. Nur 2 % der Unternehmen haben ein mit den Sicherheitsbehörden abgestimmtes Sicherheitskonzept.

- Zu den Hauptquellen „unfreundlichen Informationsabflusses“ gehören nach Angaben der Unternehmen in erster Linie die eigenen Mitarbeiter, gefolgt von inländischen Konkurrenzunternehmen und Kooperationspartnern. Firmen mit Auslandbeziehungen sind besonders betroffen. Gefahr droht dem Know-how baden-württembergischer Unternehmen der Studie zufolge in erster Linie aus dem europäischen Ausland, gefolgt von USA/Kanada und Ländern aus Fernost.

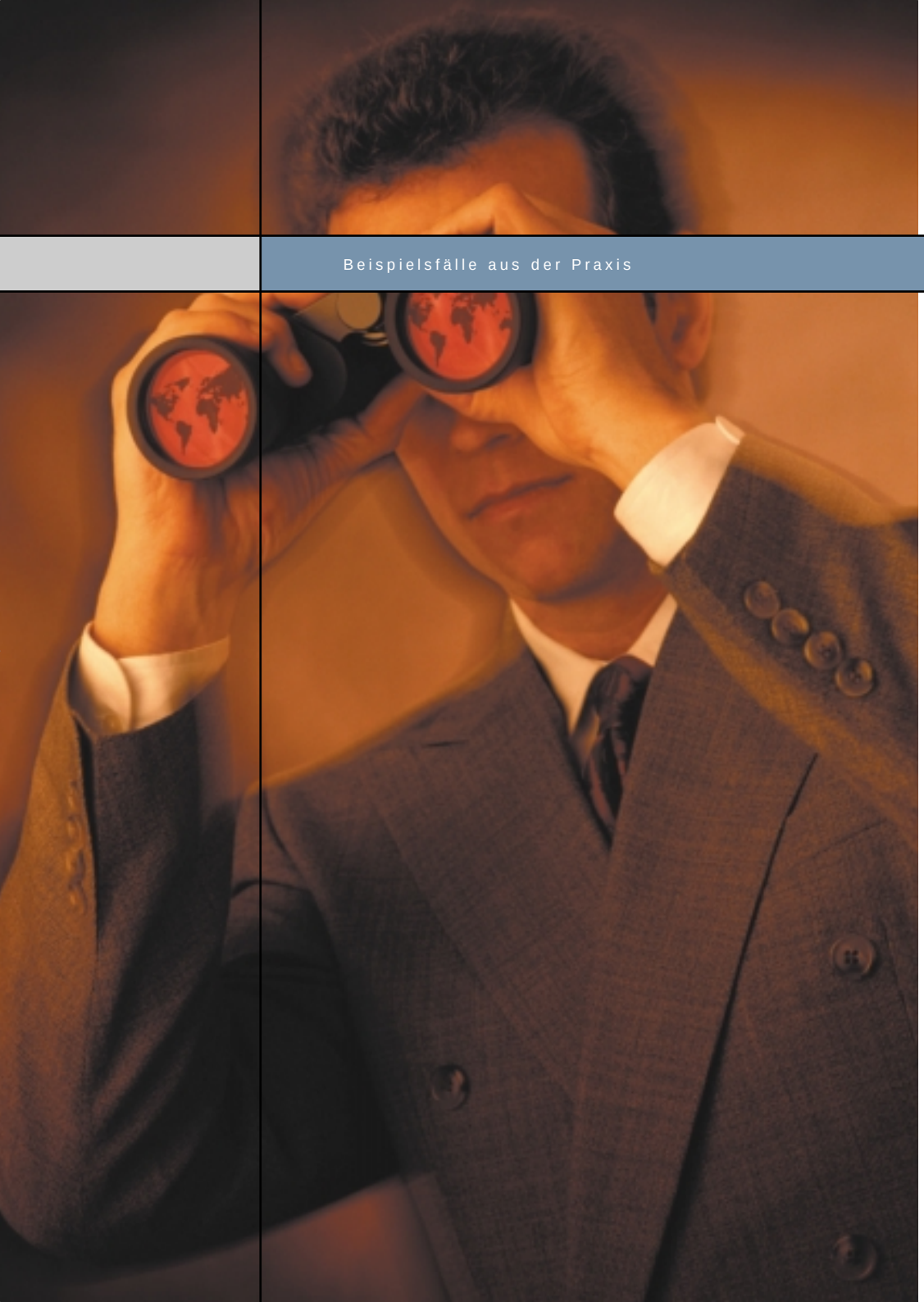


- Als Reaktion auf die Schadensfälle entschieden sich die Unternehmen vor allem für juristische, personelle und organisatorische Maßnahmen. Technische Lösungen zur Schadensvermeidung wurden bislang nur in geringem Umfang vorgesehen.

- Die Bereitschaft zur Vorbeugung gegen ungewollten Informationsabfluss und damit gegen wirtschaftliche Schäden ist bei den befragten Unternehmen eher die Ausnahme.

Die Untersuchung zeigt nach Ansicht des Sicherheitsforums, dass das Bewusstsein für die Informationsgefährdung geschärft und permanent weiterentwickelt werden muss. Informationsschutz sollte Managementaufgabe sein. Insbesondere kleinen und mittelständischen Unternehmen mit Auslandskontakten wird empfohlen, einen fundierten Sicherheits-Check durchzuführen, eine auf die eigenen Belange abgestimmte Sicherheitsstrategie zu entwickeln und ein alle Unternehmensbereiche umfassendes Sicherheitskonzept zu realisieren. Die Prävention sollte sich nach Ansicht des Sicherheitsforums besonders auf personelle, organisatorische, technische und rechtliche Maßnahmen beziehen. Konkrete Anregungen zur Verbesserung der Informationssicherheit enthalten die nachfolgenden Beispielsfälle aus der Praxis sowie die zusammenfassenden Empfehlungen zur Prävention.

Die im Sicherheitsforum zusammengeschlossenen Institutionen bieten der Wirtschaft in Baden-Württemberg ihre Hilfestellung an. Rat suchende Unternehmen finden unter www.sicherheitsforum-bw.de alle Mitgliedsinstitutionen und Ansprechpartner. Die Studie kann als pdf-Datei heruntergeladen werden.



3. Beispielsfälle aus der Praxis

Wer Zeitungen und Magazine liest, fern sieht und im Internet surft, der weiß genau, dass Konkurrenzausspähung und Wirtschaftsspionage „große Themen“ sind, dass die angewandten Methoden immer ausgeklügelter werden, dass die „andere Seite“ den Ermittlungsbehörden häufig einen – wenn auch kleinen – Schritt voraus ist und dass es jeden treffen kann.

Soviel zur grundsätzlichen Wahrnehmung der Situation. Man weiß um die Bedrohungen „für die Wirtschaft“, kennt möglicherweise auch statistische Wahrscheinlichkeiten und vielleicht sogar ein betroffenes Unternehmen – die Einschätzung der eigenen Gefährdung differiert hingegen gerade bei kleinen und mittelständischen Unternehmen in aller Regel sehr deutlich. Die Gründe hierfür mögen vielfältig sein; nachzuvollziehen sind sie nur selten.

Schließlich zeichnen die genannten Medienberichte und Veröffentlichungen in ihrer Gesamtheit ein sehr deutliches Bild. Know-how-Verlust betrifft Unternehmen aller Größen, unterschiedlichster Branchen und vollkommen unabhängig von ihrem Standort. Die Gefährdungsarten sind vielfältig, dem Erfindungsreichtum der Angreifer kaum Grenzen gesetzt. Unzufriedene Mitarbeiter nehmen Geheimnisse mit oder verkaufen sie an die Konkurrenz, Putzkolonnen kopieren Daten, Geheimdienste spähen Systeme aus, Hacker verschaffen sich Zugriff auf Konstruktionsdaten, Wissenschaftler werden gezielt ausgehorcht – für jeden etwas …

Noch zu abstrakt? Etwas konkreter? Gerne! Auf den folgenden Seiten werden einige reale Fälle analysiert, die für die betroffenen Unternehmen äußerst konkret wurden und sie eine Menge Geld gekostet haben. Die Gründe dafür liegen teilweise in der kriminellen Energie gewiefter Täter; zu einem beträchtlichen Teil aber auch an einem fahrlässigen Umgang der Unternehmen mit ihrem Wissen.

