Bundesministerium
des Innern, für Bau
und Heimat

Informationsabfluss aus Unternehmen – Innentäterschaft als unterschätztes Massenphänomen

Prävention, Detektion und Reaktion.

Impressum

Herausgeberin
Initiative Wirtschaftsschutz
Bundesministerium des Innern, für Bau und Heimat
ÖS II 4 – Spionageabwehr, ABC-Kriminalität, Wirtschaftsschutz
Alt-Moabit 140
10557 Berlin
E-Mail: oesII4@bmi.bund.de
Telefon: +49-(0)30 18 681-0

Gestaltung
Orca Affairs GmbH
Schumannstr. 5
10117 Berlin

Bildnachweis
Titel: Sergey Nivens/Shutterstock.com

Stand
Mai 2021

Die Initiative Wirtschaftsschutz dankt der Henkel AG & Co. KGaA und der Evonik Industries AG für die inhaltliche Zusammenarbeit.

Informationsabfluss aus Unternehmen – Innentäterschaft als unterschätztes Massenphänomen

Prävention, Detektion und Reaktion.

Kennen Sie das? Ein Mitarbeiter verlässt das Unternehmen und nimmt Unterlagen, Daten oder Informationen mit. Warum auch nicht, die Unterlagen sind ja selbst erstellt worden und helfen im neuen Job oder bei der Gründung des eigenen Unternehmens. Oder wurden Sie vielleicht selbst schon einmal gefragt oder haben überlegt, Daten aus dem Betrieb an Externe weiterzuleiten? Die Entdeckungswahrscheinlichkeit ist gering, schließlich fehlt anschließend nichts, die Informationen sind nur kopiert. Und im Gegensatz zu einer Geldüberweisung wird der Empfang nicht dokumentiert und es braucht keine Unterschrift einer vorgesetzten Person.

In der Öffentlichkeit werden oft nur spektakuläre Schadensereignisse bei großen Konzernen wahrgenommen. Doch diese stellen lediglich Einzelfälle eines Massenphänomens dar. Denn: Kleine und mittelgroße Unternehmen können gleichermaßen Ziel oder Opfer eines bewusst oder unbewusst verursachten Informationsabflusses werden. Dabei haben Beschäftigte, egal ob Hausmeister oder Managerin, aufgrund ihrer Zugangsmöglichkeiten und besonderen Kenntnisse oftmals leichtes Spiel bzw. stellen sie ein lohnendes Ziel für mögliche Angriffe dar. Ein Verlust sensibler Unternehmensdaten kann zu einem hohen finanziellen Schaden, Reputationsverlust oder gar zur Insolvenz führen.

Schützen Sie daher Ihre Informationen in gleichem Maße wie auch Ihre anderen Vermögenswerte. Damit bewahren Sie Ihr Unternehmen vor Schaden und demonstrieren in Geschäftsbeziehungen, dass Sie ein vertrauenswürdiges Kooperationsunternehmen sind. Mit dieser Broschüre erhalten Sie Hinweise und konkrete Tipps, wie Sie Ihre sensiblen Unternehmensinformationen am besten vor unerlaubten Zugriffen schützen können.

Inhaltsverzeichnis

I. Phänomenologie

1. Gefährdungspotenzial und Definition 6
2. Hellfeld und Dunkelfeld - Zahlen und Fakten 7
3. Materiell-rechtliche Einordnung sowie Definition Geschäftsgeheimnisse 9
4. Wer sind die Innentäter? 11
5. Welche Erscheinungsformen gibt es? 11
6. Warum werden Beschäftigte zu Innentätern? 12

II. Prävention

1. Risikoanalyse 14
2. Faires Führungsverhalten 15
3. Informationsklassifizierung 17
4. Materieller Informationsschutz – Regeln je Vertraulichkeitsklasse 20
5. Kontrolle über schützenswerte Informationen gewinnen 22
6. Personalauswahl, -einstellung und -einführung 24
7. Regelmäßige Schulungen der Beschäftigten 27
8. Sicherheitskultur und Awareness 28
9. Spezialschulung für besondere Funktionen und Know-how tragende Personen 31
10. Social Engineering 32
11. Management von Beschäftigtenaustritten 36
12. Externe Kooperationen 39

III. Detektion

Festlegung von Meldewegen für Informationsabflüsse 44

Einrichtung von technischen Analyseverfahren (UBA, NBA) 45

Physische Detektion 46

Detektion sonstiger Verhaltensauffälligkeiten 46

Detektion abgeflossener Informationen – Darknet-Monitoring 47

Indirekte Detektionsmechanismen 48

IV. Reaktion

1. Erstanalyse, Aufklärung 50

2. Erstuntersuchung 50

3. Response 51

4. Nachbereitung 53

Schlusswort **54**

I. Phänomenologie

1. Gefährdungspotenzial und Definition

Jedes Unternehmen kann durch Innentäterschaft gefährdet werden

Innentäter bergen ein hohes Gefährdungspotenzial für Unternehmen, da die eigenen Mitarbeiterinnen und Mitarbeiter weitreichende Innenansichten haben; sie verfügen über kritische Zugangsmöglichkeiten sowie umfassende kollegiale Kontakte und Netzwerke. Diese Vertrauensposition kann eingesetzt werden, um relevantes Wissen und Daten abzuschöpfen. Fehlende Schutzkonzepte, eine mangelnde Sensibilisierung des Personals und eine gewisse Sorglosigkeit im Umgang mit sensiblen Informationen erleichtern unternehmensschädigendes Verhalten erheblich.

Beschäftigte können bewusst oder unbewusst zum Innentäter werden

Als Innentäter werden im Allgemeinen Menschen bezeichnet, die in Unternehmen und Organisationen gezielt und mit Vorsatz dolose Handlungen durchführen. Diese können in Organisationen eingeschleust worden sein oder werden durch verschiedene Umstände zu Innentätern.[1] Daneben darf nicht aus dem Blick geraten, dass Beschäftigte auch unbewusst zu Innentätern werden können, indem sie beispielsweise durch Social Engineering instrumentalisiert werden.

Auch aus dem externen Geschäftsumfeld kann Gefahr drohen

Neben den aktuellen und kürzlich ausgeschiedenen Beschäftigten eines Unternehmens bezieht sich die Innentäterproblematik im weiteren Sinne auch auf geschäftliche Kontakte wie Liefer- und Reinigungsfirmen, externe Dienstleistungsunternehmen sowie Beraterinnen und Berater, sofern diese ebenfalls über einen erweiterten Zugang zum Unternehmen verfügen oder privilegierten Zugriff auf interne Informationen haben.

[1] In Anlehnung an die Definition von Grützner/Jakob: Compliance von A-Z, 2. Auflage 2015, URL: https://beck-online.beck.de/?vpath=bibdata/lex/GruetznerJakobLexC_2/cont/GruetznerJakobLexC.Innentaeter%2Ehtm. (Stand: 20.01.2020)

2. Hellfeld und Dunkelfeld - Zahlen und Fakten

63 % der Fälle von Wirtschaftskriminalität sind auf die eigenen Beschäftigten zurückzuführen

Das Phänomen der Innentäterschaft rückte in den letzten Jahren vermehrt in den Fokus. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat nach Auswertung von 2.400 Schadensfällen im Jahr 2019 festgestellt, dass Innentäter für 63 % der Fälle von Wirtschaftskriminalität verantwortlich sind, und geht davon aus, dass jährlich fünf bis 10 % der deutschen Unternehmen von eigenen Beschäftigten betrogen werden.[2]

Bei Innentäterschaft ist von einer hohen Dunkelziffer auszugehen

Statistiken zum (polizeilichen) Hellfeld lassen keine verlässlichen Rückschlüsse auf das tatsächliche Ausmaß des Phänomens zu, da eine exakte Zuordnung der Täterschaft als Innentäter aufgrund fehlender Erfassungskriterien nicht möglich ist. Dabei ist Innentäterschaft kein ausgedachtes Phänomen und nichts, das es „in meinem Unternehmen nicht gibt". Viele Vorfälle werden von den Betroffenen erst gar nicht erkannt oder schlichtweg nicht angezeigt und können somit nicht erfasst werden. Einschlägige Studien und Befragungen zeichnen ein beunruhigendes bis alarmierendes Bild und gehen von einem sehr hohen, steigenden Dunkelfeld aus.

WISKOS-Studie: Taten von innen werden als weniger gefährlich eingestuft als Taten von außen

Bei einer Aktenauswertung von 392 Strafverfahren zu den §§ 17 ff. Gesetz gegen den unlauteren Wettbewerb (UWG) im Projekt WISKOS[3] wurden in 43 % der Fälle Innentäter als Tatverantwortliche festgestellt. In 32 % der Fälle konnte die Tat Außentätern zugeordnet werden und in 23 % der Fälle handelten Innentäter und Außentäter gemeinsam. Eine Dunkelfeldbefragung speziell bei kleinen und mittelständischen Unternehmen im selben Projekt zu der Frage, welche Art von Tatbegehenden hinter einem Vorfall vermutet wurde bzw. wer auf der Täterseite involviert war, ergab allerdings, dass Angriffe von außen immer noch als deutlich gefährlicher eingeschätzt werden als Taten von innen (Anzahl der Außentäter 44 %, Innentäter 34 %, beide gemeinsam 15 %).

---

[2] Vgl. Schareika, Nora: „Diese Mitarbeiter betrügen am häufigsten ihre Unternehmen"; in WirtschaftsWoche auf www.wiwo.de vom 04.09.2019. Url: https://www.wiwo.de/erfolg/management/wirtschaftskriminalitaet-diese-mitarbeiter-betruegen-am-haeufigsten-ihre-unternehmen/24979364.html (Stand: 03.02.2020).

[3] Das Forschungsprojekt Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WISKOS) wurde von 2015 bis 2018 unter den Förderkennzeichen 13N13410 und 13N13411 vom BMBF im Rahmen des Programms „Forschung für die zivile Sicherheit" gefördert. Ergebnisse und Produkte für KMU und Wissenschaftsorganisationen stehen auf der Projekthomepage (https://wiskos.de) zum kostenfreien Download bereit.

Bitkom-Studie (2019): 75 % der Unternehmen sind von analogen und digitalen Angriffen betroffen

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) ermittelte 2020 in seiner aktuellen Studie „Wirtschaftsschutz in der digitalen Welt“[4] einen Gesamtschaden von über 100 Milliarden Euro jährlich durch analoge und digitale Angriffe gegen deutsche Wirtschaftsunternehmen. Drei Viertel der Unternehmen waren in den vergangen beiden Jahren von Angriffen betroffen, weitere 13 % vermuten dies. In den Jahren 2016/2017 wurde dagegen nur jedes zweite Unternehmen Opfer (53 %).

Eine zunehmende Gefahr geht von ausscheidenden und ehemaligen Beschäftigten aus

Dabei gewinnen ausscheidende bzw. ehemalige Beschäftigte vor dem Hintergrund einer Innentäterschaft zunehmend an Bedeutung. Ein Drittel der Betroffenen (33 %) sagt, dass sie vorsätzlich geschädigt wurden. Ein knappes Viertel (23 %) sieht vormals Beschäftigte in der Verantwortung, ohne ihnen ein absichtliches Fehlverhalten zu unterstellen. Eigene aktuell beschäftigte Personen werden von 14 % für kriminelle Handlungen benannt. Steigende Zahlen wurden ebenfalls bei Social Engineering-Angriffen festgestellt. Mehr als jedes fünfte Unternehmen (22 %) war davon analog betroffen, 15 % digital.[5] Bei einem Drittel der Unternehmen (32 %) wurden durch analoge Angriffe IT- oder Telekommunikationsgeräte entwendet. Sensible physische Dokumente, Maschinen oder Bauteile wurden bei jedem Sechsten gestohlen.

