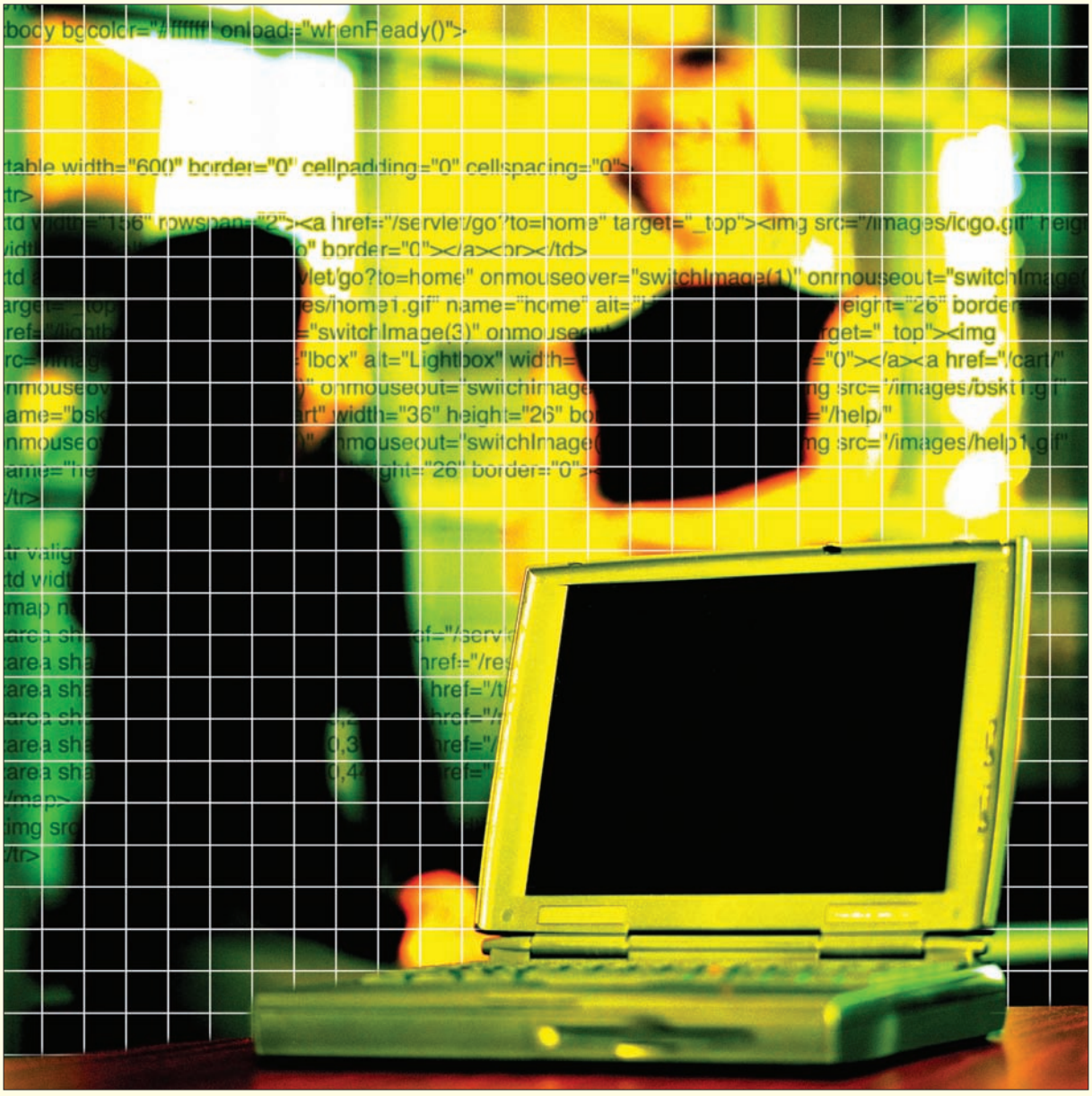
Know-how-Schutz

Handlungsempfehlungen für die gewerbliche Wirtschaft



Baden-Württemberg

LANDESAMT FÜR VERFASSUNGSSCHUTZ

Impressum:

Herausgeber: Landesamt für Verfassungsschutz Baden-Württemberg
Taubenheimstraße 85A
70372 Stuttgart
Tel.: 0711 / 95 44 - 00
Fax: 0711 / 95 44 - 444
E-Mail: lfv-bw@t-online.de

Illustrationen, Grafiken & DTP:
Landesamt für Verfassungsschutz Baden-Württemberg

Druck: E. Kurz & Co., Kernerstraße 5, 70182 Stuttgart

Zitate: Alle direkten Zitate sind in Kursivschrift gesetzt. Zitate aus Texten in alter Rechtschreibung wurden an die neue Rechtschreibung angeglichen.

Know-how-Schutz

Handlungsempfehlungen für die gewerbliche Wirtschaft

Stand: Juli 2004

Inhaltsverzeichnis Seite

Einleitung

Auch wenn Spionagefälle nur sporadisch an das Licht der Öffentlichkeit gelangen und es dementsprechend selten zur Verurteilung überführter Agenten kommt, sollte man sich keineswegs in falscher Sicherheit wiegen. Wirtschafts- und Wissenschaftsspionage stellen nach wie vor ein ernsthaftes Gefährdungspotenzial für deutsche Unternehmen dar. Leider ist jedoch vor allem bei kleineren und mittelständischen Betrieben immer wieder festzustellen, dass entsprechende Risiken entweder bagatellisiert oder überhaupt nicht wahrgenommen werden.

Mit diesem Leitfaden möchte das Landesamt für Verfassungsschutz Baden-Württemberg der gewerblichen Wirtschaft auch in Zukunft ein geeignetes Hilfsmittel an die Hand geben, um eigenverantwortlich auf das jeweilige Unternehmen zugeschnittene Präventionsmaßnahmen zu entwickeln. Im Mittelpunkt der Überarbeitung der bisherigen Broschüre „Schutz vor Spionage“ stand eine noch anwenderfreundlichere Gestaltung. In besonderer Weise war außerdem der rasch fortschreitenden Entwicklung im Bereich der Informationstechnik (IT) Rechnung zu tragen.

Thematisch behandelt die vorliegende Ausarbeitung den Gesamtprozess der Entwicklung und Umsetzung eines Informationsschutzkonzepts auf der Basis von Schwachstellen- und Risikoanalysen. Soweit in einem Unternehmen Sicherheitsmaßnahmen in Teilbereichen bereits verwirklicht sein sollten, eignet sie sich auch als Arbeitsgrundlage zur Optimierung präventiver Vorkehrungen.

Zwangsläufig konzentrieren sich die Ausführungen auf die Verhinderung des ungewollten Abflusses schutzwürdiger Informationen. Ein umfassendes Sicherheitskonzept hat darüber hinaus auch Maßnahmen gegen die Szenarien Sabotage, terroristisch motivierte Gewaltaktionen, menschliches oder technisches Versagen und höhere Gewalt etc. vorzusehen. Allerdings decken die dargestellten Schutzmaßnahmen die genannten Risikobereiche zumindest teilweise mit ab.

Der nachfolgende Selbsttest enthält grundlegende Fragestellungen zum Know-how-Schutz. Er dient der Erfassung des aktuellen Sicherheitsstandards und lenkt gleichzeitig den Blick auf eventuell vorhandene Regelungslücken. Detaillierte Informationen, wie Sie Sicherheitslücken schließen können, finden Sie im beigefügten „Handlungskonzept für Ihren Know-how-Schutz“.

Wie sicher ist mein Unternehmen?

	Ja	Nein
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[1] (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?	○	○

[1] *Staatenliste siehe Anhang.*

1. Know-how-Schutz - eine betriebliche Notwendigkeit

1.1 Bedeutung des Know-how-Schutzes

Die Notwendigkeit, sich gegen die Folgen der illegalen Nutzung des eigenen Wissens durch fremde Staaten, Konkurrenten oder Einzelpersonen zu wehren, gewinnt angesichts eines weltweit verschärften Wettbewerbs, einer angespannten Wirtschaftslage sowie einer ständig steigenden Abhängigkeit von moderner Informations- und Kommunikationstechnik zunehmend an Bedeutung. Unternehmenserfolg und präventives Sicherheitsmanagement sind in einem engen Zusammenhang zu sehen. Know-how verkörpert das strategische Potenzial eines Unternehmens. Es sichert den Wettbewerbsvorsprung am Markt und ist für den zukünftigen Unternehmenserfolg von hoher Relevanz. Der Verlust geistigen Eigentums kann von existenzieller Bedeutung für ein Unternehmen sein.

Prävention in Form von unternehmensbezogenen Schutzkonzepten bietet die Gewähr dafür, materielle und immaterielle Schäden zu verhindern oder wenigstens zu minimieren. Dabei sollte sich die Aufmerksamkeit nicht allein auf die Vereitelung des eigentlichen Spionage- oder Sabotageakts richten. Vielmehr gilt es, bereits das - häufig durch menschliche Schwächen begünstigte - „Aushebeln“ vorhandener Schutzvorkehrungen abzuwehren und dem damit verbundenen unbemerkten Eindringen in sensible Bereiche vorzubeugen.

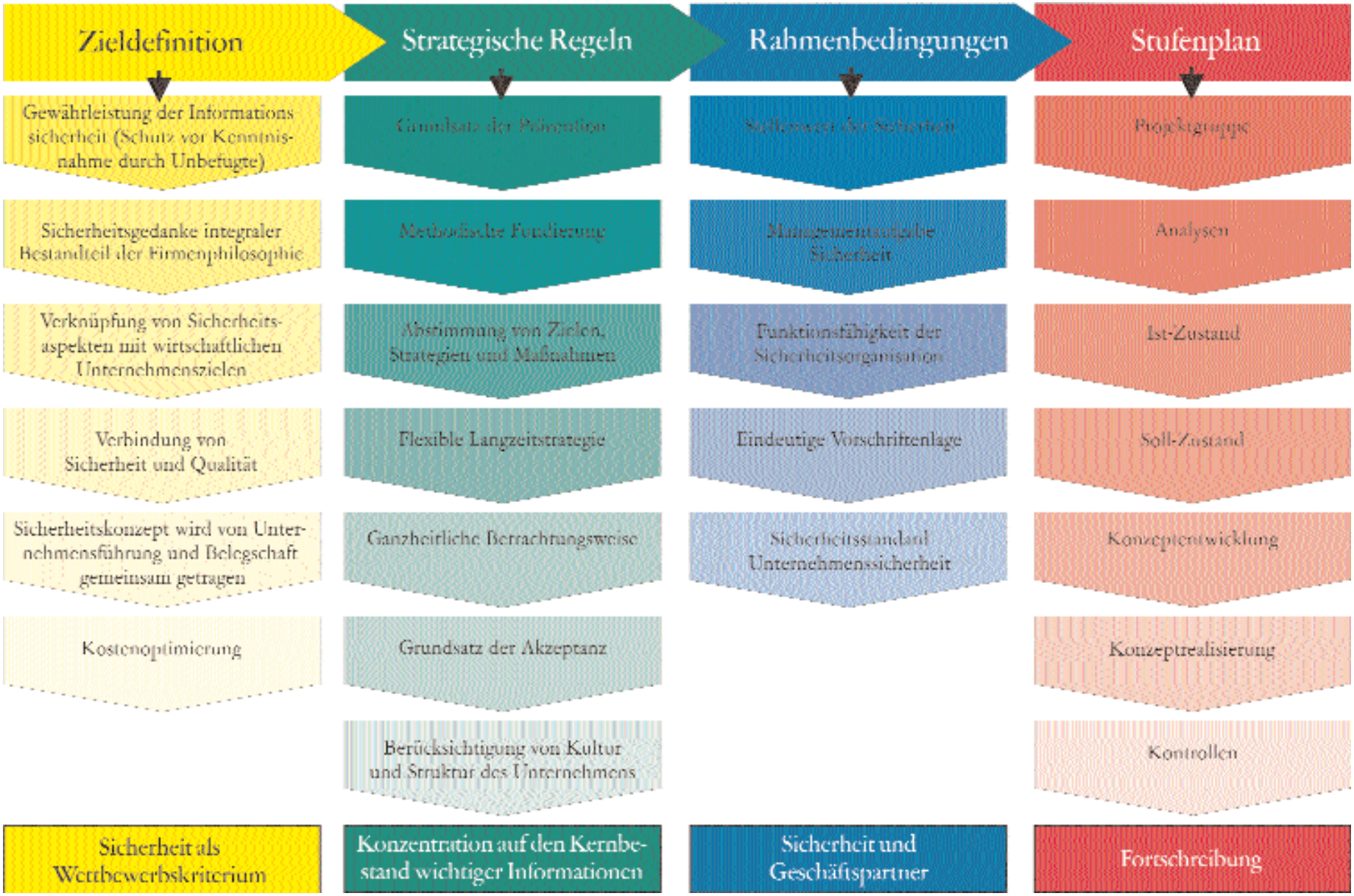
Gesellschaftliche und wirtschaftliche Veränderungen sowie verfeinerte Methoden der illegalen Informationsbeschaffung erfordern auch neue Formen der Prävention. Nur professionell gestaltete Abwehrmaßnahmen bieten die Gewähr, den heutigen Herausforderungen gerecht zu werden.

Die Idee der integrierten Sicherheit sieht die Umsetzung eines alle Unternehmensbereiche umfassenden und in die globale Unternehmenssicherheit eingebetteten, unternehmensweit durchgängigen und sowohl auf die tatsächlichen Gefährdungssituationen als auch auf die Belange der Nutzer zugeschnittenen Schutzkonzepts mit vorbeugenden und abwehrenden Komponenten vor.

Die Erarbeitung und Realisierung eines Informationsschutzkonzepts ist zu einer komplexen und interdisziplinären Managementaufgabe geworden. Konzeptionelles Vorgehen bedeutet mehr als die Addition von Einzelmaßnahmen. Vielmehr ist darunter das geplante Erfassen und strukturierte Aufarbeiten von Problemen zur Erreichung des definierten Ziels zu verstehen. Jedes Unternehmen hat in Abhängigkeit von seiner Größe, Struktur, Produktpalette, Finanzkraft und Gefährdungssituation spezifische Sicherheitsvorstellungen und -vorkehrungen zu entwickeln.

Entwicklung eines Informationsschutzkonzepts

- Ablaufschema -



1.2 Sicherheit ist „Chefsache“

Nur wer selbst durch sein Handeln der Sicherheitsphilosophie gerecht wird und durch präzise Vorgaben und vorbildliches Verhalten Kompetenz sowie Verantwortungsbereitschaft erkennen lässt, kann von den Mitarbeitern aller betrieblichen Ebenen das erforderliche Maß an Akzeptanz und Risikobewusstsein sowie von der Personalvertretung die gebotene Unterstützung bei der Realisierung von Sicherheitsvorhaben erwarten.