Es ist zu hoffen, dass die Falldarstellungen, ihre Auswertung und die jeweils abgeleiteten präventiven Aspekte dazu beitragen, bei noch nicht betroffenen Unternehmen eine realistischere Einschätzung der eigenen Gefährdung zu bewirken – wer sich konkret mit Szenarien auseinandersetzt, die sein Unternehmen bedrohen könnten, ist im Vorteil.

Methoden der Informationsbeschaffung

OFFEN

Auswertung von Veröffentlichungen (Forschungsberichte, Patentunterlagen, PR-Material), Internet und Datenbanken

Besuch von Fachveranstaltungen (Messen, Kongresse, Symposien etc.)

Gesprächsabschöpfung/Social Engineering (Erlangung nicht allgemein zugänglicher Informationen durch geschicktes „Aushorchen“)

Nutzung des „Wissenstransfers“ (Studium oder Beteiligung an wissenschaftlichen Projekten)

Teilnahme am Wirtschaftsleben (Joint Ventures, Firmenübernahmen etc.)

VERDECKT

Einschleusung von Agenten bzw. Anwerbung von Firmenangehörigen

Überwachung von Telekommunikation

Eindringen in Informationssysteme

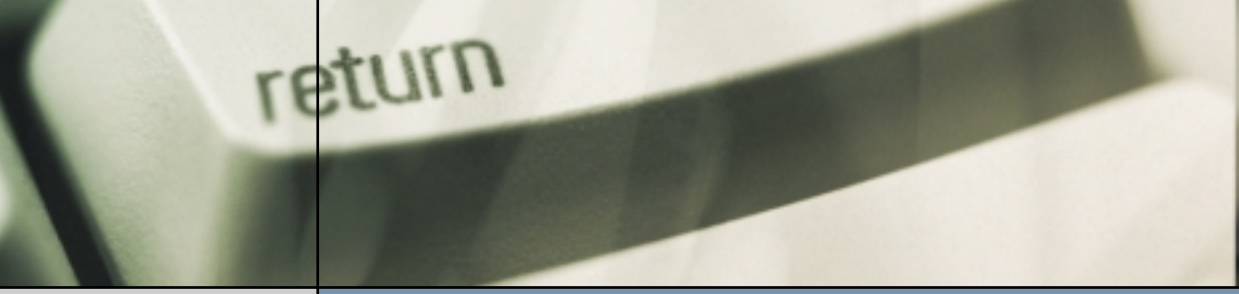
3.1 „Ideenklau“ durch eigene Mitarbeiter

Falldarstellung

Ein mittelständisches, alteingesessenes Unternehmen in der Nähe von Stuttgart, das Komponenten und Ersatzteile für Textilmaschinen entwickelt, produziert und vertreibt, wurde durch illoyales Verhalten eigener Mitarbeiter zum Opfer von Industriespionage.

Einem der Täter, der als kaufmännische und technische Fachkraft angestellt war, oblag die Aufgabe, in der überwiegenden Zeit der Abwesenheit des Geschäftsführers das Unternehmen verantwortlich zu führen. Ein weiterer Täter war als technischer Angestellter mit der Konstruktion, Kalkulation und Produktionsentwicklung von Werkzeugen bzw. Produkten betraut. Der dritte Täter, ein Kunde des geschädigten Unternehmens, verfügte über gute Kontakte zum Spinnereimarkt im Ausland.

Die drei Personen kamen überein, ein gemeinsames Unternehmen zur Herstellung und zum Vertrieb von Ersatzteilen für Textilmaschinen zu gründen. Das erforderliche Know-how in punkto Konstruktionen, Materialien, Passformen, Fertigungs-Prozessen, Werkstoffen, Kalkulationen und Kunden wollten sich die zwei Haupttäter bei ihrem Arbeitgeber beschaffen. In Ausführung ihres Plans kopierten sie vor ihrem Ausscheiden aus dem Unternehmen EDV-gespeicherte Konstruktionspläne auf Datenträger und verschafften sich Zeichnungen, Unterlagen und Kundenkorrespondenz.



Vereinbarungsgemäß wurde eine GmbH gegründet, wobei das gemeinschaftliche Vorhaben von dem dritten Täter finanziert wurde. Als Geschäftsführer wurden die beiden ehemaligen Mitarbeiter der geschädigten Firma bestellt. Die Aktivitäten des neuen Unternehmens dienten zunächst vorrangig dem Ziel, unter Verwendung des teilweise geringfügig formal abgeänderten Know-hows der geschädigten Firma Werkzeuge nachzubauen, zu produzieren und als Konkurrent auf dem Markt anzutreten.

Das geschädigte Unternehmen ist erst durch die Nachfrage von Kunden auf den Vorgang aufmerksam geworden.

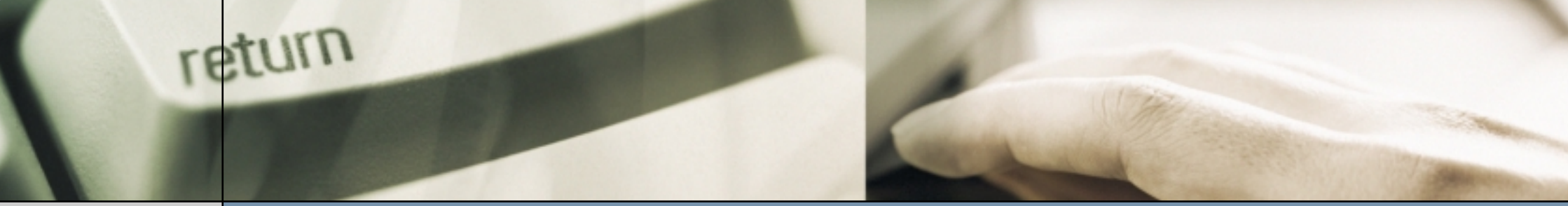
Das Motiv der Täter war eindeutig Gewinnsucht, wobei sie sich infolge ersparter Entwicklungs- und sonstiger Anlaufkosten einen dauerhaften Wettbewerbsvorteil in beträchtlicher Höhe gegenüber der geschädigten Firma versprachen. Speziell der Geldgeber hatte ein unmittelbares Interesse am Geschäftserfolg.

Die beiden Haupttäter nutzten konsequent die ihnen freiwillig eingeräumten umfassenden Zugangsmöglichkeiten und Handlungsspielräume. Der Erfolg ihres illoyalen Verhaltens wurde erst durch das große Vertrauen des Arbeitgebers in seine Mitarbeiter möglich gemacht. Ihr arglistiges Vorhaben hat er zu keiner Zeit befürchtet und deshalb auch nicht erkannt.

Das betroffene Unternehmen stand nach eigenen Angaben zeitweise am Rande der Insolvenz und konnte nur im Wege der Übernahme durch finanzkräftige eigene Mitarbeiter vor dem Ruin gerettet werden.

Der entstandene Schaden ist nicht exakt messbar. Parallel zum Strafprozess wurde auf Schadenersatz in Millionenhöhe geklagt.

Die Wirtschaftsstrafkammer des Landgerichts Stuttgart sprach im Februar 2003 die drei Angeklagten wegen mehrerer Vergehen des Verrats von Geschäftsgeheimnissen, teilweise in Tateinheit mit Diebstahl schuldig und verurteilte die Exmitarbeiter jeweils zu einer Gesamtfreiheitsstrafe von neun Monaten und den Exkunden zu der Gesamtfreiheitsstrafe von sechs Monaten. Die Vollstreckung der Strafen wurde zur Bewährung ausgesetzt, da die Angeklagten ein umfassendes Geständnis ablegten und sich verpflichteten, an die betroffene Firma eine Schadenswiedergutmachung in Höhe von insgesamt 200.000,- € zu bezahlen.
Noch heute leidet das Unternehmen unter der neu entstandenen Konkurrenz, da frühere Kunden nach dorthin abgewandert sind.



