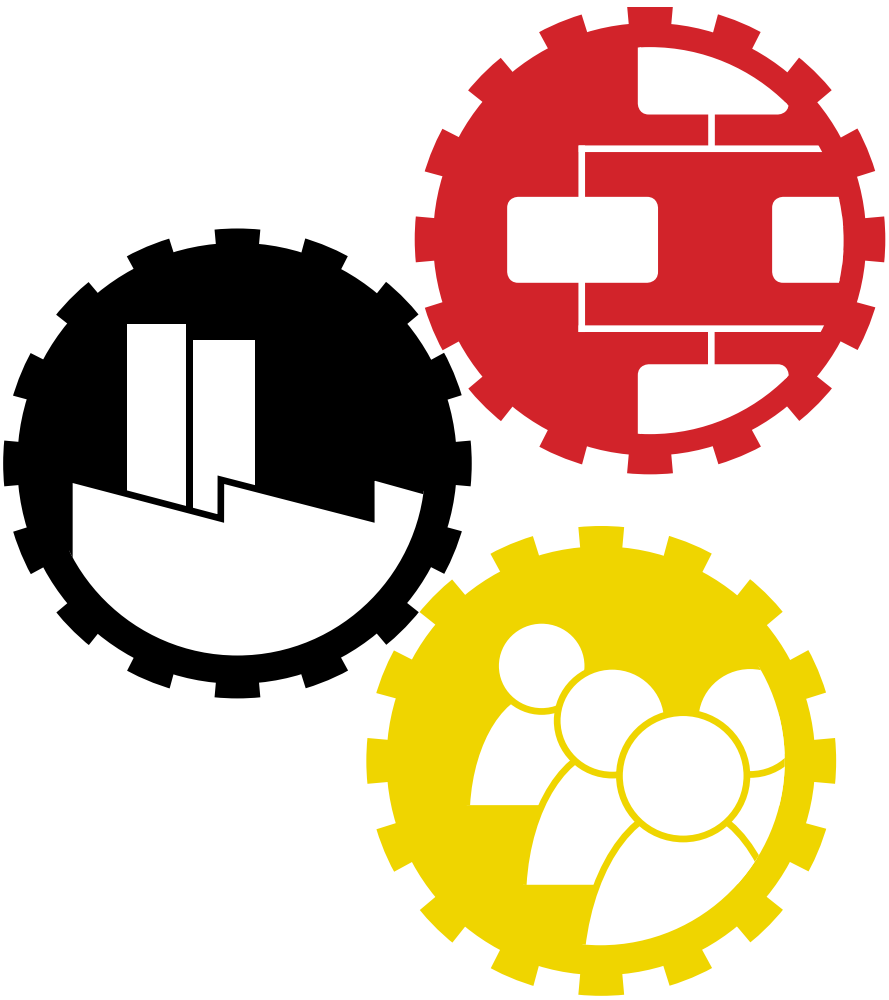
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

Wirtschaftsgrundschutz

Baustein PD1 Produkt- und Know-how-Schutz



1 Relevanzentscheidung für diesen Baustein

1. **Kontakt zu Externen**: Betreibt die Institution einen (intensiven) Wissens- und Informationsaustausch mit externen Partnern (Kunden, Lieferanten, Wettbewerbern, externen Dienstleistern)?
2. **Länderrisiken**: Hat die Institution Geschäftssitze in Ländern oder Regionen mit erhöhter Produktpirateriegefahr oder betreibt die Institution Geschäftsbeziehungen zu Partnern aus solchen Ländern?
3. **Kritisches Know-how**: Verfügt die Institution über Wissen und Informationen, die mit Wettbewerbsvorteilen verbunden sind?
4. **Finanzielle Auswirkungen**: Sind als Folge eines potentiellen Angriffs schwerwiegende finanzielle Folgen zu erwarten?
5. **Vorgeschichte**: Ist die Institution in der Vergangenheit bereits Opfer von Produktpiraterieangriffen gewesen?
6. **Mitarbeiterprofil**: Beschäftigt die Institution Mitarbeiter zeitlich beschränkt (z. B. Leiharbeiter, Praktikanten)?

Begriff Produktpiraterie

Dieser Baustein hat insbesondere im Kontext von Produktpiraterie eine sehr hohe Relevanz. Der Begriff „Produktpiraterie“ wird hier **sowohl** für **Plagiate als auch** für **Fälschungen** verwendet. **Plagiate ahmen nach**, bei **Fälschungen** wird ein **Produkt mit** einer **fremden Urheberschaft gekennzeichnet**, wie z. B. bei Markenpiraterie. Für betroffene Institutionen, deren Produkte oder Marken kopiert oder gefälscht werden[1], geht **Produktpiraterie weltweit mit gravierenden**

[1] Vergleiche Baustein ÜA4 Krisenmanagement.

wirtschaftlichen Auswirkungen einher. Dazu zählen insbesondere die folgenden:

- direkt entgangene Umsätze bzw. Gewinne
- Imageschädigung durch minderwertige Piraterieprodukte
- Haftungsklagen gegen die Originalhersteller

Plagiate werden häufig in vollem Bewusstsein erworben, wobei sich die Kunden der Nachteile bewusst sind. Der Käufer profitiert jedoch nur auf den ersten Blick von Plagiaten und Fälschungen. Diese können zwar meist günstiger erworben werden, aber dafür sind häufig **Abstriche bei Garantie und Haftung des Herstellers** hinzunehmen sowie bei der **Qualität**, was **Folgekosten und** sogar **Gefahren für Leib und Leben** verursachen kann. Besonders kritisch für den Kunden ist der unbewusste Erwerb von Plagiaten. Aufgrund des gestiegenen Organisationsgrads der Fälscher und der hohen Gewinne, die mit Piraterieprodukten erzielt werden können, ist die **Gefahr verhältnismäßig groß**. In einer Studie des VDMA von 2016 gaben mehr als zwei Drittel aller befragten Institutionen an, von Produktpiraterie betroffen zu sein.[2] Der geschätzte **Schaden**, der **2015** für deutsche Institutionen entstand, beläuft sich auf **7,3 Milliarden €**.

Inhalt und Zielsetzung dieses Bausteins

Dieser Baustein liefert Verantwortlichen einer Institution eine **Hilfestellung** für die **strukturierte Vorgehensweise** zur Erreichung eines **angemessenen Produkt- und Know-how-Schutzes** und zeigt die **wesentlichen Grundsätze** für das Etablieren eines **angemessenen Management- und Regelsystems** für diesen Bereich auf.

[2] Verband Deutscher Maschinen- und Anlagenbau: Studie Produktpiraterie 2016.