Die Studie „Insider Threat 2018 Report“[6] bestätigt diese hohen Betroffenheitszahlen. 53 % der dort befragten Unternehmen haben im Verlauf der vergangenen zwölf Monate bis zu fünf Innentäter-Angriffe auf ihr Unternehmen verzeichnen müssen. 90 % der Unternehmen fühlen sich gegenüber Innentäter-Angriffen anfällig und nicht genügend geschützt. Zu den wichtigsten Risikofaktoren gehören vor allem zu viele Personen mit überhöhten Zugriffsrechten (37 %), eine zunehmende Anzahl von Geräten mit Zugriff auf sensible Daten (36 %) und die zunehmende Komplexität der Informationstechnologie (35 %). Zwei Drittel der Unternehmen halten böswillige Innentäter-Angriffe oder versehentliche Verletzungen für wahrscheinlicher als externe Angriffe. Von einem Anstieg der von innen ausgehenden Angriffe berichteten dabei 27 % der Studienteilnehmenden.
Zur Vermeidung von Schäden durch die eigenen Beschäftigten ist ein umfassendes Sicherheitskonzept erforderlich (vgl. **Abschn. II** und **Abschn. III**).

---

4 Bitkom (2020): „Wirtschaftsschutz in der vernetzten Welt“. URL: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf (Stand: 26.02.2020)

5 ebd.

6 Vgl. URL: https://www.security-insider.de/unternehmen-sind-anfaellig-fuer-innentaeter-a-780258/ (Stand: 10.09.2019)

3. Materiell-rechtliche Einordnung sowie Definition Geschäftsgeheimnisse

Innentäterhandeln ist strafrechtlich verfolgbar

Im Zusammenhang mit einer Innentäterschaft kommen verschiedene gesetzliche Normen in Betracht. Zunächst geht mit dem Informationsabfluss in der Regel eine Verletzung strafrechtlicher Normen einher.[7] Die relevanten strafrechtlichen Normen des Strafgesetzbuches (StGB) lassen sich wie folgt kategorisieren:

- Normen, die nur bei Abflüssen bestimmter Informationen bzw. aus bestimmten Organisationen verletzt werden (z. B. §§ 94 bis 99 Staatsschutzdelikte oder § 353b Verletzung des Dienstgeheimnisses),
- Normen, die in direktem Zusammenhang mit dem Informationsabfluss verletzt werden (z. B. § 201 Verletzung der Vertraulichkeit des Wortes, § 202 Verletzung des Briefgeheimnisses oder § 202a Ausspähen von Daten) sowie Normen, die häufig in Verbindung mit dem Informationsabfluss verletzt werden, wenn der Informationsabfluss verschleiert oder monetarisiert wird (z. B. § 299 Bestechlichkeit und Bestechung im geschäftlichen Verkehr).

Die Verletzung strafrechtlicher Normen durch Beschäftigte bietet Unternehmen vielerlei Möglichkeiten zur Sanktionierung

Bei Verletzung strafrechtlicher Normen ergeben sich für die betroffenen Unternehmen verschiedene Handlungsmöglichkeiten: Sie können Ermittlungen der Strafverfolgungsbehörden anstoßen, arbeitsrechtliche Auseinandersetzungen unter Umständen beschleunigen oder Möglichkeiten der Strafprozessordnung zur Verringerung vermögensrechtlicher Schäden nutzen (vgl. Abschn. IV).

Sonstige relevante Normen:

- § 242 BGB: Leistung nach Treu und Glauben als Grundlage für die Verschwiegenheitspflicht des Arbeitnehmers
- § 404 Aktiengesetz: Verletzung der Geheimhaltungspflicht durch Mitglieder des Vorstandes, des Aufsichtsrates, durch abwickelnde oder prüfende Personen oder ihre Gehilfen
- § 85 GmbH-Gesetz: Verletzung der Geheimhaltungspflicht durch Personen der Geschäftsführung oder des Aufsichtsrats oder Liquidatoren
- § 303 Handelsgesetzbuch: Verletzung der Geheimhaltungspflicht durch Abschlussprüfende oder Gehilfen
- § 120 Betriebsverfassungsgesetz: Verletzung der Geheimhaltungspflicht durch Mitglieder der Betriebsverfassungsorgane und Gewerkschaftsvertretungen sowie sachkundige Externe

[7] Die Regelungen zum Schutz staatlicher Verschlusssachen (Geheimschutz) sind hier ausgenommen, da diese nicht Bestandteil dieser Broschüre sind.

Bessere Möglichkeiten des Know-how-Schutzes durch das neue Geschäftsgeheimnisschutzgesetz

Geschäftsgeheimnisschutzgesetz

Mit dem Inkrafttreten des Gesetzes zum Schutz von Geschäftsgeheimnissen (Geschäftsgeheimnisschutzgesetz - GeschGehG) am 26. April 2019 kam es zu wichtigen Änderungen im Know-how-Schutz. Unternehmen müssen künftig aktiv werden, um den Schutz ihrer Geschäftsgeheimnisse zu gewährleisten. Die bisherige gesetzliche Unterscheidung von Betriebsgeheimnissen und Geschäftsgeheimnissen entfällt zugunsten der einheitlichen Verwendung des Begriffs „Geschäftsgeheimnisse". § 23 des GeschGehG (Verletzung von Geschäftsgeheimnissen) entspricht im Wesentlichen den bisherigen §§ 17 bis 19 UWG, die anhand der geänderten Anforderungen an das Nebenstrafrecht modernisiert und an die Begriffe des GeschGehG angepasst wurden. Der wichtigste Unterschied besteht darin, dass die Strafvorschrift ihren eigenständigen Charakter eingebüßt hat und nun Verstöße gegen die zivilrechtlichen Handlungsverbote in § 4 GeschGehG bei Vorliegen bestimmter Tatabsichten (zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber oder der Inhaberin eines Unternehmens Schaden zuzufügen) auch strafrechtlich sanktioniert.[8]

Sensible Informationen müssen durch Geheimhaltungsmaßnahmen geschützt werden

Was ist ein Geschäftsgeheimnis?

Ein Geschäftsgeheimnis ist nach der neuen Definition des § 2 Nr. 1 GeschGehG eine Information, die nicht allgemein bekannt oder ohne Weiteres zugänglich ist und einen wirtschaftlichen Wert hat. Außerdem muss die Information durch Geheimhaltungsmaßnahmen geschützt sein. Genügte bisher ein erkennbarer subjektiver Geheimhaltungswille, um ein Geschäftsgeheimnis zu definieren, werden jetzt „angemessene Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber" gefordert (§ 2 Nr. 1b GeschGehG).

Jeglicher unbefugte Umgang mit Geschäftsgeheimnissen ist strafrechtlich verfolgbar

Welche Handlungen sind verboten?

§ 4 GeschGehG regelt die Handlungsverbote. Diese untersagen z. B. das unbefugte Aneignen oder Kopieren von „Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt". Ebenso verboten ist „jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheiten entspricht." Darunter fallen insbesondere Sachverhalte, in denen die offenlegende Person gegen vertragliche Pflichten verstößt.

[8] Vgl. Regierungsentwurf zum GeschGehG: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_GeschGehG.pdf?__blob=publicationFile&v=1 (Stand: 22.01.2020).

Was ist nun zu tun? Welche Maßnahmen müssen Sie ergreifen?
Damit Geschäftsgeheimnisse rechtlich geschützt sind, müssen diese zunächst einmal definiert, identifiziert und dokumentiert werden, um überhaupt als solche (im Unternehmen) wahrgenommen zu werden und um als solche vor Gericht als Geschäftsgeheimnis bewiesen werden zu können. Ebenso wichtig ist, diese faktisch zu schützen. Infrage kommen dafür technische, organisatorische und vertragliche Know-how-Schutzmaßnahmen (vgl. **Abschn. II**).

Geschäftsgeheimnisse müssen definiert, identifiziert und dokumentiert werden

4. Wer sind die Innentäter?

Untersuchungen zeigen: Innentäter sind meist männlich und zwischen 30 und 60 Jahre alt.[9] Im Gegensatz zu anderen Kriminalitätsfeldern gibt es im Bereich der Innentäterschaft Personen jeden Alters und aus jeder Hierarchieebene im Unternehmen. Auch langjährige Beschäftigte können Taten begehen. Allerdings sinkt die Schadenshäufigkeit, je länger die Beschäftigten im Unternehmen sind, wobei die Zahl der dann verursachten Schäden steigt. Auch sind bei Fällen mit hohen Schadenssummen häufiger Personen aus dem mittleren bis Topmanagement mit zumeist höherer Bildung vertreten. Bei bestimmten Delikten (z. B. Diebstahl, Betrug) finden sich vermehrt Täterinnen und Täter ohne Führungsverantwortung und mit niedrigerer Bildung.

Auch langjährige Betriebszugehörigkeit hindert nicht an Innentäterhandeln

5. Welche Erscheinungsformen gibt es?

Beim Tatverhalten lassen sich verschiedene Erscheinungsformen unterscheiden: von zunächst ungeplantem, unbewusstem Verhalten bis hin zu vorsätzlichen, geplanten Handlungen.

Unternehmensschädigendes Verhalten kann unbewusst oder bewusst erfolgen

Beispiele für unbewusstes Tatverhalten können sein:

- Eine Mitarbeiterin der Buchhaltung wird Opfer eines klassischen oder digitalen Social Engineering-Angriffs (z. B. CEO-Fraud).[10]
- Ein neuer Mitarbeiter missachtet aus Unkenntnis, Sorglosigkeit oder Fahrlässigkeit wichtige Sicherheitsregeln des Unternehmens und löst damit einen Schadensfall aus.

[9] BKA, Innentäter in Unternehmen 2 – Monitoringbericht, Kriminalistisches Institut (2020)

[10] Weitere Informationen zum Thema Social Engineering s. BKA: Monitoringbericht „Social Engineering/CEO-Fraud. Veröffentlicht auf dem Informationsportal der Initiative Wirtschaftsschutz. URL: https://www.wirtschaftsschutz.info/SharedDocs/Artikel/DE/BKA-Teaser-SEundCEO.html (Stand: 24.01.2020).

Unbewusstes Verhalten kann in vorsätzlichem Handeln münden

Beispiele für zunächst unbewusstes Tatverhalten, das in vorsätzlichem Handeln mündet:

- Eine zunächst ahnungslose Mitarbeiterin in einer attraktiven Funktion wird als dauerhafte Quelle im Rahmen der klassischen Wirtschaftsspionage angeworben.
- Ein Beschäftigter wird mittels kleiner Geschenke oder Einladungen von einem externen Täter zunächst „angefüttert". Nachdem der Mitarbeiter in eine Abhängigkeit bzw. Erpressbarkeit geraten ist, offenbart er sich aus Angst vor negativen Konsequenzen nicht.

Das Sammeln interner Informationen zeichnet vorsätzliches Tatverhalten aus

Beispiele für vorsätzliches, bewusstes Tatverhalten:

- Ein Mitarbeiter sammelt Informationen, um sie bei einem späteren Unternehmenswechsel zu nutzen.
- Eine Unternehmensangehörige bietet einem ausländischen Nachrichtendienst gezielt Informationen an.

6. Warum werden Beschäftigte zu Innentätern?

Die Beweggründe für kriminelles Verhalten sind vielfältig

Neben dem finanziell oder materiell erhofften Vorteil können Beschäftigte verschiedene Beweggründe haben. Beispielsweise können folgende persönlichkeitsbezogene Motive dabei eine Rolle spielen:

- Streben nach Anerkennung, Respekt oder Freundschaft,
- Überzeugungen politischer, kultureller oder religiöser Art,
- eine ichzentrierte Persönlichkeit (z. B. Wichtigtuerei, Eitelkeit bis hin zu stark auffälligen Persönlichkeitsstrukturen wie Narzissmus, niedrige Sozialverträglichkeit, Rücksichtslosigkeit, Tendenzen zur Täuschung, Nichteinhaltung von Regeln) sowie
- psychische Ängste oder Druckaufbau durch Externe (z. B. Erpressung).

Weitere Ursachen können im Arbeitskontext liegen. Beispielsweise kann sich bei einem Mitarbeiter oder einer Mitarbeiterin

- Unzufriedenheit, Neid, Missgunst, Frustration aufgrund einer Stagnation der eigenen Karriere oder aufgrund schlechter Führung aufgebaut haben oder
- die Person leidet unter sozialen Ängsten (z. B. den Arbeitsplatz zu verlieren und dadurch sozial abzusteigen).