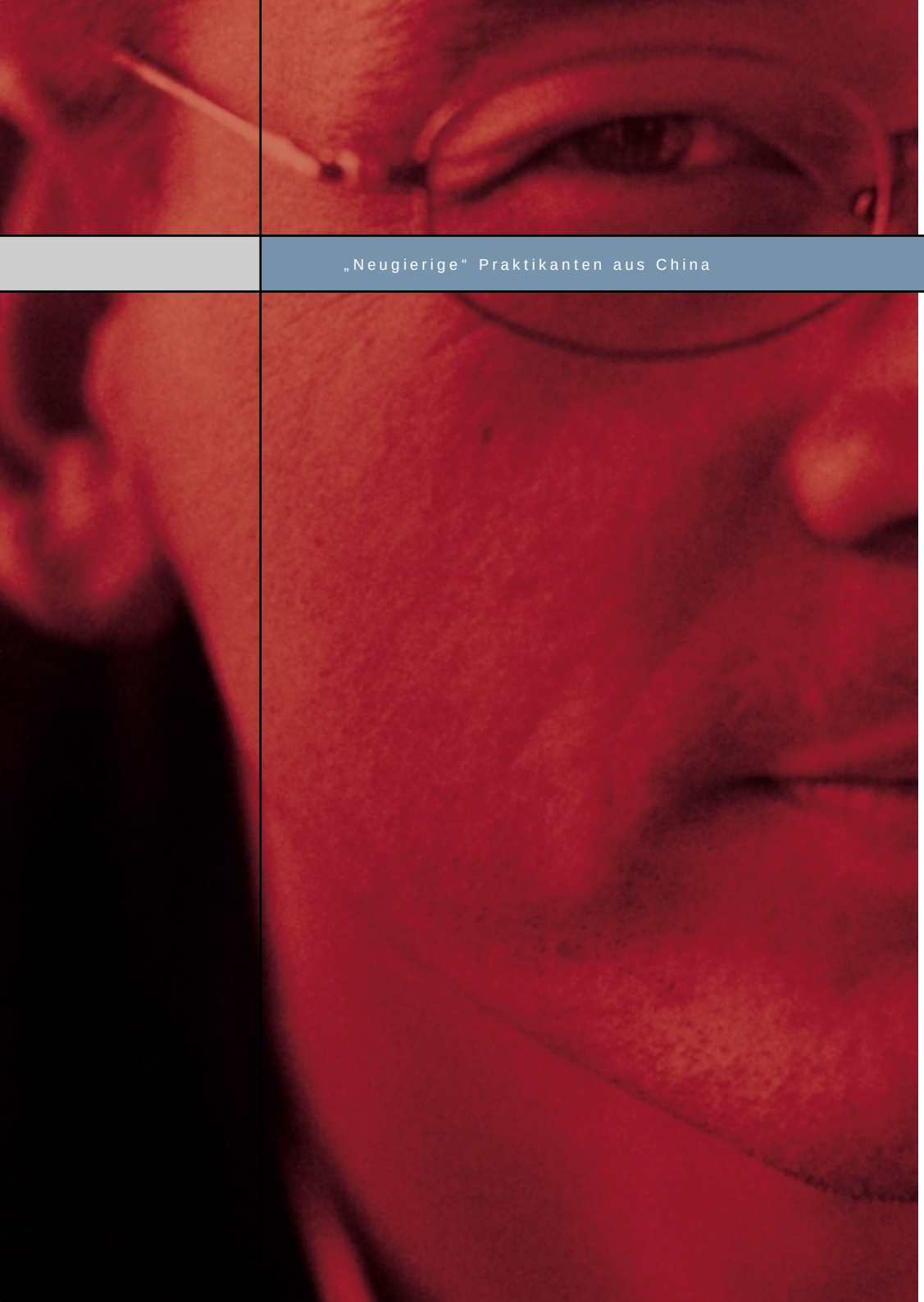
Präventive Aspekte

In dem Unternehmen fehlten selbst elementare Sicherheitsmaßnahmen personeller, technischer und organisatorischer Art.

Der Fall zeigt deutlich, dass den auch in der Fall- und Schadensanalyse der Universität Lüneburg als besondere Schwachstelle identifizierten eigenen Mitarbeitern nicht genügend Aufmerksamkeit gewidmet worden ist. Einer der Haupttäter – obwohl erst kurz im Unternehmen – wurde in fahrlässiger Weise mit umfassenden Vollmachten ausgestattet, die die Tat geradezu herausforderten und wesentlich erleichterten.

Es wurde versäumt, die Verantwortung und die Kontrolle auf mehrere Schultern zu verteilen und Zugriffsbeschränkungen für sensible Firmendaten wie Konstruktionspläne, Kalkulationen und Kundendaten einzurichten. Speziell bei Mitarbeitern im Kündigungsstatus sollte darauf geachtet werden, dass der Zugriff auf betriebsspezifisches Know-how nur noch in dem zwingend notwendigen Umfang erfolgen kann. Die Möglichkeiten der Konkurrenzbeobachtung als „Frühwarninstrument“ wurden ebenfalls nicht genutzt.

Die betroffene Firma hat inzwischen angemessene Sicherheitsmaßnahmen getroffen. So wurde eine moderne Schließanlage mit abgestuften Zugangsberechtigungen installiert, das DV-Netzwerk unter Berücksichtigung neuester IT-Sicherheitskriterien grundlegend erneuert und mit Zugangscodes versehen. Zudem erfolgt die Personalauswahl – insbesondere für sensible Unternehmensbereiche – unter Beachtung strengerer Maßstäbe.



3.2 „Neugierige“ Praktikanten aus China

Vorbemerkungen

China unternimmt größte Anstrengungen, an die Leistungsfähigkeit von Wissenschaft und Forschung hoch entwickelter Staaten anzuknüpfen. Es verschafft sich so die Möglichkeit, am Weltmarkt als wettbewerbsfähiger Partner agieren zu können. Dass die bisherigen Anstrengungen erfolgreich sind, zeigen aktuell die beachtlichen Wachstumsraten der chinesischen Volkswirtschaft. Sie weisen auf eine rasant verbesserte Wettbewerbsfähigkeit mit wachsenden Exportchancen hin.

Zahlreiche wirtschaftliche und wissenschaftliche Kooperationen zwischen chinesischen und deutschen Wirtschaftsunternehmen sowie wissenschaftlichen Einrichtungen erleichtern den weitgehend offenen Transfer von Wissen aus westlichen Industriestaaten nach China. Hinzu kommen die permanent ausgeweiteten Wirtschaftsbeziehungen. Die Zahl von Produktionsstätten und Repräsentanzen deutscher Firmen hat sich 2005 mit weit über 2.000 – darunter allein ca. 450 aus Baden-Württemberg – gegenüber den Vorjahren deutlich erhöht.

Aber auch die vielfältigen Ausprägungen der Zusammenarbeit im Hochschul- und Forschungsbereich sowie zahlreiche Studien- und Schulungsaufenthalte chinesischer Staatsbürger im Bundesgebiet zielen naturgemäß auf die Gewinnung und den Transfer von qualifiziertem Wissen ab.

Mit ca. 20.000 Studenten stellt China mittlerweile die größte Gruppe ausländischer Akademiker in Deutschland. Dies impliziert, dass Studenten und Wissenschaftler über die „Schiene Hochschule“ und sonstige Forschungseinrichtungen im Rahmen von Praktikumseinsätzen und die Mitarbeit bei betrieblichen Projekten auch Zugang zu sensiblen Bereichen der Wirtschaft erlangen.