Führungsverantwortliche größerer Unternehmen und hier insbesondere Vorstände von Aktiengesellschaften sind im Übrigen auch aufgrund gesetzlicher Vorgaben verpflichtet, Vorkehrungen im Rahmen eines Sicherheitsmanagements zu treffen, um ihren Betrieb vor existenzgefährdenden schädigenden Einflüssen zu bewahren (vgl. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich/KonTraG vom 1. Mai 1998). Im Zuge der Delegation tragen Vorgesetzte die Verantwortung für die Sicherheit der Daten und Informationen ihres jeweiligen Zuständigkeitsbereichs.

Unabhängig von den gesetzlichen Vorgaben wirkt es sich in jeder Hinsicht positiv aus, wenn die Unternehmensleitung den Regelkreis der betrieblichen Risikobewältigung selbst steuert, kontrolliert und optimiert. Sie sollte sich die Entscheidung über die konkrete Umsetzung interner und externer Informationen nicht nehmen lassen.

2. Strategische Überlegungen

2.1 Konzentration auf realistische Ziele

Absoluten Schutz gegen unfreiwillige Informationsverluste gibt es nicht. Moderne Unternehmen mit ihren vielfältigen Querverbindungen und Kommunikationsmöglichkeiten lassen es selbst bei Bereitstellung erheblicher finanzieller Mittel fast aussichtslos erscheinen, Betriebsgeheimnisse auf Dauer vor konzentrierten Angriffen von Konkurrenten oder Nachrichtendiensten zu schützen. Vielfach ist es nur eine Frage des finanziellen oder technischen Aufwands, ob Ausspähungsversuche erfolgreich verlaufen. Bei nüchterner Betrachtungsweise wird man sich darauf konzentrieren müssen,

- die Verratstätigkeit in allen relevanten Bereichen zu erschweren,
- den vom Angreifer zu betreibenden Aufwand nachhaltig zu steigern und
- das Risiko der Entdeckung unkalkulierbar zu machen.

2.2 Grundsatz der Prävention

Sicherheitsüberlegungen im Unternehmen sollten vom Grundsatz der Prävention geprägt sein. Sie sollten also nicht erst dann angestellt werden, wenn der Verratsfall bereits eingetreten ist, sondern müssen möglichst frühzeitig in Entscheidungsprozessen und betrieblichen Abläufen Berücksichtigung finden. Alle einschlägigen Entwicklungen, auch wenn sie erst in der Zukunft sicherheitsrelevant werden, müssen in die Überlegungen einbe-

zogen werden. Gleichzeitig ist anzustreben, den seitherigen Personaleinsatz, eingespielte Arbeitsroutinen und langjährig gepflegte Außenbeziehungen kritisch zu hinterfragen und vorbeugende Schutzmechanismen vorzusehen.

2.3 Grundsatz der Akzeptanz

Die weit reichende Delegation von Verantwortung auch in Sicherheitsfragen setzt bei den Mitarbeitern eine breite Akzeptanz voraus. Die Belegschaft und insbesondere die Arbeitnehmervertretung müssen - als Bestandteil einer unternehmensweiten Einführungsstrategie - von Anfang an in Sicherheitsüberlegungen eingebunden und fortlaufend über den aktuellen Sachstand unterrichtet werden. Wichtig ist, dass die Mitarbeiter ihre Erfahrungen in den Entscheidungsprozess einbringen können.

2.4 Ganzheitliche Betrachtungsweise

Moderner Informationsschutz erfordert professionelle Methoden und darf sich nicht auf die Optimierung vorhandener Strukturen und Arbeitsabläufe in vermeintlich sicherheitskritischen Bereichen beschränken. Vielmehr kommt es darauf an, alle Organisationseinheiten und betrieblichen Ebenen unter Sicherheitsgesichtspunkten zu analysieren. Nur so gelingt die Identifizierung potenzieller Risikobereiche und wird die Verknüpfung unterschiedlicher, teilweise sogar gegensätzlicher Anforderungen in einem Güter- und Interessen-Abwägungsprozess ermöglicht.

2.5 Beschränkung auf den Kernbestand

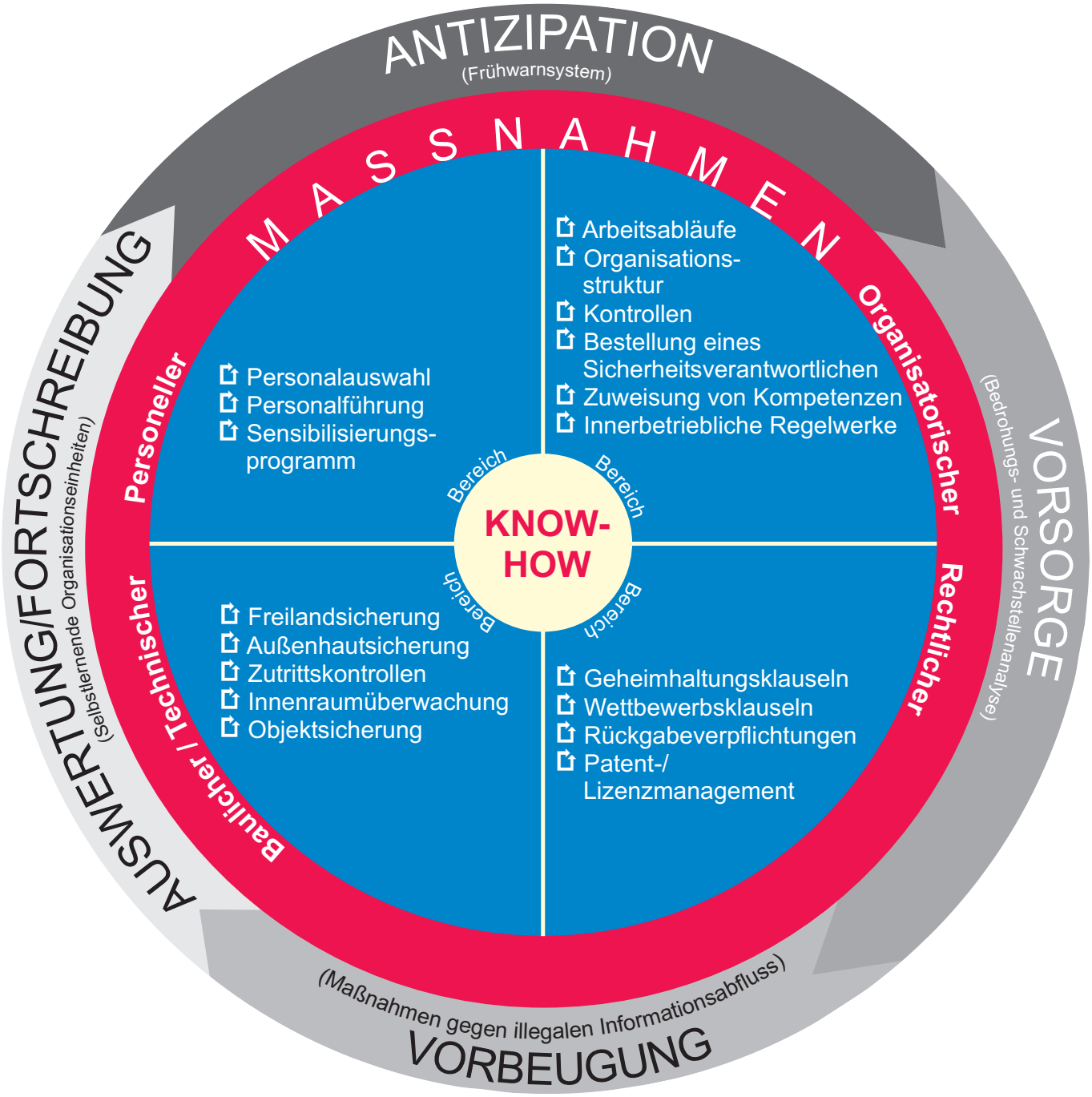
Nicht alles, was grundsätzlich als geheimhaltungsbedürftig angesehen wird, ist tatsächlich schützenswert. Ziel muss es deshalb sein, Weniges, aber wirklich Bedeutsames zumindest in der kritischen Phase effektiv zu schützen. Konkret bedeutet dies eine Konzentration auf den Kernbestand der für die Zukunft des Unternehmens wichtigen Informationen und die Inkaufnahme akzeptabler Sicherheitsrisiken.

3. Stufenplan

Ein Sicherheitskonzept sollte einem Unternehmen keineswegs voreilig oder gar unvorbereitet übergestülpt werden. Finanzielle und organisatorische Erwägungen, aber auch psychologische und nicht zuletzt qualitative Gründe lassen es geraten erscheinen, dessen Erarbeitung und Umsetzung schrittweise zu vollziehen. Die vielschichtige Aufgabenstellung und die notwendige Einbindung aller betroffenen Arbeitsbereiche legen es nahe, eine Projektgruppe mit der Erstellung einer „Konzeption Informationsschutz“ zu beauftragen. Sie kann mit Hilfe bewährter Managementmethoden

- ❑ den Rahmen für den Ressourceneinsatz definieren,
- ❑ Vorarbeiten koordinieren,

Regelkreis der Prävention



Grafik: LfV BW

- Analysen veranlassen,
- Strategien zur Umsetzung der Analyseergebnisse festlegen,
- Restrisiken aufzeigen,
- die notwendigen Kosten ermitteln,
- Entscheidungen herbeiführen und
- den Fortgang der Angelegenheit überwachen.

Im Bedarfsfall kann die Hinzuziehung externer Berater erwogen werden.

Durch Analysen unterschiedlichster Art (Bedrohungs-, Schwachstellen-, Risikoanalysen) und eine Risikoklassifizierung, in die auch die gesamte Belegschaft eingebunden werden kann, sollte zunächst eine Gesamteinschätzung (Ist-Zustand) des Unternehmens unter Sicherheitsgesichtspunkten erreicht werden. Wichtig ist eine solide Bestandsaufnahme zu den Fragen, welche Gefahren dem Unternehmen von außen drohen und wo es intern verwundbar ist. Ziel ist vor allem, das Zusammenwirken mehrerer Gefährdungsfaktoren und die daraus abzuleitende Gefahrenpotenzierung bereits im Ansatz zu erkennen. Es hat sich dabei bewährt, alle Bereiche kritisch aus dem Blickwinkel eines potenziellen Angreifers zu durchleuchten.

4. Maßnahmenkatalog

Nur die Kombination sorgfältig aufeinander abgestimmter personeller, materieller (= technischer und organisatorischer) sowie rechtlicher Maßnahmen garantiert eine umfassende Schutzwirkung. Der Verzicht auf einen der genannten Bestandteile führt zwangsläufig zu Sicherheitslücken.

4.1 Personelle Maßnahmen

Mitarbeiter in allen betrieblichen Bereichen und auf allen hierarchischen Ebenen können mehr verraten, als Spionagedienste oder Konkurrenten auf andere Weise je herauszufinden in der Lage wären. Wie eine von der Hamburger Kreditversicherung Euler Hermes in Auftrag gegebene Studie zur Wirtschaftskriminalität[2] ergab, ist festzustellen, dass in drei von vier Fällen das eigene Personal an den untersuchten Betrugs-, Untreue- oder Unterschlagungshandlungen beteiligt war.

Die meisten und schwerwiegendsten Sicherheitsverletzungen sind auf menschliches Fehlverhalten der „Geheimnisträger“ im eigenen Unternehmen zurückzuführen, da gerade sie die Abläufe und Schwachstellen ihres Betriebes am besten kennen. Die Loyalität des Personals im Konfliktfall kann für ein Unternehmen von existenzieller Bedeutung sein. Das Prinzip „Verantwortung“ muss deshalb immer mehr zu einem entscheidenden Faktor des Handelns werden. Der zunehmende Wertewandel in der Gesellschaft, der mit einer veränderten Einstellung zur Arbeit an sich und der inneren Bindung an den Arbeitgeber verbunden ist, verleitet Menschen in

[2] *Euler Hermes: Wirtschaftskriminalität - das diskrete Risiko (Die erste repräsentative Untersuchung für den Mittelstand), 2003; URL: www.eulerhermes.com.*

weitaus stärkerem Maße als früher zu illoyalem Verhalten. Nicht selten ist bei den Tätern keinerlei Unrechtsbewusstsein festzustellen. Betriebliche Sicherheitskonzepte müssen insofern gezielt auf die „Schwachstelle Mensch" ausgerichtet sein und die Erhöhung des Sicherheitsbewusstseins, der Kompetenz und der Akzeptanz bei den Mitarbeitern zum Ziel haben.

Die angesprochenen Maßnahmen umfassen den gesamten Beschäftigungszyklus eines Mitarbeiters. Die richtige Personalauswahl und die konsequente Einhaltung moderner Führungsgrundsätze sind mit die effizientesten Mittel des vorbeugenden Informationsschutzes.

Informationsverluste hätten vielfach schon durch eine sorgfältige Personalauswahl, welche die Möglichkeiten moderner Personaldiagnostik sowie Ausschöpfung aller externen Informationsquellen einbezieht, verhindert oder gemindert werden können. Hier kommt es in erster Linie auf die Echtheit, Lückenlosigkeit und Schlüssigkeit der vorgelegten Unterlagen sowie auf den persönlichen Eindruck des Bewerbers an. Im Einzelfall sollte man sich nicht scheuen, Kontakt zu Sicherheitsbehörden aufzunehmen, wenn Anhaltspunkte für einen nachrichtendienstlich beeinflussten Lebenslauf oder sonstige Auffälligkeiten zu erkennen sind.

Ferner muss dem Grundsatz der Prävention durch ein gezieltes Qualifizierungs- und Sensibilisierungsprogramm Rechnung getragen werden, das sowohl die aktuelle Gefährdungssituation als auch das gewandelte Selbstverständnis der heutigen Generation berücksichtigt. Sicherheitsmaßnahmen können nicht mehr einfach angeordnet, sondern müssen psychologisch geschickt vorbereitet werden. Es hat sich als sinnvoll erwiesen, zunächst eine allgemeine Grundsensibilisierung vorzunehmen, dieses Niveau durch ergänzende Maßnahmen zu erhalten und schließlich zielgruppenorientiert weiter zu steigern. Dabei sind die Mitarbeiter in die Lage zu versetzen, Sicherheitsvorkommnisse selbst zu erkennen. Management, Führungsverantwortliche und Beschäftigte mit Zugang zu Betriebsgeheimnissen aller Art, professionelle Informationsmittler (zum Beispiel Werbe- und PR-Mitarbeiter, Vertriebspersonal) sowie Angehörige des Bereichs Unternehmenssicherheit verdienen in diesem Zusammenhang besondere Aufmerksamkeit. Der Aufwand für ausführliche, anlass- oder zeitbezogene Gespräche lohnt sich auf jeden Fall.

Im Falle der Kündigung ist eine Entbindung von sicherheitsempfindlichen Aufgaben zu erwägen. Bei Beendigung des Arbeitsverhältnisses ist auf die vollständige Rückgabe dienstlicher Unterlagen und Gegenstände, die Löschung sämtlicher Berechtigungen und die Unterrichtung der eigenen Sicherheitskräfte, bei Bedarf auch wichtiger Geschäftspartner, zu achten.