Auch im eigenen Unternehmen gilt: Gelegenheit macht Diebe

Tatgelegenheiten für Beschäftigte entstehen in vielen Unternehmen auch aus der Situation heraus. Hierbei müssen Sie in Ihrem Unternehmen ansetzen und präventiv entgegenwirken. Günstige Gelegenheiten für Fehlverhalten ergeben sich beispielsweise durch:

- unzureichende interne Kontrollen,
- fehlende Schulungen am Produkt,
- Unkenntnis über Arbeitsprozesse oder
- Einsatz privater Geräte im geschäftlichen Kontext.

Auch der regelmäßige Umgang mit Kunden und Kundinnen, Dienstleistungsunternehmen und anderen geschäftlichen Kontakten kann zu potenziell gefährlichen Situationen führen. Achten Sie daher darauf, Informationszugänge je nach Umfang und Art der Tätigkeit zu beschränken und notwendige Datentransfers zu regulieren. Das heißt für die Unternehmenspraxis: Beschäftigte erhalten Zugriff auf die Daten, die sie für ihre Tätigkeit benötigen – das Need-to-know-Prinzip. Denken Sie auch an die Beschränkung von Zugängen zu Räumen, Laboren und Gebäuden.

II. Prävention

Die gute Nachricht: Sie können sich und Ihr Unternehmen vor einem ungewollten Informationsabfluss durch Beschäftigte schützen! In diesem Kapitel erfahren Sie, wie Sie Gelegenheiten für Taten reduzieren und die Wahrscheinlichkeit einer Entdeckung erhöhen.

1. Risikoanalyse

Die Risikoanalyse ist der erste Schritt zum Schutz der Unternehmenswerte

Der erste Schritt ist die Risikoanalyse. In dieser Phase werden zunächst die wesentlichen Schutzgüter in Ihrem Unternehmen identifiziert. Das sind diejenigen Güter, die grundlegend für das erfolgreiche Agieren am Markt sind. Analysieren Sie dabei alle Geschäftsbereiche. Denn: Die besonders schutzwürdigen Güter können sehr unterschiedlicher Natur sein, von Geschäftsgeheimnissen bis hin zu den Angestellten und ihren Fähigkeiten. Die Sicherheit für das Unternehmen erhöht sich, wenn der Identifizierungsprozess als dynamisch betrachtet wird, der nicht nach einer einzelnen Analysephase abgeschlossen ist. Schauen Sie sich immer wieder Ihre Güter und Unternehmensdaten an, denn die Wertigkeit einzelner Güter kann von äußeren Umständen abhängen und sich verändern. Auch die Belegschaft muss in den Analyseprozess einbezogen werden. Sie ist näher am Geschehen und sieht vor Ort oftmals schneller, welche Informationen, Prozesse etc. besonders schützenswert sind.

Auch organisatorische Faktoren bergen Risiken für die Unternehmenssicherheit

Auch organisatorische Faktoren müssen Teil der Analyse sein. Wie zufrieden sind Ihre Beschäftigten? Wie hoch ist der Krankenstand? Werden bestehende Regelungen zu Beförderungen als fair und transparent betrachtet? Hierbei lassen sich Anzeichen dafür finden, wie loyal Ihre Mitarbeiterinnen und Mitarbeiter dem Unternehmen gegenüber sind.

Aus der Perspektive von potentiellen Angreifern lassen sich Ziele und Tatgelegenheiten identifizieren

Insbesondere die Analysephase profitiert von einem Perspektivwechsel: Versetzen Sie sich ganz bewusst in die Rolle einer angreifenden Person. Welche Ziele erscheinen attraktiv? Welche Tatgelegenheiten bieten sich? Und: Welche Wege könnte die Person nutzen? So können Sie schnell relevante Informationen und mögliche Angriffspfade identifizieren.

Auch ausländische Nachrichtendienste haben es auf Unternehmens-Know-how abgesehen

Neben Personen aus der eigenen Belegschaft können sich auch fremde Staaten für das Know-how Ihres Unternehmens interessieren. Mit gezielter Wirtschaftsspionage wollen sie ihrer eigenen Wirtschaft einen Wettbewerbsvorteil verschaffen. Innentäter können in diesem Szenario eine zentrale Rolle spielen – verfügen sie doch über ganz spezielles Insiderwissen. Ein weiterer Vorteil: Die Angreifer müssen nicht erst eine Firewall überwinden, um an sensible Daten zu gelangen. Schauen Sie sich diese beiden Beispiele an:

- Ein ausländischer Nachrichtendienst setzt die in der Forschungsabteilung eines deutschen Unternehmens tätige eigene Staatsangehörige gezielt unter Druck, damit sie Unternehmensdaten stiehlt.
- Dem Angestellten im Produktteam wird durch eine Verbindungsperson eine lukrative Stelle im Ausland in Aussicht gestellt – gegen Information über das neue Firmenprodukt.

Die Motive und Angriffsziele von Personen, die von innen heraus kriminelle Handlungen begehen, sind überaus vielfältig und auch vom jeweiligen Unternehmensumfeld abhängig. Durch einen strukturierten Prozess sind diese im Unternehmen zu analysieren – am besten unter der Schirmherrschaft einer sicherheitsverantwortlichen Person.

Folgende ausgewählte Fragen sollten Sie im Analyseprozess beantworten:

Zielgerichtete Fragen erleichtern den Analyseprozess.

- Wo lauert der größte Schaden?
- Welche Informationen würden Sie bei der Konkurrenz interessieren?
- Bestehen klare Regeln für den Umgang mit sicherheitssensiblen Informationen?
- Sind diese Regeln den Unternehmensangehörigen bekannt?
- Wer sind die Personen, die an sicherheitsrelevanten Stellen im Unternehmen arbeiten?
- Wie loyal sind Ihre Beschäftigten?

2. Faires Führungsverhalten

Loyale Beschäftigte sind ein guter Schutz vor Informationsabflüssen

Das Führungsverhalten ist – wie unterschiedliche Studien belegen – ein Schlüssel zur Loyalität gegenüber dem Unternehmen. Beschäftigte, die sich respektlos und nicht wertschätzend behandelt fühlen oder bei Beförderungen fortlaufend übergangen werden, neigen eher zu kriminellen Handlungen und sind empfänglicher für Anwerbungsversuche durch ausländische Nachrichtendienste. Das ihnen entgegengebrachte negative Verhalten wird als Rechtfertigung für die eigenen dolosen Handlungen benutzt.

Ein wertschätzender Führungsstil ist nachweisbar ein wichtiges präventives Element gegen ungewollte Informationsabflüsse[11] und trägt zur Qualität des Arbeitsplatzes bei: Beschäftigte wissen, was bei der Arbeit von ihnen erwartet wird, sie erhalten regelmäßig Anerkennung und Lob für gute Arbeit, die eigenen Meinungen und Vorstellungen werden berücksichtigt sowie Fortschritte besprochen. Kurz: Es wird eine Wertschätzung als Mensch erlebt.

[11] Hofer, Astrid und Weiß, Martin (2016): Wirtschafts- und Industriespionage. Informationsgewinnung – Management – Kompetenz, Wiesbaden: Springer, S. 39.

Eine gelebte Informations- und Fehlerkultur fördern Motivation und Loyalität der Beschäftigten

Aus wissenschaftlicher Sicht ist auch eine dauerhaft gelebte Informationskultur wichtig, da diese Motivation und Loyalität von Beschäftigten fördern kann: „Aus Mitwissen entsteht Mitverantwortung für das Unternehmen“.[12] Eine Grundlage offener und vertrauensvoller Kommunikation ist auch eine konstruktive Fehlerkultur. Wer für Fehler nicht seines Gesichtes beraubt wird, empfindet eine größere Motivation, es das nächste Mal besser zu machen als diejenigen, die vor den Kollegen und Kolleginnen „runtergeputzt“ werden.

Das Bedürfnis der Beschäftigten nach Sicherheit muss ernst genommen werden.

Schließlich ist es im Sinne einer Innentäterprävention bedeutend, dass die Unternehmensleitung die Bedürfnisse der Beschäftigten nach wirtschaftlicher und sozialer Sicherheit ernst nimmt. Kommunizieren Sie daher einen anstehenden Verkauf von Unternehmensteilen oder ein avisiertes Outsourcing in angemessener Weise. Auch sollten negative Folgen möglichst sozial abgefedert bzw. andere Beschäftigungsmöglichkeiten geschaffen werden, damit sich die Motivation, sensible Unternehmensdaten zu missbrauchen, nicht unnötig erhöht.[13]

Die Unterstützung von Beschäftigten in Notfällen wirkt präventiv gegen Informationsabflüsse

Zu einem fairen Führungsverhalten zählt auch, dass Mitarbeiterinnen und Mitarbeiter die in private oder dienstlich bedingte Schwierigkeiten geraten, Hilfe erhalten. Dies ist sowohl aus moralischen Gründen als auch zur Prävention von unlauteren Informationsabflüssen erforderlich: Viele Beweggründe dafür entstehen erst gar nicht oder können abgefangen werden, wenn Beistand oder Hilfe zur Selbsthilfe geleistet wird.

Führungskräfte sollten in der Lage sein, persönliche Schief- und Notlagen ihrer Kolleginnen und Kollegen zu erkennen sowie ihre Sorgen und Nöte ernst zu nehmen und Hilfsangebote zu veranlassen bzw. zu vermitteln. Dieses Gespür ist deshalb wichtig, weil sich Personen mit ernsthaften privaten oder beruflichen Problemen Vorgesetzten gegenüber oft nur ungern offenbaren. Schlimmstenfalls werden Beschäftigte in Notlagen als Problemfall wahrgenommen oder gelten als schwach, weil sie sich hilfesuchend an ihre Führungskraft wenden. Dies sollte unbedingt vermieden werden.

Sozialberatungen können in Problemlagen helfen und unterstützen

Um solchen Ängsten gerecht zu werden, ist es neben der Sensibilisierung der Führungskräfte empfehlenswert, weitere institutionalisierte Ansprechpersonen zur Unterstützung anzubieten. Dies können zum Beispiel fachkundige Personen einer innerbetrieblichen Sozialberatung sein. Sozialberatungen decken in der Regel eine große Bandbreite an Themen zur Hilfestellung ab, die sie selbst oder in

---

12 Hofer, Astrid und Weiß, Martin (2016): Wirtschafts- und Industriespionage. Informationsgewinnung – Management – Kompetenz, Wiesbaden: Springer, S. 39.

13 Blume, Andreas (2018): Innentäterspionage in innovationsgetriebenen Großunternehmen, Analysen zu Sicherheitsfragen, Frankfurt: Verlag für Polizeiwissenschaft, S. 121.

Kooperation mit externen Expertinnen und Experten anbieten. Eine eigenständige Beratung führen Sozialberatungen beispielsweise häufig bei belastenden Konflikten, finanziellen Problemen oder Trauerfällen im nahen Umfeld der Hilfe suchenden Beschäftigten durch. Externe Fachpersonen werden oft bei Suchtverhalten von Beschäftigten oder bei erlebter häuslicher Gewalt hinzugezogen. Die sozialberaterischen Angebote können sowohl von Einzelpersonen als auch von Beschäftigtengruppen wahrgenommen werden.

Eine Beratung von Gruppen kann insbesondere in schwierigen Führungssituationen sowie im Rahmen von Changemanagement-Prozessen und bei Konflikten, die eine externe Mediation erfordern, sinnvoll sein. Aufgabe der Geschäftsleitung ist es dabei, die Hilfsangebote der Sozialberatung zu kennen und sie bei Bedarf für sicherheitsrelevante Themen im Rahmen des betrieblichen Gesundheitsmanagements zu optimieren.

Außerdem sollte Personen, die Ziel einer Anbahnung waren und in diesem Kontext Fehler gemacht haben bzw. erpressbar geworden sind, die Möglichkeit eingeräumt werden, konstruktiv einen Weg aus einer entsprechenden Krisensituation zu finden.

3. Informationsklassifizierung

Unternehmensinformationen sollten durchgehend klassifiziert sein

Stellen Sie sicher, dass Unbefugte keinen Zugriff auf schützenswerte Informationen erhalten. Eine stringente Klassifizierung von betrieblichen Informationen oder Kundendaten, die dem Unternehmen anvertraut werden, ist für einen effizienten Schutz unumgänglich. Nur auf Basis der Klassifizierung können Unterlagen entsprechend gekennzeichnet werden. So wird deutlich kommuniziert, dass im Umgang mit dem Dokument bestimmte Vorgaben einzuhalten sind. Ferner ist die Informationsklassifizierung eine notwendige Voraussetzung, um wertvolle betriebliche Informationen zu Geschäftsgeheimnissen nach dem Geschäftsgeheimnisschutzgesetz (GeschGehG) zu qualifizieren und damit überhaupt eine zivil-/oder strafrechtliche Handhabe bei entsprechenden Verstößen zu haben.

