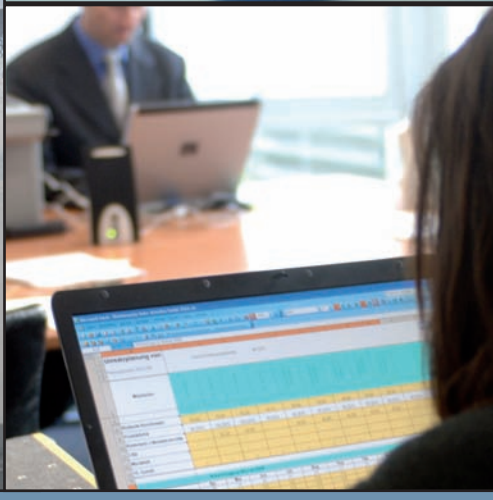
Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

SiFo-Studie 2009/10

Handlungsempfehlungen für Unternehmen



Steinbeis-Edition

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet.

Impressum

Sicherheitsforum Baden-Württemberg (Hrsg.)
SiFo-Studie 2009/10 – Handlungsempfehlungen für Unternehmen

Die Studie wurde erstellt durch das Ferdinand-Steinbeis-Institut in Kooperation mit der School of Governance, Risk & Compliance der Steinbeis-Hochschule Berlin.

1. Auflage 2010, Steinbeis-Edition Stuttgart
ISBN 978-3-941417-21-2

Satz: Steinbeis-Edition
Titelbild: USB © photocase.com/idaho
Druck: RöslerDruck GmbH, Schorndorf

www.steinbeis-edition.de | 135750-2010-01

SiFo-Studie 2009/10

Handlungsempfehlungen für Unternehmen

Inhaltsverzeichnis

1 Einführung

Unternehmer, die bereits einmal Schäden aufgrund unberechtigter Informationsweitergabe durch unternehmensnahe Personen erlitten haben, tragen sich häufig mit der Ungewissheit, ob ihre Schutzvorkehrungen ausreichend sind. Es stellen sich Fragen wie: Verhalten sich die Unternehmensangehörigen rechtstreu und im Sinne des Unternehmens? Fühlen sie sich den Interessen und Belangen des Unternehmens verbunden? Schützen sie unternehmenssensible Daten ausreichend und geben sie sie vor allem nicht unberechtigt weiter? Wie verhalten sich die Geschäftspartner? Gehen sie sorgfältig mit Unternehmensdaten um? Diese Fragen münden letztlich in der Überlegung: Wann soll das Vertrauen in Unternehmensangehörige (unabhängig von Tätigkeit und Hierarchiestufe) und Geschäftspartner – ein wichtiger Faktor für eine gute Zusammenarbeit – einem professionellen Misstrauen Platz machen?

Der „Faktor Mensch" spielt beim Know-how-Abfluss eine wesentliche Rolle. Die Unternehmen können sich nicht darauf verlassen, dass sich alle Mitarbeiter dem Unternehmen, seiner Kultur und seinen Regeln verpflichtet sehen. Personen mit krimineller Energie sind mit ethischen Ansprüchen häufig nicht erreichbar. Es ist deshalb unverzichtbar, dass die Unternehmensleitungen die Einhaltung unternehmensinterner Regeln von Unternehmensangehörigen und Geschäftspartnern konsequent einfordern und Verstöße unbeirrt verfolgen.

Um einen ungewollten Abfluss von Know-how zu vermeiden, bedarf es einer Kombination verschiedener Methoden: Sensibilisierung und Information der Unternehmensangehörigen, Vorkehrungen zum Schutz gegen schädigende Handlungen durch Unternehmensangehörige und Geschäftspartner sowie technische Schutzmaßnahmen. Allein technische Schutzmaßnahmen, wie sie viele der im Rahmen der „SiFo-Studie 2009/10" befragten Unternehmen bereits haben, genügen nicht.

Die vom Sicherheitsforum Baden-Württemberg in Auftrag gegebene und vom Ferdinand-Steinbeis-Institut in Stuttgart in Kooperation mit der School of Governance, Risk & Compliance der Steinbeis-Hochschule Berlin erarbeitete Studie „Know-how-Schutz in Baden-Württemberg" zeigt sehr deutlich, dass die Bedrohung durch Urheberrechtsverletzungen und Spionage zwar insbesondere, aber nicht nur in for-

schungsintensiven Unternehmen eine reale Gefahr ist, die noch immer unterschätzt wird. Die Studie legt vor allem auch offen, dass nach Schätzungen etwa 70–80 % der IT-Angriffe auf unternehmenssensible Daten von Unternehmensangehörigen kommen. Viele Unternehmen wissen sich vor dieser Bedrohung nicht ausreichend zu schützen.

Ein zentrales Anliegen dieser Handlungsempfehlungen ist es deshalb, den Fokus stärker als bisher auf Schutzvorkehrungen zu lenken, die einen Know-how-Missbrauch durch unternehmensnahe Personen, ob Unternehmensangehörige oder Geschäftspartner, vermeiden helfen. Denn die in der Studie festgestellte hohe Gefährdung durch unternehmensnahe Personen bedeutet zugleich, dass die Unternehmen auf das Missbrauchsrisiko Einfluss nehmen können.

Den Sicherheitsverantwortlichen in den Unternehmen ist daher zu empfehlen, die Konzepte zum Schutz vor Informationsabfluss permanent auf Lücken und Schwachstellen zu überprüfen und dabei vor allem auch dem „Faktor Mensch“ noch stärker als bisher Beachtung zu schenken. Um eine Sicherheitskultur im Unternehmen zu erreichen, die nicht allein auf Kontrolle und Repression gründet, sollte ein besonderes Augenmerk auch darauf gelegt werden, das Verständnis und die Unterstützung vor allem der Unternehmensangehörigen und auch der Geschäftspartner zu gewinnen.

Die nachfolgenden Handlungsempfehlungen stellen beispielhaft Leitideen sowohl zum strategischen als auch zum operativen Management für unternehmenswirksame Schutzmaßnahmen vor. Sie sind nicht abschließend, da Unternehmen in unterschiedlichen Geschäftsbereichen auch individuelle Schutzmechanismen benötigen. Diese Handlungsempfehlungen geben Anregung und Hilfestellung, Netzwerke zum Schutz vor Know-how-Abfluss zu knüpfen oder zu erweitern. Sie sollen helfen, Ideen aus anderen Unternehmen für das eigene Unternehmen nutzbar zu machen. Die Unternehmen sollen in die Lage versetzt werden, das Mögliche zu tun, um Sicherheitslücken zu schließen und nicht Opfer von Know-how-Missbrauch und ungewolltem Informationsabfluss zu werden.

Sicherheitsforum Baden-Württemberg

Das Sicherheitsforum Baden-Württemberg ist ein unabhängiges Gremium aus Unternehmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden. Es verfolgt keine geschäftlichen Interessen und ist politisch nicht gebunden. Die Kernaufgabe des Sicherheitsforums ist es, den Technologievorsprung der baden-württembergischen Wirtschaft und Forschung vor Wirtschaftsspionage zu schützen.