4.2 Organisatorische Maßnahmen

Der Bedeutung des innerbetrieblichen Informationsschutzes ist ferner durch organisatorische Maßnahmen Rechnung zu tragen. Die Organisationsstrukturen und Arbeitsabläufe sind auf der Basis von Schwachstellenanalysen modernen informationstechnischen Gegebenheiten anzupassen. „Selbstlernende Organisationseinheiten" tragen dazu bei, die Sicherheitslage eines Unternehmens auf Dauer positiv zu gestalten. Grundlegende organisatorische Maßnahmen sind

- ❑ die Herausgabe schriftlicher Anweisungen und Empfehlungen,
- ❑ die Festlegung von Funktionstrennungen und Kompetenzabgrenzungen sowie
- ❑ die räumliche Abschottung sensibler Arbeitsbereiche („Sicherheitsinseln").

4.2.1 Bestellung eines Sicherheitsverantwortlichen

Die Einsetzung eines fachlich versierten, unternehmensweit zuständigen, mit umfassenden Kompetenzen und einem fest umrissenen Aufgabenfeld ausgestatteten Sicherheitsverantwortlichen („Security-Manager") mit entsprechendem Persönlichkeitsprofil ist für die Erreichung eines akzeptablen Sicherheitsniveaus unerlässlich. Eine ausreichende personelle Ausstattung und Budgetierung der mit Sicherheitsaufgaben betrauten Organisationseinheit sollte selbstverständlich sein.

Der Sicherheitsverantwortliche sollte möglichst hochrangig in der Firmenhierarchie verankert sein, in alle sicherheitsrelevanten Abläufe wie neue Programme und Kooperationen, Beraterverträge mit Fachfirmen und Einzelpersonen eingebunden werden und auf die Unterstützung aus den unterschiedlichsten Sparten (Datenverarbeitung, Datensicherheit, Technik) zurückgreifen können. Besonders bedeutsam erscheint die enge Zusammenarbeit mit den Bereichen Forschung/Entwicklung und Vertrieb (Projekt-Manager, Produkt-Manager, Begutachtung der zur Veröffentlichung vorgesehenen Prospekte, Handbücher, Dokumentationen, Internet-Präsentation), der Personalabteilung (Inhalt von Stellenanzeigen, Einfluss auf Personalauswahl) sowie mit den Verantwortlichen für Revision und für Datenschutz. Durch intensive Kontakte zu Sicherheitsbehörden, Selbstschutzeinrichtungen der Wirtschaft und zu Sicherheitsverantwortlichen anderer Unternehmen können der aktuelle Wissensstand verbessert und mögliche Problemstellungen frühzeitig erkannt werden.

4.2.2 Durchführung von Kontrollen

Die dynamische Entwicklung technischer Möglichkeiten sowie betriebsinterne Veränderungen bei Geschäftsabläufen und Produktionsprozessen erfordern eine regelmäßige, im Idealfall begleitende Überprüfung der konzeptionellen Überlegungen und Tests der Sicherheitssysteme. Die Beteiligung der internen Revision als wesentlicher Bestandteil des innerbetrieblichen Risikomanagements wird empfohlen. Festgestellte Mängel müssen beseitigt werden. Sicherheitsverstöße dürfen nicht ohne Konsequenzen bleiben. Prävention ist ein stumpfes Schwert, wenn Sicherheitsverstöße nicht sanktioniert werden. Die bloße Ankündigung von Sanktionen ohne entsprechende Ahndung führt zur Nichtbeachtung von Schutzmaßnahmen.

4.3 Bauliche und technische Maßnahmen

Spionagefälle werden oft dadurch begünstigt, dass Betriebsfremde unerkannt und ohne dass sie große Hindernisse überwinden müssen, schutzwürdige Bereiche eines Unternehmens betreten können. Dieser Gefahr kann durch die bauliche, mechanische und elektronische Absicherung des gesamten Werkskomplexes sowie einzelner Gebäude, Gebäudeteile, Räume oder Objekte entgegengewirkt werden. Die Schutzfunktion der meisten technischen Einrichtungen steht und fällt mit ihrer sachgemäßen Bedienung. Voraussetzung hierfür sind Anwender-

freundlichkeit, Nutzerakzeptanz, Transparenz und Nachvollziehbarkeit technischer Lösungen. Sicherheitsrelevante Meldungen und Protokolle müssen konsequent erfasst und zentral ausgewertet werden können.

Bei der Planung von Bauvorhaben sind von Anfang an Sicherheitsüberlegungen zu berücksichtigen, da eine nachträgliche technische Aufrüstung oft nicht mehr möglich oder mit erheblichen zusätzlichen Kosten verbunden ist. Die Beteiligung des Sicherheitsverantwortlichen sollte grundsätzlich bei jedem Planungsvorhaben erfolgen.

4.4 Rechtliche Maßnahmen

Die Schutzwirkung rechtlicher Maßnahmen wie Geheimhaltungs- und Wettbewerbsklauseln, Rückgabeverpflichtungen, Patent- und Lizenzanmeldungen ist nicht immer unmittelbar zu erkennen, sie wird deshalb gerne unterschätzt. Dennoch tragen diese Maßnahmen dazu bei, potenzielle Betriebsspione abzuschrecken und finanzielle Verluste in Grenzen zu halten. Die erfolgreiche Durchsetzung arbeits-, straf- und zivilrechtlicher Ansprüche setzt allerdings ausgefeilte vertragliche Regelungen voraus. So bietet beispielsweise eine Wettbewerbsvereinbarung nach § 74 Handelsgesetzbuch (HGB) und damit dem Verbot für maximal zwei Jahre, dem früheren Arbeitgeber Konkurrenz zu machen oder seine Betriebsgeheimnisse zu verwerten, mehr Sicherheit als eine Verschwiegenheitsvereinbarung, denn § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) stellt eine Weitergabe von Betriebsgeheimnissen nur während des Arbeitsverhältnisses unter Strafe.

Die Anmeldung von Patenten und Gebrauchsmustern kann durchaus eine geeignete Schutzmaßnahme darstellen. Allerdings sollte man sich darüber im Klaren sein, dass möglicherweise erst dadurch die Aufmerksamkeit potenzieller Täterkreise auf ein Unternehmen gelenkt wird.

4.5 Maßnahmen für besondere Risikobereiche

Die Realisierung von Sicherheitsmaßnahmen auf der Basis einer Gesamteinschätzung des Unternehmens wirkt sich grundsätzlich auf alle Organisationseinheiten positiv aus. Dennoch macht es Sinn, Arbeitsfelder mit spezifischen Problemstellungen oder neu auftretende Risikobereiche eigenständigen Untersuchungen zu unterziehen.

4.5.1 Informations- und Kommunikationstechnik

Der Erhalt und das Wachstum eines funktionierenden Gemeinwesens sind heutzutage ohne den breiten Einsatz moderner Informations- und Telekommunikationssysteme (ITS) kaum mehr vorstellbar. Der mit Hilfe dieser Techniken möglichen Effizienzverbesserung steht jedoch eine deutlich gesteigerte Verletzlichkeit sensibler und zugleich besonders wichtiger Informationsstrukturen gegenüber. So weist auch der „Nichtständige Ausschuss über das Abhörsystem ECHELON“ des Europäischen Parlaments in seinem Abschlussbericht vom 11. Juli 2001[3] eindringlich auf die Verwundbarkeit der modernen Kommunikationssysteme hin. Neben der individuellen Privatsphäre des einzelnen Bürgers wird vor allem die Informationssicherheit von Wirtschaftsunternehmen als gefährdet betrachtet.

[3] *Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) vom 11. Juli 2001; URL: www.europarl.de.*

„Goldene Regeln der Prävention“

Die nachfolgenden Merksätze fassen abschließend 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!

Nach einer Umfrage der Wirtschaftsberatungsgesellschaft Ernst & Young[4] hielten zwar 90% der IT-Verantwortlichen in den Unternehmen die Sicherheit ihrer ITS für wichtig. Jedoch räumte gleichzeitig ein Drittel der Befragten ein, im Falle eines Angriffs nur unzureichend reagieren zu können. Weitere 34% gaben sogar an, nur bedingt einen Überblick zu haben, ob und wann ihre Systeme überhaupt attackiert werden.

Informationsverluste sind in erster Linie durch

- Angriffe am unternehmenseigenen Computer,
- Hacking-, Abhör- und Lauschangriffe auf Räume, Netze, IT-Systeme und Telekommunikationseinrichtungen,
- unbefugte Zugriffe auf logische wie physikalische Datenfernübertragungskanäle, interne (vor Ort) und externe (Remote-Access) Fernwartungs- und Administrationskomponenten,
- Einschleusung von Viren, Würmern, Trojanern und anderen ausführbaren Programmen mit Schadfunktion,
- Manipulation von System- und Anwendungssoftware sowie
- Diebstahl von Hardware/-komponenten (PCs, Laptops, Notebooks, mobile bzw. kabellose IT- und TK-Systeme, Datenträger und sonstige Speichermedien)

zu erwarten.

Zusätzlich fördert und bedingt die stetig wachsende Mobilität im Arbeitsalltag die rasante Verbreitung kleiner handlicher digitaler „Helfer" (Pocket-PCs, Handhelds, PDAs, Tablet-PCs, Smartphones, BlackBerrys, Telematiksysteme, USB- und Datensticks etc.). Mit deren Einsatz verschärft sich das Risiko gleich mehrfach, dass Informationen in falsche Hände gelangen können. Einerseits bieten diese Geräte derzeit keine oder nur schwach ausgeprägte Schutzmechanismen, enthalten aber eine Fülle sensibler, scheinbar unentbehrlicher Informationen. Außerdem werden sie überwiegend außerhalb gesicherter Bereiche eingesetzt und sind in hohem Maße verlustgefährdet. In den allermeisten Fällen steht der Hardwareverlust in keinem Verhältnis zum Schaden, der durch den Verlust des darauf gespeicherten Know-hows entsteht. Andererseits eignen sie sich auch ganz hervorragend zum unbemerkten und bequemen „Daten-Klau".

Auf diese Szenarien sollten sich auch die Schutzmaßnahmen konzentrieren. Die komplexen Herausforderungen, die das Thema „IT-Sicherheit" mit sich bringt, legen allerdings die Inanspruchnahme kompetenter interner und/oder externer Fachkräfte nahe. Nach dem Grundsatz der Trennung von IT-Sicherheit und DV-Betrieb sollte intern ein eigenständiger IT-Sicherheitsverantwortlicher bestellt werden, um von vornherein Aufgabenkollisionen und Zielkonflikte mit originären betrieblichen Problemstellungen zu vermeiden.

4.5.2 Outsourcing und Einsatz von Fremdfirmen

Mit der Neigung von Unternehmen, aus Kostengründen einzelne Bereiche auszugliedern oder bestimmte Aufgaben an Fremdfirmen zu übertragen, geht auch regelmäßig die Gefahr des ungewollten Know-how-Abflusses

[4] *Ernst & Young: Global Information Security Survey 2003 (Weltweite Umfrage zur IT-Sicherheit); URL: www.ernst-young.de.*

einher. Besonders kritisch erscheinen in diesem Zusammenhang Aufträge an Fremdentwickler, der Einsatz privater Sicherheitsdienstleister oder die Übertragung von EDV-Aufträgen an Externe sowie die Inanspruchnahme von Unternehmensberatern und (technischen) Übersetzern. Geschäftsverbindungen, die das Risiko von Informationsverlusten in sich bergen, sollten intensiv auf Schwachstellen untersucht werden. Über die sorgfältige Auswahl der Geschäftspartner hinaus muss besonderes Augenmerk auf die Gewährleistung eines vergleichbaren Sicherheitsniveaus wie im eigenen Unternehmen gelegt werden. Dies könnte durch die Integration der Partnerfirma in das eigene Sicherheitssystem und die vertragliche Zusicherung bestimmter Sicherheitsstandards wie getrennte Räume für Fremdentwickler erreicht werden. Der laufenden Kontrolle, dass die Sicherheitsanforderungen auch eingehalten werden, kommt ebenfalls entscheidende Bedeutung zu. Für den Fall der Insolvenz der Fremdfirma sollten Vorkehrungen zur Sicherung des eigenen Know-hows getroffen werden.

4.5.3 Beschäftigung von Praktikanten

Unter sicherheitsmäßigen Aspekten wird der Beschäftigung von Diplomanden und Praktikanten seit jeher viel zu wenig Beachtung geschenkt. Vor allem bei Personal aus Ländern mit großem Technologierückstand liegt die Gefahr des Know-how-Verlustes auf der Hand. Zumindest die Beschäftigung in besonders sensiblen Bereichen mit umfangreichen Zugangsmöglichkeiten (Führungsebene, Forschung/Entwicklung, EDV) sollte sorgfältig geprüft und gegebenenfalls der Einsatz von Sicherheitsmaßnahmen begleitet werden.

5. Verhalten im Schadensfall

Auch das ausgefeilteste Sicherheitskonzept garantiert keinen absoluten Schutz gegen Informationsverluste. Um den im konkreten Einzelfall drohenden Schaden möglichst gering zu halten, müssen alle erdenklichen Anstrengungen unternommen werden, die „undichte Stelle" möglichst frühzeitig zu entdecken und wirksame Gegenmaßnahmen zu treffen. Nichts sollte dem Zufall überlassen bleiben, denn selbst in diesem Stadium kann professionelles Verhalten noch eine erhebliche Schutzwirkung entfalten.