Betriebliche Informationen können verschiedenen Vertraulichkeitsklassen zugeordnet werden

Um Kosten-Nutzen- und Praktikabilitätserwägungen Rechnung zu tragen, hat es sich in der Praxis bewährt, betriebliche Informationen in ein mehrstufiges System von Vertraulichkeitsklassen einzustufen und den Umgang der Daten nach entsprechender Klasse verbindlich zu regeln (siehe dazu Werkzeug II.4). Meist werden vier Informationsklassen verwendet, beispielsweise öffentlich, intern, vertraulich und streng vertraulich. Alternativ ist auch vereinfacht eine zweistufige Klassifizierung (nicht vertraulich/vertraulich) möglich.

Der Wert und das Schutzbedürfnis einer Information steigen von Klasse zu Klasse an. Ein Beispiel einer vierstufigen Informationsklassifizierung ist hier dargestellt:

Informationsklasse	Schadenspotenzial
öffentlich	Kein Schaden aus Unternehmenssicht durch Veröffentlichung bzw. Weiterleitung an Dritte zu erwarten.
intern	Ein (geringer) Schaden durch Offenlegung oder unautorisierte Weitergabe an Dritte ist nicht auszuschließen.
vertraulich	Eine Offenlegung oder unautorisierte Weitergabe an Dritte kann einen finanziellen Schaden, eine Schwächung der Marktposition, negative rechtliche Konsequenzen oder eine Schädigung des Ansehens des Unternehmens, der Geschäftsführung bzw. seiner Organe oder von Beschäftigten nach sich ziehen.
streng vertraulich	Eine Offenlegung oder unautorisierte Weitergabe an Dritte kann einen erheblichen Schaden für die Geschäftszwecke und Ziele des Unternehmens, gravierende negative rechtliche Konsequenzen, ein Sinken des Aktienkurses oder eine schwere Schädigung des Ansehens des Unternehmens, der Geschäftsführung bzw. seiner Organe oder von Beschäftigten nach sich ziehen.

Vgl.: Blume, Andreas (2018): Innentäterspionage in innovationsgetriebenen Großunternehmen, Analysen zu Sicherheitsfragen, Frankfurt: Verlag für Polizeiwissenschaft, S. 101.

Eine regelmäßige Überprüfung der vertraulichen und streng vertraulichen Informationen ist unerlässlich

Schwellenwerte für die Schadenspotenziale der Klassen müssen dabei unternehmensindividuell festgelegt werden. Sie sollten ein Inventar der vertraulichen und streng vertraulichen Informationen der einzelnen Abteilungen erarbeiten und dieses in regelmäßigen Abständen überprüfen, z. B. alle zwei Jahre. Dies geschieht am besten in Arbeitsgruppen, bei denen auch die Ergebnisse der zuvor durchgeführten Risikoanalyse Know-how (siehe Werkzeug II.1) einbezogen werden. Dabei ist es sinnvoll, nicht Einzelinformationen zu betrachten, sondern „Informationscluster“ und die Klassifizierung verbindlich im Unternehmen zu regeln.

In den folgenden Tabellen finden Sie Beispiele für vertrauliche bzw. streng vertrauliche Informationen. Dabei liegt in der Regel der Unterschied zwischen vertraulichen und streng vertraulichen Informationen in der drohenden Schadenshöhe bei Verlust der Vertraulichkeit oder basiert auf rechtlichen Anforderungen, zum Beispiel dem Bundesdatenschutzgesetz.

Mögliche Klassifizierungskriterien für vertrauliche bzw. streng vertrauliche Informationen Informationen, die …
• durch eigene umfangreiche Forschung und Entwicklung entstanden sind,
• ein Konkurrenzunternehmen nutzen könnte, um in kurzer Zeit einen Verdrängungswettbewerb erfolgreich durchzuführen (z. B. Kundendateien),
• konkurrierende Unternehmen bereits (ein-)lizensieren wollten,
• kritisches Erfahrungswissen aus der Produktion von Anlagen darstellen,
• am Markt nicht zu beschaffen sind (keine Kaufoption vorhanden),
• bereits Gegenstand von Wettbewerbsanalyse oder Spionage waren,
• das Unternehmen signifikant vom Wettbewerb unterscheidet und abhebt,
• man selbst gern von der Konkurrenz hätte,
• eine besonders vorteilhafte Kostenposition des Unternehmens stützen,
• durch Gesetze, z. B. Bundesdatenschutzgesetz, besonders geschützt sind.

Vgl.: Blume, Andreas (2018), Innentäterspionage in innovationsgetriebenen Großunternehmen, Analysen zu Sicherheitsfragen, Frankfurt: Verlag für Polizeiwissenschaft, S. 102.

Beispiele für vertrauliche bzw. streng vertrauliche Informationen
• Marketingstrategien, spezielle Informationen über Märkte, Kundendaten und Wettbewerbsteilnehmende
• Investitionspläne
• Preislisten in Kombination mit Produktionskosten
• spezifische Lieferantendaten
• noch nicht veröffentlichte Produktanpassungen
• Mittelfristplanungen, Industriekostenkurven
• Forschungsberichte, Entwürfe zu Patentanmeldungen (i. d. R. streng vertraulich)
• Rezepturen und Verfahrensparameter, Massenbilanzen etc.
• Produktionsdetails für strategische oder neu auf den Markt kommende Produkte
• Liste der Personen in Schlüsselpositionen
• Personalunterlagen
• schützenswerte Revisionsberichte
• schützenswerte Daten Dritter

Vgl.: Blume, Andreas (2018), Innentäterspionage in innovationsgetriebenen Großunternehmen, Analysen zu Sicherheitsfragen, Frankfurt: Verlag für Polizeiwissenschaft, S. 102.

Die Klassifizierung unternehmensbezogener Informationen hat für Sie zwei wesentliche Vorteile: Die Beschäftigten müssen sich mit einer Risikoeinschätzung der Informationen im eigenen Arbeitsumfeld auseinandersetzen und es wird nur dort ein besonderer Schutzaufwand betrieben wird, wo es tatsächlich notwendig ist.

4. Materieller Informationsschutz – Regeln je Vertraulichkeitsklasse

Zu den Schutzklassen gehören konkrete Schutzregeln

Informationen werden klassifiziert, damit diese in Abhängigkeit ihrer Schutzbedürftigkeit angemessen vor unbefugtem Zugriff sowohl von innen als auch von außen geschützt werden. Je Schutzklasse bedarf es konkreter Regeln (Schutzmaßnahmen), die besagen, wie die Informationen sowohl intern als auch gegenüber Dritten zu handhaben sind.

Schutzmaßnahmen müssen im Sinne des GeschGehG dokumentiert werden

Ferner müssen Sie die Schutzmaßnahmen im Sinne des GeschGehG dokumentieren, spätestens, wenn es sich um Informationen handelt, die als Geschäftsgeheimnis gelten. Regelungsbereiche müssen unternehmensindividuell für die einzelnen Vertraulichkeitsklassen definiert, in einer verbindlichen Verfahrensanweisung oder einem Standard festgelegt und unternehmensweit kommuniziert werden. Dazu müssen vorab die entsprechenden IT-Voraussetzungen, z. B. für verschlüsselte E-Mails, geschaffen werden. Grundsätzlich werden dabei die Regeln für den Umgang mit den Informationen über die Vertraulichkeitsklassen „intern", „vertraulich" bis hin zu „streng vertraulich" zunehmend verschärft.

Regelungsbereiche für Vertraulichkeitsklassen von unternehmensbezogenen Informationen

Regelungsbereiche	Beispiele
Kreis der Zugriffsberechtigten	offen, begrenzt, eng begrenzt, namentlich gelistet
Kennzeichnung	die Vertraulichkeitsklasse, z. B. „vertraulich", steht auf jeder Seite des Dokuments
Gesprochenes Wort in der Umgebung	Beschränkungen, Sprechdisziplin, Kreis der Zuhörenden
Speicherung digitaler Dateien	verschlüsselt, auf welchem Medium bis Vertraulichkeitsklasse…
Übermittlung digital	Verschlüsselung von E-Mails, Videokonferenzen, Telefonie etc.
Nutzung von speziellen Internetdiensten	erlaubt/verboten
Nutzung von Fax	erlaubt bis Vertraulichkeitsklasse…
Nutzung von Messenger-Diensten, Whatsapp usw.	erlaubt, verboten oder bis Vertraulichkeitsklasse…
Restriktionen zur Beschränkung der Handhabbarkeit	kein Ausdrucken, kein Export bei streng vertraulichen Dateien
Entsorgung digital	Formatierungs- oder Vernichtungsanforderungen, keine Rückgabe an die herstellenden Unternehmen
Lagerung von Papierdokumenten	im Schrank, Sicherheitsschrank, Tresor
Bestimmte Anforderungen an Räume, die zur Aufbewahrung von Geschäftsgeheimnissen geeignet sind	Verstärkte Wände, Fenster und Türen, Einbruchmeldeanlage
Entsorgung von Papierdokumenten	Schredder, z. B. Kreuzschnitt Klasse 5 für vertrauliche und streng vertrauliche Informationen

Quelle: Eigene Darstellung

Sehr sensible Unternehmensdaten benötigen gesonderte Regelungen

Zu den Anforderungen können Sie auch prozessuale Vorschriften definieren wie: „Keine Übermittlung vertraulicher oder streng vertraulicher Informationen an Dritte ohne zuvor abgeschlossene Geheimhaltungsvereinbarung." Streng vertrauliche Dateien oder Dokumente müssen nach dem Need-to-know-Prinzip entsprechend „gestrippt" bzw. „geschwärzt" werden, bevor sie sowohl an interne als auch an externe Personen weitergeleitet werden.
Darüber hinaus kann es sinnvoll sein, den Kreis der Zugriffsberechtigten für streng vertrauliche Dateien sehr stark zu beschränken und eine Namensliste der Zugriffsberechtigten durch den „Information Owner" führen zu lassen. Eine Erweiterung des Kreises der Mitwissenden um die spezielle Information darf dann nur durch den „Information Owner" erfolgen.

Schließlich sollten Sie auch grundsätzliche Überlegungen zur Beschränkung von Informationszugängen anstellen wie:

- Personen im Praktikum erhalten keinen Zugang zu vertraulichen oder streng vertraulichen Informationen,
- Beschäftigte erhalten erst nach Ablauf der Probezeit Zugang zu streng vertraulichen Informationen,
- bei Mitarbeiterinnen und Mitarbeitern die aus dem Unternehmen ausscheiden, wird individuell geprüft, ob Zugriffsberechtigungen vollumfänglich bis zum letzten Arbeitstag notwendig sind oder auf eher unkritische limitiert werden können.

5. Kontrolle über schützenswerte Informationen gewinnen

Etablieren Sie ein systematisches Daten- und Informations-management

Die zunehmende Digitalisierung führt zu einer zunehmenden Datenflut. Um das Volumen, die Geschwindigkeit und die Vielfalt der Informationen zu beherrschen und um ihre Integrität zu bewahren, ist ein systematisches Daten- und Informationsmanagement notwendig. Ein schneller und kontrollierter Zugriff auf selektierte Informationen ist dabei für Unternehmen essenziell, da Informationen als Grundlage für einen effizienten Betrieb und für die Optimierung von Prozessen dienen. Wissen Sie, welche Informationen sich in Ihrem Unternehmen an welchen Stellen befinden?

Wichtig zu wissen: Welche Informationen befinden sich wo

Nachdem grundsätzlich definiert wurde, welche Informationen innerhalb Ihres Unternehmens als schützenswert gelten, ist es notwendig, diese innerhalb des Unternehmens zu verorten: Wo befinden sich welche Informationen zu welcher Zeit? Dies lässt sich zunächst auf einen einzelnen Informationsstrang anwenden. Im nächsten Schritt müssen die unterschiedlichen Informationsstränge und ihre jeweilige Verortung im Unternehmen zusammengeführt werden.