Homepage: **www.sicherheitsforum-bw.de**

Ansprechpartner: **Dr. Christiane Meis**

Geschäftsstelle Sicherheitsforum Baden-Württemberg
Innenministerium Baden-Württemberg
Telefon: 0711 231-3460
E-Mail: christiane.meis@im.bwl.de

Klaus Zimmer

Innenministerium Baden-Württemberg
Telefon: 0711 231-3461
E-Mail: klaus.zimmer@im.bwl.de

2 Problemaufriss

Die Ergebnisse der „SiFo-Studie 2009/10“ zeigen:

Über 60 % der forschungsintensiven Unternehmen waren in den letzten vier Jahren mindestens von einem eindeutigen Fall von Verstößen gegen Patent- und Markenrechte oder Gebrauchs- und Geschmacksmusterrechte betroffen und/oder hatten einen konkreten Verdacht hinsichtlich einer solchen Rechtsverletzung. Mehr als jedes vierte forschungsintensive Unternehmen (27 %) wurde in den letzten vier Jahren Opfer von Spionage bzw. unfreiwilligem Informationsabfluss.

Diese Fälle führten bei den Unternehmen zu erheblichen Umsatzeinbußen, Beeinträchtigungen von Geschäftsbeziehungen und strategischen Nachteilen gegenüber Wettbewerbern. Besonders Zeit und Kosten für die Bearbeitung der einzelnen Vorfälle stellten für Unternehmen einen gravierenden bis sehr gravierenden Schaden dar. Dabei lagen die finanziellen Schäden zwischen unter 10.000 Euro bis über zwei Millionen Euro je Vorfall.

Aus Sicht der Unternehmen ist das Risiko, in den nächsten Jahren Opfer von Urheberrechtsverletzungen bzw. Geheimnisverrat zu werden, weiterhin hoch. Daher rüsten sich Unternehmen mit Sicherheitsmaßnahmen zur Abwehr von Industrie- und Wirtschaftsspionage. Staatliche Organisationen und Verbände werden von den Unternehmen in den seltensten Fällen genutzt, um sich über Abwehr- und Vorsorgemaßnahmen zu informieren bzw. sich im Rahmen von Präventionsmaßnahmen unterstützen zu lassen. Zumeist wird das Know-how hierfür im eigenen Unternehmen aufgebaut, oder es werden private Dienstleister hinzugezogen. Im Bereich Objekt- und IT-Schutz haben viele Unternehmen bereits Präventionsmaßnahmen ergriffen bzw. planen deren Einführung. Zwar wurden auch im Bereich Personal und in den Geschäftsabläufen Maßnahmen eingeführt, doch gerade die Risikoerfassung im eigenen Unternehmen und die Sensibilisierung der Unternehmensangehörigen für diese Risiken sind bislang in wenigen Unternehmen vorhanden. Zur Beseitigung dieses Sicherheitsdefizits existiert ein breites Arsenal an Instrumenten, wie z. B. Mitarbeiterschulungen.

Allerdings gibt es auch für die Prävention gegen Spionage bzw. Informationsabfluss keine Musterlösung. Vielmehr müssen die Maßnahmen auf das jeweilige Unternehmen, die individuelle Bedrohungslage sowie die unterschiedlichen wirtschaftlichen Anforderungen und Gegebenheiten zugeschnitten werden. Es gibt jedoch einige Standardsicherheitsvorkehrungen, um sich effektiv gegen den Zugriff auf das sogenannte Firmen-Know-how zu schützen, die jedes Unternehmen einhalten sollte. Dabei ist anzumerken, dass ein 100 %iger Schutz nicht erreicht werden kann.

Zum einen sind Unternehmen zwangsläufig auf risikobehaftete Schnittstellen beim „Faktor Mensch“ (Unternehmensangehörige, Kunden, Lieferanten) sowie beim „Faktor Technik“ (Telekommunikationsverbindungen etc.) angewiesen. Zum anderen sind die Angriffsmöglichkeiten zu vielfältig, um die Schutzmaßnahmen jederzeit auf dem technisch aktuellsten Stand zu halten. Das Gut „Know-how“ hat Merkmale, insbesondere die Eigenschaften der Immaterialität und der unendlichen Teilbarkeit, die einen umfassenden Schutz erschweren. Allein herkömmliche Zugangsbeschränkungen oder Personenkontrollen sind aus diesen Gründen nur bedingt geeignet, ein Unternehmen nachhaltig und langfristig vor Know-how-Abfluss zu schützen.

3 Sicherheitskonzept und strategische Managementaufgaben

Besonders unternehmerrelevantes Wissen sowie schützenswerte Informationen zu sichern und vor Risiken zu bewahren, setzt voraus, dass sie als solche überhaupt erkannt und lokalisiert werden. Eine technische Ausstattung hilft hierbei weiter, noch wichtiger aber ist die Einbindung der Unternehmensangehörigen.

Risikomanagement

Ein Risikoportfolio kann bei der Neu- oder Weiterentwicklung eines Sicherheitskonzeptes die Basis bilden, um die Ist-Situation im Unternehmen zu erfassen und so einen Überblick über mögliche Risiken zu erhalten. Die Entwicklung eines Risikoportfolios sollte unter Einbeziehung der Unternehmensführung stattfinden, da bei der späteren Festlegung und Umsetzung von Maßnahmen ebenso wie in Konfliktsituationen die Unterstützung der Unternehmensführung entscheidend ist.

Zu Beginn der Risikoanalyse steht die Entscheidung, was als schützenswertes Betriebsgeheimnis anzusehen ist, d. h. welche Entwicklungen, Forschungsergebnisse und Geschäftsgeheimnisse für die Konkurrenz von besonderem Interesse sind oder sein könnten. Neben der Feststellung, welches Wissen gefährdet ist, muss auch erfasst werden:

- wer dieses Wissen im Unternehmen besitzt bzw. Zugang zu diesem Wissen hat,
- wo die Informationen gespeichert sind,
- wo die Informationen verarbeitet werden,
- welche organisatorischen Abläufe betroffen sind.

Je mehr schützenswerte Informationen vorhanden sind, desto schwieriger ist ein erfolgreicher Schutz.

Die anschließende Risikobewertung gibt ein Bild darüber, welche Informationen und Objekte absoluten Schutz benötigen, bei welchen ein Teilschutz ausreichend ist, welche Risiken in Kauf genommen werden können und in welcher zeitlichen Reihenfolge notwendige Sicherheitsmaßnahmen ergriffen werden müssen. Hierzu gehören auch die Analyse potenzieller oder realer Angriffe bzw. der allgemeinen Bedrohungslage, also die Identifikation etwaiger Angreifer und ihrer Möglichkeiten sowie der Abgleich mit den eigenen Schwachpunkten. Eine Überprüfung der aktuellen Bedrohungslage sollte regelmäßig erfolgen, um das Schutzkonzept entsprechend anzupassen und technisch möglichst aktuell, zumindest aber angemessen zu halten. Das Schutzkonzept setzt sich dabei immer aus aufeinander abgestimmten personellen, baulichen, technischen, organisatorischen und rechtlichen Maßnahmen zusammen.