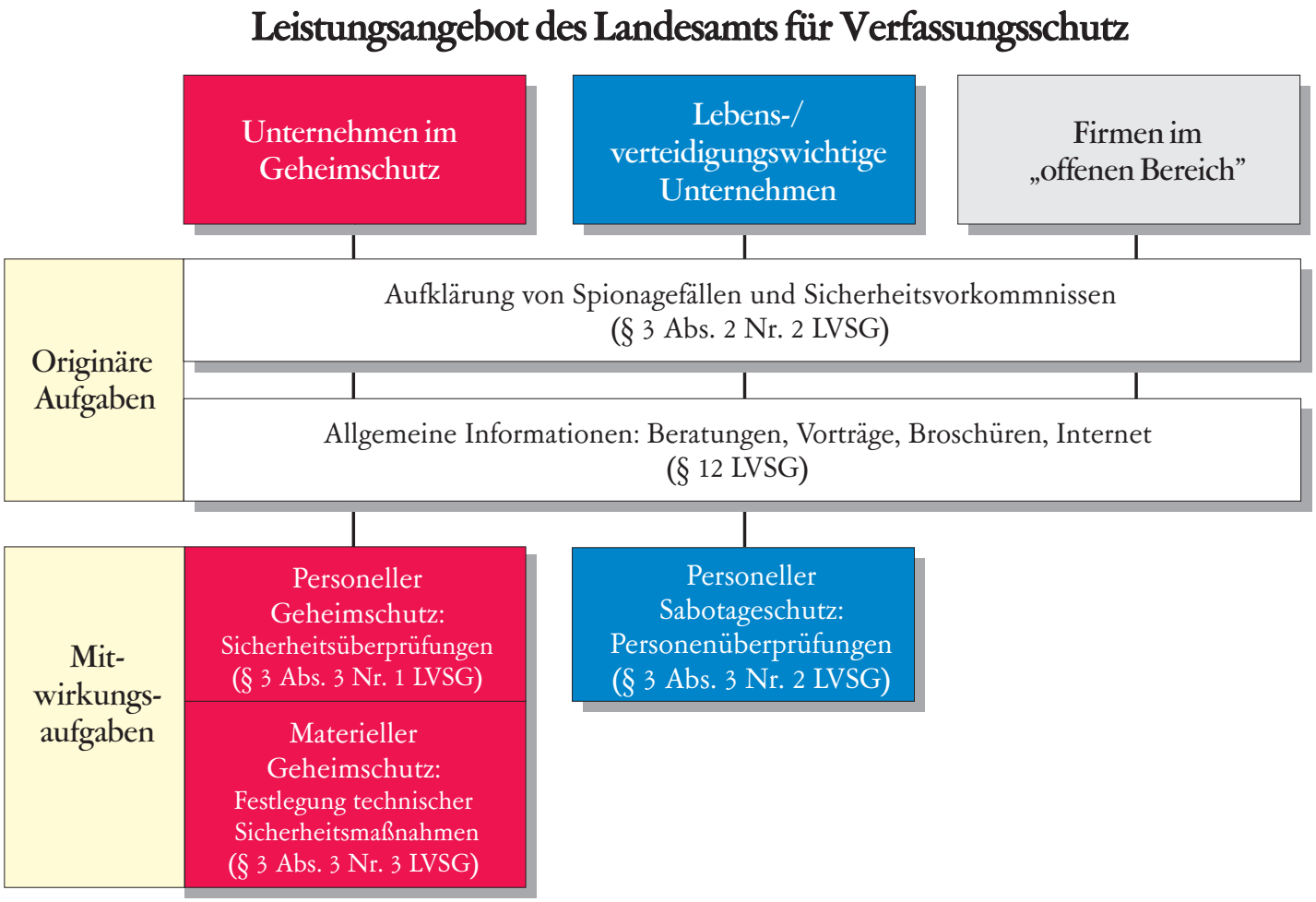
Immer noch werden nach einer von der Unternehmensberatungsgruppe PricewaterhouseCoopers zum Thema Wirtschaftskriminalität veröffentlichten Studie[5] viele Fälle nur durch Zufall aufgedeckt. Eher selten gibt es dagegen konkrete Hinweise auf bestimmte Personen oder es wird gar ein Spion auf frischer Tat ertappt. In der Regel ist die Aufdeckung von Spionagefällen auf die Auswertung mehr oder weniger vager Hinweise zurückzuführen, die einzeln oder in ihrer Gesamtheit betrachtet auf einen Verrat hindeuten. Durchaus Erfolg versprechend ist auch der Ansatz, durch gezielte Analysen wie Beobachtung von Umfeldveränderungen, systematische Auswertung von Auffälligkeiten, Begutachtung von Kontrollergebnissen oder Bewertung von Sicherheitsgesprächen Hinweise auf drohende Gefahren zu erhalten. Durch eine derartige Vorgehensweise kann die „Frühwarnzeit" entscheidend verkürzt werden.

[5] *PricewaterhouseCoopers: Industriestudie „Wirtschaftskriminalität 2003" (Internationale und deutsche Ergebnisse); URL: www.pwcglobal.com/de.*

Indikatoren für das Vorliegen eines Spionagefalls können direkt eine bestimmte Person betreffen, aber auch auf das eigene Unternehmen oder auf das Gebaren von Geschäftspartnern bezogen sein. Daneben gilt es, eine Reihe sonstiger Faktoren, die im Einzelfall den Verlust von Know-how begünstigen können, zu berücksichtigen. Hinweise von Betriebsangehörigen sind ausnahmslos ernst zu nehmen. Im Bedarfsfall muss eine vertrauliche Behandlung der Mitteilung zugesichert und auch eingehalten werden. Der Sicherheitsverantwortliche koordiniert die notwendigen Ermittlungsschritte und entscheidet über die Einschaltung externer Spezialisten. Die Furcht vor etwaigen Imageverlusten sollte kein Unternehmen davon abhalten, vertrauensvoll mit Sicherheitsbehörden zusammenzuarbeiten, da sonst die Chance vertan wird, die eigenen Erfahrungen auch Dritten zukommen zu lassen. Für die Behandlung von Fällen des Spionageverdachts gibt es praktikable und Erfolg versprechende Empfehlungen. Speziell die nachträgliche Auswertung eines abgeschlossenen Falls sollte mit besonderer Sorgfalt vorgenommen werden, weil sie unter Umständen bislang noch nicht erkannte Schwachstellen im Unternehmen offenbart und in jedem Fall wichtige Fingerzeige für zukünftige Präventivmaßnahmen nicht nur im eigenen Unternehmen gibt.

6. Hilfe zur Selbsthilfe

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) bietet Zusammenarbeit und Beratung bei der Aufklärung von Spionagefällen und sonstigen Sicherheitsvorkommnissen an. Es unterrichtet darüber hinaus die



Öffentlichkeit durch Broschüren, Vorträge und Informationen im Internet (**www.verfassungsschutz-bw.de**) aus sämtlichen originären Aufgabenbereichen (Spionageabwehr, Beobachtung des Links-, Rechts- und Ausländerextremismus/Islamismus sowie der Scientology-Organisation).

Unternehmen in Baden-Württemberg können anlassbezogen oder in allgemeiner Form individuelle Empfehlungen zur personellen, organisatorischen und technischen Sicherheit erhalten. Personenbezogene Auskünfte (beispielsweise im Rahmen von „Sicherheits-Checks") dürfen in diesem Zusammenhang allerdings nur unter ganz bestimmten Voraussetzungen (§ 10 Abs. 4 Landesverfassungsschutzgesetz) erteilt werden.

Interessenten wenden sich bitte an das

Landesamt für Verfassungsschutz Baden-Württemberg
- Abteilung 4 -
Taubenheimstraße 85 A
70372 Stuttgart
Telefon: (0711) 95 44-301
Fax: (0711) 95 44-313
E-Mail: Spionageabwehr@lfvbw.bwl.de

7. Vertrauliches Telefon der Spionageabwehr

Um rund um die Uhr einen direkten Kontakt zur Spionageabwehr zu ermöglichen, wurde beim LfV ein VERTRAULICHES TELEFON eingerichtet. Unter den Rufnummern

Telefon (0711) 9 54 76 26 und
Fax (0711) 9 54 76 27

stehen erfahrene Mitarbeiter bereit, um Hinweise auf einschlägige Sachverhalte aufzunehmen oder Anrufer in persönlichen Konfliktsituationen sachkundig zu beraten.

8. „Sicherheitsforum Baden-Württemberg - die Wirtschaft schützt ihr Wissen"

Das 1999 ins Leben gerufene Sicherheitsforum Baden-Württemberg setzt sich aus Vertretern von Firmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden (unter anderem auch dem LfV) zusammen. Es versteht sich als Bindeglied zwischen Wirtschaft und Staat und will mit einem Bündel sicherheitsbezogener Maßnahmen dazu beitragen, den Technologievorsprung der baden-württembergischen Wirtschaft und Forschung zu sichern und vor Spionage zu schützen. In regelmäßigen Arbeitssitzungen werden aktuelle Sicherheitsthemen und spezifische Bedürfnisse der Wirtschaft erörtert. Weitere Informationen zu den Aktivitäten des Sicherheitsforums sind im Internet unter **www.sicherheitsforum-bw.de** abrufbar.

9. Verzeichnisse

9.1 Literaturhinweise

9.1.1 Fachbücher

Die nachfolgende Buchauswahl ermöglicht eine Vertiefung der in der Broschüre angesprochenen Themen. Sie erhebt allerdings keinen Anspruch auf Vollständigkeit.

Autor	Titel	Verlag, etc.
BEER, Daniel, HOHL, Peter, SABITZER, Werner (Hrsg.)	Sicherheits-Jahrbuch 2003/2004	SecuMedia Verlag, Ingelheim, 2002
DREGER, Wolfgang	Konkurrenz-Analyse und Beobachtung: Mit System zum Erfolg im Wettbewerb	Expert Verlag, Ehningen b. Böblingen, 1992
DREGER, Wolfgang	Counter Intelligence: Betriebliche Spionageabwehr; so schützen Sie Ihr Firmen-Know-how gegen Ausspähung und Konkurrenz	Expert Verlag, Renningen-Malmsheim, 1998
ECKERT, Claudia	IT-Sicherheit: Konzepte, Verfahren, Protokolle	Wissenschaftsverlag Oldenbourg, München, 2001
EHSES, Herbert (Hrsg.)	Unternehmensschutz: Praxishandbuch Werkssicherheit	Richard Boorberg Verlag, Stuttgart, 1999
FINK, Manfred	Lauschziel Wirtschaft: Abhörgefahren und -techniken, Vorbeugung und Abwehr	Richard Boorberg Verlag, Stuttgart, 1996
GAULKE, Markus	Digitale Abgründe: Was die Computerindustrie ihren Kunden verschweigt, Risiken ausschließen - Investitionen sichern - Systeme optimieren	Verlag Moderne Industrie, Landsberg, 1996
HUMMELT, Roman	Wirtschaftsspione auf dem Datenhighway: Strategische Risiken und Spionageabwehr	Carl Hanser Verlag, München, Wien, 1997
von KNOP, Jan, HAVERKAMP, Wilhelm (Hrsg.)	Zukunft der Netze: Die Verletzbarkeit meistern (16. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf)	Gesellschaft für Informatik/Köllen Druck+Verlag, Bonn, 2002
KOCH, Egmont R., SPERBER, Jochen	Die Datenmafia: Geheimdienste, Konzerne, Syndikate; Computerspionage und neue Informationskartelle	Rowohlt Verlag, Reinbek b. Hamburg, 1995
LUX, Christian, PESKE, Thorsten	Competitive Intelligence und Wirtschaftsspionage	Gabler Verlag,Wiesbaden, 2002
SCHNEIER, Bruce	Angewandte Kryptographie	Addison-Wesley Publishing Company, Bonn, 1996
SCHNEIER, Bruce	Secrets & Lies. IT-Sicherheit in einer vernetzten Welt	dpunkt.verlag, Heidelberg, 2001
SITT, Axel	Erfolgsfaktor Sicherheit - Schützen Sie Ihr Unternehmens-Know-how vor dem Zugriff der Konkurrenz	Econ-Verlag, Düsseldorf, 1998
STROBEL, Stefan	Firewalls und IT-Sicherheit	dpunktverlag, Heidelberg, 2002
TRAUBOTH, Jörg H.	Krisenmanagement bei Unternehmensbedrohungen: Präventions- und Bewältigungsstrategien	Richard Boorberg Verlag, Stuttgart, 2002
ULFKOTTE, Udo	Marktplatz der Diebe: Wirtschaftsspionage in Deutschland	C. Bertelsmann Verlag, München, 1999
ULFKOTTE, Udo	Wirtschaftsspionage: Wie deutsche Unternehmen von ausländischen Geheimdiensten ausgeplündert und ruiniert werden (aktualisierte Taschenbuchausgabe)	Goldmann Verlag, München, 2001
VOSSBEIN, Jörn	Integrierte Sicherheitskonzeptionen für Unternehmen: Stand und Perspektiven	SecuMedia Verlag, Ingelheim, 1999

9.1.2 Fachzeitschriften

Weiterhin findet sich in folgenden Zeitschriften eine Vielzahl interessanter Beiträge, die sich mit Themenstellungen dieser Broschüre befassen:

Autor	Titel	Verlag, etc.
Funkschau	Telekommunikation - Netzwerke - IT	WEKA Fachzeitschriften-Verlag GmbH, Poing, www.funkschau.de
KES	Die Zeitschrift für Informations-Sicherheit (Organ des BSI)	SecuMedia Verlags-GmbH, Ingelheim, www.kes.info; www.secumedia.de
Sicherheits-Berater	Informationsdienst zur Sicherheit in Wirtschaft und Verwaltung	VZM von zur Mühlen' sche Unternehmensberatungs GmbH, Bonn, www.vzm.de
WIK	Zeitschrift für die Sicherheit in der Wirtschaft (Organ der ASW)	SecuMedia Verlags-GmbH, Ingelheim, www.wik.info; www.secumedia.de
W+S	Sicherheitsmagazin für Trends, Technik und Dienstleistung	Hüthig GmbH & Co KG, Heidelberg, www.ws-huethig.de

9.1.3 BSI-Publikationen

Diverse Veröffentlichungen zu der komplexen Materie „IT-Sicherheit" werden auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben. Näheres dazu findet sich unter www.bsi.de.

9.2 Informationsangebote im Internet

www. ...	aus Baden-Württemberg
verfassungsschutz-bw.de	Landesamt für Verfassungsschutz Baden-Württemberg
sicherheitsforum-bw.de	Sicherheitsforum Baden-Württemberg
polizei-bw.de	Polizei Baden-Württemberg
baden-wuerttemberg.datenschutz.de	Der Landesbeauftragte für den Datenschutz Baden-Württemberg
vsw-bw.com	Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V.

www. ...	aus der Bundesrepublik Deutschland
verfassungsschutz.de	Bundesamt für Verfassungsschutz
bka.de	Bundeskriminalamt
bfd.bund.de	Der Bundesbeauftragte für den Datenschutz
datenschutz.de	Virtuelles Datenschutzbüro
bmwi.de	Bundesministerium für Wirtschaft und Arbeit
sicherheit-im-internet.de	Sicherheit in der Informationsgesellschaft
mittelstand-sicher-im-internet.de	Sicherheit im Internet - gerade für den Mittelstand

www. ...	aus der Bundesrepublik Deutschland
regtp.de	Regulierungsbehörde für Telekommunikation und Post
asw-online.de	Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V.
initiatived21.de	Initiative D21 e.V. – Fit fürs Informationszeitalter
bsi.bund.de/certbund	Computer Emergency Response Team (CERT-Bund)
bsi.bund.de/taskforce	Task Force „Sicheres Internet“
heise.de	Heise Medien Gruppe GmbH & Co. KG (u.a. heise online, c’t, iX, Telepolis, Security)
bitkom.org	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
vds.de	VdS Schadenverhütung GmbH

www. ...	aus dem Ausland[6]
europa.eu.int./comm/internal_market/privacy	Datenschutz in der Europäischen Union
conventions.coe.int/Treaty/EN/Treaties/Html/185.htm	EU convention on cybercrime, ETS No.: 185

[6] *Weitere ausländische Internetseiten wurden nicht berücksichtigt, da die Seriosität meist nicht überprüft werden kann. Ferner könnten einzelne Informationsangebote unter dem Einfluss bzw. der Kontrolle eines fremden Nachrichtendienstes stehen.*

Anhang

Staatenliste[7] zur „Anleitung zum Ausfüllen der Sicherheitserklärung":[8]

1. Afghanistan (Islamischer Staat Afghanistan),
2. Albanien (Republik Albanien),
3. Algerien (Demokratische Volksrepublik Algerien),
4. Armenien (Republik Armenien),
5. Aserbaidschan (Republik Aserbaidschan),
6. Bosnien und Herzegowina,
7. China (Volksrepublik China),
   ab 01.07.1997 einschl. Sonderverwaltungsregion (SVR) Hongkong,
   ab 20.12.1999 einschl. Sonderverwaltungsregion (SVR) Macau,
8. Georgien,
9. Irak (Republik Irak),
10. Iran (Islamische Republik Iran),
11. Kambodscha (Königreich Kambodscha),
12. Kasachstan (Republik Kasachstan),
13. Kirgisistan (Kirgisische Republik),
14 Korea (Demokratische Volksrepublik Korea),
15. Kuba (Republik Kuba),
16. Laos (Demokratische Volksrepublik Laos),
17. Libanon (Libanesische Republik),
18. Libysch-Arabische Dschamahirija (Sozialistische Libysch-Arabische Volks-Dschamahirija),
19. Moldau (Republik Moldau),
20. Russische Föderation,
21. Serbien und Montenegro,
22. Sudan (Republik Sudan),
23. Syrien (Arabische Republik Syrien),
24. Tadschikistan (Republik Tadschikistan),
25. Turkmenistan,
26. Ukraine,
27. Usbekistan (Republik Usbekistan),
28. Vietnam (Sozialistische Republik Vietnam),
29. Weißrussland (Republik Weißrussland).