Ein Beispiel: Eine Produktherstellungsformel befindet sich innerhalb Ihres Unternehmens in verschiedenen Abteilungen. In der Forschungs- und Entwicklungsabteilung liegen die „Erfindungsdokumentation“, Formelzusammenstellung und Testberichte, in der Patentabteilung wird die Formel zur Patentanmeldung hinterlegt, an den Produktionsstandorten werden genaueste Instruktionen und die entsprechende Formel zur Herstellung benötigt und in den Laboren wird die Zusammensetzung zur Qualitätsanalyse des Produktes aufbewahrt. Unter Umständen findet sich die Produktherstellungsformel in weiteren Abteilungen des Unternehmens, die diese alle unter dem Mantel der Verschwiegenheit verwahren müssen.

Erste Schritte zu einem Informationssicherheitssystem

Bevor Sie also ein funktionierendes Informationssicherheitsmanagementsystem (ISMS) in Ihrem Unternehmen verankern können, bedarf es einiger Vorarbeit:

- **Durchführung einer Informationsinventur**
  Zunächst sollten Sie eine Bestandsaufnahme aller relevanten Informationen durchführen, sodass klar wird, welche Art Informationen in welcher Abteilung in welchem Kontext existiert. Dabei müssen alle schützenswerten Daten und Informationen erfasst und katalogisiert werden. Ziel ist es, ein Verständnis für den Aufenthaltsort der Informationen im Unternehmen zu entwickeln. Eine regelmäßige Inventur – mindestens einmal jährlich – ist empfehlenswert. Dabei sollte jede Abteilung eine entsprechende Zusammenstellung durchführen, die Ergebnisse werden dann in einer abteilungsübergreifenden oder prozessorientierten Inventur zusammengeführt. Um die Aktualität der Informationsübersicht zu steigern, können zusätzlich Stichprobeninventuren durchgeführt werden. Diese sollten sich dann vorwiegend auf sensible und vertrauliche Informationsbestände konzentrieren.

- **Durchführung einer Informationsflussanalyse**
  Im Rahmen einer Überblicksmatrix können Sie den Informationsfluss von der Entstehung, Eingabe, Speicherung und Weitergabe bis hin zur Auswertung, Verfügbarkeit und zum Abruf skizzieren. Eine Informationsflussanalyse beinhaltet die Überprüfung bestehender System- und Prozessdokumentationen und die Befragung von Schlüsselpersonen, um alle Nutzungen von Informationen zu ermitteln. Hierbei sollte der Fokus darauf liegen zu verstehen, wer Zugriff auf Informationen hat und welche Systeme an der Informationsverarbeitung beteiligt sind. Verwendungen, die sich außerhalb eines definierten Geschäftsprozesses befinden, können größeren Sicherheitsrisiken ausgesetzt sein. Alle Nutzungen von Informationen, die einer Regulierung unterliegen, müssen katalogisiert und beschrieben werden, damit angemessene Vorkehrungen zur Sicherstellung der Einhaltung getroffen werden können. Durch den Einsatz von Interviews, Listen, Prozessanalysen und Diagrammen können Sie die verschiedenen Systeme und Abläufe beschreiben und identifizieren, um nach Abschluss der Informationsflussanalyse eine weitere Risikoanalyse durchzuführen.

Diese Vorgehensweise lässt sich nun auf viele andere Bereiche und Informationsstränge, zum Beispiel Akquisitionspläne, Finanzzahlen, neue Produkte oder Marken, übertragen. Dabei müssen auch Kommunikationsabteilungen, Strategiebüros, externe Beratungsfirmen und Rechtsabteilungen berücksichtigt werden.

Zusätzliche Schutzmaßnahmen in zentralen Abteilungen

Mit dem Vorgehen gelingt es Ihnen auch, Abteilungen auszumachen, in denen sich mehrere schützenswerte Informationsstränge konzentrieren. Diese Abteilungen bedürfen dann eines gesonderten Augenmerks, da zusätzliche Sicherheitsmaßnahmen und -prozesse sowie Trainings für Beschäftigte in diesen Bereichen zu empfehlen sind. Nur auf dieser Grundlage kann Informationsabfluss überhaupt detektiert oder gar im Vorfeld verhindert werden.

6. Personalauswahl, -einstellung und -einführung

Personalauswahl ist ein präventiver Faktor gegen Informationsdiebstahl

Beschäftigte, ihr fachliches Können, ihre Ideen, ihre Motivation, ihre Leistungsfähigkeit, aber auch ihre charakterliche Eignung und ihre Widerstandsfähigkeit gegen kriminelle Versuchungen sind essenziell für den Unternehmenserfolg – sowohl im Kleinstunternehmen als auch im Weltkonzern. Der Personalauswahl kommt daher eine wichtige Schlüsselfunktion zu. Dies ist auch im Sinne einer Prävention gegen Informationsdiebstahl wichtig.

Fünf Schritte für einen besseren Informationsschutz

Folgende fünf Schritte sollten Sie bei Personalauswahl und beim Onboarding aus Informationsschutzperspektive berücksichtigen:

Maßnahme	Beschreibung
Funktionsbewertung	Festlegung, welche Funktionen im Unternehmen sicherheitsrelevant sind. Bei der Neubesetzung welcher Stellen soll besondere Sorgfalt angewandt werden?
Check der Bewerbungsunterlagen	Eine systematische Überprüfung der Bewerbungsunterlagen kann häufig schnell und kostengünstig betrügerische Personen entlarven oder zumindest Risiken im Hinblick auf den bisherigen Werdegang aufzeigen.
Plausibilitäts- bzw. Background-Check	Plausibilitätsprüfung im Hinblick auf besuchte Hochschulen durch Check der Ortskenntnis, Kenntnis von Lehrpersonal, Identifizierung etwaiger Hinweise, dass Bewerbende von dritter Seite mithilfe von Interna vorbereitet wurden. Background-Checks können je nach Rechtslage auch Selbstauskünfte umfassen (z. B. polizeiliches Führungszeugnis, Schufa).
Fachliche Prüfung	Es ist vergleichsweise leicht, in Bewerbungsunterlagen besondere Kenntnisse, Erfahrungen und Fertigkeiten vorzutäuschen. Fachliche Prüfungen im Bewerbungsgespräch und Arbeitsproben sowie Abfragen von Kenntnissen und Erfahrungen, die laut Lebenslauf auf jeden Fall vorhanden sein müssten, können helfen, unwahre Angaben aufzudecken.
Vertragliche Regelungen	In jeden Arbeitsvertrag gehören rechtlich wirksame Klauseln zur Geheimhaltung und zur Rückgabe/Vernichtung/Löschung aller dienstlichen Unterlagen bei Beschäftigungsende. Auch Wettbewerbsverbote können in besonderen Fällen vereinbart werden. Das neue Geschäftsgeheimnisschutzgesetz (GeschGehG) erlaubt, bei angemessener Formulierung(stiefe), Geheimhaltungsvereinbarungen zu schließen.

Vgl.: Blume, Andreas (2018): Innentäterspionage in innovationsgetriebenen Großunternehmen, Analysen zu Sicherheitsfragen, Frankfurt: Verlag für Polizeiwissenschaft, S. 101.

Um sich darüber klar zu werden, welche Funktionen in Ihrem Unternehmen besonders sicherheitssensibel sind, können Sie sich sogenannte Worst-Case-Szenarien der einzelnen Funktionen vorstellen: Was würde geschehen, wenn Mitarbeiterin X auf der Funktion Y alle Informationen an den direkten Wettbewerber Z weitergeben würde?

Bestimmte Unternehmensfunktionen bedingen eine genauere Betrachtung bei Einstellungen

Beispiele für Funktionen, die eine Überprüfung von Bewerberinnen und Bewerbern bedingen
• Mitarbeitende der Geschäftsführung und ihre Assistenzen
• Leitung, einschließlich Assistenzen von know-how-relevanten Abteilungen
• Personen mit umfangreichem Zugang zu besonders schützenswerten Unternehmensinformationen, insbesondere aus den Bereichen Forschung und Entwicklung, Marketing und Vertrieb, Produktion, Geschäftsentwicklung, Revision, Finanzen, Rechts- und Patentabteilung
• Beschäftigte im Bereich des Werkschutzes, interner Poststellen, Fahrdienst der Geschäftsführung
• IT-Funktionen mit umfangreichen Administrator- und Zugriffsrechten
• Personen, die über ein Vorschlagsrecht zur Besetzung von kritischen Stellen verfügen – seien es eigene Beschäftigte oder Dienstleistungsunternehmen.

Quelle: Eigene Darstellung

Schützen Sie sich vor Betrug im Bewerbungsprozess

Manipulationen im Bewerbungsprozess sind keine Seltenheit. Diese gehen oft weit über die üblichen Selbstdarstellungstechniken hinaus. Außerdem ist es aufgrund der heutigen technischen Möglichkeiten ein Leichtes, Unterlagen und Zeugnisse zu manipulieren. Der systematischen Überprüfung von Bewerbungsunterlagen kommt daher eine erhebliche Bedeutung zu.

Grundsätzlich haben Sie die Möglichkeit, eine entsprechende Überprüfung von Bewerbungsunterlagen an ein qualifiziertes Dienstleistungsunternehmen in einem transparenten Verfahren abzugeben. In den meisten Fällen wird dies jedoch auch die eigene Personalabteilung mit geringem Schulungsaufwand erledigen können. Der Gegenwert dieses Aufwandes ist aus Sicht der Informationssicherheit nicht zu unterschätzen und bemisst sich nicht nur an der Zahl der aufgedeckten Betrugsversuche, da zusätzlich eine erhebliche Abschreckungswirkung erzielt wird.

Maßnahmen gegen Manipulationen im Bewerbungsprozess

Folgende Maßnahmen sind empfehlenswert und in der Regel mit nur minimalem finanziellem Aufwand verbunden und beispielsweise anhand einer Checkliste durchführbar:

- Anforderung und Sichtprüfung aller Originalzeugnisse, Überprüfung auf Manipulationsmerkmale wie auffällige Briefköpfe, Kopierzeichen, fehlende Unterschriften, ungewöhnliches Datum der Zeugnisausstellung,
- Abgleich der Stationen des angegebenen Lebenslaufs mit den eingereichten Zeugnissen einschließlich Kontrolle auf Vollständigkeit und Widerspruchsfreiheit,
- Identifizierung eventueller längerer Lücken im Lebenslauf,
- Recherche nach von der sich bewerbenden Person angegebenen eigenen Publikationen und Abschlussarbeiten,
- Telefonische Überprüfung von angegebenen Referenzen (ggf. nach schriftlicher Einverständniserklärung),
- Check der Arbeitszeugnisse auf Unregelmäßigkeiten, deutliche Über- oder Unterqualifikation, sehr häufige Firmenwechsel bzw. die Beendigung von Arbeitsverhältnissen zu ungewöhnlichem Datum.[14]

Diese Maßnahmen stellen eine Art „Basischeck“ dar, weitergehende Überprüfungen können Background-Checks im Hinblick auf Straftaten darstellen oder Integritäts- und Eignungstests für spezielle Berufsgruppen sein.

[14] Vgl.: Blume, Andreas (2018): Innentäterspionage in innovationsgetriebenen Großunternehmen, Analysen zu Sicherheitsfragen, Frankfurt: Verlag für Polizeiwissenschaft, S. 105.

7. Regelmäßige Schulungen der Beschäftigten

Sie stimmen bestimmt der Feststellung zu, dass es besser ist, Innentäterschaft durch präventive Maßnahmen zuvorzukommen, als sich mit Schäden durch Sabotage, Know-how-Abflüssen etc. auseinandersetzen zu müssen. Dafür bedarf es angemessener Sicherheitsstrukturen und gezielter Maßnahmen: Hierzu zählen z. B. Ein- und Auslass- sowie Arbeitsplatzkontrollen oder das Management von Zutritts- und Zugriffsrechten.