Falldarstellungen

Welche Auswirkungen das haben kann, wird an aktuellen Vorfällen deutlich, die sich in Baden-Württemberg und in Frankreich zugetragen haben:

In einem metallverarbeitenden Betrieb in Baden-Württemberg ist ein chinesischer Praktikant durch die massive Missachtung von Sicherheitsvorschriften aufgefallen. Er schleuste verbotswidrig seinen privaten Laptop in das Unternehmen ein und lud aus dem firmeninternen Computernetz die gesamten Daten eines kurz vor Beendigung stehenden Projekts auf seine Festplatte. Darüber hinaus bemühte er sich in aufdringlicher Weise, Gespräche von Kollegen mitzuhören, und hielt sich auch außerhalb der üblichen Arbeitszeiten bevorzugt im Unternehmen auf.

Die Erfahrung im Umgang mit chinesischen Praktikanten hat gezeigt, dass diese bereits in ihrer Heimat hohe Qualifizierungsstufen erlangt haben und aufgrund ihrer Vorbildung in der Lage sind, das gebotene Wissen selektiv aufzunehmen und sich zielorientiert für sie interessante Informationsinhalte zu erschließen. Die oftmals vorhandene Kenntnis mehrerer Sprachen senkt zudem die Barrieren der Informationsgewinnung und der Kommunikation.

In diesem Zusammenhang wird auch das bei Chinesen im Vergleich zu Europäern festzustellende unterschiedlich ausgeprägte Unrechtsbewusstsein deutlich. Chinesen sahen bislang in der Imitation von Produkten, der Ausspähung beziehungsweise dem illegalen Technologietransfer kein gravierendes Problem. Im Gegenteil: In ihrem Wertebewusstsein wird derjenige besonders geachtet, dessen Leistungen der Nachahmung wert sind beziehungsweise auch tatsächlich nachgeahmt werden.

Internationale und nationale Initiativen sollen den chinesischen „Ideenklau“ eindämmen. So ist China zwischenzeitlich verschiedenen internationalen Konventionen zum Schutz des geistigen Eigentums beigetreten. Allerdings beklagt zum Beispiel die deutsche Wirtschaft nach wie vor die unzulängliche Umsetzung dieser Richtlinien durch die Chinesen, nicht zuletzt zum Schaden der einheimischen Firmen.

Angesichts der Intensivierung internationaler Zusammenarbeit im europäischen Wirtschaftsraum hat auch ein

Sicherheitsvorfall in Frankreich für Aufmerksamkeit gesorgt. Die entsprechende Berichterstattung der Medien[1] ergänzt die Gesamtproblematik der chinesischen Ausspähung in exemplarischer Weise:

Im Februar 2005 begann die chinesische Studentin Li-Li W. ein auf ein halbes Jahr angelegtes Praktikum bei einem französischen Automobilzulieferer in der Nähe von Paris. Sie war dort in der Abteilung „Wärme- und Kältetechnik Fahrgastzelle“ eingesetzt, die sich mit der Forschung und Entwicklung im Bereich Klimaanlagen befasst. Die Praktikantin stammt aus der Stadt Wuhan in der Provinz Hubei – einem Zentrum der Autoindustrie Chinas und Sitz eines der stärksten Weltmarkt-Konkurrenten der betroffenen französischen Firma.

Während ihres Praktikums fiel auf, dass Li-Li W. ein privates Notebook mit sich führte. Der von den Vorgesetzten gehegte Verdacht eines Missbrauchs führte zur Einschaltung der Polizei mit anschließender Wohnungsdurchsuchung. Dort wurden mehrere Computer mit enormer Speicherkapazität aufgefunden und beschlagnahmt, auf denen auch firmenvertrauliche Daten aus dem Besitz des französischen Automobilzulieferers gespeichert sein sollen. Die Einlassungen der Praktikantin im Rahmen der polizeilichen Vernehmungen ließen selbst vor dem Hintergrund der gegenüber dem Unternehmen abgegebenen Geheimhaltungserklärung kein Schuldbewusstsein erkennen.

[1] FOCUS vom 17. Mai 2005, Seite 170;
Securicon-Tageslage vom 16./17. Mai 2005
(Securicon GmbH, 82131 Stockdorf).

Die chinesische Studentin wurde zunächst in Untersuchungshaft genommen, aber am 20. Juni 2005 vorläufig auf freien Fuß gesetzt. Ob sich die in den Medien unterstellte Spionagetätigkeit anklagereif beweisen lässt, muss abgewartet werden, zumal die Chinesin weiterhin jegliche Spionageabsicht bestreitet.

Präventive Aspekte

Die Volksrepublik China setzt – neben der international breit angelegten offenen Informationsbeschaffung – bei konspirativem Vorgehen nach wie vor auf ihre personalintensiven Nachrichtendienste. Diese betreiben ihre Aufklärung auch in Baden-Württemberg in verschiedenen gesellschaftlichen Bereichen – insbesondere aber auf den Gebieten von Wirtschaft, Wissenschaft und Forschung.

Bei der Beschäftigung von Praktikanten und Diplomanden – vor allem aus Ländern mit einem großen Technologierückstand bzw. mit hohem Wettbewerbsdruck – liegt die Gefahr des Know-how-Verlusts auf der Hand. Eine unbeaufsichtigte Tätigkeit außerhalb der regelmäßigen Arbeitszeiten erleichtert den Zugriff auf Unternehmensdaten. Zumindest die Beschäftigung in sensiblen Bereichen mit umfangreichen Zugangsmöglichkeiten sollte sorgsam geprüft und ggf. von Sicherheitsmaßnahmen begleitet werden.

3.3 Der „geheime“ Mitarbeiter

Falldarstellung

Im Oktober 2004 wurde der Sicherheitsdienst eines IT-Unternehmens in der Metropolregion Rhein-Neckar von Mitarbeitern eingeschaltet, da sich anscheinend eine Person unberechtigt in einem Gebäude aufhielt. Der Mann wurde in einem Bereich angetroffen, in dem normalerweise betriebsfremde Spezialisten Systemtests durchführen.

Die Person konnte sich nicht ausweisen und keine Berechtigung für ihren Aufenthalt in der Firma nachweisen. Sie wurde durch den Sicherheitsdienst der Polizei übergeben. Die weiteren Feststellungen ergaben, dass sie möglicherweise schon seit drei Wochen in den Firmenräumen eine Art „privates Büro“ unterhielt und sich während dieser Zeit Zugang zu internen Systemen und zum Internet verschafft hat. Über einen dort eingerichteten Account versandte sie u.a. Bewerbungsschreiben an verschiedene Firmen in der IT-Branche, wobei sie stets den Eindruck erweckte, Beschäftigter des betroffenen Unternehmens zu sein, und eine Nebenstelle der firmeneigenen Telefonanlage als Rückrufmöglichkeit angab.

Der Verdächtige ist seit längerer Zeit ohne Anstellung und betrachtet sich selbst als IT-Fachmann. Durch die Vorspiegelung der Tatsache, Beschäftigter des bekannten Unternehmens zu sein, erhoffte er sich Vorteile bei verschiedenen Bewerbungen in der IT-Branche.

Als Mitarbeiter einer Zeitarbeitsfirma war er 2003 bei dem IT-Unternehmen eingesetzt und kannte daher die Vorgehensweise bei der Vergabe von Systemzugängen. Aus dieser Zeit waren ihm die Räumlichkeiten ebenso bekannt wie die einschlägigen Zugangsregelungen.

Unter Ausnutzung der Gutgläubigkeit von Mitarbeitern des betroffenen Unternehmens hat sich der Mann unauffällig unter Personengruppen gemischt, die zum Beispiel vom gemeinsamen Mittagessen zurückkamen. Er profitierte dann davon, dass – ohne eine weitere Prüfung – ein Berechtigter den Zugang für die gesamte Personengruppe eröffnen konnte.

Innerhalb der Geschoßebene suchte sich der Mann ein abgelegenes Büro, wo er sich einen „Arbeitsplatz“ einrichtete. Durch seine Vorkenntnisse konnte er sich eine User-ID verschaffen und das voreingestellte Initialpasswort ändern.

Durch sein Vorgehen hatte der Mann die Möglichkeit, auf interne Systeme (Organisationsdaten) zuzugreifen und dort Veränderungen vorzunehmen, zum Beispiel in den Daten des Firmenfuhrparks. Bisher sind keine Umstände bekannt geworden, die zu einem echten Schaden bei der betroffenen Firma geführt hätten.