Entwicklung einer Sicherheitsvision

Bei der Entwicklung des Schutzkonzeptes sollte gleichzeitig von der Unternehmensleitung eine Sicherheitsvision entwickelt werden. Diese Vision bringt zum Ausdruck, welches Idealbild bezüglich des Sicherheitsniveaus in Zukunft bestehen soll. Dies könnte etwa in einem umfassenden Sinne lauten: „Wir wollen in unserer Branche Qualitätsführer im Sicherheitsmanagement werden“, oder konkreter auf einzelne Sicherheitsrisiken bezogen: „Wir schützen uns und unsere Mitarbeiter so, dass wir auf Messen keine ungewollten Know-how-Verluste erleiden“.

Einbindung aller Unternehmensangehörigen

Während des gesamten Prozesses der (Weiter-)Entwicklung eines Sicherheitssystems ist die Einbindung aller Unternehmensangehörigen entscheidend.
Einerseits verfügen Unternehmensangehörige über umfangreiche Insiderinformationen, die sie fahrlässig oder absichtlich verraten können. Innerbetrieblicher Schutz ist daher die Aufgabe aller Unternehmensangehörigen (unabhängig von Tätigkeit und Hierarchiestufe), auch beispielsweise des Betriebsrates, und nicht nur der Sicherheitsexperten im Unternehmen.

Andererseits können Unternehmensangehörige erheblich zur Aufdeckung von möglichen Schwachstellen im Unternehmen beitragen. Frühzeitige Einbindung erhöht deren Sensibilität gegenüber möglichen Gefahrenquellen sowie das Verständnis und die Akzeptanz von neu implementierten Maßnahmen.

Häufig werden diese Maßnahmen zu einem Gesamtpaket (Awareness-Kampagne) zusammengefügt, welches das Sicherheitsbewusstsein im Unternehmen erhöhen soll.

Mit Hilfe von Monitoringsystemen kann zu einem späteren Zeitpunkt überprüft werden, ob eingeführte Regeln und Maßnahmen jeden Unternehmensangehörigen erreicht haben und welche Risikoposition ein Unternehmen im relevanten Branchenumfeld einnimmt (siehe Kapitel 7).

Pflege und Aufbau von Netzwerken

Für jedes Unternehmen ist der rechtzeitige und konsequente Aufbau eines umfangreichen, personenbezogenen Sicherheitsnetzwerkes von immenser Bedeutung. Neben dem regelmäßigen Austausch von Informationen und neuen Entwicklungen dient es auch dazu, im Falle einer Unternehmensgefährdung oder -schädigung zeitnah die richtigen Ansprechpartner zu identifizieren.

Wenn es in einem Unternehmen zu einem Fall von Spionage oder zum Verrat von Geschäfts- und Betriebsgeheimnissen kommt, sollten die Unternehmen proaktiv vorgehen können. Dafür ist eine lernende Organisation Voraussetzung, denn nur so können gleiche oder ähnliche Schädigungen in Zukunft vermieden und darüber hinaus potenziell gefährdete Geschäftspartner im Netzwerk beraten oder sogar geschützt werden. Unabhängig von der Täterherkunft erscheint es empfehlenswert, dass die Unternehmensleitung einen Reaktionsplan für potenzielle Schadensfälle entwickelt. Dieser Plan kann neben den notwendigen Einzelaktionen auch die Grundsatzentscheidung beinhalten, gegen erkannte Straftäter immer Strafanzeige zu erstatten oder auch internen Tätern in jedem Fall zu kündigen. Nicht zuletzt ist eine professionelle Unternehmenskommunikation im Kontext von aufgedeckten Straftaten unerlässlich.

4 Schulungskonzepte

Ein Unternehmen kann nur wirklich erfolgreich sein, wenn seine Unternehmensangehörigen sich mit ihm identifizieren und gemeinsam die Unternehmenswerte pflegen. Dies zu erreichen, setzt voraus, die Unternehmensangehörigen auch in den Know-how-Schutz einzubinden und zu schulen.

Unternehmensangehörige müssen ständig hinsichtlich der Risiken und Folgen eines unbedarften Umgangs mit kritischen Daten sensibilisiert werden. Vorträge, Seminare und unternehmensinterne Mitteilungen sollten dazu genutzt werden, mögliche Angriffsszenarien von Industrie- und Wirtschaftsspionage vorzustellen. Hierzu gehört etwa die Vorbereitung und Aufklärung von Unternehmensangehörigen vor dem Besuch von Messen, Kongressen, bei Werksführungen oder ähnlichen Veranstaltungen. Auch das korrekte, nicht schädliche Verhalten auf Reisen, insbesondere beim Führen von Gesprächen mit Kollegen, Partnern etc. über unternehmensrelevante Inhalte in öffentlichen Räumen, wie z. B. Zügen und Wartezonen, sollte durch Schulungen oder zumindest durch entsprechendes Informationsmaterial beispielhaft aufgezeigt werden. Dazu muss herausgearbeitet werden, was kritische Daten sind und welchen Wert sie für das Unternehmen haben.

Vor allem muss den Unternehmensangehörigen verdeutlicht werden, dass sie selbst Ziel von Abschöpfungsversuchen durch Wirtschafts- und Industriespione werden könnten. Zudem sollte eine Sensibilisierung in Bezug auf Fahrlässigkeit und Unachtsamkeit erfolgen, die den Unternehmensangehörigen verdeutlicht, dass besonders bei Geschäftsreisen Unterlagen, Notizen und Hilfsmittel wie Laptops oder mobile Datenspeicher mit entsprechenden Daten im höchsten Maße gefährdet sind. Binnen kurzer Zeit können sie von professionellen Tätern entwendet oder kopiert werden.

Ziel der Schulungen sollte immer sein, das Bewusstsein der Unternehmensangehörigen für das Thema Know-how-Abfluss zu schärfen und sie über die möglichen Schädigungen für das Unternehmen aufzuklären. Dabei ist darauf zu achten, dass die Schulungen problemorientiert und an die jeweilige Zielgruppe angepasst sind. Oft ist es hilfreich, anhand von Studienergebnissen (vgl. „SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg“) und konkreten Fällen aus dem Unter-

nehmen den Unternehmensangehörigen die Gefahren zu vergegenwärtigen und die Regeln zu veranschaulichen. Diese Schulungen können ebenfalls Geschäftspartnern angeboten werden, um somit die Schutzmaßnahmen auszuweiten. Auch diese Schulungen sollten mit Fallbeispielen unterlegt sein und eher einen Workshop-Charakter haben, um die Teilnehmer aktiv einzubinden.

Es empfiehlt sich darüber hinaus, neu hinzukommende Unternehmensangehörige sofort in das Schulungskonzept zu integrieren. Auch sind Train-the-Trainer-Lösungen im Unternehmen eine bedenkenswerte Alternative, um hausinterne Schwachstellen gezielter und nachhaltiger zu minimieren.

5 Operative Managementaufgaben

Unternehmen stehen diverse Möglichkeiten zum Schutz vor Know-how-Abfluss und zur Einrichtung von Sicherheitsstandards zur Verfügung, die sie auch bereits mit geringem Aufwand ergreifen können. Dazu gehören etwa standardisierte Kontrollen ebenso wie vertragliche Vereinbarungen zur Geheimhaltung bis hin zu Ansprechpartnern im Unternehmen für Verdachtsmomente. Eine Vertrauenskultur im Unternehmen ist dabei unerlässlich.