2 Beschreibung

Zur **Sicherung** ihrer **Wettbewerbsvorteile** sollten Institutionen ihre **Produkte und Prozesse sowie** ihr **Wissen durch** den Einsatz moderner **Produktschutztechnologien** und durch Maßnahmen zum Know-how-Schutz **schützen**. Hierfür müssen zunächst **Ziele, Zweck, Zielgruppen und Prozessintegration** bestimmt werden. Ein erklärtes Institutionsziel sollte es sein, **Strategien** zu **entwickeln, die** die **Gefährdung durch Produktpiraterie eliminieren oder** zumindest so weit wie möglich **reduzieren**. Dies erfordert **koordinierte technische und organisatorische Maßnahmen auf allen Ebenen des Produktlebenszyklus** und über alle Abteilungen und Prozesse der Institution hinweg. Die Maßnahmen können in **präventive und reaktive** unterteilt werden. Präventive Schutzmaßnahmen setzen vor Eintritt eines Schadenfalls ein, reaktive Maßnahmen, wenn Plagiate[3] bereits auf dem Markt sind und die damit einhergehenden Verluste minimiert werden sollen.

Ansatzpunkte für Produktpiraterie sind einerseits die fertigen Produkte des Originalherstellers, die z. B. mittels **Reverse Engineering** analysiert werden können. Andererseits werden zur Erlangung von Wissen über bereits auf dem Markt sowie noch in der Entwicklung befindliche Produkte **frei zugängliche oder auf illegale Weise erlangte Informationen** genutzt. Hierzu gehören u. a. das **Abwerben von Mitarbeitern** sowie Industriespionage. Durch die **vielfältigen Beziehungen zwischen Institutionen**, die heutzutage in **komplexe Wertschöpfungsnetzwerke** eingebunden sind, werden in unterschiedlicher

[3] Ein Glossar mit relevanten Begriffen findet sich zum Beispiel im VDMA-Leitfaden (vgl. VDMA 2016).

Intensität **Informationen und Wissen ausgetauscht**, unter Umständen auch **Firmengeheimnisse**. Ein Beispiel hierfür ist der **Informationsaustausch über Produkteigenschaften und -spezifikationen entlang der Lieferkette** mit **Lieferanten, Logistikdienstleistern und Kunden**, meist auch unter Beteiligung von OEMs (Original Equipment Manufacturer). Es entstehen somit diverse Gelegenheiten zum vorsätzlichen oder fahrlässigen Verlust von Betriebsgeheimnissen, die sowohl durch den Faktor Mensch als auch durch Unzulänglichkeiten auf der organisatorischen oder technischen Ebene verursacht werden.

Instrumente des technischen Plagiatschutzes

Unentbehrlich für die Institution ist in diesem Zusammenhang der **technische Plagiatschutz**. Um **bei Rechtsstreitigkeiten Originalprodukte von Fälschungen unterscheiden und Produkte eindeutig** der eigenen Produktion **zuordnen** zu **können**, sind die **folgenden Instrumente** unabdingbar[4]:

- Produktkennzeichnungen
- Herstellernachweise
- Detektion/Authentifizierung (zur automatisierten Erfassung und Prüfung von Produktkennzeichnungen)
- Tracking- und Tracingsysteme (zur Überwachung und Überprüfung der Sendungen/Lieferungen in der Logistikkette)
- embedded Security (Informationssicherheit für eingebettete Systeme[5] durch Vermeidung unbefugter Manipulationen bei der Beschaffung, Übertragung, Bearbeitung und Speicherung von Informationen)
- technischer Know-how-Schutz

Der **technische Schutz – Kennzeichnungen durch Hologramme, RFID, Mikroschriften** u. ä. – kann zwar helfen zu klären, ob es sich um ein Originalprodukt handelt, Plagiate aber nicht verhindern. Um Plagiate zu verhindern, sollte der Schutz entlang der gesamten Kunden- und Händlerwertschöpfungskette lückenlos überprüft werden. **Ausgangspunkt für Produktpiraterie ist Wissen über Produkte, Herstellverfahren und Absatzmärkte**. Deshalb sollten Institutionen den **Produktschutz mit** einem **präventiven Know-how-Schutz verbinden**. Zu diesem gehören **folgende Maßnahmenbereiche**:

- **personelle** Maßnahmen
- **organisatorische** Maßnahmen

[4] Vgl. VDMA 2016: Studie Produktpiraterie 2016.

[5] Systeme zur Informationsverarbeitung, die in ein technisches System eingebunden sind.

- Maßnahmen zum **direkten Schutz von Informationen und Wissen**
- Maßnahmen für **besondere Risikobereiche**

Ebenfalls wichtig, auch wenn nicht explizit im Fokus dieses Bausteins, ist der rechtliche Schutz der Produkte und Technologien. Strafbar sind z. B. die Verletzung der Schutzrechte des geistigen Eigentums, der Verrat von Geschäftsgeheimnissen sowie Betrug. Zivilrechtliche Ansprüche bestehen z. B. auf Unterlassung, Schadensersatz, Vernichtung/Beseitigung (z. B. von Plagiaten), Produktrückruf, Gewinnabschöpfung u. ä. Öffentlich-rechtliche Maßnahmen zum Schutz des geistigen Eigentums bestehen z. B. in der Beschlagnahme von Plagiaten durch den Zoll oder in der Grenz- oder Messebeschlagnahme. Beides kann bei der Zentralstelle Gewerblicher Rechtsschutz (ZGR) beantragt werden. Sowohl zivilrechtliche Ansprüche als auch Ansprüche auf Umsetzung öffentlich-rechtlicher Maßnahmen zum Schutz des geistigen Eigentums sind in unterschiedlichen gesetzlichen Regelungen normiert.

Ohne die nationale und ggf. internationale Anmeldung von Patenten, Marken, Gebrauchsmustern, Designs etc. sind die Durchsetzung von Rechten zum Schutz von Know-how sowie die Unterstützung durch Behörden (z. B. durch Beschlagnahme von Plagiaten an der Grenze) in den meisten Fällen nicht möglich.

3 Gefährdungslage

Sowohl fertige Produkte als auch Ideen und Wissen können einen Wettbewerbsvorteil darstellen, der jederzeit gegen Produktpiraten und Wettbewerber geschützt werden sollte.