Der Mann wurde nach Durchführung von Ermittlungsmaßnahmen bei der Staatsanwaltschaft wegen des Ausspähens von Daten zur Anzeige gebracht. Das Verfahren ist noch nicht abgeschlossen.

Präventive Aspekte

Bei dem Firmengebäude handelt es sich um eine angemietete Immobilie, deshalb entsprach der Sicherheitsstandard nicht den sonst üblichen Gepflogenheiten des Unternehmens. Durch den späteren Einbau einer Personenvereinzelungsanlage konnte eine Wiederholung des geschilderten Falles ausgeschlossen werden. Allerdings wäre eine solche Vorgehensweise auch schon vorher nicht möglich gewesen, wenn den Mitarbeitern ein entsprechendes Sicherheitsbewusstsein vermittelt worden wäre. Dann hätten sie wohl keine ihnen unbekannte Person in ihrer Gruppe mit in das Gebäude genommen.

Außerdem entsprach die Userverwaltung nicht den heutigen Anforderungen. Mit einem unwesentlich aufwändigeren Verfahren hätte der Zugriff des Mannes auf ein internes System verhindert werden können.

3.4 Ausfall des Administrators[2]

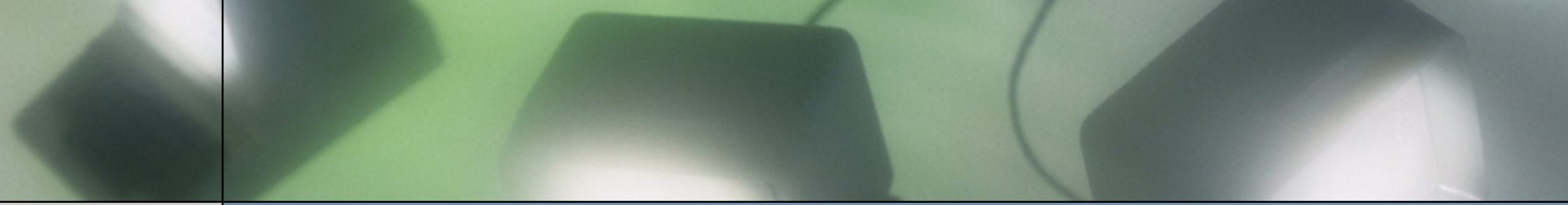
Falldarstellung

Wie viele andere Unternehmen beschäftigte ein innovativer mittelständischer Maschinenbauer nur einen DV-Administrator, der seit vielen Jahren sowohl für Installation und Konfiguration aller PCs und der gesamten Standard- bzw. Spezial-Software als auch für den ausfallsicheren Betrieb der Netze zuständig war. Durch einen schweren, nicht selbst verursachten Verkehrsunfall fiel der Administrator plötzlich komplett aus und war in der Folge nicht mehr arbeitsfähig.

Nach nur wenigen Tagen häuften sich die Probleme mit den Servern im Netz: Fehlermeldungen und Warnhinweise erschienen, die von den Mitarbeitern nicht korrekt interpretiert oder gar bearbeitet werden konnten. Kurze Zeit später standen mehrere Rechner still. Versuche, das Netz neu zu starten, blieben erfolglos. Der Ausfall der gesamten Systemlandschaft ließ einen normalen Betriebsablauf nicht mehr zu und nahm rasch existenzbedrohende Ausmaße an. Auch Kunden und Lieferanten blieben die Probleme nicht verborgen.

Das eiligst einberufene Krisenteam musste feststellen, dass die über Jahre unkontrolliert gewachsene DV-Architektur fehlerhaft und vom Administrator unvollständig dokumentiert worden war. Da selbst Administrator-Passwörter nicht hinterlegt waren, scheiterte eine zunächst beauftragte IT-Support-Firma daran, das System wieder zum Laufen zu

[2] Bundesamt für Sicherheit in der Informationstechnik, Leitfaden IT-Sicherheit 2004, S. 12.



bringen. Weitere externe IT-Spezialisten mussten über mehrere Wochen hinzugezogen werden, bis neben den Standardanwendungen insbesondere die branchen- bzw. firmenspezifischen Individuallösungen wieder fehlerfrei eingesetzt werden konnten.

Die materiellen und immateriellen (Image-)Schäden durch Produktions-/Umsatzausfälle, Kundenverluste u. ä. summierten sich auf einen sechsstelligen Betrag.

Präventive Aspekte

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt im Maßnahmenkatalog „Personal“ des IT-Grundschutzhandbuchs (IT-GSHB) im Baustein M 3.10 („Auswahl eines vertrauenswürdigen Administrators und Vertreters“)[3] zur Verhinderung solcher Schäden u. a. folgendes:

“Da der Administrator hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle inne hat, muss auch bei seinem Ausfall die Weiterführung seiner Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über den aktuellen Stand der Systemkonfiguration verfügen sowie Zugriff auf die für die Administration benötigten Passwörter, Schlüssel und Sicherheitstoken haben.

Hat ein Unternehmen oder eine Behörde mehrere Administratoren mit vergleichbaren IT-Systemkenntnissen, so können sich diese auch wechselseitig vertreten, sofern diese dafür noch freie Kapazitäten haben. In allen Bereichen, in denen nur ein Administrator hauptverantwortlich IT-Systeme betreut, sollten zwei Stellvertreter eingearbeitet werden, da bei längerer Abwesenheit des Administrators erfahrungsgemäß auch der Stellvertreter zeitweise nicht für Administrationsaufgaben zur Verfügung steht.

Um die Funktionsfähigkeit des IT-Betriebs zu gewährleisten, muss insbesondere bei bevorstehenden Personalveränderungen oder Veränderungen der Organisationsstruktur geprüft werden, ob die erforderlichen Administrationstätigkeiten auch durch die benannten Administratoren und deren Vertreter bewältigt werden können.“

Folgende konkrete Maßnahmen hätten sich im geschilderten Fall angeboten:

- Stellvertreterregelungen schaffen,
- Systemlandschaft vollständig, detailliert und verständlich dokumentieren,
- sicheres Passwort-Management installieren,
- Datensicherungskonzept erstellen,
- Daten konsequent sichern,
- Krisenpläne für mögliche Schadensfälle ausarbeiten,
- innerbetriebliches Krisenteam bilden und Notfälle konkret durchspielen,
- Aus- und Fortbildungskonzepte für die involvierten Mitarbeiter erstellen,
- für Notfälle externes Experten-Know-how sichern (personell und räumlich).

[3] URL: www.bsi.bund.de/gshb/deutsch/m/m03010.html.

3.5 Hackerangriff aus dem Internet[4]

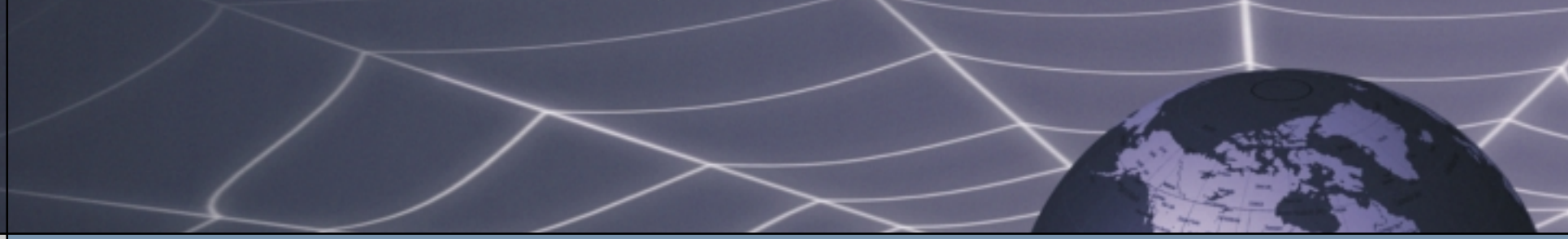
Falldarstellung

In einer Kleinstadt betrieb ein Psychologe seine Praxis. Seine Patientenakten verwaltete er auf einem PC mit Internetanschluss. Er kannte sich mit seinem PC gut aus und installierte seine Software in der Regel selbst. Seine Daten hielt er für sicher, da er sich mit einem Passwort am System anmelden musste. Eines Tages verbreitete sich in der ganzen Stadt wie ein Lauffeuer die Nachricht, dass vertrauliche Patienteninformationen anonym in einem lokalen Internet-Diskussionsforum der Stadt veröffentlicht wurden. Die Polizei stieß bei ihren Ermittlungen auf den Psychologen und stellte fest, dass sein Praxis-PC völlig unzureichend gegen Fremdzugriffe gesichert war und vermutlich Ziel eines Hackerangriffs wurde. Der Staatsanwalt erhob Anklage, da mit vertraulichen Patientendaten fahrlässig umgegangen wurde. Der entstandene Schaden für die betroffenen Patienten war enorm und kaum quantifizierbar.