Transparenz und Kommunikation

Die zentrale Norm zum Schutz von Unternehmens-Know-how (§ 17 UWG) schützt Unternehmensinformationen nur dann, wenn bestimmt und erkennbar ist, dass es sich um Geschäfts- und Betriebsgeheimnisse handelt. Folglich muss im Unternehmen sichergestellt sein, dass der Zugang zu diesem geheimen Know-how eingeschränkt ist und der Geheimhaltungswille des Unternehmens in Bezug auf Geschäftsgeheimnisse für alle Unternehmensangehörige offenkundig wird. Empfehlenswert sind in diesem Fall Maßnahmen, die den Willen zur Geheimhaltung dokumentieren, ebenso wie Verschwiegenheitsvereinbarungen der Mitarbeiter. Um den Schutz von Geschäfts- und Betriebsgeheimnissen auch nach Beendigung eines Arbeitsverhältnisses zu gewährleisten, können Wettbewerbsvereinbarungen (§ 74 HGB) mit betroffenen Unternehmensangehörigen geschlossen werden.

Neben der rechtlichen Absicherung gegenüber den Unternehmensangehörigen empfiehlt es sich, auch in Verträgen mit Zulieferern und Abnehmern sowie in Forschungs- und Entwicklungsverträgen eine Geheimhaltungsklausel kombiniert mit einer Vertragsstrafe zu integrieren. Diese Vertragsstrafe sollte eine empfindliche Sanktion darstellen und in jedem Fall den zu erwartenden Mindestschaden abdecken.

Mitarbeiterauswahl

Die größten Bedrohungspotenziale entstehen im leichtfertigen Umgang mit Sicherheitsstandards sowie im Datenmissbrauch durch Unternehmensangehörige. Daher ist schon bei der Personalauswahl außerordentliche Sorgfalt geboten. Die Anwendung moderner Verfahren der Personaldiagnostik sowie die Ausschöpfung externer Informationsquellen vor der Entscheidung über die Einstellung eines Bewerbers können Sicherheitsrisiken vermeiden bzw. minimieren.

Dabei kommt es vor allem auf die Echtheit, Lückenlosigkeit und Schlüssigkeit der Bewerbungsunterlagen an. Kontakt zu Sicherheitsbehörden sollte dann aufgenommen werden, wenn Anhaltspunkte für eine Spionagetätigkeit oder sonstige sicherheitsrelevante Auffälligkeiten – wie Reisen und Aufenthalte in Staaten mit besonderen Sicherheitsrisiken – zu erkennen sind. Sollte sich das Unternehmen unsicher sein, kann vom Bewerber eine schriftliche Erklärung bezüglich nachrichtendienstlicher Verbindungen eingefordert werden. Der zur Tat bereite Bewerber wird allerdings in der Regel hier falsche Angaben machen. Zusammen mit etwaigen Anhaltspunkten muss diese Erklärung dann Teil weiterer Nachforschungen sein. Wie bei jeder vergleichbaren Entscheidung kommt es darauf an, das Risiko möglichst gut zu kennen. Letztendlich muss das Unternehmen eine Abwägung zwischen den Chancen und Risiken treffen, welche der Bewerber in sich birgt.

Für die Bereitschaft der Mitarbeiter, bewusst Unternehmensgeheimnisse zu verraten, spielt das Arbeitsumfeld eine große Rolle. Unternehmensangehörige mit einer subjektiv als angemessen empfundenen Bezahlung und einem angenehmen Arbeitsumfeld, die vom Arbeitgeber gerecht behandelt und mit einem Vertrauensvorschuss bedacht werden, sind besser integriert, identifizieren sich stärker mit dem Unternehmen und fühlen sich deshalb weniger dazu veranlasst, eigenmotiviert als Spion oder Verräter tätig zu werden, als ein Unternehmensangehöriger, der sich häufig benachteiligt fühlt. Auch entsprechende Bonus- und Malussysteme können die Durchsetzung von Sicherheitsmaßnahmen unterstützen und dem schädigenden Verhalten von eigenmotivierten Tätern entgegenwirken.

Um die Möglichkeiten des Angriffs auf Daten zu verringern, sollten die Unternehmensangehörigen dazu angehalten werden, Unternehmensdaten nur im Unternehmen und falls extern, nur besonders geschützt zu verwenden (beispielsweise in Verbindung mit besonders gesicherter Technik). Ein besonderes Gefahrenpotenzial geht von Heimarbeitsplätzen aus, da die Daten außerhalb des Unternehmens nicht den gleichen Schutz erfahren können und somit die Weitergabe von Daten oder das Ausspionieren erleichtert wird.

Für Unternehmensangehörige, die zum Verrat an einen Wettbewerber verleitet werden sollen oder sogar erpresst werden, muss es die Möglichkeit geben, sich mit dieser sie verunsichernden Situation an einen Ansprechpartner im Unternehmen wenden zu können. Dazu sollte von der Unternehmensleitung ein Unternehmensangehöriger benannt und dessen Profil sowie Kontaktdaten im Unternehmen kommuniziert werden (vgl. Hinweisgebersystem, S. 24 ff.).

Know-how-Schutz-Verantwortlicher

Ein sogenannter „Know-how-Schutz-Verantwortlicher“ kann als neue Funktion im Unternehmen geschaffen werden; möglich ist auch, dass eine bereits vorhandene Funktion diesen Bereich zusätzlich übernimmt. Hierfür bieten sich z. B. folgende Funktionen an:

- Leiter IT- und Objektschutz,
- Leiter Sicherheit,
- Datenschutzverantwortlicher,
- Leiter des Bereiches Forschung und Entwicklung,
- Leiter der Rechts-/Compliance-Abteilung.

Um als Ansprechpartner für die Unternehmensangehörigen fungieren zu können, sollte der Know-how-Schutz-Verantwortliche umfassend geschult sein, damit er mit Anfragen oder Bitten aus den Fachabteilungen sachgerecht umzugehen weiß.

Neben seiner Funktion als vertrauensvoller Ansprechpartner für die Unternehmensangehörigen ist der Know-how-Schutz-Verantwortliche zudem Adressat für Geschäftspartner und Behörden und kann so alle Informationen und Aktivitäten in Bezug auf Know-how-Schutz bündeln. Darüber hinaus unterstützt er die Unternehmensleitung bei der Einführung von neuen Maßnahmen und bei der Anpassung bestehender Maßnahmen im Unternehmen.

Hinweisgebersystem

Parallel zu der Etablierung eines Know-how-Schutz-Verantwortlichen kann die Einführung eines Hinweisgebersystems sinnvoll sein. Ein Hinweisgebersystem ermöglicht den Unternehmensangehörigen – sowie externen Dritten – die anonyme Weitergabe ihrer Verdachtsmomente (z. B. direkt an einen im Unternehmen etablierten Vertrauens- oder Ombudsmann bzw. indirekt an anonyme, elektronische und/oder physische, speziell eingerichtete Briefkästen). Sowohl die Möglichkeiten an sich, als auch die nach dem Hinweis im Regelfall folgenden allgemeinen Schritte sollten im Unternehmen transparent und bekannt sein (z. B. durch Schulungen und über Dokumente, beispielsweise innerhalb der Dokumentation des Qualitätsmanagementsystems).