Gründe hierfür liegen einerseits in dem **hohen Stellenwert von Wissen und Informationen** in der modernen Informationsgesellschaft. Diese spielen insbesondere im Hinblick auf immer **kürzer werdende Produktlebenszyklen** und die **steigende Bedeutung von Produktinnovationen e**ine wichtige Rolle. Andererseits handeln Unternehmen immer **globaler** und **interagieren mit Kooperationspartnern aus** sogenannten **Risikoländern**[6] bzw. **lassen** ihre Produkte **in diesen Ländern produzieren**. Die daraus resultierende **Übertragung der Produktionsprozesse** sowie die **Stärkung und Intensivierung der Beziehungen** erlauben Partnern einen besseren **Einblick in** die eigenen eventuell **schützenswerten Informationen und Prozesse**. Ungewollter Wissensabfluss kann ebenso aus externen, seitens der Organisation unkontrollierbaren Gründen erfolgen – z. B. aufgrund erhöhter behördlicher Informationsanforderungen in Genehmigungsverfahren und im Rahmen von Behörden-Audits, die mit Korruption oder mit unsicherer behördlicher Handhabung von Registrierungsdaten verbunden sein können. Nicht alle diese Gefahren können durch eigene Handlungen und Wachsamkeit vermieden werden. Die angemessene Berücksichtigung der spezifischen Gefährdungen, die aus einem ungewollten Informations- und Wissensabfluss entstehen können, liegt in der Verantwortung der Institution und ihrer Mitarbeiter.

Verantwortung der Institution

[6] Einen Überblick über die Risikoländer findet sich bei der VDMA (pks.vdma.org). Im Jahr 2016 war die Volksrepublik China auf dem ersten Platz als Ursprungsland für Plagiate.

Folgende Gefährdungen stehen häufig in Zusammenhang mit der Notwendigkeit eines erhöhten Produkt- und Know-how-Schutzes:

G 1 Spionageaktivitäten und gezielte (technische) Angriffe

G 2 Ungewollter Wissensabfluss (z. B. in Richtung bestehender und potentieller Geschäftspartner, Konkurrenten, Besucher oder Externer allgemein), verursacht durch Nichtwissen oder durch Fahrlässigkeit auf verschiedenen Ebenen

G 3 Geschäftliche Beziehungen mit Risikoländern

G 4 Missbrauch der gewährten Zugriffsmöglichkeiten durch Kurzzeitarbeiter, Leiharbeiter, Praktikanten sowie weitere zeitlich befristete Mitarbeiter

G 5 Bewusstes oder unbewusstes Mitarbeiterfehlverhalten hinsichtlich des Produkt- und Know-how-Schutzes (z. B. Gewährleistung des Zutritts zu schützenswerten Gebäudebereichen für unbefugte Externe, Preisgabe schützenswerter Informationen im Rahmen von formellem und informellem Austausch, Missachtung von Sicherheitsregeln beim Datenverkehr)

G 6 Bewusst verursachter Wissensabfluss durch austretende Mitarbeiter

G 7 Fehlende Zusammenarbeit mit Sicherheitsbehörden bei Vorfällen oder Verdacht

G 8 Publikationen sowie Teilnahme von Mitarbeitern an Konferenzen, Messen und weiteren öffentlichen Events (evtl. mit eigenen Vorträgen)

G 9 Entwicklung und Herstellung von Produkten, die für einen physischen Angriff/unmittelbare Einwirkung auf das Produkt geeignet sind (z. B. Nachbau des Produkts, Reverse Engineering)

G 10 Externe Betreuung der eigenen Informations- und Kommunikationssysteme

4 Maßnahmen

Der **bedachte und zielgerichtete Umgang mit Wissen und Informationen**, der **proaktive Schutz** dieser wichtigen Institutionsressourcen sowie der **Schutz von Produkten** bilden die **Grundlage für die Erreichung der Zielsetzung dieses Bausteins**.

Basis für die Gewährleistung **des Produkt- und Know-how-Schutzes ist** ein **ganzheitliches Schutzkonzept, das** die **zu implementierenden Verfahrensweisen und Methoden zur Konzeption, Umsetzung und Aufrechterhaltung** der notwendigen und angepassten Maßnahmen **abbildet**.

Die **Institution beschreibt** ihre **Ziele** und **führt** zu ihrer Erreichung die nachfolgend detailliert beschriebenen **Maßnahmen** entsprechend ihren individuellen Anforderungen **ein**. Die Maßnahmen folgen hierbei dem Plan-Do-Check-Act-Regelkreis und unterteilen sich in diese drei wesentlichen Prozessblöcke:

1. **Führungsprozess**
2. **Betriebsprozess** (Planung, Umsetzung, Überprüfung, Verbesserung)
3. **Berichts-/Kontrollwesen**

Abbildung 1 stellt dies grafisch dar.