---

[7] *Festgelegt durch das Bundesministerium des Innern im Sinne von § 13 Abs. 1 Nr. 17 SÜG, Stand: 15. Juni 2004.*

[8] *Die Schreibweise der Staatennamen richtet sich nach dem vom Auswärtigen Amt herausgegebenen „Verzeichnis der Staatennamen für den amtlichen Gebrauch in der Bundesrepublik Deutschland" in der jeweils geltenden Fassung, die im Gemeinsamen Ministerialblatt bekannt gegeben wird.*

VERTEILERHINWEIS

Diese Informationsschrift wird vom Landesamt für Verfassungsschutz Baden-Württemberg im Rahmen seiner gesetzlichen Verpflichtung zur Unterrichtung der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel.

Untersagt ist auch die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Auch ohne zeitlichen Bezug zu einer Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zugunsten einzelner politischer Gruppen verstanden werden könnte. Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist.

Erlaubt ist jedoch den Parteien, die Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.

SONSTIGE PUBLIKATIONEN DES
LANDESAMTS FÜR VERFASSUNGSSCHUTZ BADEN-WÜRTTEMBERG

Öffentlichkeitsarbeit, Taubenheimstraße 85 A, 70372 Stuttgart

Tel.: 0711/9544-181/182, Fax: 0711/9544-444

Das Landesamt für Verfassungsschutz Baden-Württemberg - Aufbau und Arbeitsweise
(Broschüre - Januar 1999, gedruckte Auflage vergriffen, Neuauflage geplant)

Extremisten im Internet - Eine Herausforderung für die Sicherheitsbehörden
(Broschüre - Dezember 2001, 44 Seiten)

Rechtsextremismus in Baden-Württemberg - Allgemeine Entwicklung
(Broschüre - April 2003, 65 Seiten)

Die Partei „Die Republikaner" (REP) - konservativ oder rechtsextremistisch?
(Broschüre - August 2000, 23 Seiten)

Rechtsextremistische Skinheads
(Broschüre - Dezember 2001, 32 Seiten, gedruckte Auflage vergriffen, Neuauflage geplant)

Linksextremismus in der Bundesrepublik Deutschland - Allgemeine Entwicklung
(Broschüre - Februar 2003, 49 Seiten)

Antifaschismus als Aktionsfeld von Linksextremisten
(Broschüre - März 2002, 40 Seiten)

Die „Partei des Demokratischen Sozialismus" (PDS) - Auf dem Weg in die Demokratie?
(Broschüre - August 2000, 23 Seiten)

Islamismus
(Broschüre - April 2004, 47 Seiten)

Erscheinungsformen des Ausländerextremismus
(Broschüre - März 2001, 52 Seiten)

„Arbeiterpartei Kurdistans" (PKK) - Organisationsaufbau
(Broschüre - Juli 1998, 20 Seiten)

Die „Scientology-Organisation" (SO)
(Broschüre - Juli 2003, 80 Seiten)

Der Kampf der „Scientology-Organisation" um die Anerkennung der Gemeinnützigkeit in den USA und seine Auswirkungen auf Deutschland
(Broschüre - April 2004, 43 Seiten)

Scientology - ein Fall für den Verfassungsschutz
(Broschüre - August 1997, 35 Seiten)

Wirtschaftsspionage - Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste
(Broschüre - Oktober 1998, 48 Seiten; gedruckte Auflage vergriffen, Neuauflage geplant)

Alle Publikationen können auf unserer Internetseite

http://www.verfassungsschutz-bw.de

eingesehen und heruntergeladen werden.

Handlungskonzept

für Ihren Know-how-Schutz

Baden-Württemberg

Inhaltsverzeichnis[1] Seite

Unterkapitel auf.

Hinweis

Die nachfolgenden Handlungsempfehlungen bieten eine Grundlage für die eigenständige Erarbeitung eines individuellen Know-how-Schutzkonzeptes. Sie enthalten nahezu alle für die Sicherheit eines Unternehmens relevanten Gesichtspunkte. Gleichwohl eröffnen unternehmensspezifische Gegebenheiten sowie die technische Entwicklung immer wieder neue bzw. zusätzliche Risiken.

Einen ersten Überblick über den aktuellen Sicherheitsstandard Ihres Unternehmens erhalten Sie, indem Sie die einzelnen Positionen des Handlungskonzeptes als

relevant und berücksichtigt

zu vernachlässigen

nicht relevant

kennzeichnen.

Präventive Aspekte

1. Personeller Bereich

Grundregeln

- Vorbildfunktion des Vorgesetzten
- Sicherheitsgesichtspunkte von der Einstellungsphase bis zur Beendigung des Beschäftigungsverhältnisses (und danach!) berücksichtigen
- Den Sicherheitsverantwortlichen an allen sicherheitsrelevanten Personalmaßnahmen beteiligen
- Das Sicherheitsverhalten der Mitarbeiter durch Förderung ihrer Persönlichkeit stärken

1.1 Maßnahmen bei der Personalgewinnung

	☑	⊖	⊘
● Personalakquisition			
❍ Keine Preisgabe sicherheitsrelevanter Firmeninterna im Ausschreibungstext	❑	❑	❑
❍ Funktionsbeschreibung an der Sicherheitsempfindlichkeit der Aufgabe orientieren	❑	❑	❑
● Auswahlverfahren (Feststellung der Eignung für sicherheitsempfindliche Tätigkeit)			
❍ Eingehende Prüfung der Bewerbungsunterlagen	❑	❑	❑
❍ Lückenloser Nachweis aller bisherigen Ausbildungs- und Beschäftigungszeiten	❑	❑	❑
❍ Erkenntnisse moderner Personaldiagnostik berücksichtigen	❑	❑	❑
❍ Alle Informationsmöglichkeiten (z.B. frühere Arbeitgeber, Referenzen, polizeiliches Führungszeugnis) ausschöpfen	❑	❑	❑
❍ Persönlicher Eindruck (intensives Einstellungsgespräch und Dokumentation des Gesprächsergebnisses)	❑	❑	❑
❍ Berücksichtigung individueller Risikofaktoren (z.B. nachrichtendienstlich beeinflusster Lebenslauf, Kontakte zu/Aufenthalte in Staaten mit besonderen Sicherheitsrisiken[2])	❑	❑	❑
❍ Schriftliche Erklärung zu nachrichtendienstlichen Verbindungen	❑	❑	❑
● Vertragsabschluss/Einstellung			
❍ Sicherheitsgespräch/Eingangsbelehrung	❑	❑	❑
❍ Sicherheitsvorschriften erläutern und aushändigen	❑	❑	❑
❍ In Einrichtungen der Sicherheitstechnik einweisen	❑	❑	❑
❍ Datenschutzrechtliche Verpflichtung	❑	❑	❑

[2] Staatenliste siehe Anhang.

	☑	⊟	⊘
❍ Zur Geheimhaltung verpflichten	❑	❑	❑
❍ Konkurrenzklauseln und nachvertragliches Wettbewerbsverbot vereinbaren	❑	❑	❑

1.2 Sicherheitsbewusstes Personalmanagement

● Sicherheitsbewusstes Verhalten durch leistungsgerechte Bezahlung und Anerkennung im Beruf fördern	❑	❑	❑
● Schaffung einer hohen Identifikation mit dem Unternehmen durch Vermittlung aktueller Informationen über innerbetriebliche Angelegenheiten (z.B. Sicherheitsmaßnahmen)	❑	❑	❑
● Betreuungsangebot in persönlichen Ausnahme-/Konfliktsituationen	❑	❑	❑
● Bei Personalumsetzungen auch Sicherheitsaspekte berücksichtigen	❑	❑	❑

1.3 Beendigung des Arbeitsverhältnisses

● Bei regulärem Ausscheiden			
❍ Vollständige Rückgabe betrieblicher Unterlagen und Gegenstände (inkl. einer entsprechenden Erklärung)	❑	❑	❑
❍ Vollmachten und Berechtigungen zurücknehmen	❑	❑	❑
❍ Den Sicherheitsverantwortlichen und ggf. (wichtige) Geschäftspartner informieren	❑	❑	❑
● Bei nicht einvernehmlichem Ausscheiden zusätzlich			
❍ Sofortige Entbindung von sicherheitsempfindlichen Aufgaben	❑	❑	❑
❍ Zugänge zu sicherheitsrelevanten Bereichen beschränken	❑	❑	❑
● Nach Beendigung des Arbeitsverhältnisses			
❍ Auf Auffälligkeiten achten (z.B. Kontakte zu Wettbewerbern, Kundenverhalten, Veränderungen im persönlichen Bereich)	❑	❑	❑

1.4 Systematische und qualifizierte Sicherheitsunterweisung

Grundregeln

➲ Grundsensibilisierung zur Förderung des Sicherheitsbewusstseins

➲ Zielgruppenorientiertes, nach Sicherheitsbereichen abgestuftes Aufbauprogramm

● Sensibilisierung für Auffälligkeiten (z.B. über nachrichtendienstliche Vorgehensweisen)	❑	❑	❑
● Innerbetriebliches Sicherheitssystem erläutern	❑	❑	❑
● Sicherheitsrelevante Vorschriften vermitteln	❑	❑	❑

	☑	⊖	⊘
● Verhaltens-, Sorgfalts-, Melde- und Geheimhaltungspflichten aufzeigen	❑	❑	❑
● Vertrauliche Behandlung bei Problemfällen zusichern	❑	❑	❑
● Anlass- und zeitbezogene Sicherheitsgespräche (z.B. vor und nach Geschäftsreisen in Staaten mit besonderen Sicherheitsrisiken, Empfehlungen für entsprechende private Auslandsaufenthalte)	❑	❑	❑
● Aktuelle, anlassbezogene Unterrichtung über sicherheitsrelevante Themen (Rundschreiben, Aushänge, Presseartikel über Internet)	❑ ❑	❑ ❑	❑ ❑
● Kreativität der Mitarbeiter für das betriebliche Vorschlagswesen in punkto Sicherheit nutzen	❑	❑	❑

2. Organisatorischer Bereich

2.1 Bestellung eines Sicherheitsverantwortlichen

Grundregeln

- ➲ Zentraler Ansprechpartner und Koordinator in allen Sicherheitsangelegenheiten
- ➲ Einbindung in alle sicherheitsrelevanten Vorgänge
- ➲ Rückhalt durch die Geschäftsleitung
- ➲ Organisatorische Anbindung auf der Managementebene
- ➲ Ausreichende personelle und finanzielle Ausstattung
- ➲ Eindeutige Vertretungsregelung

2.1.1 Anforderungen

	☑	⊖	⊘
● Persönliche Eignung			
❍ Sicherheitsbewusstsein	❑	❑	❑
❍ Integrativ, mit Potenzial für Vorbildfunktion	❑	❑	❑
❍ Stärken im sozialen, kommunikativen und kreativen Bereich	❑	❑	❑
❍ Ökonomische Denkweise	❑	❑	❑
❍ Organisationstalent	❑	❑	❑
● Fachliche Eignung			
❍ Kenntnis der Firmenstruktur (Schwachstellen, sicherheitskritische Bereiche)	❑	❑	❑

	☑	⊖	⊘
❍ Verständnis für technische/wirtschaftliche Abläufe und Zusammenhänge	❑	❑	❑
❍ Aktueller Kenntnisstand in Sicherheitsfragen	❑	❑	❑
❍ Rechtliche Qualifikationen	❑	❑	❑

2.1.2 Aufgaben/Kompetenzen

- Informationsbeschaffung bei

❍ Sicherheitsbehörden	❑	❑	❑
❍ Selbstschutzorganisationen der Wirtschaft	❑	❑	❑
❍ Sicherheitsverantwortlichen anderer Unternehmen	❑	❑	❑
❍ Anbietern von Sicherheitstechnik und Sicherheitsdienstleistungen	❑	❑	❑
❍ Fachleuten mit Spezialkenntnissen	❑	❑	❑

● Vorbereitung und Umsetzung risikopolitischer Entscheidungen des Managements	❑	❑	❑
● Beratung der Unternehmensleitung und anderer betrieblicher Entscheidungsträger in allen Sicherheitsangelegenheiten (unmittelbares Vortragsrecht bei der Unternehmensleitung)	❑	❑	❑
● Durchführung von Risiko- und Schwachstellenanalysen sowie Kontrollen	❑	❑	❑
● Steuerung des Informationsflusses in Sicherheitsangelegenheiten und Mitwirkung bei der Erarbeitung sicherheitsorientierter Arbeitsabläufe	❑	❑	❑
● Regelmäßige Pflege und Aktualisierung des Sicherheitssystems	❑	❑	❑
● Kooperation mit dem Personal sicherheitskritischer Arbeitsbereiche (Forschung/Entwicklung, PR-Bereich, Vertrieb, Personalwesen, Datenschutz/Datensicherheit, Revision)	❑	❑	❑

2.2 Anweisungen und Empfehlungen

Grundregeln

- ➲ Unternehmensgrundsätze auf dem Gebiet des Know-how-Schutzes konkretisieren
- ➲ Formulierte Sicherheitserfordernisse müssen der tatsächlichen betrieblichen Praxis entsprechen
- ➲ Knappe, übersichtliche und verständliche Darstellung
- ➲ Sicherheitsbelange auch bei der Öffentlichkeitsarbeit mit berücksichtigen

2.2.1 Inhalt

● Notwendigkeit des Informationsschutzes	❑	❑	❑
● Festlegen besonders gefährdeter Unternehmensbereiche (Bildung von „Sicherheitsinseln“)	❑	❑	❑
● Definition des Begriffs Firmen-/Betriebsgeheimnis	❑	❑	❑