Präventive Aspekte

Es ist ein weit verbreiteter Irrglaube, dass moderne Kommunikationstechnik automatisch vor Informationsverlusten schützt. Insbesondere durch den Anschluss eines IT-Systems an das Internet entstehen weit reichende Gefährdungsmomente.

[4] Bundesamt für Sicherheit in der Informationstechnik, Leitfaden IT-Sicherheit 2004, S.12.



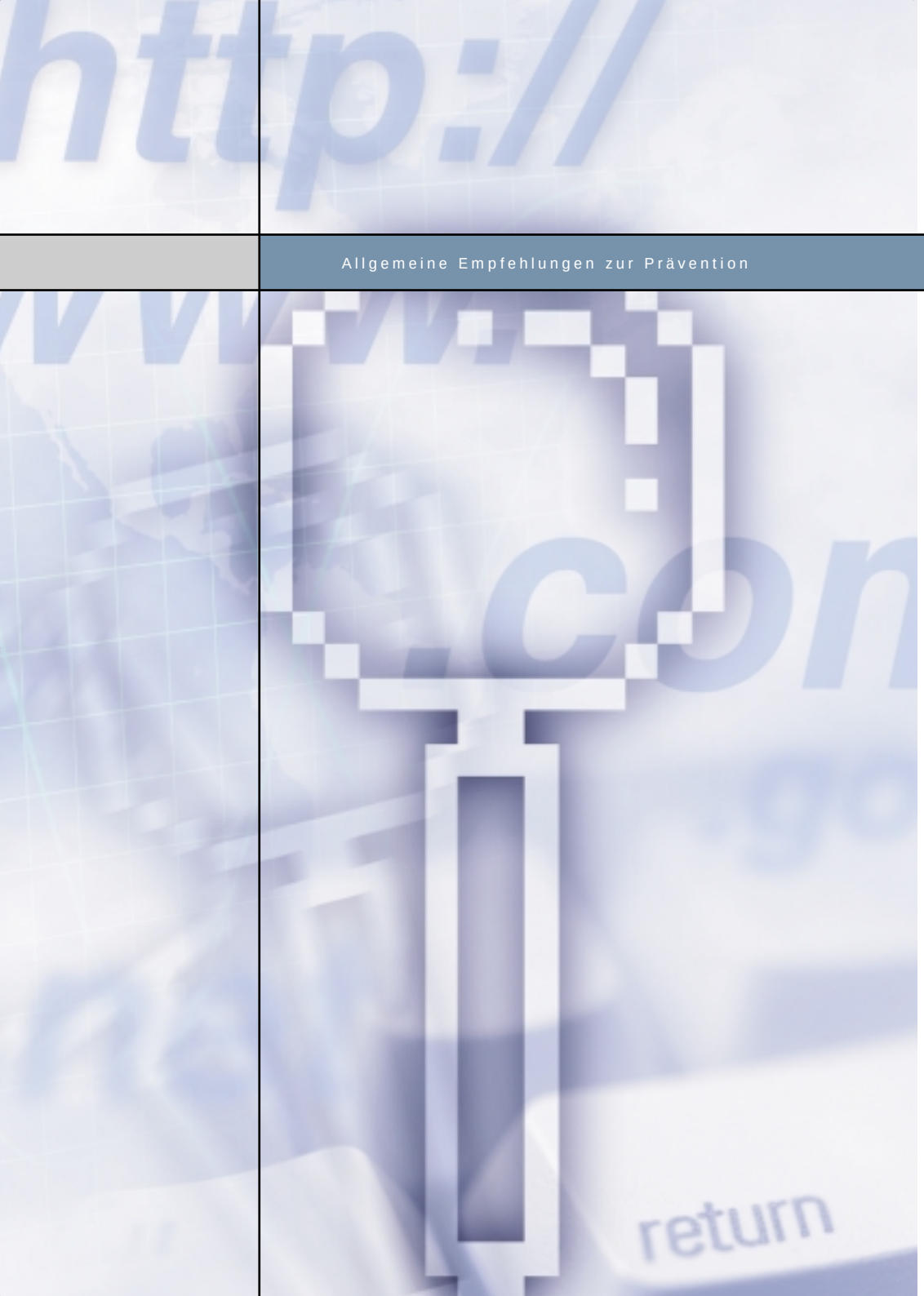
Um die Patientendaten ausreichend zu schützen, hätten zumindest die Absicherung des Internet-Zugangs und die Verschlüsselung der vertraulichen Informationen erfolgen müssen.

Neben den vom BSI in den Kapiteln 5 und 6 des IT-GSHB[5] beschriebenen Standardsicherheitsmaßnahmen für vernetzte PC-Systeme hätten sich im geschilderten Fall zur Absicherung des Internet-Anschlusses speziell folgende konkrete Maßnahmen nach Kapitel 5.8 IT-GSHB angeboten:

- Regelung des Passwortgebrauchs (Form, Länge, Güte, Wechsel),
- Regelmäßiger Einsatz eines Viren-Suchprogramms,
- Prüfung eingehender Dateien auf Makro-Viren,
- Sichere Installation und Konfiguration sowie sicherer Betrieb von Internet-PCs, WWW-Browsern und E-Mail-Clients,
- Schutz vor DNS-Spoofing[6],
- Verwendung von Standard-Verschlüsselungsverfahren,
- Einsatz von Personal Firewalls,
- Sichere Internet-Anbindung durch Auswahl eines geeigneten Internet Service Providers (ISP) und Beschaffung geeigneter Netzkomponenten,
- Erstellung eines Datensicherungskonzepts (Umfang, Häufigkeit und Zeitpunkt, Sicherungsmedium, Verantwortlichkeiten, Aufbewahrungsort). Regelmäßige Datensicherung (BackUp) der System-, Programm- und Konfigurationsdateien.

[5] URL: www.bsi.bund.de/gshb/deutsch/m/m03010.html.

[6] Mit gefälschten IP-Adressen wird im Internet Kontakt zu anderen Rechnern gesucht.



4. Allgemeine Empfehlungen zur Prävention[7]

Die Ergebnisse der Fall- und Schadensanalyse der Universität Lüneburg sowie die geschilderten Fallbeispiele machen deutlich, dass der Umgang mit betrieblicher Sicherheit und der Schutz von Betriebsgeheimnissen für kleine und mittelständische Unternehmen eine besondere Herausforderung darstellen. Nach Auffassung des Sicherheitsforums muss die Prävention professionell betrieben und dabei den gesellschaftlichen und wirtschaftlichen Veränderungen sowie den verfeinerten Methoden der Informationsbeschaffung angepasst werden.

Erste konsequente Folgerung für Ihr Unternehmen sollte sein, den Know-how-Schutz zur Chefsache zu erklären und die Sicherheitsstrategien kritisch zu hinterfragen.