Der Mensch ist der erste Ansatzpunkt für mehr Sicherheit

Technische Aufrüstung allein reicht aber nicht aus. Die Praxis zeigt immer wieder: Erster Ansatzpunkt für mehr Sicherheit ist der Mensch. Auch motivierte und gutmeinende Mitarbeiterinnen und Mitarbeiter, die in jedem Unternehmen zweifelsohne die große Mehrheit bilden, können Fehler machen. Ebenso können sie in eine schwierige Situation geraten, in der sie sich gezwungen fühlen, Dinge zu tun, die sie eigentlich nicht wollen. Ferner können die Schutzwirkung eines Virenscanners, einer Firewall und auch der Passwortschutz aufgrund falscher Anwendung scheitern. Selbst bei hochspezialisierten Cyberangriffen, die z. B. mittels sogenannter Spear-Phishing-Mails durchgeführt werden, setzen die Angreifenden auf unaufmerksame Beschäftigte. Es besteht also immer das Risiko, dass Personen des eigenen Unternehmens auch ungewollt zu Innentätern werden.

Hilfreich sind hier zwei Ungleichungen:
1. Awareness ≠ Training
2. Detektion ≠ Reaktion.

Die Awareness erhöhen – für mehr Sicherheit

Der erste Schritt für Sicherheit ist die Awareness. Ihre Beschäftigten müssen über die Gefahren von Ausforschung und Know-how-Abfluss informiert sein, um eine grundsätzliche Sensibilität für diese Phänomene zu entwickeln. Wer sich der Gefahren nicht bewusst ist, wird Sicherheitsmaßnahmen als „unnötigen Mehraufwand“ empfinden und vernachlässigen. Hierbei helfen insbesondere Beispiele aus der Praxis, welche die zum Teil erheblichen wirtschaftlichen Auswirkungen von Datendiebstahl etc. für ein Unternehmen drastisch belegen.

Auch die konkrete Umsetzung vor Ort muss eingeübt werden

Mit abstraktem Wissen über die Gefahren allein ist es aber noch nicht getan. Training ist genauso wichtig. Dafür ist es notwendig, dass Sie arbeitsplatzscharf und praxistauglich definieren, was sicheres Verhalten im Arbeitsalltag bedeutet. Es reicht nicht, über unternehmenseigene Kanäle wie das Intranet, Flyer oder Poster aktuelle Sicherheitsanweisungen bereitzustellen. Vielmehr gilt es, die Frage zu beantworten, wie sich Ihre Beschäftigten in ihrer jeweiligen Arbeitsumgebung sicher verhalten können. Hierzu praxisgerechte Lösungen zu finden ist keine einfache Aufgabe. Aber es lohnt sich: Sie schaffen damit eine wesentliche Voraussetzung für ein angemessenes Sicherheitsniveau. Denn ohne sensibilisierte und sinnvoll geschulte Mitarbeiterinnen und Mitarbeiter versagen auch die teuersten technischen Sicherheitsmaßnahmen.

Wichtig: Klare Regeln für Verhaltensweisen aufstellen

Gut geschultes und sensibilisiertes Personal ist bei der Detektion von Schadensereignissen ein wichtiges Sensorium, da den Mitarbeiterinnen und Mitarbeitern in der täglichen Praxis Unregelmäßigkeiten unmittelbar auffallen. Damit aber tatsächlich Angriffe abgewehrt werden können, müssen Sie zunächst klare Verhaltensregeln festlegen (Reaktion). Entscheidend ist, dass das Wissen vorhanden ist, was bei einem Vorfall oder einem Verdacht die nächsten Schritte sind. Hierbei gilt es, klare Meldewege zu etablieren. Auch eine positive Fehlerkultur spielt eine wichtige Rolle. Unter Sicherheitsgesichtspunkten betrachtet verhält sich die Mitarbeiterin, die auch eigene Fehler selbst einräumt, sehr viel besser als der Mitarbeiter, der aus Angst vor Konsequenzen bis zuletzt hofft, dass ein begangener Fehler unentdeckt bleibt.

Leider neigt der Mensch dazu, einmalig erlerntes Wissen wieder zu vergessen. Angesichts der heutigen Informationsflut ist es daher umso wichtiger, dass Sie Sensibilisierungs- und Schulungsmaßnahmen regelmäßig wiederholen, um das Wissen Ihrer Firmenangehörigen aufzufrischen. Es geht darum, Einstellung und Arbeitsroutinen nachhaltig unter Sicherheitsgesichtspunkten zu verändern. Auch müssen die vermittelten Inhalte im Interesse der Akzeptanz immer wieder an sich ändernde Arbeitsprozesse angepasst werden. Nur praktikable Sicherheitsanweisungen werden auch tatsächlich befolgt.

Ein wichtiger Baustein im Rahmen der Prävention ist nicht zuletzt eine frühzeitige und enge Verzahnung mit den Sicherheitsbehörden. Dies schafft ein gegenseitiges Verständnis und erhöht im Krisenfall die Reaktionsgeschwindigkeit.

8. Sicherheitskultur und Awareness

Informationsschutz ist Teil einer Sicherheitskultur

Gut gemeinte Schulungen zu Sicherheitsthemen und Informationsschutz verpuffen regelmäßig, wenn sie nicht in eine Sicherheitskultur „eingebettet“ sind. Der Begriff „Sicherheitskultur“ wird definiert als „die Summe von Merkmalen und Einstellungen in Organisationen und von Personen, die sicherstellen, dass als oberste Priorität Themen der Sicherheit die Aufmerksamkeit erhalten, die sie aufgrund ihrer Bedeutung verdienen“.[15] Somit ist auch der Informationsschutz ein Teil der Sicherheitskultur.

[15] International Atomic Energy Agency (Hrsg.) (1991): Safety Culture. A Report by the International Nuclear Safety Advisory Group, Wien.

Erfolgsfaktoren für eine Sicherheit- und Informationsschutzkultur

Sie können durch die Verankerung einer Sicherheitskultur kriminellen Aktivitäten von Beschäftigten erheblich entgegenwirken. Wesentliche Erfolgsfaktoren dafür sind:

- ein klares und wiederkehrend kommuniziertes Bekenntnis der Geschäftsführung zur hohen Bedeutung einer Sicherheits- bzw. Informationsschutzkultur,
- das entsprechende Verhalten aller Führungskräfte als Vorbild für die Belegschaft,
- das Schaffen der physischen und digitalen Voraussetzungen, um ein definiertes Schutzniveau erreichen zu können,
- die Aufstellung und konsequente Vermittlung umsetzbarer Regeln und Techniken
- sowie die nachhaltige Motivierung der gesamten Belegschaft zur Einhaltung der Regeln und zur Kommunikation von Missständen, Vorfällen oder Verdachtsmomenten.

Sensibilisierungs- und Schulungsmaßnahmen regelmäßig wiederholen

Der letzte Punkt ist erfahrungsgemäß besonders herausfordernd. Der Verhaltensforscher Konrad Lorenz sagte sinngemäß: Gehört ist nicht immer verstanden, verstanden ist nicht immer einverstanden, einverstanden ist nicht immer umgesetzt, umgesetzt ist nicht immer beibehalten. Die Kunst ist also, dass Sie es schaffen, eine nachhaltige Einstellungs- und Verhaltensänderung bei Ihren Mitarbeiterinnen und Mitarbeitern zu erreichen. Es stehen Ihnen dazu unterschiedliche Möglichkeiten zur Verfügung, die man unternehmensindividuell ausgestalten und festlegen kann.

Maßnahmen zur Förderung einer Informationsschutzkultur

Maßnahmen zur Förderung einer Informationsschutzkultur
• Persönliche Ansprache neuer Beschäftigter (z. B. „10 goldene Regeln des Informationsschutzes“) durch die Führungskraft und entsprechende explizite (schriftliche) Verpflichtung
• Awareness-Maßnahmen, wiederholte Schulungen und Trainings
• Zielvereinbarungen im Kontext des Informationsschutzes
• Regelmäßige Begehungen und konsequente Einforderung der Regeleinhaltung
• Konsequente, abgestufte Sanktionierung bei Nichtbefolgung
• Regelmäßige Überprüfung der Regeleinhaltung durch Fachaudits und der Revision (falls vorhanden)
• Einrichtung einer Meldestelle – falls möglich auch anonymer Meldeweg
• Regelmäßige Kommunikation über entsprechende Vorfälle

Quelle: Eigene Darstellung

Mit Penetrationstest lassen sich Sicherheitslücken und Schwachstellen finden

Es existiert eine lange Reihe unterschiedlicher Awareness-Maßnahmen, die eingesetzt werden können, um das Thema Informationsschutz innerhalb Ihres Unternehmens zu fördern. Ein Beispiel für eine solche Awareness-Maßnahme stellen sogenannte Penetrationstests dar. Bei diesen handelt es sich um Überprüfungen, die in der Regel ein Unternehmen bei einem externen Dienstleistungsunternehmen in Auftrag gibt, um etwaige Sicherheitslücken und Schwachstellen bei sich selbst zu identifizieren. Nach Abschluss der Checks werden die Resultate dem Unternehmen mitgeteilt, damit dieses ggf. notwendige Sicherheitsmaßnahmen ergreifen kann.

Mittels eines Penetrationstests wird versucht, ein System mit Mitteln und Methoden, die auch von realen Angreifern genutzt werden, zu infiltrieren und als unbefugte Person einen Zugriff auf schützenswerte unternehmenseigene Daten zu erhalten. Dies kann auf verschiedenen Wegen geschehen:

- Analog: Man testet physische Beschränkungen im Unternehmen aus, etwa Zugangsbeschränkungen zum Werksgelände oder in bestimmte sicherheitsrelevante Bereiche (Perimeterschutz/Objektschutz/Innenhaut).
- Digital: Das Ziel des Datenabgriffs wird über klassisches Hacking und Cyberangriffe auf das Unternehmensnetzwerk verfolgt.
- Social Hacking: Man versucht mittels Kommunikationstechnik (Telefon, E-Mail, Messenger-Dienste usw.) und trickreicher Manipulation Unternehmensangehörige zu veranlassen, entweder Datenzugriffe durch eine unbefugte Person zu ermöglichen oder selbst die Daten nichtautorisiert weiterzugeben.

Beispiele für Awareness-Maßnahmen

Die folgende Auswahl an weiteren Maßnahmen kann – je nach Situation – eine gute bis sehr gute Wirkung entfalten:

Überblick über Awareness-Maßnahmen bezüglich Informationsschutz
• Präsenztrainings mit interaktiven Elementen/Workshops
• Anonymisierte Kommunikation von aktuellen Vorfällen („aus gegebenem Anlass …“)
• Regelkommunikation in Abteilungsbesprechungen, Teammeetings
• Videos mit unterschiedlichen Inhalten zum Thema Informationsschutz, ggf. auch mit O-Tönen von Beschäftigten mit unterschiedlichen Funktionen, Kurzvideos auf der Startseite des Intranets, die wöchentlich wechseln
• Ansprechend gestaltete Security-Plattform im Intranet (Überblick über Regularien, Hilfsmittel, Ansprechpersonen) mit aktuellen Meldungen
• Gamification (Integration spielerischer Elemente zur Motivationssteigerung)
• Externe Fachvorträge

Quelle: Eigene Darstellung

Eine Vielzahl von Awareness-Materialien wie Videos oder Broschüren finden Sie auf der Internetseite www.wirtschaftsschutz.info der Initiative Wirtschaftsschutz oder bei spezialisierten Dienstleistungsunternehmen.

www.wirtschaftsschutz.info für mehr Awareness-Materialien

Erfahrungsgemäß bedarf es einer längerfristigen intensiven und wiederkehrenden Kommunikation zum Informationsschutz, bis verhaltenswirksame Einstellungen bei einem Großteil der Belegschaft erreicht sind. Die Bemühungen um Informationsschutz dürfen aber auch danach nicht „einschlafen". Ein webbasiertes Training mit Verständnisfragen am Ende und einer Teilnahmebestätigung kann dabei helfen, das Verständnis zu überprüfen. Dank der automatischen Dokumentation der Schulungsteilnahme ist Ihr Unternehmen auch für ein etwaig notwendiges zivil- oder strafrechtliches Verfahren gewappnet.

Prüfen Sie das Sicherheitsverständnis der Beschäftigten

Sie können auch prüfen, ob bei den Mitarbeitern und Mitarbeiterinnen bereits eine informationsschutzaffine Einstellung erzielt wurde und das Wissen in der Praxis angewandt werden kann. Dazu können Situationen dienen, die im Regelwerk nicht beschrieben sind, also dementsprechend keine Standardlösung vorgegeben ist. Wenn die Beschäftigten dann selbständig nach sicheren Lösungen suchen und diese mit ihren Kolleginnen und Kollegen oder ihren Führungskräften besprechen, ist ein wichtiger Schritt hin zu einer funktionierenden Informationsschutzkultur vollzogen.