	☑	⊟	⊘
● Klassifizierung, Kennzeichnung und Handhabung von Firmen-/Betriebsgeheimnissen (Prinzip „Kenntnis nur, wenn nötig“, Vier-Augen-Prinzip)	❑	❑	❑
● Hinweise auf bestehende Sicherheitsmaßnahmen/-einrichtungen	❑	❑	❑
● Individuelle Pflichten benennen und über die Folgen von Sicherheitsverstößen unterrichten	❑	❑	❑

2.2.2 Regelungsbereiche

● Unternehmensweite Sicherheitsanweisung (z.B. Grundsatzangelegenheiten)	❑	❑	❑
● Informationsverarbeitung (Entstehung, Bearbeitung, Kennzeichnung, Vervielfältigung, Aufbewahrung, Weitergabe und Vernichtung schützenswerter Informationen)	❑	❑	❑
● Objektschutz/Werkschutz (Wach- und Pfortendienst)	❑	❑	❑
● Geheimschutz	❑	❑	❑
● Besucherverkehr (Delegationen, Betriebsbesichtigungen, Filmen/Fotografieren im Unternehmen)	❑	❑	❑
● Zusammenarbeit mit Fremdfirmen	❑	❑	❑
● Umgang mit den Medien (Anfragen, Veröffentlichungen)	❑	❑	❑
● Registraturwesen	❑	❑	❑
● Schlüsselmanagement/Zugangsberechtigung	❑	❑	❑
● Schutz der Informations- und Kommunikationstechnik	❑	❑	❑
● Verhalten im Gefährdungs-/Not-/Krisen-/Schadensfall	❑	❑	❑
● Beschäftigung von Diplomanden, Praktikanten, Leasingpersonal, Gelegenheits- und Aushilfskräften	❑	❑	❑
● Veranstaltungsschutz (z.B. Verbot des Mitschneidens, Verbot - eingeschalteter - Mobiltelefone etc.)	❑	❑	❑

2.2.3 Kontrollen

● Institutionalisierte Kontrollen			
❍ Zeit-/anlassbezogen	❑	❑	❑
❍ Flächendeckend/stichprobenweise	❑	❑	❑
❍ Während/außerhalb der Arbeitszeit	❑	❑	❑
● Dokumentation von Kontrollen			
❍ Kontrollbereiche und -maßnahmen	❑	❑	❑
❍ Kontrollergebnisse	❑	❑	❑
❍ Sicherheitsvorkommnisse (Ereignisdatei)	❑	❑	❑
● Einzelmaßnahmen			
❍ Torkontrollen (z.B. stichprobenweise Taschenkontrollen, Kontrolle der Frachtführer, Servicefirmen etc.)	❑	❑	❑

- ❍ Kontrollen der Arbeitsbereiche
  (clean-desk-policy, Aktivierung der Sicherheitseinrichtungen) ❑ ❑ ❑

2.2.4 Konsequenzen bei Sicherheitsverstößen

- Personalgespräch ❑ ❑ ❑
- Nachschulung ❑ ❑ ❑
- Arbeitsrechtliche Folgen ❑ ❑ ❑
- Einbeziehung der Revision ❑ ❑ ❑
- Auswertung und Untersuchung von Sicherheitsvorkommnissen ❑ ❑ ❑
- Sicherheitslücken beheben ❑ ❑ ❑

3. Baulicher und technischer Bereich

Grundregeln

- ➲ Sicherheitsaspekte bereits in der Planungsphase von Bauvorhaben berücksichtigen
- ➲ Ausgewogenheit baulicher und technischer Sicherheitsmaßnahmen
- ➲ Keine Überdimensionierung (Orientierung der Maßnahmen an der Risikoanalyse)

3.1 Anwendungsbereiche

- Freigeländesicherung ❑ ❑ ❑
- Außenhautsicherung ❑ ❑ ❑
- Innenraumüberwachung ❑ ❑ ❑
- Sicherung von Einzelobjekten ❑ ❑ ❑

3.2 Bauliche Maßnahmen

- Beseitigung/Ertüchtigung erkannter Schwachstellen
  - ❍ Geländesicherung (Zaun, Außenpforte, Werkstore) ❑ ❑ ❑
  - ❍ Wände, Decken, Böden, Dächer, Unterkellerung ❑ ❑ ❑
  - ❍ Parkplatz, Dach- und Tiefgarage ❑ ❑ ❑
  - ❍ Türen, Fenster, Lichtschächte, Notausgänge, Fluchtwege ❑ ❑ ❑

- Abhörschutz
  - ❍ Abhörsichere/abhörgeschützte Büro- und Besprechungsräume ❑ ❑ ❑

	☑	⊟	⊘
❍ Absichern von Geräten, Leitungen, Verteilerkästen, Abzweigdosen, drahtlosen Verbindungen (z.B. Kommunikationseinrichtungen, Datennetze, Hardware)	❑	❑	❑
❍ Inventarnachweise und Inventarkontrollen	❑	❑	❑

3.3 Technische Maßnahmen

Grundregeln

- ➲ Genereller Vorrang der Organisation vor Technikeinsatz
- ➲ Hoher Qualitäts- und Produktstandard. Durch Einsatz minderwertiger Produkte wird Scheinsicherheit erzeugt.
- ➲ Akzeptanz bei der Belegschaft und bei den Geschäftspartnern

3.3.1 Technische Mittel

● Freigeländesicherung (Zäune, Perimeterfelder, Lichtschranken)	❑	❑	❑
● Mechanische/elektronische Zugangs-/Zutrittskontrolle (Schleusenkonzept, Einsatz biometrischer Verfahren, Gebäudeleitsysteme)	❑	❑	❑
● Aktensicherungsräume, Stahlschränke, Datensicherungsschränke	❑	❑	❑
● Kamera-/Videoüberwachung, Bewegungssensorik	❑	❑	❑
● Türsicherung/-management, Fluchttürsicherung/-steuerung	❑	❑	❑
● Schließanlagen/-systeme, Schlüsselverwaltung	❑	❑	❑
● Überfall- und Einbruchmeldeanlagen (Aufschaltung auf Polizeinotruf, Werkschutzzentrale, externe Sicherheitsdienstleister)	❑	❑	❑
● Lauschabwehrmaßnahmen	❑	❑	❑

4. Rechtlicher Bereich

Grundregeln

- ➲ Sicherheitskonzeption durch rechtliche Maßnahmen mit Innen- und Außenwirkung ergänzen
- ➲ Sicherung und Ausschöpfung aller zivil-, straf- und arbeitsrechtlichen Ansprüche im Verratsfall

4.1 Interner Bereich

- Berücksichtigung von Aspekten des Informationsschutzes
  - Geheimhaltungsklauseln ❑ ❑ ❑
  - Wettbewerbsklauseln ❑ ❑ ❑
  - Sanktionen bei unbefugter Nutzung sensibler Daten (Haftungsregelungen) ❑ ❑ ❑
  - Vereinbarung von Pflichten für den Fall des Ausscheidens aus dem Unternehmen (Rückgabeverpflichtungen) ❑ ❑ ❑
  - Ausdehnung von Geheimhaltungsklauseln auf die Zeit nach dem Ausscheiden ❑ ❑ ❑

4.2. Externer Bereich

- Vertragliche Vereinbarungen von Sicherheitsmaßnahmen mit Fremdfirmen, wissenschaftlichen Einrichtungen ❑ ❑ ❑
- Anmeldung von Patent- und Gebrauchsmustern ❑ ❑ ❑

4.3 Innen- und Außenwirkung

- Vertragliche Verpflichtung von Kunden, Lieferanten und sonstigen Geschäftspartnern auf die im Unternehmen geltenden Sicherheitsstandards ❑ ❑ ❑

5. Informationstechnik (IT)

Grundregeln

- Sicherstellen und Bewahren von Vertraulichkeit, Verfügbarkeit und Integrität der Daten und Systeme
- Dauerhafte IT-Sicherheitsprozesse initiieren
- Grundsatz von Besitz und Wissen einhalten
- Restriktive Rechteverwaltung

5.1 Erstellung eines IT-Sicherheitskonzepts

- Systematische Analyse und Planung
  - Struktur wie Know-how-Schutz Konzept (siehe Kapitel 1 - 4) ❑ ❑ ❑

	☑	⊟	⊘
● Hilfsmittel			
❍ Checklisten, Merkblätter, Richtlinien, Kriterienwerke	❑	❑	❑
❍ Auswahl geeigneter Kriterienwerke	❑	❑	❑
siehe hierzu:			
Initi@tive D21: IT-Sicherheitskriterien im Vergleich			
Ein Leitfaden der Projektgruppe			
IT-Sicherheitskriterien und IT-Grundschutz-Zertifikat/Qualifizierung			
❍ Tools	❑	❑	❑
BSI-Tools „IT-Grundschutz/GSTOOL“ und „sichere UNIX-Administration/USEIT“,			
CC-Toolbox, CobiT Advisor/CobiT Self Assessment			
❍ Sicherheitshandbücher/-richtlinien, Normen	❑	❑	❑
BSI-IT-Grundschutzhandbuch (IT-GSHB), BSI-IT-Sicherheitshandbuch (IT-SHB),			
ITSEC/Common Criteria (CC), ISO/IEC 17799, BS 7799, ISO 13335, ISO 9000 ff.,			
CobiT, Task Force sicheres Internet, FIPS 140			

5.1.1 Personeller Bereich

Personaleinsatz

● Trennung der Bereiche Sicherheit und Betrieb	❑	❑	❑

Systematische und qualifizierte Sicherheitsunterweisung

● Fachliche Aus-/Fortbildung	❑	❑	❑
● Anwenderschulung	❑	❑	❑
● Schulung der Administratoren	❑	❑	❑

5.1.2 Organisatorische Maßnahmen

Bestellung eines IT-Sicherheitsverantwortlichen

● Einbindung in die Organisation des (allgemeinen) Sicherheitsverantwortlichen	❑	❑	❑
● Zentraler Ansprechpartner in allen IT-Sicherheitsangelegenheiten (unternehmensweite Zuständigkeit)	❑	❑	❑
● Aufgabengerechtes Persönlichkeitsprofil	❑	❑	❑
● Fachliche Eignung (umfassende IT-Kenntnisse/Spezialkenntnisse IT-Sicherheit)	❑	❑	❑
● Aufgaben			
❍ Sicherheitscontrolling im IT-Bereich	❑	❑	❑
❍ Planung, Umsetzung, Kontrolle von IT-Sicherheitsmaßnahmen	❑	❑	❑
❍ Erstellung von IT-Grundschutz-/Geheimschutzdokumentationen	❑	❑	❑
❍ Analyse von IT-Sicherheitsvorfällen	❑	❑	❑

	☑	⊟	⊘
Funktions-/Aufgabentrennungen			
● Programmentwicklung, Informationsverarbeitung, Systemwartung	❑	❑	❑
● Test-/Produktionsbetrieb	❑	❑	❑
● Sicherheit, Betrieb, Datenschutz	❑	❑	❑
Bei komplexen Systemen ggf. Aufbau einer internen IT-Sicherheitsorganisation			
● Aufgaben			
❍ Schwachstellenanalyse	❑	❑	❑
❍ Notfall- und Krisensimulation	❑	❑	❑
❍ Analyse neuer Software/-verfahren auf Testsystemen	❑	❑	❑
❍ Erarbeitung von Notfallplänen	❑	❑	❑
❍ Durchführung von Planspielen	❑	❑	❑
❍ Durchführung von Penetrationstests, Sicherheits-Audits, Passwortanalysen	❑	❑	❑
❍ Zusammenarbeit mit privaten/öffentlichen CERTs (Computer Emergency Response Teams)	❑	❑	❑
Anweisungen und Empfehlungen			
● Detaillierte Organisations- und Arbeitsanweisungen (Benutzerrichtlinien) mit folgendem Inhalt:			
❍ Beschreibung des jeweiligen Verfahrens/IT-Systems	❑	❑	❑
❍ Verantwortung von Nutzern, Vorgesetzten, Benutzerservice, Administratoren, Sicherheitspersonal	❑	❑	❑
❍ Zuständigkeiten bei Beschaffung von Hard- und Software	❑	❑	❑
❍ Nutzung des jeweiligen Verfahrens/IT-Systems	❑	❑	❑
❍ Schutzmaßnahme jeweils beschreiben	❑	❑	❑
❍ Verantwortlichkeiten/Zuständigkeiten für Virenschutz und Sofortmaßnahmen	❑	❑	❑
❍ Verantwortlichkeiten/Zuständigkeiten für Datensicherung	❑	❑	❑
❍ Regelungen zum Umgang mit Verfahren/IT-System (dienstliche Nutzung, Lizenzbestimmungen, Datenträgerhandling, Aufbewahrung, Weitergabe, Löschung, Vernichtung, Dokumentation)	❑	❑	❑
❍ Internet- und E-Mail-Nutzung	❑	❑	❑
❍ Verbot des Einbringens privater/fremder Hard-/Software	❑	❑	❑
❍ Pflege, Wartung, Revision	❑	❑	❑
❍ Notfall-, Katastrophen-, Krisen- und Wiederanlaufplanung	❑	❑	❑
❍ Mitteilung über Behandlung von sicherheitsrelevanten Ereignissen	❑	❑	❑
❍ Protokollierung, Beweissicherung und Kontrollen	❑	❑	❑
Regelung von Verfahrensabläufen			
● Ausgabe von Arbeitsmaterial (Hardware, Software, Datenträger, Dokumentationen)			

	☑	⊟	⊘
❍ Ressourcenzuweisung nach Bedarf („soviel wie nötig, sowenig wie möglich“)	❑	❑	❑
❍ Quittung (Verbleibskontrolle)	❑	❑	❑
● Datenfernübertragung			
❍ Zugriffskontrolle für alle DFÜ-Verbindungen	❑	❑	❑
❍ Verschlüsselte Übertragung (Regelung der Verschlüsselungsverfahren)	❑	❑	❑
❍ Protokollierung	❑	❑	❑
❍ Fernwartung/Remote-Access-Zugänge sichern	❑	❑	❑
● Planung und Regelung von Datenzugriff und Datenfluss (Informationsaustausch)			
❍ Definition von Arbeitsgebieten	❑	❑	❑
❍ (Vertragliche) Regelung des Datenzugriffs/des Umgangs der Mitarbeiter mit den Daten	❑	❑	❑
❍ Regelung von Zuständigkeiten/Zugriffsrechten (Benutzerhierarchien: Aufgaben, Verantwortung, Kompetenzen, Benutzerkennung)	❑	❑	❑
❍ Erstellung/Weiterleitung von Verarbeitungsnachweisen an Auftraggeber	❑	❑	❑
● Datensicherung			
❍ Datensicherungskonzept (Back-Up-Strategie, Recovery-Konzept, Wiederanlaufplanung)	❑	❑	❑
❍ Auswahl/Kombination geeigneter Methoden (Volldatensicherung, inkrementelle Datensicherung, differentielle Datensicherung)	❑	❑	❑
❍ Auswahl geeigneter Sicherungsmedien (Bandlaufwerke, Wechselfestplatten, ZIP-Laufwerke, CD-ROM-/DVD-Brenner, USB-/Daten-Sticks etc.) und Datensicherungstools	❑	❑	❑
❍ Sichere interne und externe Aufbewahrung der Sicherungskopien von Betriebssystemen, Programmen und Anwendungsdaten	❑	❑	❑
❍ Prüfung der Backup-Medien (Funktionsfähigkeit, Inhalt, Stand)	❑	❑	❑
❍ Prüfung, inwieweit Datenbestand mit gesicherten Daten wiederhergestellt werden kann (regelmäßige Übung unerlässlich!)	❑	❑	❑
❍ Erstellung einer PC-/Boot-/Rettungs-/Notfalldiskette	❑	❑	❑
❍ BIOS (Basic Input/Output System) sichern und regelmäßig (sicher) updaten	❑	❑	❑
❍ Images erstellen	❑	❑	❑
● Umgang mit Datenträgern			
❍ Kennzeichnung, Aufbewahrung, Zugriffsregelung, Verwaltung, Versand, Archivierung, Löschung, Entsorgung von Datenträgern	❑	❑	❑
❍ Überwachung von Transport und Vernichtung	❑	❑	❑
❍ Datenlöschung durch (mehrfaches) vollständiges Überschreiben (physikalisch z.B. BSI-Tool VS-CLEAN) oder mechanische Zerstörung der Datenträger	❑	❑	❑