Sanktionskatalog

Neben einem intakten Arbeitsumfeld und einer etablierten Vertrauenskultur im Unternehmen bedarf es trotzdem auch regelmäßiger, standardisierter Kontrollen. Sollten stichhaltige Hinweise dafür gefunden werden, dass ein Unternehmensangehöriger sein Unternehmen verrät oder es verraten will, sollte das Unternehmen Sanktionen ergreifen. Wie und in welchem Umfang dies stattfindet, muss das Unternehmen bereits im Vorfeld von Störfällen in einem Sanktionskatalog festlegen.

Ein solcher Sanktionskatalog beinhaltet z. B. Eskalationsstufen und Maßnahmen, wie sofortige Freistellung des Unternehmensangehörigen mit Entzug der Zugangsberechtigung (Zutritt zu Räumen, Zugriff auf Dateien etc.) und auch die Sicherstellung von unternehmenseigenen Geräten (Mobiltelefone, Computer, Unterlagen etc.). Der Katalog enthält auch Festlegungen, wann bzw. wie Unternehmensangehörige (Sicherheitskräfte, Management, Belegschaft etc.) sowie Externe (Geschäftspartner, Behörden etc.) informiert werden.

Externe Dritte

Doch nicht nur bei den Unternehmensangehörigen müssen Maßnahmen zum Schutz des Firmen-Know-hows ergriffen werden, sondern auch im Umgang mit Unternehmensfremden. Dazu zählen sowohl Unternehmensangehörige von Fremdunternehmen, die unternehmensbezogene Dienstleistungen erbringen, als auch Besucher. Grundsätzlich sollte sichergestellt werden, dass Unternehmensfremde nur schwer bzw. gar nicht an Betriebs- und Geschäftsgeheimnisse des Unternehmens gelangen. Insbesondere beginnt dies bereits damit, dass Unternehmensangehörige dazu angehalten werden, vertrauliche Informationen auf mobilen Datenträgern und in gedruckter Form nicht offen und unbeaufsichtigt liegen zu lassen sowie diese nicht im normalen Abfall/Papier-Recycling zu entsorgen, sondern fachgerecht über Sicherheits-Schredder oder Aktenvernichtungssysteme. Inhalte mobiler Datenträger sind unwiderruflich zu löschen.

Die Gefahr, durch Besucher ausspioniert zu werden, lässt sich durch eine aufmerksame Betreuung reduzieren. Hierzu gehören die Überprüfung des Besuchers am Empfang bzw. am Eingang des Betriebsgeländes, die Ausgabe von Besucherausweisen sowie die grundsätzliche Begleitung des Besuchers auf dem Gelände. Um den Unternehmensangehörigen das schnelle Erkennen von unternehmensfremdem Personal zu erleichtern, kann etwa die Pflicht zum offenen Tragen der Firmen- bzw. Besucherausweise oder zum Tragen von Firmenkleidung eingeführt werden.

Insbesondere bei den unternehmensbezogenen Dienstleistungen durch Externe, bei denen die Zusammenarbeit einen Einblick in Unternehmensinterna und einen intensiven persönlichen Austausch erfordert, muss bei der Auswahl und den Vereinbarungen besondere Sorgfalt herrschen. Beispielsweise sollte vor einer Entscheidung bekannt sein, ob und wenn ja, wie der Dienstleister für Wettbewerber tätig ist und war. Auch Informationen aus Auskunftsdateien zur personellen, wirtschaftlichen und rechtlichen Situation sowie zu Haftungsmöglichkeiten können mit in die Entscheidung einfließen. Vor der Dienstleistung muss z. B. der Umgang mit vertraulichen Informationen sowie (noch) nicht geschütztem Know-how schriftlich geregelt sein. Es muss unternehmensintern sichergestellt sein, dass der unternehmensbezogene Dienstleister nur solche Informationen und Zugänge erhält, die zur Erfüllung seiner Dienstleistung notwendig sind.

Zugangsberechtigung

Der Zugang zu Unternehmensbereichen, in denen mit Geheimnissen gearbeitet wird (z. B. Labore, Forschungs- und Entwicklungsabteilungen etc.) sollte im notwendigen Umfang nur den dort tätigen Unternehmensangehörigen und anderen bewusst ausgewählten und mit den notwendigen Berechtigungen versehenen Befugten (z. B. Dienstleistern) gestattet sein. Dies muss organisatorisch geregelt sein und durch bauliche, mechanische und elektronische Absicherungen des gesamten Werkskomplexes sowie einzelner Gebäude, Gebäudeteile, Räume oder Objekte gewährleistet werden. Zugänge sollten kontrolliert bzw. zumindest protokolliert werden.

Sicherheitsaudits

Da ein Unternehmen mit Geschäftspartnern ständig Informationen austauscht, empfiehlt es sich auch, die Geschäftspartner und deren Schutzmaßnahmen durch regelmäßige passive oder aktive Audits zu überprüfen. Bei einem passiven Audit gibt das Unternehmen den Geschäftspartnern durch eigene Richtlinien – sogenannte „Policies“ – vor, welche Schutzmaßnahmen als notwendig erachtet werden und über-

prüft deren Einführung und Umsetzung. Besser und für viele Unternehmen leichter praktizierbar sind aktive Audits, in denen die Geschäftspartner nach einer gründlichen eigenen Vorbereitung über die vorhandenen und geplanten Schutzmaßnahmen befragt werden. Somit wird ein reales Bild geschaffen. Zur Vorbereitung gehört beispielsweise die Aktualisierung der vor der Zusammenarbeit gesammelten Informationen. Bei gemeinsamen Workshops wird dann über Verbesserungspotenziale gesprochen und somit der Schutz auf die Geschäftspartner ausgedehnt. Neu eingeführte Maßnahmen oder Verbesserungen sind regelmäßig stichprobenartig zu überprüfen.

Bei Maßnahmen im IT- und Telekommunikations-Bereich bietet es sich an, auf Experten zurückzugreifen, da das spezielle Know-how hierfür nur selten im Unternehmen vorgehalten und nur spezifisch benötigt wird. Im Telekommunikations-Bereich gehören hierzu beispielsweise das Absuchen nach Wanzen mit technischen Geräten, die Verschlüsselung der Kommunikation (Telefon, Fax, E-Mail, VoIP) oder der Einbau abhörsicherer Räume. Sollte der Einbau eines abhörsicheren Raumes für ein Unternehmen zu aufwändig sein, empfiehlt es sich, die Besprechungsräume ins Innere des Gebäudes zu verlegen (keine Außenwände oder Fenster). Im IT-Bereich bieten sich sowohl hardwaretechnische Maßnahmen (z. B. die Schreib- und Lesesicherung von Datenträgern) als auch softwaretechnische Lösungen (z. B. die Vergabe von restriktiven Zugriffsrechten) an.