9. Spezialschulung für besondere Funktionen und Know-how tragende Personen

Der potenzielle Schaden durch Innentäter hängt auch von deren Position ab

Jede Mitarbeiterin und jeder Mitarbeiter kann bewusst oder unbewusst Schaden zum Nachteil des Unternehmens verursachen. Die Bandbreite des potenziellen Schadens, der von Einzelnen verursacht werden kann, variiert nach Position und Funktion im Unternehmen und kann existenzbedrohliche Ausmaße annehmen. Daher ist es wichtig, dass sich die Geschäftsführung darüber klar wird, welche Funktionen im eigenen Unternehmen besonders sicherheitsrelevant sind:

- Wer sind die Kompetenz tragenden Personen?
- Welche Personen verfügen über weitreichende Entscheidungsbefugnisse, die bei erfolgter Manipulation dem Unternehmen erheblich schaden könnten?
- Wer trägt zur Aufrechterhaltung der Unternehmenssicherheit besonders bei?

Spezifische Sensibilisierungen für spezielle Positionen

Diese Gruppen stehen potenziell besonders im Fokus von Dritten und müssen daher überdurchschnittlich geschützt werden. Dieser Schutz beginnt beispielsweise mit einer intensiven Sensibilisierung und Schulung zu folgenden Themen:

Beispiel für Schulungsthemen für Personen auf herausgehobenen Positionen: Identifizierung und sichere Abwehr von …
• Methoden des Ausfragens am Telefon bzw. per E-Mail (Social Engineering/Social Hacking)
• offener Gesprächsabschöpfung (ausgefragt werden im persönlichen Gespräch)
• Korruptionsanbahnung und -versuchen
• „Kultivierungsbemühungen“ von Konkurrenzunternehmen oder Nachrichtendiensten

Quelle: Eigene Darstellung

Sensibilisierung schützt vor unbeabsichtigter Informationspreisgabe

Beschäftigte, die nicht ausreichend zu diesen Themen sensibilisiert werden, laufen Gefahr, ungewollt zu Innentätern zu werden, da die Gegenseite oft sehr trickreich und psychologisch gekonnt ihre Ziele verfolgt. Dies gilt auch für Verhandlungen mit Lieferunternehmen und im Rahmen von Geschäftspartnerschaften, in denen durch geschickte Gesprächsführung entscheidende Informationen unabsichtlich preisgegeben werden (siehe auch Social Engineering).

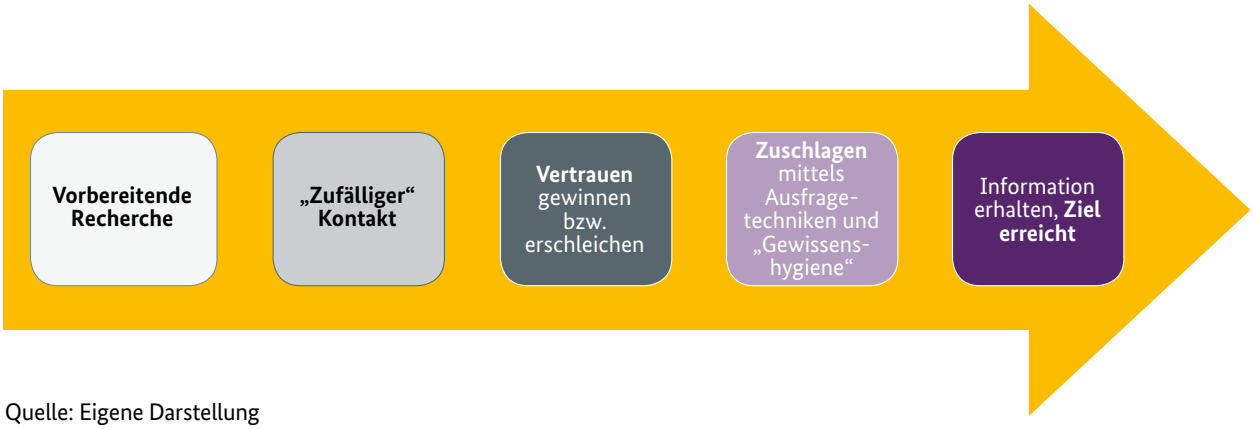
10. Social Engineering

Social Engineering ist eine reale Gefahr für die Informationssicherheit

Um an Informationen zu kommen, nutzen viele Angreifende das sogenannte Social Engineering. Darunter versteht man eine Form der zwischenmenschlichen Beeinflussung mit dem Ziel, unbemerkt an kritische Informationen zu gelangen. Dabei werden häufig menschliche Schwächen oder sogenannte Reiz-Reaktions-Schemata genutzt. Kriminelle Personen spionieren zunächst das Umfeld ihres Opfers aus, informieren sich in sozialen Netzwerken oder mittels anderer offen zugänglicher Quellen über die Zielperson, erfinden vielfach plausibel klingende Lügengeschichten und nehmen passende Identitäten an, um eine Rechtfertigung ihrer Nachfrage nach sensiblen Informationen vorzutäuschen.

Telefonische Attacken abzuwehren ist vergleichsweise leicht: eine angezeigte Telefonnummer nicht als Identitätsbeweis akzeptieren, bei kritischen oder unklaren Anliegen den Rückruf anbieten oder sich die Anfrage kurz per Mail bestätigen lassen. Im persönlichen Gespräch ist es dagegen oft schwierig, normale Fachgespräche von manipulativer offener Gesprächsabschöpfung zu unterscheiden, z. B. auf Konferenzen oder einer Messe.

Eine Social Engineering-Attacke läuft oft in mehreren Phasen ab:



Quelle: Eigene Darstellung

In der vierten Phase, dem „Zuschlagen", kommen häufig spezielle Ausfragetechniken zur Anwendung. Diese sind sehr vielfältig und führen oft zum Ziel. Gleichzeitig wird der Person das Gefühl vermittelt, eigentlich auch gar nichts falsch zu machen.

Beispiele für manipulative Ausfragetechniken

Beispiele für manipulative Ausfragetechniken (offene Gesprächsabschöpfung)	
Konfrontation mit Falschaussagen: Fachliche Statements „ins Blaue" und gezielte Falschaussagen nutzen das Überraschungsmoment aus. Es wird eine spontane, affektive Reaktion ausgelöst, weil das Gegenüber die Aussage berichtigen will bzw. klären möchte, ob selbst ggf. ein falscher Kenntnisstand vorliegt.	→ Bsp.: „Das Marktvolumen des Produktes X beträgt 2,4 Mio. Euro pro Jahr."
Köder legen: Die angreifende Person gibt ein Thema vor und erzählt vorgeblich etwas über sich, Erfahrungen und die eigene Situation. Aufgrund des tief im Menschen verwurzelten Gegenseitigkeitsprinzips wird die Zielperson oft in die Diskussion zu diesem Thema einsteigen und etwas über sich erzählen.	→ Bsp.: „Mein Gott, was ich da schon alles erlebt habe …"
Hilfe erbitten: Man bittet jemanden um Hilfe bei der Lösung eines Problems. Trickreich dabei ist, nicht direkt nach einer sensiblen Information zu fragen, sondern nur ein „Signal" erhalten zu wollen, ob man grundsätzlich richtig oder falsch liegt. Ferner wird das Gegenüber als fachkundige Person gelobt, deren Rat man sehr schätzen würde.	→ Bsp.: „Sie müssen mir keine kritischen Informationen geben, aber ich wäre sehr erleichtert, wenn Sie als Expertin mich etwas unterstützen könnten."
Angebliche Entscheidungsfreiheit geben: Eine Zielperson soll durch eine sogenannte „verneinte Aufforderung" zur Aussage verleitet werden. Man vermittelt der Zielperson eine angebliche große Entscheidungs- und Handlungsfreiheit, erzeugt damit jedoch künstlich ein schlechtes Gefühl beim Gegenüber.	→ Bsp.: „Ich verstehe, dass Sie jetzt darüber nicht sprechen wollen, das müssen wir auch nicht. Ich stelle ihnen aber gerne alle unsere Informationen zum Projekt zur Verfügung." → **Diese gelieferten Projektinformationen können gefälscht sein.**

Quelle: Eigene Darstellung

Möchte die angreifende Person z. B. den zuständigen Sachbearbeiter eines Unternehmens bestechen, um an Geschäftsgeheimnisse zu gelangen oder bei einer Ausschreibung zum Zuge zu kommen, wird er diesen Mitarbeiter in den meisten Fällen davon überzeugen müssen, dass diese Tat – wenn auch offensichtlich nicht legal – dann doch zumindest irgendwie gerechtfertigt sei. Das häufig aufkommende schlechte Gewissen muss daher „beruhigt" werden. Dies kann unter anderem dadurch geschehen, dass man das Gegenüber Glauben macht, dass die Handlung doch gar nicht mit negativen Folgen verbunden sein könnte.

→ Bsp.: „Die Informationen sind doch gar nicht als streng vertraulich klassifiziert, also ist es auch kein Problem"; oder: „von Ihrem Wissen kann doch nicht nur ein Unternehmen profitieren – das ist doch wichtig für alle."

Alternativ kann der Angreifer anbringen, dass das doch nur gerecht sei:

→ Bsp.: „Ihr Chef sieht nicht, was Sie können, und honoriert Ihre Arbeit nicht ausreichend. Dann ist das doch nur gerecht, wenn Sie sich die Anerkennung woanders holen!"

Bereiten Sie die Beschäftigten auf Social Engineering-Attacken vor

Es ist wichtig, dass Sie Ihre Beschäftigten auf solche Situationen vorbereiten. Dadurch können Sie die Wahrscheinlichkeit erhöhen, dass diese standhaft bleiben und entsprechende Offerten ablehnen und umgehend unternehmensintern melden. Dies gilt noch mehr für den Fall, wenn psychologisch versierte Angreifende (z. B. Anwerber von Nachrichtendiensten) versuchen, Know-how-Träger und -Trägerinnen für sich zu gewinnen. Methoden und Tiefe dieser sogenannten „Verstrickungen" sind sehr vielfältig und können hier nicht ausführlich beschrieben werden. Allen Methoden – außer dem sogenannten „Crash-Approach", wobei die angreifende Person unverblümt und schnell zur Sache kommt und Geld gegen Informationsverrat anbietet – ist gemein, dass die Zielperson im Hinblick auf ihre Stärken mehr noch auf ihre Schwächen und unerfüllten Wünsche sowie Bedürfnisse hin genau analysiert wird.

Werden entsprechende Anbahnungsversuche jedoch früh identifiziert und gemeldet, ist es durchaus möglich, dem Angriff unbeschadet zu entkommen. Im Folgenden wird beispielhaft der Verlauf einer Anbahnung durch einen ausländischen Nachrichtendienst dargestellt.