	☑	⊟	⊘
● Dokumentationswesen			
❍ IT-Infrastrukturen (Hardware und Systeme), Vernetzung	❑	❑	❑
❍ Abläufe und Zugänge	❑	❑	❑
❍ Systemeinstellungen und -Parameter	❑	❑	❑
❍ Geräte (Nachweis über eingesetzte und ausgegebene Geräte)	❑	❑	❑
❍ Software (Applikationen, Eigenentwicklungen, Versionen, Updates, Lizenzen)	❑	❑	❑
❍ Kommunikationsinfrastrukturen (Leitungen, Leitungsführung, Verteiler, Verlegesysteme, Hardwareeinrichtungen)	❑	❑	❑
❍ Informationsbestände und Datenbanken	❑	❑	❑
❍ Rechteverwaltung/-vergabe, Nutzerdokumentation	❑	❑	❑
● Zugang zum Internet			
❍ Oberster Grundsatz: Alles, was nicht ausdrücklich erlaubt wurde, ist verboten!	❑	❑	❑
❍ Analyse aller Prozesse, die zu einer Internetverbindung führen können	❑	❑	❑
❍ Analyse entstehender Kommunikationsbeziehungen (uneingeschränkt zulässig, eingeschränkt zulässig, unzulässig)	❑	❑	❑
❍ Risikoanalyse, Datenschutz- und Datensicherheitskonzept (Security Policy)	❑	❑	❑
❍ Auswahl wirklich benötigter Dienste, Abschalten und ggf. Löschen ungenutzter Programme	❑	❑	❑
❍ Untersuchung der Schwachstellen der verbliebenen Dienste	❑	❑	❑
❍ Entwicklung von Sicherheitskonzepten und Benutzerrichtlinien (dienste-, protokoll- und serviceorientiert)	❑	❑	❑
❍ Erstellung eines E-Mail-„Knigge“	❑	❑	❑
❍ Zentrales IT- und IT-Sicherheits-Management einrichten	❑	❑	❑
❍ Sicherung von Servern und Clients	❑	❑	❑
❍ Sichere Konfiguration (Browser) und sicherer Betrieb (Web-Server)	❑	❑	❑
❍ Abschaltung der automatischen Ausführung aktiver Inhalte im eingesetzten Web-Browser	❑	❑	❑
❍ Richtiger und vollständiger Einsatz der genutzten Hard-/Software (Vermeidung von Konzeptions-, Konfigurations-, Administrations- und Installationsfehlern)	❑	❑	❑
❍ Protokollierung von Verbindungen und Nutzerdaten	❑	❑	❑
❍ Schutz vor Computerviren, Würmern, Trojanern (aktuelle Virenschutz-Software/regelmäßige Updates)	❑	❑	❑
❍ Schutz vor Schadsoftware (ausführbare Programme mit Schadfunktion)	❑	❑	❑
❍ Schutz vor verteilten Denial of Service Angriffen (DDoS)	❑	❑	❑
❍ Einsatz sicherer Authentisierungsverfahren (Challenge/Response-Verfahren, Einmalpasswörter)	❑	❑	❑
❍ Starker Integritätsschutz z.B. durch Einsatz digitaler Signaturen	❑	❑	❑

	☑	⊟	⊘
❍ Einsatz von Verschlüsselungshard- und/oder -software	❑	❑	❑
❍ Nutzung von Anonymisierungsdiensten/-software	❑	❑	❑
❍ Umfangreiche Sensibilisierung, Information und Schulung der Administratoren und Nutzer	❑	❑	❑
❍ Durchführung von Sicherheits-, System- und Penetrationstests	❑	❑	❑
❍ Absicherung durch eine strukturierte, permanent gepflegte Internet-Firewall (Bildung von „Sicherheitsinseln“, Abschottung sowohl gegen interne als auch externe Angriffe in und aus dem Netz), multi-homed Application Gateway	❑	❑	❑
❍ Dezidierte Erarbeitung und Implementierung von Filterregeln (Nutzung von Denie- oder Access-Listen), Paketfilter, gesicherte Routingtabellen, Spam-Filter	❑	❑	❑
❍ Zugriffsschutz (Access Security)/zentraler Virenschutz (Content Security)	❑	❑	❑
❍ Einsatz von Intrusion Detection-/Intrusion Response-Systemen	❑	❑	❑
❍ Einsatz von Tools zur Erkennung/Behandlung/Dokumentation/Beweissicherung von Angriffen (forensische Software)	❑	❑	❑
● Schutzmaßnahmen gegen kompromittierende Abstrahlung			
❍ EMV-Schutzkonzept	❑	❑	❑
❍ BSI-Zonenmodell: Einsatz von Zonen-Geräten innerhalb festgelegter - vermessener - Grenzen (COMSEC-Bereichsgrenzen)	❑	❑	❑
❍ Erneute Prüfung/Vermessung nach Wartung, Reparatur und möglichem unberechtigtem Zugriff	❑	❑	❑
● Kontrollen (vgl. § 9 i.V. Anl. zu § 9 Satz 1 Bundesdatenschutzgesetz (BDSG), § 9 Landesdatenschutzgesetz (LDSG)			
❍ Regelmäßig, in unregelmäßigen Zeitabständen, Stichproben (Funktion, Zweck, Effizienz, Wirtschaftlichkeit)	❑	❑	❑
● Netzwerke			
❍ Systematische Planung von Netzwerken und ihren Topologien (Vermeidung von „Wildwuchs“), Regelung der Kommunikationsbeziehungen	❑	❑	❑
❍ Bildung in sich geschlossener und gesicherter Netze (Intranets, Closed-User-Groups, SINA-VPN) und Abschottung gegen offene, fremde, unsichere, externe Netze (z.B. durch Firewalls)	❑	❑	❑
❍ Einsatz zertifizierter Betriebssysteme und geeigneter Filter, Schutz gegen Aufschaltung Dritter	❑	❑	❑
❍ Beachtung und konsequente Umsetzung der sog. 3-A/3-W-Regel:			
◆ Authentikation: Wer bin ich (Prüfung der Berechtigungen)	❑	❑	❑
◆ Authorisation: Was darf ich (Rechtezuweisung an befugte Nutzer)	❑	❑	❑
◆ Accounting: Was habe ich getan (Protokollierung, Dokumentation, Beweissicherung)	❑	❑	❑

	☑	⊖	⊘
❍ Schutz externer Einwahlmöglichkeiten vor unautorisiertem Zugriff	❑	❑	❑
❍ Benutzertrennung/Authentisierung auf Anwendungsebene bei multi-User-Clients	❑	❑	❑
❍ Einsatz von Diskless-PCs	❑	❑	❑
❍ CERT Advisorys/Sicherheitsbenachrichtigungen abonnieren und zeitnah umsetzen	❑	❑	❑
❍ Sicherheit im Funk-LAN (WLAN) (s. BSI-Broschüre „Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte“)	❑	❑	❑
◆ Sichere Konfiguration und Administration der Funkkomponenten	❑	❑	❑
◆ Aktivierung der Basisschutzmaßnahmen nach IEEE 802.11/IEEE 802.11i (Vergabe eines Netzwerknamens - ESSID/SSID -, Filterung von MAC-Adressen, WEP-Verschlüsselung, Integritätsschutz, Authentisierung)	❑	❑	❑
◆ Zusätzliche Sicherheitslösungen implementieren (VPN, digitale Zertifikate/ PKI-Infrastrukturen, Firewall, IDS/IDR, mobile Clients sichern)	❑	❑	❑
● Outsourcing			
❍ Adaptierung und ggf. Anpassung der IT-Sicherheitsmaßnahmen des Auftraggebers auf die Fremdfirma (Outsourcing-Dienstleister)	❑	❑	❑
❍ Regelung des Remote-Access-Zugriffs auf Ressourcen und Systeme des Auftraggebers	❑	❑	❑
❍ Einsatz von geeigneten Authentisierungsverfahren	❑	❑	❑
❍ Nutzung von Verschlüsselung	❑	❑	❑
❍ Protokollierung des Datenverkehrs	❑	❑	❑
● Passwortregeln			
❍ Vgl. Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zum „Umgang mit Passwörtern“ (http://www.baden-wuerttemberg.datenschutz.de/material-lfd/passwort.html)	❑	❑	❑
❍ Vergabe eines Zusatzpassworts für besonders kritische Anwendungen/Daten	❑	❑	❑
❍ Passwort des Systemverwalters/Administrators für den Vertretungsfall versiegelt und gesichert aufbewahren; ggf. Einsatz nur nach dem Vier-Augen-Prinzip (Sicherheit und Betrieb)	❑	❑	❑
● Sicherheitsmanagement			
❍ Eigene Benutzerkennung mit befristeter Geltungsdauer	❑	❑	❑
❍ Verschlüsselung der Datei der Passwörter und Benutzerkennungen	❑	❑	❑
❍ Limitierung/Protokollierung von Anmeldefehlversuchen	❑	❑	❑
❍ Anzeige der letzten korrekten Anmeldung	❑	❑	❑
❍ Zeitliche Begrenzung der Zugangsberechtigung	❑	❑	❑
❍ Verhinderung der Anmeldung mit Funktionstaste („auto-log-in“)	❑	❑	❑
❍ Automatisches Sperren oder Abmelden des PC nach längerer Nichtbenutzung	❑	❑	❑

	☑	⊖	⊘
❍ Zusätzliche Sicherungsmaßnahmen bei Verbindung des Systems mit öffentlichen oder fremden Netzen	❑	❑	❑
❍ Zusätzlicher Einsatz von Chipkarten, Smartcards, Token, biometrischen Verfahren	❑	❑	❑
❍ Einschränkung von Administratorenrechten und Benutzer-/Programmprivilegien auf das unbedingt erforderliche Maß	❑	❑	❑
● Auftragsverfahren für Programm- und Verfahrensänderungen	❑	❑	❑
❍ Beschränkung auf vorgegebene Veränderungen/Einhaltung von Veränderungsverboten	❑	❑	❑
❍ Vergabe nur an zuverlässige Fremdfirmen	❑	❑	❑
● Protokollierungsverfahren/Beweissicherung			
❍ Stör-/Fehlerprotokolle	❑	❑	❑
❍ Permanente Protokollierung der Systemaktivitäten	❑	❑	❑
❍ Automatische Protokollierung sicherheitsrelevanter Vorgänge	❑	❑	❑
❍ Regelmäßige Auswertung der Protokolle unter Zuhilfenahme geeigneter Analysetools	❑	❑	❑
❍ Einsatz forensischer IT-Analysesoftware (Dokumentation, Analyse, Beweissicherung und graphische Darstellung von Sicherheitsverstößen)	❑	❑	❑
● Verhalten im Sicherheitsfall			
❍ Festlegung von Ansprechpartnern	❑	❑	❑
❍ Bereitstellung von qualifiziertem Personal zur Schadenserkennung/-bekämpfung	❑	❑	❑
❍ Beweissicherung	❑	❑	❑
❍ Notfall- und Maßnahmenpläne (Hackerangriff, Virenbefall, Katastrophen)	❑	❑	❑
❍ Wiederanlaufplanung	❑	❑	❑
● Schutzmaßnahmen gegen Softwaremanipulationen			
❍ Zulassungs- und Zertifizierungsverfahren für (standardisierte) Hard- und Software (einheitliche und zentralisierte Genehmigungsverfahren)	❑	❑	❑
❍ Einrichten von Clearingstellen für Software (Tests von individueller Software)	❑	❑	❑
❍ Erhaltung des Originalzustandes (Code-Inspektionen, Funktionsprüfungen, Programmtests), aber: Anpassung der Standardeinstellungen	❑	❑	❑
❍ Dokumentation von Installationen/Systemen/Eigenentwicklungen	❑	❑	❑
❍ Erstellen von Images	❑	❑	❑
❍ Regelmäßiger Einsatz aktueller Viren-Such- und Entfernungsprogramme	❑	❑	❑
❍ Verhaltensregeln bei Virenbefall (Erhebungsbogen: betroffenes System, Feststellung, Art der Infizierung, getroffene Schutzmaßnahmen, Information anderer Betroffener, Schätzung des Aufwands)	❑	❑	❑
❍ Filterung von ausführbaren Programmen mit eventueller Schadfunktion	❑	❑	❑

- Telearbeit (z.B. Tele-Heimarbeit, alternierende Telearbeit, Satellitenbüro, Nachbarschaftsbüro, mobile Telearbeit)
  - Beteiligung der Verantwortlichen (Betriebs-/Personalrat, Personalabteilung, IT-Sicherheitsverantwortlicher, Datenschutzbeauftragter, Administratoren, Vorgesetzte, Telearbeiter) ❑ ❑ ❑
  - Sorgfältige Personalauswahl ❑ ❑ ❑
  - Vereinbarung von Arbeitszeit- und Vertreterregeln ❑ ❑ ❑
  - Schulung, Betreuung des Telearbeiters und seiner IT-Konfiguration ❑ ❑ ❑
  - Sicherheitsmaßnahmen zum Schutz von Hard-/Software und Daten (Diebstahlschutz; Virenschutz; Zugangs- und Zugriffsschutz; Aufbewahrung, Transport, Löschung, Vernichtung, Entsorgung von Datenträgern, Speichermedien und Akten; Verbot der Nutzung von Fremdsoftware und -programmen) ❑ ❑ ❑
  - Auswahl geeigneter DFÜ-Komponenten (z.B. ISDN-Karten und -Router, Modem, Chipkarten), Deaktivierung nicht benötigter Leistungsmerkmale ❑ ❑ ❑
  - Einsatz sicherer (geprüfter) Kommunikationssoftware ❑ ❑ ❑
  - Korrekte Installation der Komponenten und Nutzung vorhandener oder zusätzlicher Sicherheitsfunktionalitäten ❑ ❑ ❑
  - Einsatz von sicheren Authentisierungsverfahren (z.B. CLIP/COLP, Callback-Funktion, PAP/CHAP ❑ ❑ ❑
  - Verschlüsselung der übertragenen Daten ❑ ❑ ❑
  - Einsatz von VPN-Technologien ❑ ❑ ❑