Abschließend sei darauf hingewiesen, dass die meisten Maßnahmen selten losgelöst voneinander betrachtet werden können. Sind in einem Unternehmen die Unternehmensangehörigen umfassend geschult und herrscht eine wertebasierte Vertrauenskultur vor, ist es bereits gegen viele Angriffe aus dem technischen Bereich geschützt. Im Gegenzug ist der vollständige Schutz vor Angriffen mit Hilfe von technischer Ausrüstung ohne die Einbindung der Unternehmensangehörigen schlicht unmöglich.

6 Zusammenarbeit mit Behörden und Verbänden

Unternehmen stehen regional als auch deutschlandweit eine Vielzahl an Experten und Ansprechpartnern auf behördlicher und Verbandsebene zur Verfügung, die sowohl aus normativer als auch operativer Sicht Unterstützung bieten.

Auf Know-how-Schutz spezialisierte Behörden und Verbände ermöglichen es den regional ansässigen Unternehmen, von den Erfahrungen anderer zu profitieren.

Einschlägige Organisationen, allein in Baden-Württemberg, sind beispielsweise

- das Landesamt für Verfassungsschutz Baden-Württemberg,
- der Verband für Sicherheit in der Wirtschaft Baden-Württemberg e. V.,
- die Industrie- und Handelskammern in Baden-Württemberg,
- der Landesverband der Baden-Württembergischen Industrie e. V.,
- der Verband Deutscher Maschinen- und Anlagenbau e. V. Baden-Württemberg.

Sie alle sind Mitglieder im Sicherheitsforum Baden-Württemberg (SiFo BW). Ebenfalls maßgeblich beteiligt sind das Innenministerium und das Wirtschaftsministerium Baden-Württemberg, die Steinbeis-Stiftung sowie verschiedene Unternehmen.

Das Sicherheitsforum Baden-Württemberg bietet besonders kleinen und mittleren Unternehmen Unterstützung beim Schutz ihres Wissens und ihrer Innovationen. Es hat eine Informationsplattform im Internet eingerichtet, gibt Informationsmaterial heraus und wirkt an Veranstaltungen mit. Seit 2007 verleiht das Sicherheitsforum Baden-Württemberg im zweijährigen Turnus den „Sicherheitspreis Baden-Württemberg“ für herausragende Projekte der betrieblichen Sicherheit.

Die Verbände und Behörden befassen sich mit dem Thema Unternehmenssicherheit im weitesten Sinne und sind zudem Ansprechpartner für die Know-how-Schutz-Verantwortlichen der Unternehmen. Die meisten Verbände und Behörden bieten Beratungsgespräche an, in denen gemeinsam Lösungen für die Probleme der Unternehmen erarbeitet und bei Bedarf auch Experten vermittelt werden.

Landesamt für Verfassungsschutz Baden-Württemberg (LfV BW)

Das Landesamt bietet eine breite Palette an Dienstleistungen: von Informationsmaterial mit praxisgerechten Handlungsempfehlungen über allgemeine Beratungsgespräche bis hin zur Erörterung unternehmensspezifischer Problemstellungen. Es ist im Besonderen Ansprechpartner, wenn es um Wirtschaftsspionage geht, d. h. Nachrichtendienste involviert sind.

Zur allgemeinen Information („Hilfe zur Selbsthilfe“) werden folgende Broschüren empfohlen:

- „Wirtschaftsspionage – Risiko für Ihr Unternehmen“,
- „Wirtschaftsspionage in Baden-Württemberg und Bayern, Daten – Fakten – Hintergründe“,
- „Know-how-Schutz – Handlungsempfehlungen für die gewerbliche Wirtschaft“ (inkl. Selbsttest mit grundlegenden Fragestellungen und Handlungskonzept zum Know-how-Schutz).

Homepage: **www.verfassungsschutz-bw.de**

Ansprechpartner: **Harald Woll**
Leiter der Abteilung Spionageabwehr,
Geheim- und Sabotageschutz, Mitwirkungsaufgaben,
Scientology-Organisation
Telefon: 0711 9544-300
E-Mail: harald.woll@lfvbw.bwl.de

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

Der Verband für Sicherheit in der Wirtschaft bietet Sicherheits- und Schwachstellenanalysen sowie Beratungen in allen Sicherheitsfragen auch für Nicht-Mitglieder an. Für Mitglieder gibt es darüber hinaus die bundesweiten Verbandszeitschriften „WIK – Zeitschrift für die Sicherheit der Wirtschaft“ und „KES – Zeitschrift für Kommunikations- und EDV-Sicherheit“ sowie das verbandseigene „VSW aktuell“ und regionale „ERFA-Kreise“ für den Erfahrungsaustausch unter den Sicherheitsfachleuten der Unternehmen.

Homepage: **www.vsw-bw.com**
Ansprechpartner: **Karl Schotzko**
Geschäftsführer
Telefon: 0711 954609-15
E-Mail: schotzko@vsw-bw.com

Baden-Württembergischer Industrie- und Handelskammertag (IHK-Tag)

Die Industrie- und Handelskammern bieten ihren Mitgliedsunternehmen eine Erstberatung an und suchen gemeinsam mit ihnen nach Problemlösungen. Gegebenenfalls werden die Mitgliedsunternehmen an Spezialisten weiterverwiesen.

Homepage: **www.bw.ihk.de**
Erstkontakt: **Linda Jeromin**
Industrie- und Handelskammer Karlsruhe
Federführung Industrie der baden-württembergischen IHKs
Telefon: 0721 174-265
E-Mail: linda.jeromin@karlsruhe.ihk.de

Landesverband der Baden-Württembergischen Industrie e. V. (LVI)

Der Landesverband für die Baden-Württembergische Industrie informiert und sensibilisiert seine Mitgliedsverbände und -unternehmen über sicherheitsrelevante Themen. Er bietet über die LVI-Beratungs- und Service-GmbH in Zusammenarbeit mit Dritten Informationsveranstaltungen an, organisiert den Erfahrungsaustausch zwischen seinen Mitgliedern und verweist gegebenenfalls an externe Sicherheitsexperten.

Homepage: **www.lvi.de**
Ansprechpartner: **Wolfgang Wolf**
Geschäftsführendes Vorstandsmitglied
Telefon: 0711 327325-00
E-Mail: wolf@lvi.de
Manuel Geiger
Referatsleiter
Telefon: 0711 327325-11
E-Mail: geiger@lvi.de

Verband Deutscher Maschinen- und Anlagenbau e. V. Baden-Württemberg (VDMA)

Mit einem Netzwerk von 450 Mitarbeitern in Deutschland und im Ausland informiert und berät der VDMA besonders Unternehmen aus dem Bereich Investitionsgüter. Darüber hinaus werden Erfahrungsaustausche organisiert und die Interessen gegenüber Politik, Verwaltung und Wissenschaft vertreten.

Homepage: **www.vdma.org**
Ansprechpartner: **Jan Sibold**
IT-Sicherheit
Telefon: 0711 2280-117
E-Mail: jan.sibold@vdma.org
Steffen Zimmermann
IT-Sicherheit
Telefon: 069 6603-1978
E-Mail: steffen.zimmermann@vdma.org

Die in den einschlägigen Organisationen verantwortlichen Ansprechpartner halten eine Vielzahl an Informationen z. B. in Form von Broschüren und Handlungsempfehlungen bereit und bieten ein hochspezialisiertes Netzwerk, um sich mit anderen Sicherheitsverantwortlichen auszutauschen. Diese Netzwerke werden regelmäßig auf Informationsveranstaltungen, Fachtagungen und Arbeitskreisen erweitert.