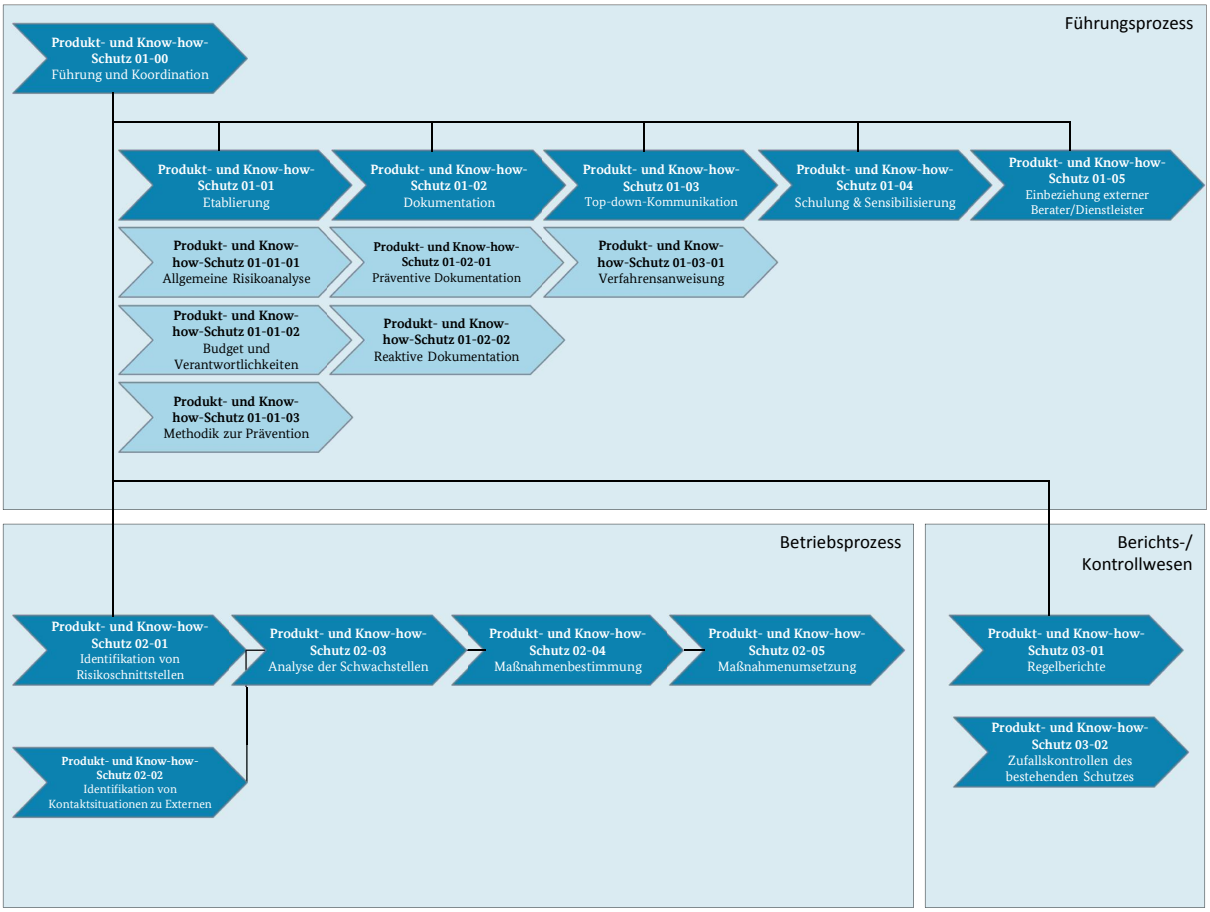


Abbildung 1: Prozessschaubild Produkt- und Know-how-Schutz

Die **Maßnahmen** dieses Bausteins sind **in drei Kategorien eingeteilt**. Sie richten sich nach dem **erforderlichen Detailgrad** bzw. der **gewünschten Ausprägung** (siehe Relevanzentscheidung) auf Basis der Anwendungsentscheidung gemäß Standard 2000-1:

A-Kategorie – Basismaßnahmen: unabdingbarer Wirtschaftsgrundschutz
B-Kategorie – Standardmaßnahmen: vollständiger Wirtschaftsgrundschutz
C-Kategorie – erweiterte Maßnahmen: erweiterter Schutz bei hohem Risikopotential

M 1 Festlegen der zentralen Strukturen zur Vorbeugung und Bekämpfung von Produkt- und Know-how-Risiken (A)

Die Institution ist dafür verantwortlich, **Strukturen zu schaffen, mittels derer** nicht nur die **Folgen** von Produktpiraterie, sondern auch die **Ursachen bekämpft werden können**. Es geht somit nicht nur um **reaktive Schutzmaßnahmen**, sondern auch um die frühzeitige Implementierung **ganzheitlicher präventiver Schutzkonzepte in** die **Institutionsstruktur**. Dies ist ein **bereichs- und themenübergreifender Prozess**, in dem die Institution **zentral** alle betroffenen Bereiche und alle Maßnahmen **miteinander verknüpft und steuert**. Dabei sollen langfristig orientiert und zentral gesteuert folgende Grundlagen und organisatorischen Rahmenbedingungen für die Vorbeugung und Bekämpfung von Produkt- und Know-how-Risiken geschaffen werden:

Grundlagen Risikobekämpfung

- Es ist eine zentrale Aufgabe, **Verantwortliche** für die Auseinandersetzung mit dieser Thematik in **der Institution** zu **bestimmen**. Empfehlenswert ist die Ernennung eines **Produkt- und Know-how-Schutz-Beauftragten** (Intellectual Property Manager). Dieser übernimmt **explizit** entsprechende **Aufgaben** und ist **zentrale Ansprechperson für alle Mitarbeiter**.
- Um die **Handlungssicherheit der Mitarbeiter** zu gewährleisten, sollen zentral zunächst einmalig **potentielle Möglichkeiten der Produkt- und Know-how-Gefährdung aufgelistet und** für diese konkrete Verfahrensanweisungen für jede Mitarbeiterebene **erfasst werden**. Hierzu gehört ebenso die Erfassung und Darstellung der **internen Organisationsstruktur** mit **Fokus** auf die (hierarchischen) **Beziehungen zwischen den Mitarbeitern**. Auf diese Weise wird zentral ein Überblick über **schutzrelevante Organisationsbereiche** und **betroffene Mitarbeiter** geschaffen. Die Institution hat dafür zu sorgen, dass die **Anweisungen allen Mitarbeitern bekannt gemacht** werden. Diese Maßnahmen sollten sich darüber hinaus **über** die **Organisationsgrenze hinaus auf** die Ebene der **Lieferanten und Kooperationspartner** erstrecken.
- Die Institution sorgt dafür, dass die Entscheidungen über **Vorgehensweise und Methodenanwendung** zur **Prävention und Reaktion in** für den **Produkt- und Know-how-Schutz**

relevanten Fällen zentral getroffen und klar kommuniziert werden. Sie legt die **Kommunikationswege** und **Dokumentationsform** bei Vorfällen fest.

Die Institution berücksichtigt die **Notwendigkeit** einer ganzheitlichen Betrachtung von **Technologie, Organisation und Wissensmanagement** und begrenzt sich nicht nur auf die eigene Institution, sondern **berücksichtigt** die **gesamte Lieferkette**. Zudem sollen die Maßnahmen möglichst **früh im Produktentstehungsprozess** greifen.

M 2 Festlegen der notwendigen Rollen (B)

Aufgabe Produkt- und Know-how-Schutz-Beauftragte (IPM)

In der Maßnahme M1 wurde bereits die Notwendigkeit thematisiert, zentral und seitens der Führungsebene einen **Intellectual Property Manager** zu bestimmen, der **hauptverantwortlich für** den Themenbereich **Produkt- und Know-how-Schutz** ist. Um sich vertieft und nachhaltig mit der Thematik auseinanderzusetzen, soll hierfür zudem **ein Team zusammengestellt** werden. Dieses **agiert bei akuter Gefährdung sowie einmalig bei** der **allgemeinen Erhebung und Bewertung** der aktuellen Situation in der Institution und bei der Bestimmung des Soll-Zustands und der Maßnahmen. Das Team besteht aus **Leitern und Vertretern aller Fachabteilungen**. Dem Intellectual Property Manager obliegt die **Projektkoordination**. Die **operativ tätigen Vertreter** aus den Fachabteilungen sind **in die Erhebungs- und Bewertungsphase involviert**. Ziel ist es, ein möglichst **genaues und umfassendes Abbild der Realität** in der Institution zu **erreichen**. Die Leitungsebene der jeweiligen Fachabteilungen ist vor allem bei der Bestimmung und Umsetzung der Maßnahmen relevant. Ihr obliegt in der Regel auch die Gestaltung der operativen Umsetzung nach Abschluss der Konzeption der Maßnahmen und Schritte zum institutionsangepassten Produkt- und Know-how-Schutz.

M 3 Identifizieren und Erheben von Informations- und Wissensschnittstellen (A)

Die Maßnahmen M3, M4 und M5 sind Teil des Konzepts zur Prävention und Reaktion bei Risiken des ungewollten Know-how-Abflusses.