- Schutz digitaler Telekommunikationsanlagen
  - Absicherung der Anlage(n), d.h. Zugang, Zutritt, Elementarschäden ❑ ❑ ❑
  - Absicherung der Anlagenschnittstellen und Wartungszugänge, d.h. Sicherung der internen und externen Fernwartung ❑ ❑ ❑
  - Nicht benötigte Leistungsmerkmale deaktivieren oder entfernen ❑ ❑ ❑
  - Regelmäßiges Backup der Anlagenkonfiguration erstellen ❑ ❑ ❑
  - Zugang/Zugriff zum System absichern ❑ ❑ ❑
  - Optionaler Einsatz eines D-Kanal-Filters ❑ ❑ ❑
  - Verschlüsselung der B-Kanäle ❑ ❑ ❑
  - Protokollierung aller Maßnahmen ❑ ❑ ❑
  - Regelmäßige Revision der Anlagenkonfiguration (Soll-Ist-Vergleich) ❑ ❑ ❑
  - Passwortschutz der Endgeräte ❑ ❑ ❑
  - Information der Nutzer über mögliche Gefahren und Details der Bedienung (Warnanzeigen, Symbole, Töne) ❑ ❑ ❑
  - Regelung der Wartungs- und Reparaturarbeiten ❑ ❑ ❑

- Wartung/Systempflege/Benutzerservice
  - Regelmäßige Wartung aller Komponenten durch autorisiertes Fachpersonal ❑ ❑ ❑

	☑	⊟	⊘
❍ Rechtzeitiges Einspielen von Sicherheitspatches/-updates	❑	❑	❑
❍ Fernwartung: Verzicht oder individuelle Sicherheitsmaßnahmen (Zugriff nur von der berechtigten Stelle aus, Call-back-Verfahren, physikalischer Verbindungsaufbau im Bedarfsfall, Verschlüsselung)	❑	❑	❑
❍ Wartungs- und Reparaturarbeiten nur unter Kontrolle des IT-Systemverantwortlichen durch qualifiziertes Fachpersonal	❑	❑	❑
❍ Bei externen Reparaturen: physikalische Löschung vertraulicher Daten auf der Festplatte oder Entfernung/mechanische Vernichtung der Speicher	❑	❑	❑
❍ Anwenderbetreuung	❑	❑	❑

5.1.3 Technische Maßnahmen

Hardware

● Zugangs- und Zugriffsschutz für Systeme (Server, Konsolen, Clients) und Datenträger (z.B. mechanische und elektronische Schlösser, Tastatur-/Festplattenverriegelung, Gehäuseverplombung, Identifikationskarte, Chipkarte, Einsatz von Thin-Clients)	❑	❑	❑
● Einsatz abstrahlarmer Geräte	❑	❑	❑
● Versiegelung von Gehäusen und nicht genutzten/offenen Schnittstellen	❑	❑	❑
● Gewährleistung der Stromversorgung (unterbrechungsfreie Stromversorgung, Netzersatzanlage, Überspannungsschutz)	❑	❑	❑
● Komponentenspiegelung	❑	❑	❑
● Absicherung der aktiven und passiven Netzkomponenten	❑	❑	❑
● (Automatische) Verschlüsselung von Daten (Festplatten, Disketten, DFÜ)	❑	❑	❑
● Sicherung der IT-Systeme gegen Diebstahl/unbefugte Nutzung	❑	❑	❑

Software

● Einsatz zertifizierter Softwareprodukte	❑	❑	❑
● Einsatz von Sicherheitssoftware/Virenschutzprogrammen	❑	❑	❑
● Nutzung der angebotenen Sicherheitsfunktionen (Verpflichtung zur Nutzung)	❑	❑	❑
● Vermeidung von Konzeptions-, Installations-, Konfigurationsfehlern	❑	❑	❑

5.1.4 Infrastruktur

Gebäude/Räume

● Kontrollierter Zugang zum Gebäude, Rechenzentrum und zu sensiblen Unternehmensbereichen	❑	❑	❑
● Bauliche, mechanische, (elektro-)technische und ggf. personelle Sicherungsmaßnahmen	❑	❑	❑
● Verhinderung der Erkennbarkeit von IT-Einrichtungen durch Außenstehende; ggf. Veränderung des Standorts	❑	❑	❑
● Zugangssicherung (Closed-shop-Betrieb)	❑	❑	❑

Kabel

- Verkabelungs- und EMV-Schutzkonzept ❑ ❑ ❑
- Strukturiertes Verkabelungskonzept nach DIN EN 50 173 ❑ ❑ ❑
- Verwendung geeigneter Kabeltypen und geschirmter Anschlussdosen ❑ ❑ ❑
- Absicherung der Kabelinfrastruktur, Verlegesysteme und Verteiler (HUBs) ❑ ❑ ❑
- Verlegung der DV-Kabel mit ausreichendem Abstand zu anderen parallel geführten Leitungen ❑ ❑ ❑

6. Zusammenarbeit mit Fremdfirmen

Grundregeln

- Sorgfältige Auswahl der Geschäftspartner
- Aufbau gegenseitigen Vertrauens
- Geschäftspartner ggf. in das eigene Sicherheitssystem integrieren
- Schwachstellen-/Risikoanalyse der Geschäftsverbindungen

6.1 Auswahlkriterien

- Einstellung der Unternehmensführung zum Know-how-Schutz ❑ ❑ ❑
- Bereits vorhandene Regelungen/Erfahrungen im Umgang mit vertraulichen Informationen ❑ ❑ ❑
- Personelle und materielle Maßnahmen zum Schutz vor illegalem Informationsabfluss ❑ ❑ ❑
- Schutz von Neuentwicklungen ❑ ❑ ❑
- Konkurrenzsituation ❑ ❑ ❑
- Mitgliedschaft in anerkannten Gremien/Fachverbänden ❑ ❑ ❑
- Referenzenliste ❑ ❑ ❑
- Geschäftsverbindungen in Staaten mit besonderen Sicherheitsrisiken[3] ❑ ❑ ❑
- Firmenbeteiligung aus Risikoländern (Besitz-/Kapitalverhältnisse) ❑ ❑ ❑

6.2 Vertragsverhältnis

6.2.1 Vertragliche Vereinbarungen

- Zusicherung der Einhaltung von Sicherheitsstandards ❑ ❑ ❑
- Verpflichtung zur Geheimhaltung ❑ ❑ ❑

[2] Staatenliste siehe Anhang in den „Handlungsempfehlungen".

	☑	⊟	⊘
● Vergleichbare Sicherheitsanforderungen an das Fremdpersonal	❑	❑	❑
● Konsequenzen bei Sicherheitsverstößen	❑	❑	❑
● Geschäftsabwicklung durch Fremdfirma nur mit ausgewähltem Personal (keine Leiharbeitnehmer)	❑	❑	❑
● Sicherstellung von weitergegebenem/auftragsgemäß erarbeitetem Know-how im Falle eines Konkurses/Vergleichs	❑	❑	❑

6.2.2 Auftragsabwicklung

● Gegenseitige Unterrichtung über spezifische Sicherheitsmaßnahmen und -vorkommnisse	❑	❑	❑
● Ansprechpartner benennen	❑	❑	❑
● Kundenspezifische Projektentwicklungen in gesicherten separaten Einzelräumen	❑	❑	❑
● Regelmäßige Kontrollen über die Einhaltung der Sicherheitsanforderungen	❑	❑	❑

6.2.3 Einsatz von Fremdkräften im eigenen Unternehmen

● Identische Sicherheitsanforderungen analog dem eigenen Personal	❑	❑	❑
● Spezifische Arbeitsbedingungen (z.B. Sonderausweis, Begleitung/Aufsicht, Zugangs-/Zutrittsbeschränkungen)	❑	❑	❑

6.3 Sicherheitscontrolling

Grundregeln

- ➲ Zielvereinbarungen regelmäßig analysieren und kontrollieren
- ➲ Laufende Überprüfung der eingesetzten Mittel

● Wirksamkeit des Schutzkonzeptes	❑	❑	❑
● Realisierung der Schutzziele	❑	❑	❑
● Personelle, organisatorische und technische Sicherheitsmaßnahmen im eigenen Unternehmen	❑	❑	❑
● Auswirkungen der Fremdvergabe von Leistungen (Outsourcing) auf das Gesamtkonzept Sicherheit	❑	❑	❑

Entdeckung/Behandlung von Sicherheitsfällen

7. Auswertung von Indikatoren

Grundregeln

- ➲ Permanente Auswertung von Informationen zum Know-how-Schutz
- ➲ Erstellen von Umfeld- und Marktanalysen
- ➲ Vom Alltagsgeschehen abweichende Auffälligkeiten beachten

7.1 Personenbezogene Auffälligkeiten - Schwachstelle Mensch

	☑	⊖	⊘
● Frustration, Unzufriedenheit im Beruf/am Arbeitsplatz	❑	❑	❑
● Besondere Neugier, auffälliger Arbeitseifer, nicht nachvollziehbares Interesse an Dokumentationen und Berechtigungen	❑	❑	❑
● Überqualifikation	❑	❑	❑
● Vorschriftswidriges Verhalten am Arbeitsplatz	❑	❑	❑
● Besitz/Nutzung von Spionagehilfsmitteln (z.B. private Film-/Foto-/Diktiergeräte, Foto-Handys etc.) am Arbeitsplatz	❑	❑	❑
● Auffällige/nicht plausible Verbesserung der finanziellen Situation, aufwändiger Lebensstil, Anzeichen für Bestechlichkeit	❑	❑	❑
● Anzeichen für menschliche Schwächen	❑	❑	❑
● Nicht eindeutig geklärter beruflicher Werdegang	❑	❑	❑
● Abnehmende bzw. fehlende Identifizierung mit dem Unternehmen oder dessen Zielen	❑	❑	❑
● Auffälligkeiten im persönlichen Umfeld (einschlägige Äußerungen - auch von Familienangehörigen - in der Öffentlichkeit)	❑	❑	❑
● Dubiose Kontakte zu Vertretungen ausländischer Staaten/Konkurrenzunternehmen	❑	❑	❑
● Reisen und Aufenthalte in Staaten mit besonderen Sicherheitsrisiken	❑	❑	❑
● Herkunft aus Ländern mit besonderen Sicherheitsrisiken (z.B. Repräsentanten/Dolmetscher)	❑	❑	❑

7.2 Unternehmensbezogene Auffälligkeiten

● Nicht erklärbarer Auftrags- bzw. Umsatzrückgang, Verlust von Marktanteilen, auffallendes Konkurrenzverhalten	❑	❑	❑

		☑	⊟	⊘
●	Wettbewerbsnachteile bei Ausschreibungen	❑	❑	❑
●	Angebot identischer/vergleichbarer Produkte bei Konkurrenzunternehmen	❑	❑	❑
●	Offensichtlicher Know-how-Verlust	❑	❑	❑

7.3 Methodische Auffälligkeiten beim Geschäftspartner

●	Verschleierung des eigentlichen Auftraggebers bzw. Geschäftsziels (Verwendungszweck)	❑	❑	❑
●	Illegale Weitergabe von ABC-Waffentechnik und deren Herstellungsmitteln, Trägertechnologien, konventionellen Kriegswaffen und deren Nebenprodukten an Krisenländer außerhalb der NATO	❑	❑	❑
●	Vorsätzlich falsche Zolldeklarationen	❑	❑	❑
●	Warentransfer unter Umgehung des Bundesausfuhramtes/der Zollbehörden	❑	❑	❑
●	Fälschung von Endabnehmerbescheinigungen	❑	❑	❑
●	Umleitung von Warensendungen über Drittländer mit Hilfe internationaler Speditionen/ausländischer (staatl.) Fluggesellschaften	❑	❑	❑
●	Hinweis auf verdeckte Materialbeschaffung	❑	❑	❑

7.4 Risikofaktoren, die den Verlust von Know-how begünstigen

●	Beschäftigung nicht einschätzbaren (Fach-)Personals (z.B. längere Auslandsaufenthalte) in sensiblen Bereichen	❑	❑	❑
●	Mangelhafte Sicherung sensitiver Bereiche (z.B. unbeaufsichtigte Besucher etc.)	❑	❑	❑
●	Zusammenarbeit mit (ausländischen) Fremdfirmen im Forschungs-/Entwicklungs-/EDV-Bereich	❑	❑	❑
●	Abhängigkeit von staatlich kontrollierten Produktions- und Handelseinrichtungen des Auslands (länderspezifisches Zertifikationssystem)	❑	❑	❑
●	Verbindungen zu staatlichen Einrichtungen von Ländern mit besonderen Sicherheitsrisiken (z.B. Konsulate/Botschaften)	❑	❑	❑
●	Zusammenarbeit mit staatlich gelenkten Lehr- und Forschungsanstalten im Ausland	❑	❑	❑

8. Vorgehen im Sicherheitsfall

Grundregeln

- ➲ Unverzügliche Unterrichtung des Sicherheitsverantwortlichen bzw. der Geschäftsleitung
- ➲ Beachtung aller - auch anonymer und unbedeutend erscheinender - Hinweise
- ➲ Vertrauliche Behandlung zusichern und einhalten
- ➲ Keine Vertuschung von Auffälligkeiten (z.B. aus Imagegründen)

	☑	⊖	⊘
● Sicherung/Dokumentation von Spuren und Beweismitteln	❑	❑	❑
● Begrenzung des Mitwisserkreises; Verpflichtung zur besonderen Verschwiegenheit	❑	❑	❑
● Analyse relevanter Unterlagen und Informationen			
❍ Sachverhaltsprüfung	❑	❑	❑
❍ Prüfung der Personalakten	❑	❑	❑
❍ Suche nach Auffälligkeiten (Umfeld, Auslandskontakte, Lebensstil, Urlaubs- und Freizeitverhalten verdächtiger Personen)	❑	❑	❑
● Rechtzeitige und vertrauensvolle Zusammenarbeit mit externen Spezialisten			
❍ Sicherheitsbehörden/Sicherheitsgremien in der Wirtschaft	❑	❑	❑
❍ Sicherheitsberater	❑	❑	❑
❍ Rechtsanwälte	❑	❑	❑
❍ Detekteien	❑	❑	❑
● Nachträgliche Auswertung eines abgeschlossenen Sicherheitsfalles			
❍ Aufspüren weiterer Schwachstellen/Risiken sowie deren Ursachen	❑	❑	❑
❍ Bewertung der Sicherheitssysteme	❑	❑	❑
❍ Definition zukünftiger Schwerpunkte/Prioritäten	❑	❑	❑
❍ Erstellung/Fortschreibung des Schutzkonzeptes	❑	❑	❑

Landesamt für Verfassungsschutz
Baden-Württemberg

Taubenheimstraße 85 A · 70372 Stuttgart · Telefon 0711/ 95 44-00 · Fax 0711/95 44-444

www.verfassungsschutz-bw.de

lfv-bw@t-online.de