Ergebnisse dieser Netzwerke sind u. a. themeneinschlägige Studien (z. B. die „SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg"), die helfen, das Dunkelfeld von wirtschaftskriminellen Handlungen zu erhellen und somit die Schutzmaßnahmen der Unternehmen anzupassen. Daher ist es zum einen wichtig, dass sich die Unternehmen an solchen Studien beteiligen. Sie helfen Tatmuster aufzudecken und Risiken vorzubeugen. Zum anderen lassen sich aus veröffentlichten Studien große Erkenntnisgewinne generieren, da sie ein realistisches Bild der Bedrohungslage wiedergeben und die Unternehmer hierdurch ihre eigenen Schutzmaßnahmen entsprechend optimieren können.

7 Nachhaltigkeitsprüfung (Monitoring)

Wie resistent ein Unternehmen gegenüber gefährdenden Eingriffen ist und ob sich Unternehmensrichtlinien durchgesetzt haben, lässt sich schwer an einzelnen Maßnahmen zum Schutz und zur Sicherheit bemessen. Vielmehr muss dies in einer Gesamtschau aller Vorkehrungen erfolgen. Einen Ansatz hierfür stellt das Monitoring dar.

Die Frage, die sich viele Sicherheitsexperten – aber auch Compliance-Verantwortliche, Justitiare etc. – stellen, ist, auf welche Weise in einer komplexen Organisation Regelkonformität gewährleistet werden kann. In vielen Unternehmen gibt es bereits umfangreiche Maßnahmen, wie z. B. ethische Richtlinien, Schulungen, Hinweisgebersysteme, Anti-Korruptions-Programme, Wettbewerbsklauseln in Arbeitsverträgen etc. Unter dem Begriff Compliance rangieren insofern zahlreiche Einzelmaßnahmen.

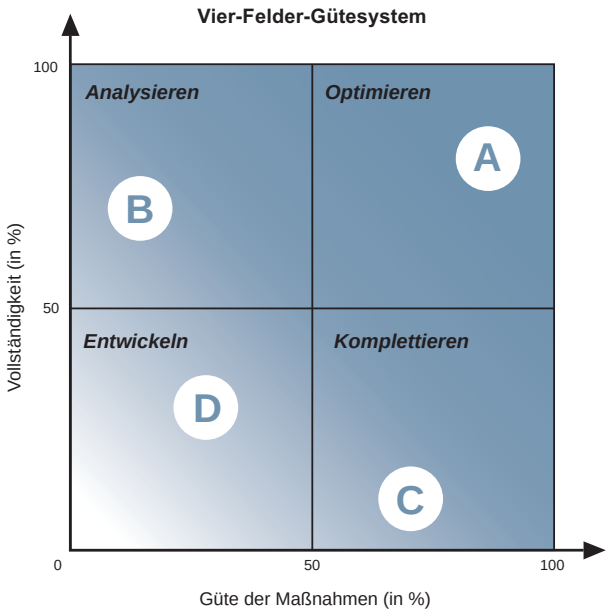
Ein Monitoring dient dazu, sich einen Überblick zu verschaffen, ob die eingeführten Maßnahmen ausreichen und wie gut deren Qualität ist. Das Monitoring bietet im Gegensatz zu formalisierten Checklisten aus Ratgebern und Literatur die Möglichkeit, die eigenen Maßnahmen einer kritischen Überprüfung durch Dritte zu unterziehen. Der kritische Blick von außen fördert zum einen die interne Diskussion über die weitere Entwicklung von Compliance im Unternehmen und hat zum anderen eine rechtliche Schutzfunktion sowie eine positive Außenwirkung. Denn ein objektives Reviewing der eigenen Arbeit überzeugt sowohl Geschäftspartner und Auftraggeber als auch im Ernstfall vor Gericht.

Der Steinbeis Compliance Monitor überprüft mit Hilfe eines standardisierten Verfahrens die Compliance-Organisation, die Implementation der Maßnahmen und ihre Durchsetzung im Geschäftsalltag. Er bietet für die Analyse eine sinnvolle thematische Struktur (Organisation), da jedes Compliance-Programm nicht nur ausreichend implementiert (Implementation), sondern auch bei Verstößen durchgesetzt (Enforcement) und regelmäßig überprüft (Reviewing) werden muss:

Das Monitoring setzt drei Verfahren ein. Zuerst beruht es auf einer in Abhängigkeit von Branche und Größe bedarfsgerechten Bestandsaufnahme. Des Weiteren erfolgt bei einigen Compliance-Elementen eine inhaltliche Eignungsprüfung. Hierzu gehört beispielsweise ein Check der ethischen Richtlinien und des Code of Conduct hinsichtlich der Eignung zur Prävention von Wirtschaftskriminalität. Denn definierte Werte entfalten nicht per se eine kriminalpräventive Wirkung. Ethische Richtlinien sind häufig sehr abstrakt formuliert und werden so weder akzeptiert noch gelebt.

Begleitet werden diese beiden Verfahren durch Gespräche mit den Verantwortlichen z. B. Compliance-Verantwortlichen, Sicherheitsverantwortlichen, Unternehmensleitung etc. So wird eine praxisorientierte Einschätzung gewährleistet, welche die Besonderheiten des Unternehmens berücksichtigt.

Auf dieser Basis wird ein Ergebnisbericht erstellt. Der Steinbeis Compliance Monitor verzichtet dabei auf eine simple Bewertung in Kategorien von gut bis schlecht oder nach der Ampellogik (rot-gelb-grün). Stattdessen erfolgt eine Einstufung nach einem Vier-Felder-Gütesystem, das aus den beiden Kriterien Vollständigkeit (Pro-



zentskala) und Güte der Maßnahmen (Bewertung) gebildet wird. Hieraus ergibt sich ein Vier-Felder-Schema, das den Stand der Compliance-Maßnahmen nach den vier Bewertungsgruppen differenziert und anschaulich darstellt.

Die Vollständigkeit und die Bewertung der Güte orientieren sich sowohl an den Durchschnittswerten vergleichbarer Unternehmen als auch an den Anforderungen, die nach heutigem Kenntnisstand an ein effizientes Compliance-Programm gestellt werden. Die Kriterien ergeben sich aus der Fachdiskussion, der empirischen Forschung sowie der Rechtsprechung.

Dieser Bewertungsprozess ist keineswegs statisch, da jedes Feld die Möglichkeit der Veränderung bietet. Befindet sich ein Unternehmen (B) im oberen linken Quadranten (Analysieren), so wurden die Maßnahmen im Unternehmen nahezu vollständig implementiert, jedoch mangelt es noch an einer überzeugenden Umsetzung. Im unteren rechten Quadranten (Komplettieren) finden sich Unternehmen (C) wieder, die zum Beispiel noch am Anfang der Compliance-Organisation stehen, d. h. noch sehr wenige Elemente eingeführt haben. Ist die Güte dieser wenigen Elemente

jedoch sehr hoch, kann das Hauptaugenmerk auf das Komplettieren der Compliance-Maßnahmen gelegt werden. Die höchste erreichbare Kategorie wäre der obere rechte Quadrant (Optimieren), der aber nicht einem perfekten Compliance-System entspricht (A). Zum einen gibt es immer Schwächen, und zum anderen ist der dynamische Erkenntnisprozess in Wissenschaft und Rechtsprechung unaufhaltsam.