Um einen **proaktiven und umfassenden Know-how-Schutz** zu implementieren, ist eine zielgerichtete Vorgehensweise zu empfehlen, die **grundlegend in den Maßnahmen M3, M4 und M5** beschrieben wird.[7] Wenn die Institution sich gegen Produktpiraterie und ungewollten Know-how-Abfluss schützen möchte, muss sie sowohl die **Beziehungen der Mitarbeiter untereinander** als auch die **zu externen Akteuren analysieren**. Diese Analyse wird initial durchgeführt und bei relevanten Veränderungen für die betroffenen Bereiche wiederholt. Sie führt zu **institutionsspezifischen Maßnahmen**. Die Anwendung dieser Maßnahmen sowie die erzielten Ergebnisse sollten **regelmäßig überprüft werden**.

Die Institution bzw. die **verantwortlichen Mitarbeiter identifizieren** zuerst **innerhalb der betrieblichen Prozesse** die **Schnittstellen zwischen Gruppen mit unterschiedlichem Know-how oder unterschiedlichen Vertraulichkeitsanforderungen**. Die Gruppen der relevanten Akteure werden durch die Analyse von Organigrammen und Prozessbeschreibungen identifiziert. Zur Vervollständigung der Angaben werden Gespräche mit Vertretern aus unterschiedlichen Bereichen der Institution geführt. Auf diese Weise entsteht ein erstes **Modell der Akteure als Grundlage für die Analyse**.

Im Anschluss daran erfolgt die **inhaltliche Erhebung und Dokumentation der identifizierten Informations- und Wissensschnittstellen**. Hierfür sollen **alle Mitarbeiter, die Informationen und Wissen für** andere **interne oder externe Akteure zur Verfügung stellen, zwei Leitfragen beantworten**. Externe Partner werden normalerweise durch die zu analysierende Institution beurteilt und nicht direkt befragt, da die Aussagen von potentiellen Produktfälschern nicht immer wahrheitsgemäß erfolgen.

Folgende Leitfragen sind zu beantworten:

- **Welche Informationen/welches Wissen** in Ihrem Bereich halten Sie für **besonders schützenswert**?
- **Welche Informationen/welches Wissen** ist bei welcher Aktivität **für weitere Mitarbeiter oder Externe zugänglich**?

[7] Eine ausführliche Darstellung findet sich bei Gronau/Meier/Bahrs 2011.

In der Praxis hat sich ein **kombiniertes Durchlaufen von Aktivitäten** des befragten Akteurs und der Empfänger, mit denen er eine Austauschbeziehung pflegt, als sinnvoll erwiesen.

Zur **besseren Dokumentation und** leichteren **Analyse** wird die Modellierung der erhobenen Daten empfohlen, also die **Übertragung der Antworten in Modelle**. Hierfür können Modellierungssprachen genutzt werden, insbesondere solche, die für die Visualisierung und Analyse von **Wissens- und Informationsflüssen** geeignet sind. Weiterhin existieren bereits (auch kostenfreie) **Analysewerkzeuge**, in denen eine entsprechende **Modellierungsumgebung** für die Analyse von Risiken des ungewollten Wissenstransfers integriert ist.

M 4 Ermitteln von Schutzbedarf und Risiken (A)

Diese Maßnahme ist zusammen mit den Maßnahmen M3 und M5 Teil des Konzepts zur Prävention und Reaktion bei Risiken des ungewollten Know-how-Abflusses.

Ermittlung Schutzbedarf

Zur Analyse aller identifizierten Schnittstellen der Wissens- und Informationsübertragung (s. M3) sind drei Fragen zu beantworten:

1) Ist der Verlust des an dieser Stelle übertragenen Wissens oder der Information kritisch für uns?

Hier geht es um die Einschätzung des Risikopotentials bzw. der Kritikalität von Informationen und Wissen, die an jeder Schnittstelle ausgetauscht werden. Dies ist notwendig, damit die **Institution nur dort in Schutzmaßnahmen investiert, wo kritische Daten und Wissen betroffen sind**. Um diese zu bestimmen, sollten **alle identifizierten** geteilten **Informationen und alles identifizierte geteilte Wissen** gezielt mit Fragen **überprüft** werden. Hierdurch soll bestimmt werden, ob bzw. inwieweit das Wissen oder die Information zu den **Risikofaktoren Kern-Know-how, Einmaligkeit und Nachahmungsrelevanz** gehört. Dies soll durch Fragen überprüft werden, deren Antworten eine Einschätzung möglich machen, ob der Verlust des konkret übermittelten Wissens negative Folgen für das Unternehmen haben könnte. Der Faktor **„Nachahmungsrelevanz“** deckt **mögliche**

Angriffspunkte von Produktpiraten durch das jeweilige Know-how auf. Eine entsprechende Frage ist beispielsweise: „Kann diese Information/dieses Wissen dafür genutzt werden, das Produkt oder den Produktionsprozess nachzuahmen?“ .
Der Faktor **„Einmaligkeit“** beschreibt, ob das Wissen auch aus anderen Quellen verfügbar ist, und gibt damit **Auskunft über die Notwendigkeit des Schutzes**. Eine entsprechende Frage ist: Kann diese Information in entsprechenden Fachbüchern gefunden werden? Der Faktor **„Kern-Know-how“** erfasst, ob es sich um wesentliches, für die betriebliche Leistungserstellung erforderliches Wissen handelt. Eine hierzu entsprechende Frage untersucht beispielsweise die Entwicklung und Eingliederung eines bestimmten Wissens durch bzw. in das Unternehmen. Zu jedem Faktor sind diverse Fragen zu beantworten. Ihre **zusammengefasste Analyse** gibt eine **Auskunft über den Faktorenwert**.

2) Ist der Empfänger des Wissens/der Information (der Kommunikationspartner) potentiell daran interessiert oder geneigt, unser Know-how unbefugt anzuwenden?

Bei dieser Frage geht es um die **systematische Ermittlung der Pirateneigung der Akteure. Folgende Aspekte** sollen dabei berücksichtigt werden:

- **Voraussetzungen und Möglichkeiten** der Akteure, von Produktpiraterie zu profitieren
- **Vorgeschichte** der Beziehung zu diesem bestimmten Akteur
- **Vernetzung** des Akteurs zu typischen Produktionsstätten von Plagiaten
- ggf. weitere Faktoren:
    - große Nachfrage für das Produkt
    - hohe Gewinnmarge
    - keine komplexe Infrastruktur oder Einrichtungen notwendig für die Produktion
    - Lücken in der Durchsetzung von Gegenmaßnahmen
    - mangelnde Rechtsvorschriften sowie geringe Sanktionen
    - ineffiziente Zusammenarbeit zwischen den legalen Akteuren

Zusätzliche Untersuchungsschwerpunkte sollten für eigene Mitarbeiter (interne Akteure) gelten. **Insbesondere Experten und Personen mit Schlüssel-Know-how sollten identifiziert und langfristig an die Institution gebunden werden**, da sie unter Umständen eine potentielle Gefahrenquelle darstellen. Der Überblick über relevante externe Akteure ist notwendig, um diese auf ihr Risikopotential untersuchen zu können. Notwendige Eckdaten hierzu betreffen die Länge und Intensität des Austauschs, die bisherige Vorgeschichte, insbesondere relevante Vorfälle, usw.