Unterschätzen Sie dabei nicht den Aufwand. Sehen Sie für diese anspruchsvolle Aufgabe ein ausreichendes Zeitfenster vor. Benennen Sie einen Sicherheitsverantwortlichen mit klaren Kompetenzzuweisungen oder bedienen Sie sich bei

[7] Vgl. auch die Präventionsempfehlungen des Sicherheitsforums als Ergänzung zur Fall- und Schadensanalyse der Universität Lüneburg sowie die Broschüre „Know-how-Schutz – Handlungsempfehlungen für die gewerbliche Wirtschaft“ des Landesamts für Verfassungsschutz. Beide Ausarbeitungen können auf der Homepage des Sicherheitsforums abgerufen werden (URL: www.sicherheitsforum-bw.de).

Bedarf eines renommierten Beratungsunternehmens. Es ist sicher besser, einen Partner zu beauftragen, der sich in der Materie auskennt und über das erforderliche Netzwerk verfügt, als sich selbst in Themen zu engagieren, die einem von der Materie her eigentlich fremd und zudem gelegentlich unangenehm sind.

Viele Schäden werden durch das bewusste oder fahrlässige Fehlverhalten von Mitarbeitern oder von Kooperationspartnern verursacht. Vermitteln Sie diesem Personenkreis die Überzeugung, dass Sicherheit für das gesamte Unternehmen und damit auch für den Arbeitsplatz des Einzelnen eminent wichtig ist.

Strukturieren Sie Ihre Einstellungspolitik sowie das Personalmanagement unter Berücksichtigung von Sicherheitsaspekten. Securitychecks sind heute weithin üblich. Je höher die Position im Unternehmen, desto höher auch das Risiko und die Möglichkeit, dem Unternehmen nennenswerten Schaden zuzufügen.

Alle wichtigen Informationen zu Ihren Produkten oder Herstellungsverfahren werden heute mit Hilfe von Informations- und Kommunikationssystemen erstellt, bearbeitet und dokumentiert. Auch für diesen Bereich muss ein umfassendes Sicherheitskonzept mit einer restriktiven Rechteverwaltung entwickelt werden. Bewahren Sie die entsprechende Dokumentation in einem besonders gesicherten Bereich (z. B. in einem hochwertigen Tresor) oder außerhalb der Firmenräume (z. B. in einem Bankschließfach) auf. Bauen Sie insbesondere bei komplexen Systemen eine interne Sicherheitsorganisation auf. Treffen Sie Vorkehrungen für den Ausfall des Administrators. Bestellen Sie immer einen Stellvertreter, der diese Funktion auch fachlich ausfüllen kann. Bestimmen Sie eine Systematik für die Datensicherung und deren sichere Aufbewahrung.

Sorgen Sie für eine starke Authentifizierung des Berechtigten. Stellen Sie über das System den regelmäßigen Wechsel von Passwörtern sicher. Bestimmen Sie die Mindestlänge und die Form.

Denken Sie auch an vermeintliche Nebensächlichkeiten: Führen Sie ein regelmäßiges Update Ihrer Virenscanner, Firewalls und sonstigen Sicherheitssysteme durch. Schließen Sie erkannte Sicherheitslücken in Betriebssystemen und Anwendungsprogrammen durch zeitnahes Einspielen von Patches[8]. Stellen Sie die sichere Entsorgung von Daten-

[8] Kleines Programm zur temporären Korrektur von Softwarefehlern.

trägern, schriftlichen Aufzeichnungen und Druckerzeugnissen mit sensiblen Inhalten sicher.

Schützen Sie die wichtigen Einrichtungen Ihres Unternehmens auch physikalisch. Nicht jeder muss permanent Zutritt zu allen Betriebsteilen haben. Setzen Sie Zugangsbeschränkungen über eine Schließanlage oder eine elektronische Lösung um. Damit stellen Sie sicher, dass nur ein berechtigter Personenkreis bestimmte Bereiche betreten kann. Prüfen Sie das Berechtigungskonzept periodisch auf notwendige Änderungen.

Um Risiken besser erkennen und bewerten zu können, sollten Sie vorab eine Gefährdungsanalyse für alle Unternehmensteile erstellen und sich bei der Umsetzung der Sicherheitsmaßnahmen daran orientieren. Das daraus abzuleitende ganzheitliche Informationsschutzkonzept sollte personelle, organisatorische, baulich-technische und rechtliche Schutzvorkehrungen enthalten. Detaillierte Organisations- und Arbeitsanweisungen (Benutzerrichtlinien) helfen Ihren Mitarbeitern bei der Umsetzung strategischer Sicherheitsvorgaben.

Scheuen Sie sich nicht, die Sicherheitsbehörden des Landes für Ihre Anliegen in Anspruch zu nehmen. Nehmen Sie Kontakt auf und halten Sie diesen auch. Aufgrund jahrzehntelanger Erfahrung im Bereich der Sicherheit stehen Ihnen dort ausgewiesene Experten zur Verfügung, die sich gerne und intensiv Ihren ganz speziellen Problemen widmen.

Betrachten Sie Aufwendungen für die Informationssicherheit nicht als unproduktive Kosten, sondern als gut angelegte Investition in die Zukunftssicherung Ihres Unternehmens.

5. Wie sicher ist Ihr Unternehmen?

1. Ist Ihr Unternehmen in der Vergangenheit schon einmal von Spionageaktivitäten betroffen gewesen?

2. Haben Sie den Know-how-Schutz in Ihrem Betrieb zur „Chefsache“ erklärt?

3. Existiert in Ihrem Unternehmen ein Informationsschutzkonzept, das alle betrieblichen Bereiche und Ebenen umfasst?

4. Haben Sie durch schriftliche Anweisungen oder Empfehlungen Ihre Unternehmensgrundsätze zum Know-how-Schutz konkretisiert?

5. Ist der Know-how-Schutz in Ihrem Unternehmen gezielt auf die „Schwachstelle Mensch“ ausgerichtet?

6. Gibt es einen Sicherheitsverantwortlichen, der als zentraler Ansprechpartner und Koordinator für sämtliche Fragen des Know-how-Schutzes zuständig ist?

7. Ziehen bei Kontrollen festgestellte Sicherheitsverstöße Sanktionen nach sich?

8. Werden Hinweise auf Know-how-Verluste systematisch erfasst und analysiert?

9. Sind Ihre Informations- und Kommunikationssysteme gegen unbefugten Zugriff (intern/extern) geschützt?

10. Enthalten die Arbeitsverträge in Ihrem Unternehmen Geheimhaltungsklauseln und haftungsrechtliche Bestimmungen im Hinblick auf die unbefugte Nutzung von Firmen-Know-how?