Am Ende des Compliance-Monitorings kann eine Zertifizierung des erreichten Compliance-Gesamtstatus erfolgen, sofern der Bereich des „Optimierens“ erreicht ist, somit Güte und Vollständigkeit nur geringe Schwächen aufweisen. Das Monitoring kann sich auch auf Compliance hinsichtlich bestimmter Wirtschaftsdelikte beschränken, wie Compliance gegen Korruption oder gegen Know-how-Abfluss.

Mittelfristig ergibt sich für Unternehmen aus dem Monitoring die Möglichkeit, die eigene Entwicklung aufzuzeigen, sich mit Branchenvertretern zu vergleichen oder sich an den Best-Practice-Standards zu messen. Nicht zuletzt für Geschäftspartner, für Auftraggeber im öffentlichen Bereich, aber auch für Fachkräfte sind dies wesentliche Indikatoren für Sicherheit und Kompetenz dieser Unternehmen.

Steinbeis-Hochschule Berlin
School of Governance, Risk & Compliance (School GRC)
Homepage: **www.school-grc.de**
Ansprechpartner: **Birgit Galley**
Direktorin School GRC
Telefon: 030 27581748-0
E-Mail: sicherheit@school-grc.de

Prof. Dr. Kai-D. Bussmann
Leiter Institute Corporate Integrity Management
Telefon: 030 27581748-0
E-Mail: sicherheit@school-grc.de

8 Daten und Fakten zur Studie

Auftraggeber

- Sicherheitsforum Baden-Württemberg

Unterstützt von

- Steinbeis-Stiftung für Wirtschaftsförderung
- Baden-Württembergischer Industrie- und Handelskammertag

Durchgeführt von

- Ferdinand-Steinbeis-Institut
- School of Governance, Risk & Compliance an der Steinbeis-Hochschule Berlin

Zeitrahmen

Februar 2009 bis Dezember 2009

Methodik

Befragung in Form eines standardisierten Online-Fragebogens

Teilnehmer der Befragung

Baden-Württembergische Unternehmen aus folgenden Branchen

- verarbeitendes Gewerbe
- Baugewerbe
- Handel
- Verkehr und Lagerei
- Information und Kommunikation
- Erbringer von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen

Hintergrund zur Studie

- Zum Teil geringes bis mangelndes Bewusstsein für Wirtschaftsspionage und Konkurrenzausspähung in den Unternehmen
- Deutlichere Definition der realistischen Gefährdungslage
- Praxisbezogene Handlungsempfehlungen für die Unternehmen

Thema der Befragung

- Informationen zum derzeitigen Know-how-Schutz in den Unternehmen
- Konkrete Fragen zum Bewusstsein und zu (potenziellen) eigenen Schädigungen des Unternehmens
- Basisdaten Unternehmen

9 Hintergrundinformation

Im **Sicherheitsforum Baden-Württemberg** haben sich Unternehmen, das Innenministerium und das Wirtschaftsministerium Baden-Württemberg, das Landesamt für Verfassungsschutz Baden-Württemberg, der Baden-Württembergische Handwerkstag (BWHT), der Landesverband der Baden-Württembergischen Industrie e. V. (LVI), der Verband für Sicherheit in der Wirtschaft Baden-Württemberg e. V. (VSW), der Baden-Württembergische Industrie- und Handelskammertag, der Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA) Baden-Württemberg sowie das Karlsruher Institut für Technologie (KIT) und die Steinbeis-Stiftung zusammengeschlossen, um die Wirtschaft in Baden-Württemberg vor Wirtschafts- und Industriespionage zu schützen.
www.sicherheitsforum-bw.de

Die **Steinbeis-Stiftung** ist ein weltweit tätiges Dienstleistungsunternehmen im Bereich Technologie- und Wissenstransfer. Zum dezentral organisierten Steinbeis-Verbund gehören derzeit rund 800 rechtlich unselbstständige wie auch selbstständige Steinbeis-Unternehmen sowie Kooperations- und Projektpartner in 50 Ländern, die in den Bereichen Forschung und Entwicklung, Beratung, Analysen und Expertisen sowie Aus- und Weiterbildung tätig sind.
www.stw.de

Das **Ferdinand-Steinbeis-Institut** ist ein Transferzentrum in der Steinbeis-Stiftung und hat die Aufgabe der Koordination und Durchführung von wissenschaftlichen Studien im Steinbeis-Verbund. Der für das Projekt verantwortliche Leiter ist Max Pfeiffer.
www.fsti.info

Die **School of Governance, Risk & Compliance (School GRC)** ist ein Forschungs- und Ausbildungsinstitut der privaten Steinbeis-Hochschule Berlin. Sie bildet Führungskräfte und Spezialisten aus und fort. Die an der School GRC durchgeführten Studien und Forschungen sind bewusst praxisnah ausgerichtet mit dem Ziel, Nutzwert in Branchen, Betrieben und Verbänden zu erzeugen. Die für das Projekt verantwortliche Direktorin der School GRC ist Birgit Galley.
www.school-grc.de

10 Mitglieder im Sicherheitsforum Baden-Württemberg

- **Innenministerium Baden-Württemberg**
  www.innenministerium.baden-wuerttemberg.de
- **Wirtschaftsministerium Baden-Württemberg**
  www.wm.baden-wuerttemberg.de
- **Landesamt für Verfassungsschutz Baden-Württemberg**
  www.verfassungsschutz-bw.de
- **Baden-Württembergischer Handwerkstag**
  www.handwerk-bw.de
- **Landesverband der Baden-Württembergischen Industrie e. V.**
  www.lvi.de
- **Verband für Sicherheit in der Wirtschaft Baden-Württemberg e. V.**
  www.vsw-bw.com
- **Baden-Württembergischer Industrie- und Handelskammertag**
  www.bw.ihk.de
- **Verband Deutscher Maschinen- und Anlagenbau e. V.**
  www.vdma.org
- **Karlsruher Institut für Technologie**
  www.kit.edu
- **Daimler AG**
  www.daimler.com
- **EnBW Energie Baden-Württemberg AG**
  www.enbw.de
- **SAP AG**
  www.sap.de
- **Steinbeis-Stiftung**
  www.stw.de

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

www.sicherheitsforum-bw.de

Baden-Württemberg
INNENMINISTERIUM

Baden-Württemberg
WIRTSCHAFTSMINISTERIUM

Baden-Württemberg
LANDESAMT FÜR VERFASSUNGSSCHUTZ

IHK Die Industrie- und Handelskammern in Baden-Württemberg

VSW

LVI
Landesverband der Baden-Württembergischen Industrie e. V.

VDMA

KIT
Karlsruher Institut für Technologie

DAIMLER

EnBW

SAP

BWHT

Steinbeis

ISBN 978-3-941417-21-2

Steinbeis-Edition