3) Haben wir bisher ausreichende und passende Maßnahmen ergriffen, um kritisches Wissen und kritische Informationen zu schützen?

Der dritte Schwerpunkt der Analyse und Bewertung ist die **systematische Überprüfung der vorhandenen Schutzmaßnahmen und -konzepte**. Hierbei sollten vor allem **folgende Punkte** untersucht werden:

- Zugriffsschutz gegenüber Dritten
- Kopierbarkeit der Information bzw. des Wissens
- Nachvollziehbarkeit des Wissenstransfers

Vorhandene Instrumente wie **Hintergrundchecks, Geheimhaltungsvereinbarungen, bereits erkannte Ereignisse der Vergangenheit, Sensibilisierung der Akteure und Nutzung öffentlicher Netzwerke** sollten hierfür genutzt werden.

M 5 Ableiten, Festlegen und Umsetzen notwendiger Maßnahmen (A)

Diese Maßnahme ist zusammen mit den Maßnahmen M3 und M4 Teil des Konzepts zur Prävention und Reaktion bei Risiken des ungewollten Know-how-Abflusses.

In dieser Maßnahme soll die Institution alle Entscheidungen zu den folgenden Punkten treffen:

1. **Welche Informations- und Wissensschnittstellen** unterliegen den potentiellen Risiken des ungewollten Wissensabflusses?
2. **Welche Maßnahmen behandeln diese Risiken?**

Als Ergebnis erstellt die Institution einen **Maßnahmenplan** (To-do-Liste) **für jede Abteilung**. Dieser sollte Änderungen der Schnittstellen beinhalten und ein Regelwerk bereitstellen, das bestimmt, welche Inhalte wem gegenüber preisgegeben werden dürfen. Zusätzlich sind die **zu ergreifenden Schutzmaßnahmen aufgeführt**.

M 6 Schulen und Sensibilisieren von Mitarbeitern mit Zugriff auf kritisches Know-how (Wissen und Informationen) (B)

Die **Institution erstellt** ein **Schulungs- und Sensibilisierungskonzept für** den **Umgang mit kritischem Know-how**. Dieses basiert unter anderem auf den Ergebnissen der Maßnahme M2. Die **Mitarbeiter** sollen **zielgruppenspezifisch informiert und sensibilisiert** werden. Es werden dabei **explizit** die **individuellen Voraussetzungen und Relevanzen** des jeweiligen Mitarbeiters **berücksichtigt**. Dazu gehören unter anderem die **Abteilungszugehörigkeit sowie die Wahrscheinlichkeit, Art, Häufigkeit und Intensität der Beziehungen zu externen Akteuren, die Länge der Betriebszugehörigkeit sowie der gewährte Zugriff zu kritischem Wissen und Informationen**. Unterschieden wird zwischen einem **allgemeinen Schulungs- und Sensibilisierungsplan** für alle Mitarbeiter und den **spezifischen Schulungsplänen** für Mitarbeiter mit Zugriff auf **kritisches Wissen und Informationen**. Der allgemeine Plan beinhaltet:

- **Hinweise bezüglich des kritischen Know-hows**: Jedem Mitarbeiter muss sichtbar gemacht werden, **welches Wissen kritisch ist** (die „Kronjuwelen" der Institution), wie dieses zu identifizieren ist sowie welche negativen Auswirkungen der Verlust dieses Wissens und dieser Informationen hätte. Das kritische Wissen an sich sollte nicht jedem Mitarbeiter zugänglich gemacht werden. Bei allen Mitarbeitern ist jedoch ein Bewusstsein dafür zu schaffen, dass das kritische Wissen schützenswert ist und seine Weitergabe an Unbefugte strafbar sein kann
- Beschreibungen der **externen Akteursgruppen**, mit denen die Institution interagiert, und Hinweise auf zentral erstellte Richtlinien, **zu welchem Know-how jede dieser Gruppen Zugriff haben darf**
- Hinweise auf für die Institution geltende Maßnahmen und

Regeln des präventiven Know-how- und Produktschutzes sowie auf das Verhalten und die Ansprechpartner bei bestehender potentieller Gefahr oder beim Auftreten eines Know-how-Abflusses

- vertragliche Verschwiegenheitsverpflichtungen für Mitarbeiter, sofortige Freistellungen in Verdachtsfällen inkl. Sperrung der Systemzugriffe bis zur Klärung sowie ggf. sofortige Sperrung der Systemzugriffe bei Kündigung von Know-how-Trägern

In diesem Kontext ist die Berücksichtigung der menschlichen Risikofaktoren (legitim berechtigte Mitarbeiter als mögliche Innentäter) notwendig. Die Motivationsgründe für Mitarbeiter, kritisches Know-how bewusst an Externe zu übermitteln, können sehr unterschiedlich sein. Aus diesem Grund sind unterschiedliche und an die jeweilige Institution angepasste Bekämpfungsansätze notwendig: gezielte motivierende Personalmaßnahmen, fördernde Arbeitsbedingungen und Unternehmenskultur, angemessenes Gehalt. Daneben sind den Wissensabfluss bewusst verhindernde Maßnahmen nötig, wie technische Kontrollen, Aufteilung von Zugriffsrechten und angepasste Informationsversorgung.

Die Durchführungsphase beinhaltet die **notwendigen Analyseschritte**, um schützenswertes Know-how zu identifizieren, die **internen und externen Austauschbeziehungen** aufzudecken und die **internen und externen Akteure** einschätzen zu können, die Zugriff auf das kritische Wissen und die kritischen Informationen haben. Zudem wird hier festgestellt, inwieweit sich die Institution bereits schützt bzw. eine potentielle Gefahr erkannt hat. Das generelle **Konzept der Organisation und** die **Schulungsmaßnahmen** werden **regelmäßig überprüft und angepasst**.

M 7 Etablieren eines Regelwerks zum sicheren Umgang mit Externen (A)

Die Institution definiert weitgehend standardisierte Richtlinien zum Umgang mit externen Akteuren. Tabelle 1 dient, ohne Anspruch auf Vollständigkeit[8], zur Orientierung, welche Situationen entstehen kön-

[8] Für weiterführende Informationen sei auf die Broschüre „Know-how-Schutz. Handlungsempfehlungen für die gewerbliche Wirtschaft“ des Landesamts für Verfassungsschutz Baden-Württemberg (s. Literaturverzeichnis) verwiesen.

nen, bei denen der **Umgang mit externen Akteuren unter Umständen zu ungewolltem Know-how-Abfluss führen kann**, sowie durch welche Maßnahmen die Institution ihre **Mitarbeiter sensibilisieren** kann. Externe Akteure sind sowohl Kunden, Lieferanten und Geschäftspartner als auch die breite Öffentlichkeit (vgl. hierzu die Möglichkeiten zur Identifikation solcher für die konkrete Organisation relevanter Gruppen in M2). **Ziel ist** die **Identifikation, systematische Erfassung, Darstellung und Analyse der Beziehungen nach außen** (Kunden, Lieferanten und Öffentlichkeit).