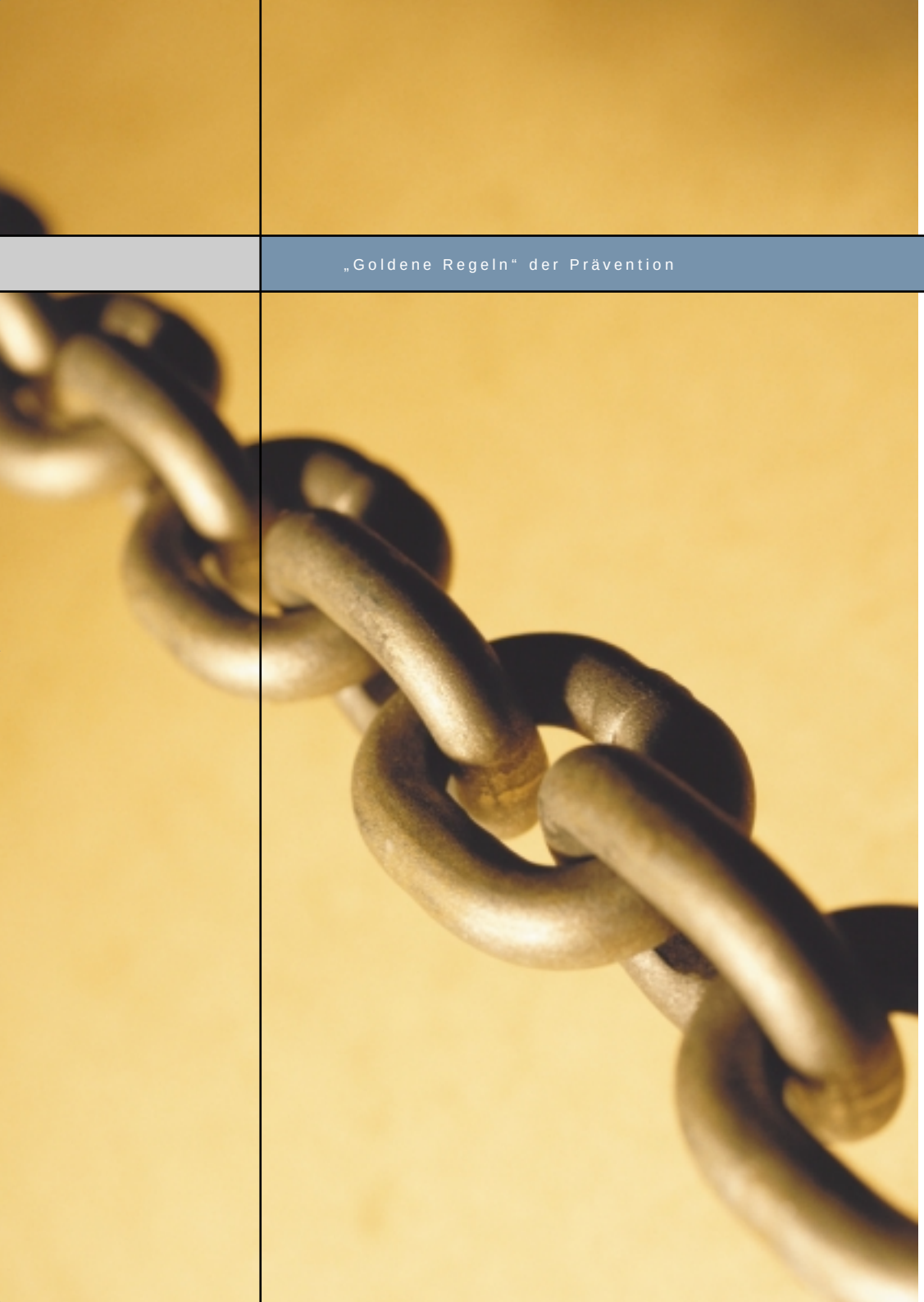
11. Spielen bei der Auswahl von Fremdfirmen auch Sicherheitsaspekte eine Rolle?

12. Unterhalten Sie geschäftliche Beziehungen in Staaten mit besonderen Sicherheitsrisiken (z. B. Russland, China, Iran)?

13. Schalten Sie bei Verdacht auf illegalen Informationsabfluss Sicherheitsbehörden ein?

14. Betreibt Ihr Unternehmen Markt-/Konkurrenzbeobachtung, um möglichst frühzeitig Hinweise auf Know-how-Verluste zu erhalten?

15. Fühlen Sie sich über die Gefahren des illegalen Informationsabflusses durch Spionage ausreichend informiert?



6. „Goldene Regeln“ der Prävention

Die nachfolgenden Merksätze fassen kurz und prägnant die wesentlichen Aspekte des Informationsschutzes zusammen. Bei Bedarf können sie durch unternehmensspezifische Gesichtspunkte ergänzt werden.

1. Nicht warten, bis der Spionagefall eingetreten ist!
2. Aktuelle Informationen bei kompetenten Partnern einholen!
3. Informationsschutz als wichtigen Bestandteil der Firmenphilosophie und Firmenstrategie verankern!
4. Sicherheitsstandards regelmäßig analysieren!
5. Ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben!
6. Schutzmaßnahmen auf den Kernbestand zukunftssichernder Informationen konzentrieren!
7. Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren!
8. „Frühwarnsystem“ zur Erkennung von Know-how-Verlusten installieren!
9. Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen!
10. Informationsschutz als strategischen Erfolgsfaktor nutzen!

7. Ansprechpartner

Baden-Württembergischer Handwerkstag

Jürgen Schäfer
Geschäftsführer
Telefon: 07 11 / 16 57 - 0
E-Mail: jschaefer@hwk-stuttgart.de

Homepage: http://www.handwerk-bw.de

Baden-Württembergischer Industrie- und Handelskammertag

Dr. Hans-Jürgen Reichardt
Geschäftsführer; Abteilungsleiter
Telefon: 07 11 / 20 05 - 0
E-Mail: hans-juergen.reichardt@stuttgart.ihk.de

Elke Voelkel
Referentin
Telefon: 07 11 / 20 05 - 0
E-Mail: elke.voelkel@stuttgart.ihk.de

Homepage: http://www.stuttgart.ihk.de

DaimlerChrysler

Dr. Thomas Menk
Leiter Konzernsicherheit
Telefon: 07 11 / 17 - 0
E-Mail: thomas.menk@daimlerchrysler.com

Michael Volle
Konzernsicherheit
Telefon: 07 11 / 17 - 0
E-Mail: michael.volle@daimlerchrysler.com

Homepage: http://www.daimlerchrysler.com

Forschungszentrum Karlsruhe

Dr.-Ing. Hanns-Günther Mayer
Telefon: 07 24 7 / 82 - 0
E-Mail: hgmayer@map.fzk.de

Homepage: http://www.fzk.de

Innenministerium Baden-Württemberg

Rainer Fichter
Referatsleiter
Telefon: 07 11 / 231 - 3530
E-Mail: Rainer.Fichter@im.bwl.de

Barbara Cremer
Referentin
Telefon: 07 11 / 231 - 3532
E-Mail: Barbara.Cremer@im.bwl.de

Homepage: http://www.innenministerium.baden-wuerttemberg.de

Landesamt für Verfassungsschutz Baden-Württemberg

Johannes Schmalzl
Präsident
Telefon: 07 11 / 95 44 - 123
E-Mail: lfv-bw@t-online.de

Harald Woll
Leiter der Abteilung Spionageabwehr,
Geheim- und Sabotageschutz
Telefon: 07 11 / 95 44 - 300
E-Mail: Harald.Woll@lfvbw.bwl.de

Homepage: http://www.verfassungsschutz-bw.de

Landesverband der Baden-Württembergischen Industrie e.V.

Wolfgang Wolf
Geschäftsführendes Vorstandsmitglied
Telefon: 0711 / 32 73 25 - 00
E-Mail: wolf@lvi.de

Manuel Geiger
Referent
Telefon: 0711 / 32 73 25 - 11
E-Mail: geiger@lvi.de

Homepage: http://www.lvi.de

SAP AG

Prof. Dr. Sachar Paulus
Chief Security Officer
Telefon: 06227 / 747439
E-Mail: sachar.paulus@sap.com

Thomas Ostermann
Sicherheitsbevollmächtigter
Telefon: 06227 / 747806
E-Mail: thomas.ostermann@sap.com

Homepage: http://www.sap.com

Steinbeis-Stiftung

Prof. Dr. Michael Auer
Telefon: 07 11 / 18 39 - 5
E-Mail: auer@stw.de

Homepage: http://www.stw.de

VDMA Baden-Württemberg

Jens Geißmann
Ansprechpartner IT-Sicherheit
Telefon : 0711 / 2 28 01-17
E-Mail : jens.geissmann@vdma.org

Homepage: http//www.vdma.org

Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V.

Karl Schotzko
Geschäftsführer
Telefon: 07 11 / 95 46 09 15
E-Mail: schotzko@vsw-bw.com

Homepage: http://www.vsw-bw.com

Wirtschaftsministerium Baden-Württemberg

Günther Leßnerkraus
Abteilungsleiter
Telefon: 07 11 / 12 3 - 0
E-Mail: poststelle@wm.bwl.de

Volker Weidemann
Referatsleiter
Telefon: 07 11 / 12 3 - 0
E-Mail: poststelle@wm.bwl.de

Homepage: http://www.wm.baden-wuerttemberg.de

Impressum

Herausgeber:
Innenministerium
Baden-Württemberg
für das Sicherheitsforum
Baden-Württemberg

Gestaltung:
Compart Werbeagentur,
Karlsruhe

Druck:
Wilhelm Stober GmbH,
Eggenstein

Stand:
November 2005