Potentielle Kontaktsituation	Maßnahme zur Prävention
Umgang mit Externen auf Messen, Veranstaltungen und Konferenzen allgemeine Öffentlichkeitsarbeit und Internetpräsenz	Vor- und Nachbesprechung bei erstmaligen Kontaktaufnahmen zu Externen zur Sensibilisierung für den Umgang mit sensiblen Informationen (Briefing und Debriefing) Identifikation und Schulung von Mitarbeitern, die die Institution in solchen Situationen vertreten im Rahmen von Vorträgen und Präsentationen: Erstellung eines zentral geprüften Präsentationsteils zum Institutionshintergrund und Überprüfung von in die Präsentation aufgenommenen anlassspezifischen Inhalten durch den zentral Verantwortlichen zum Thema Produkt- und Know-how-Schutz auf Messen: klare Regelungen zur Freigabe und zentrale Überprüfung des Messeexponats mit dem Ziel, durch das Exponat die Wettbewerbsfähigkeit zu zeigen, jedoch nicht zu viel Einblick in derzeitige Forschung und Entwicklung zu gewähren; klare Regelungen zur Freigabe und Überprüfung der Inhalte von Flyern, Broschüren und Pressematerial; Anweisungen in Bezug auf erlaubte Fotoaufnahmen durch die Besucher und auf deren Detailgrad Sensibilisierung der Mitarbeiter sowohl hinsichtlich des formellen Kontakts (z. B. Detailgrad der Erklärungen bei Nachfragen) als auch hinsichtlich des informellen Kontakts (After-Work-Parties, Geschäftsessen, zufällige

Potentielle Kontaktsituation	Maßnahme zur Prävention
	Begegnungen bei der Hin- und Rückreise usw.) Richtlinien zu Publikationswesen, Vortragsgestaltung und Gestaltung der Internetpräsenz der Institution
Umgang mit Externen in der eigenen Institution (z. B. bei Besuchen, organisierten Führungen, Vorstellungsgesprächen, im Rahmen von Projektmeetings und Veranstaltungen)	Vor- und Nachbesprechung bei erstmaliger Kontaktaufnahme zu Externen (Briefing und Debriefing) zentral definierte Grundsätze des Verlaufs von Führungen durch das Gebäude und gesonderte Kennzeichnung und Zugriffsbegrenzung von schützenswerten Bereichen ggf. permanente Betreuung von Externen in Sicherheitsbereichen zentrale Freigabe vor Besucherführungen durch schützenswerte Bereiche zentral festgelegte Bestimmungen für Foto- und Videoaufnahmen durch Besucher
Umgang mit Externen, zu denen eine Geschäftsbeziehung besteht	Vor- und Nachbesprechung bei erstmaliger Kontaktaufnahme zu Externen (Briefing und Debriefing) Geheimhaltungsvereinbarungen
Umgang mit besonderen Gruppen von Externen: Lohnarbeiter, Praktikanten, externe Dienstleistungsanbieter wie Reinigungsfirmen und Veranstaltungsorganisatoren	Bestimmung von Sicherheitsstufen und Zugriffsberechtigungen Begrenzung der Zugriffsrechte für Angestellte auf Zeit Ernennung hauptverantwortlicher Kontaktpartner für die Externen

Potentielle Kontaktsituation	Maßnahme zur Prävention
allgemeine Prävention und Reaktion im Bedarfsfall (bei relevanten Vorfällen, Verdacht und Unsicherheit)	vertragliche Geheimhaltungsvereinbarung im Vorfeld für alle externen Partner, die Zugriff zu Produkten und Know-how bekommen sollen sofortige Sperrung des Zugriffs auf IT und des Zugangs zu Gebäuden für Mitarbeiter bei Ende des Beschäftigungsverhältnisses Dokumentation von Vorfällen und Definition von Verfahren und Ansprechpartnern bei Verdacht Erstellung von Risikoprofilen nach Gruppen von Externen (s. zur Orientierung M2) Richtlinien und Hinweise an Mitarbeiter zu sicherheitsrelevantem Verhalten (z. B. Türen abschließen, wenn das Zimmer verlassen wird) Einführung spezifischer Bekleidung oder von Namensschildern für Mitarbeiter in sicherheitsrelevanten Gebäudebereichen Benachrichtigung aller Mitarbeiter, wenn Besuchergruppen im Haus sind (Zeitraum, Hintergrund des Besuchs, Ansprechpartner etc.) technischer/IT-Schutz für frei zugängliche Systeme oder Anlagen technischer/IT-Schutz bei registrierten Auffälligkeiten (z. B. Kopieren oder Versenden großer Dateimengen) technischer/IT-Schutz für alle Rechner (sicheres Einloggen, Verschlüsselung, Virenscanner etc.) sichere Verpackung und Beschriftung von Lieferungen an die und aus der Institution (Teile oder ganze Produkte), Zusammenarbeit mit Lieferanten und Kunden hierzu

Potentielle Kontaktsituation	Maßnahme zur Prävention
	Hintergrundchecks für Externe beim erstmaligen Kontaktwunsch durch diese (Herkunftsland, Institutionsgeschichte, gemeinsame Partner etc.) Hintergrundchecks und Geheimhaltungsvereinbarungen für die Zusammenarbeit mit externen Dienstleistern (z. B. externe Betreuer der Inter- und Intranetpräsenz der Institution)

Tabelle 1: Kontakt zu externen Akteuren und proaktive Maßnahmen

Das Verfahren kann für die verschiedenen Akteursrisikogruppen unterschiedlich ausgeprägte Maßnahmen umfassen.

M 8 Erstellen und Anwenden einer Richtlinie zum Produktschutz (A)

Die Institution definiert **einheitliche Richtlinien zur Nutzung von Technologien zum Produktschutz**. Die Richtlinie zum Produktschutz adressiert wesentliche Produktbereiche im **technischen Plagiatsschutz**:

- Produktkennzeichnungen
- Detektion/Authentifizierung (zur automatisierten Erfassung und Prüfung von Produktkennzeichnungen)
- Tracking- und Tracingsysteme (zur Überwachung und Überprüfung der Sendungen/Lieferungen in der Logistikkette)
- embedded Security (Informationssicherheit für eingebettete Systeme[9] durch Vermeidung unbefugter Manipulationen bei der Beschaffung, Übertragung, Bearbeitung und Speicherung von Informationen)
- technischer Know-how-Schutz

Die Richtlinie umfasst Informationen über Schutzmöglichkeiten, Verweise auf Informationsquellen, Auflistung der in der Institution angewendeten Verfahren und Hinweise zu diesen.

[9] Systeme zur Informationsverarbeitung, die in ein technisches System eingebunden sind.

Als nächsten Schritt trifft die Institution Entscheidungen hinsichtlich der Auswahl und Anwendung des technischen Schutzes und setzt diese um. In diesem Zusammenhang gilt es einzuschätzen, ob die **Institution über ausreichende eigene finanzielle und personelle Kapazitäten sowie das notwendige Fachwissen verfügt**. Unter Umständen ist eine **Kosten-Nutzen-Analyse** als Entscheidungsgrundlage empfehlenswert. Hierzu gehört auch die **Überlegung, ob ein externer Berater hinzugezogen werden soll** sowie ggf. wie die Zusammenarbeit mit diesem rechtlich und formal gestaltet werden soll.

M 9 Überprüfen und Gestalten des Technologieschutzes (B)

Die Aufgaben der Institution bei der Gestaltung des Technologieschutzes beziehen sich auf die Identifikation technologischer Einflussgrößen und Stellhebel, um schützenswerte Produkte in Zukunft kopiersicherer zu gestalten.

Die schützenswerten Komponenten eines Produkts, die seine **funktional relevanten Module, Baugruppen und Bauteile umfassen, sind zuerst zu identifizieren** (s. M2) sowie nach Möglichkeit technologisch kopiersicher zu gestalten. Diese werden als ein sicherer, geschützter Kern betrachtet. Berücksichtigt werden dabei auch die Systembaugruppen und Module von Lieferanten und Partnerfirmen, die ebenso technisch sicher gestaltet werden sollten.

Dabei berücksichtigt die Institution im Hinblick auf die Wettbewerbsfähigkeit **Markt- und Kundenanforderungen**, die **branchenspezifische Marktsituation, gesetzliche Vorschriften, Funktionskosten, Herstellungskosten** auf Teilebene sowie die **bestehende Produktstruktur**[10].

[10] Ausführliche Beschreibung, Hinweise und Methoden finden sich bei Gronau/Meier/Bahrs 2011.

5 Weiterführende Informationen

Weiterführende Informationen zum Produkt- und Know-how-Schutz können den nachfolgenden Veröffentlichungen[11] entnommen werden.

- *Neemann, Christoph Wiard 2007: Methodik zum Schutz gegen Produktimitationen, Shaker*
- *Gronau, Norbert/Meier, Horst/Bahrs, Julian (Hrsg.) 2011: Handbuch gegen Produktpiraterie. Prävention von Produktpiraterie durch Technologie, Organisation und Wissensflussmanagement, Gito*
- *Wildemann, Horst 2007: Ganzheitliche Strategien gegen Produktpiraterie, in: Intelligenter Produzieren, 6. Jg., S. 5-7*
- *VDMA 2016: Studie Produktpiraterie 2016, http://pks.vdma.org/article/-/articleview/13069313*
- *Landesamt für Verfassungsschutz Baden-Württemberg 2004: Know-how-Schutz. Handlungsempfehlungen für die gewerbliche Wirtschaft, http://www.verfassungsschutz-bw.de/site/lfv/get/documents/IV.Dachmandant/Datenquelle/stories/public_files/spionageabwehr/know_how_schutz_2004.pdf*

[11] Links zuletzt am 20.03.2017 auf Funktionalität geprüft.

6 Anlage

Das Wichtigste auf einen Blick (Themenübersicht)

Vorbereitung
Bestimmung von Verantwortlichen für die Thematik
Auflistung möglicher Produkt- und Know-how-Gefahren
Auflistung von Verfahrensanweisungen
Erfassung und Darstellung der internen Organisationsstruktur
Erstellung eines Überblicks über schutzrelevante Organisationsbereiche
Bekanntmachung und Kommunikation von Maßnahmen und Entscheidungen
Bereitstellen notwendiger Systeme und Dienstleistungen

Schulung und Sensibilisierung
Schulungen und Sensibilisierungskampagnen für Mitarbeiter und relevante Partner
Trainings und Briefings zu potentiellen Gefahrensituationen und zur Prävention

Dokumentation
Dokumentation von Strukturen und Maßnahmen
Dokumentation von Vorfällen
Dokumentation von Verdachtsfällen

relevante Bereiche
Gestaltung des Technologieschutzes
Gestaltung des Produktschutzes
Gestaltung des Know-how-Schutzes
Umgang mit Externen

Vorgehen zur Prävention
Identifikation von Schnittstellen
Schutzbedarf- und Risikoanalyse
Maßnahmendefinition und Umsetzung

Maßnahmenübersicht und -kategorien

A - Basismaßnahmen	B - Standardmaßnahmen	C - erweiterte Maßnahmen
M 1 Festlegen der zentralen Strukturen zur Vorbeugung und Bekämpfung von Produkt- und Know-how-Risiken M 3 Identifizieren und Erheben von Informations- und Wissensschnittstellen M 4 Ermitteln von Schutzbedarf und Risiken M 5 Ableiten, Festlegen und Umsetzen notwendiger Maßnahmen M 7 Etablieren eines Regelwerks zum sicheren Umgang mit Externen M 8 Erstellen und Anwenden einer Richtlinie zum Produktschutz	A + M 2 Festlegen der notwendigen Rollen M 6 Schulen und Sensibilisieren von Mitarbeitern mit Zugriff auf kritisches Know-how (Wissen und Informationen) M 9 Überprüfen und Gestalten des Technologieschutzes	A und B +

Danksagung

Wir bedanken uns bei den vielen Experten, die ihr Fachwissen bei der Erstellung dieses Bausteins einfließen ließen und durch ihr Engagement die Entstehung erst ermöglicht haben. Insbesondere gilt unser Dank folgenden Autoren und Mitwirkenden: Frau Gergana Vladova und Herr Prof. Dr.-Ing. Norbert Gronau (Lehrstuhl für Wirtschaftsinformatik, insb. Prozesse und Systeme, an der Universtität Potsdam) sowie Frau Michaela Duda (HiSolutions AG).

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
www.verfassungsschutz.de

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn
www.bsi.bund.de

Herausgeber
ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.
Rosenstraße 2, 10178 Berlin
asw-bundesverband.de

Redaktion/Bezugsquelle/Ansprechpartner
Prof. Timo Kob (Gesamtprojektleitung)

Gestaltung, Produktion
HiSolutions AG

Stand
Mai 2017

Auflage
1. Auflage