Verlauf einer Anbahnung durch einen ausländischen Nachrichtendienst

Typischer Verlauf einer Anbahnung durch einen ausländischen Nachrichtendienst

- Die Kontaktaufnahme (insbesondere durch spezialisierte Personen eines ausländischen Nachrichtendienstes) kann sehr unspektakulär und beiläufig passieren, zum Beispiel am Rande einer Veranstaltung oder auch im privaten Bereich. Anfangs wird sich der Kontakt im Rahmen einer ganz normalen Bekanntschaft bewegen. Man kommt z. B. auf einer Messe ins Gespräch und tauscht Kontaktdaten aus.
- Das Gegenüber ist meist äußerst freundlich und zeigt großes Interesse am Berufs- und Privatleben der Zielperson. Es fragt nach Hobbies, Wünschen, Zielen, aber auch nach der Stellung im Unternehmen und der Zufriedenheit mit dem Beruf. Man ist sich „auf Anhieb“ sympathisch und vereinbart ein Telefonat oder direkt ein Folgetreffen.
- Wiederkehrende Einladungen in Cafés, Restaurants, Nachtclubs etc.; die Initiative geht dabei vom Gegenüber aus. Es bestimmt, wo und wann man sich trifft. Bei den Trefforten handelt es sich stets um neutrale Plätze. Die Rechnung wird in der Regel vom Gegenüber übernommen.
- Während bei den ersten Begegnungen lediglich beiläufige Themen besprochen werden, lenkt das Gegenüber den Fokus mit zunehmender Vertrautheit auf sein eigentliches Ziel. So wird etwa konkreter nach Arbeitsschwerpunkten, technischen Details oder anderen Personen mit dem gesuchten Know-how gefragt.
- Es werden Geschenke gemacht, oftmals auch eine „Aufwandsentschädigung“ für die gelieferten nützlichen Informationen.
- Die Zielperson erhält Angebote über Honorartätigkeiten, bspw. Fachvorträge oder schriftliche Ausarbeitungen oder die Einladung, ein gut bezahltes „Consulting-Projekt“ im Ausland (während des Urlaubs) anzunehmen. Im Ausland bieten sich dem fremden Nachrichtendienst dann bessere Möglichkeiten für einen direkten Anwerbungsversuch. Möglicherweise wird im Zuge dessen auch eine neue Ansprechperson eingeführt, welche die Verbindungsführung übernehmen soll.
- Die Überführung in ein dauerhaftes Informationsverhältnis als „Quelle“ kann auf unterschiedliche Art und Weise erfolgen. Eine Möglichkeit ist, dass das Gegenüber sich offenbart und offen wirbt. Alternativ wird auch „unter falscher Flagge“ aufgetreten und sich z. B. als Mitarbeiterin eines Konkurrenzunternehmens oder eines wissenschaftlichen Instituts ausgeben.
- Wenn sich die Zielperson nicht aus freien Stücken zur Zusammenarbeit bereit erklärt, besteht auch die Möglichkeit, dass das Gegenüber Druckmittel einsetzt und z. B. mit (angeblich vorliegendem) kompromittierendem Material, z. B. Filmaufnahmen sowie Browser- oder Chatverläufen, droht.

Quelle: Eigene Darstellung

Eine erhöhte Gefahr besteht bei Geschäftsreisen ins Ausland

Erfahrungsgemäß bergen Auslandsreisen von besonders sicherheitsrelevanten Personen sowie Entsendungen in sogenannte Hochrisikoländer ein deutlich erhöhtes Gefährdungspotenzial, in das Visier eines Nachrichtendienstes zu geraten und angebahnt zu werden. Auf eigenem Territorium unter Nutzung lokaler menschlicher und technischer Netzwerke ist eine Überwachung bzw. Manipulation ausländischer Geschäftsreisender komfortabel: Bei Personen, die länger im Land verbleiben, kann der häufig auftretende Kulturschock gezielt für Anbahnungsversuche, z. B. mittels einer vorgetäuschten freundschaftlichen Verbindung oder Liebesbeziehung, ausgenutzt werden.

Bereiten Sie Ihre Unternehmensangehörigen intensiv auf diese oben skizzierten Risiken mittels Schulungen, Workshops oder anderen Awareness-Maßnahmen vor. Bedenken Sie: Auch kleine und mittelständische Unternehmen können genauso in den Fokus solcher Aufklärungsbemühungen von Konkurrenzunternehmen oder Nachrichtendiensten rücken wie multinationale Konzerne.

11. Management von Beschäftigtenaustritten

Besondere Vorsicht bei der Beendigung von Beschäftigungsverhältnissen

Wenn Unternehmensangehörige aus dem Unternehmen ausscheiden, steigt das Risiko des Datendiebstahls erfahrungsgemäß erheblich an. Beschäftigte werden gekündigt, sie kündigen von sich aus, ihr Arbeitsvertrag wird nicht verlängert oder sie gehen vorzeitig in Rente und möchten noch für einige Jahre freiberuflich tätig sein. In allen Fällen sollten Sie aus Unternehmenssicht besondere Vorsicht walten lassen, denn in einem signifikanten Anteil der Fälle verschaffen sich ausscheidende Firmenangehörige Unternehmensdaten, um diese in irgendeiner Weise selbst weiter zu nutzen. Eine Analyse von 48 öffentlich gewordenen Fällen von Datendiebstahl ergab: In rund 65 % der Fälle hatten die Personen bereits eine neue Tätigkeit bei einem Konkurrenzunternehmen vereinbart oder sie bereiteten eine Selbständigkeit vor. Über die Hälfte der kriminellen Personen entwendeten im letzten Monat der Beschäftigung sensible Firmendaten. Dabei ist besonders brisant, dass in drei Viertel der Fälle die Beschäftigten regulär bis zum Schluss Zugriff auf sensible Daten hatten.[16]

4 wichtige Schritte beim Unternehmensaustritt aus Sicht des Informationsschutzes

Sie können sich vor diesem Datenverlust schützen, indem Sie einen systematischen Prozess des „Exits“ aus dem Unternehmen einführen und konsequent durchsetzen. Folgende vier Schritte sind für den Informationsschutz empfehlenswert:

[16] Moore, A.P. et al. (2011): A Preliminary Model of Insider Theft of Intellectual Property, Pittsburgh.

Maßnahme	Beschreibung
Funktionsbewertung	Festlegung, bei welchen Funktionen ein Exit-Prozess ausgelöst werden soll. Dies sollten auf jeden Fall alle Funktionen sein, die auch bei der Neubesetzung überprüft werden, es können jedoch noch weitere Stellen sein – die Einschätzung sollte sich nach den tatsächlichen Informationszugängen und der Höhe des Schadenspotenzials richten.
Risikoerhebung	Über welche konkreten kritischen Informationszugänge verfügt der oder die Beschäftigte? Wie lange war die Person auf der kritischen Funktion beschäftigt? Gab es Auffälligkeiten? Ließen sich Hinweise erkennen, dass die Person Know-how nach dem Ausscheiden verwenden will?
Risikobewertung und Umsetzung fallindividueller Maßnahmen	**Geringes Risiko („grün"):** Regulärer Verbleib bis zum letzten Arbeitstag, Übergabe aller notwendigen Daten an die Führungskraft, Sperrung aller Zutritts- und Zugriffsmöglichkeiten zum letzten Arbeitstag. **Mittleres Risiko („gelb"):** Ggf. Beschränkung der Informationszugriffe bis zum letzten Arbeitstag, etwaige Freistellung zum flexiblen Datum, das Betriebserfordernissen gerecht wird; Durchführung eines dokumentierten Exit-Gesprächs. **Hohes Risiko („rot"):** Durchführung eines Exit-Gesprächs, falls belegbarer Anfangsverdacht, Durchführung von unternehmensinternen Ermittlungen, ggf. Freistellung und falls erforderlich Erteilung eines Werksverbots.
Weitere Maßnahmen im Verdachtsfalle	Als weitere rechtliche Maßnahmen kommen nach Überführung bzw. bei konkretem Tatverdacht u. a. in Betracht: Strafbewehrte Unterlassungs- und Verpflichtungserklärung mit Auskunft über den Verbleib und die Nutzung der kopierten/entwendeten Daten Erstattung Strafanzeige nebst Strafantrag Erhebung der zivilrechtlichen Klage auf Auskunft, Herausgabe, Unterlassung und Schadensersatz dem Grunde nach Schadensersatzklage (falls Schaden konkret bemessen und die Beweiskette sicher geführt werden können)

Quelle: Eigene Darstellung

Wichtig sind sowohl reaktive als auch präventive Maßnahmen

Da erfahrungsgemäß die Motivation, sich Firmendaten beim Ausscheiden unerlaubt privat zu sichern, nicht unterschätzt werden sollte, ist zu empfehlen, in relevanten Fällen sowohl präventive als auch reaktive Maßnahmen zu treffen. Zu den präventiven Maßnahmen zählt insbesondere das Exit-Gespräch, das man als Baustein in ein normales Abschiedsgespräch einbauen kann, wenn das Risiko (s. o.) es als notwendig erscheinen lässt.

Mögliche Themen und Elemente eines Exit-Gesprächs

Mögliche Elemente/Themen eines „Exit-Gesprächs“
• Erinnerung an arbeitsvertraglich eingegangene Pflichten zur Geheimhaltung und Verbot der „privaten Datensicherung“ von Geschäftsgeheimnissen
• Hinweis auf Pflicht zur Rückgabe aller dienstlichen Unterlagen jedweder Art, also von Datenträgern, Speichermedien, Aufzeichnungen, Modellen, Prototypen usw.
• Hinweis auf die nachvertragliche Treuepflicht einschließlich entsprechender Erläuterung
• Erinnerung an etwaig gesondert unterzeichnete Geheimhaltungsvereinbarungen (GeschGehG)
• Mögliche Rechtsfolgen bei Verstößen gegen strafrechtliche und zivilrechtliche Vorschriften
• Mögliche Schadensersatzansprüche nach BGB
• Auszüge der relevanten gesetzlichen Normen (als Anhang)

Quelle: Eigene Darstellung

Wenn das Ausscheiden eines Mitarbeiters feststeht, dessen Risikobeurteilung mindestens als „mittel“ eingestuft wird, ist es opportun, das Gespräch schnellstmöglich zu führen und zu dokumentieren. Im Falle eines festgestellten hohen Risikos („rot“) ist es empfehlenswert, bei vorliegendem Anfangsverdacht Ermittlungen im Hinblick auf einen etwaigen Verstoß gegen § 23 GeschGehG aufzunehmen. Wichtig dabei ist, dass der Anfangsverdacht dokumentiert wird und qualitativ auch einer etwaigen Überprüfung vor Gericht standhält (mehr dazu siehe Kapitel III Detektion).

12. Externe Kooperationen

7 Punkte für mehr Informationssicherheit in Geschäftskooperationen

Eine unternehmerische Tätigkeit, die vollständig auf externe geschäftliche Beziehungen verzichtet, ist heutzutage für viele Unternehmen quasi undenkbar: Kooperationen bieten einen erleichterten Zugang zu Ressourcen, Technologien und Märkten. Und doch müssen auch die Risiken eines Informationsabflusses ins Kalkül gezogen werden. Zum Schutz Ihrer Informationen empfiehlt es sich daher, dass Sie bei externen Kooperationen die folgenden sieben Punkte berücksichtigen:

Maßnahme	Beschreibung
Prüfung der Kooperationseignung	Nicht jedes Projekt eignet sich zur Kooperation. Manche Entwicklungen sind so geheimhaltungsbedürftig, dass eine Kooperation über die Unternehmensgrenzen hinweg nicht angebracht ist.
Hintergrundrecherche	Prüfung der Zuverlässigkeit und Vertrauenswürdigkeit des avisierten Gegenübers: Ist davon auszugehen, dass auch das gehalten wird, was versprochen wurde? Ferner kann es bei besonders know-how-lastigen Kooperationen empfehlenswert sein, auch die Informationsschutz-Architektur des Kooperationspartners zu überprüfen (analog zu z. B. ISO 27001).
Festlegung der Form der Kooperation	Welche Kooperationsform ist für das geplante Projekt angemessen? Wie weit möchten Sie sich der anderen Seite öffnen? Soll nur ein Service beauftragt oder ein gesamtes Gewerk vom Gegenüber übernommen werden? Für welchen Zeitraum ist die Kooperation angedacht? Ist ggf. die Gründung eines neuen, eigenständigen Unternehmens (z. B. Joint Venture) erforderlich?
Festlegung und Begrenzung der Kooperationsinhalte	Innerhalb des betroffenen Teams sollte festgelegt werden, welche Informationspakete geteilt werden sollen – und welche nicht. Insbesondere wenn das Kooperationsunternehmen in anderen Bereichen eine Konkurrenz darstellt, ist es wichtig, die eigenen Beschäftigten zum Beispiel anhand einer „Black-and-White-List“ zu schulen und dazu zu verpflichten, nur diejenigen für die Kooperation notwendigen Informationen – und keine darüber hinaus – zu teilen. Es gilt das sogenannte Need-to-know-Prinzip: Kenntnis nur, wenn für die Aufgabenerledigung notwendig.
Abschluss einer Geheimhaltungsvereinbarung	Schließen Sie eine projektindividuelle, rechtsverbindliche Vereinbarung zur Geheimhaltung ab.
Festlegung von Mindestanforderungen zum Informationsschutz	Es ist empfehlenswert, sich bei besonders know-how-sensiblen Kooperationen auf ein Mindestniveau für den Informationsschutz zu verständigen und dies schriftlich festzulegen.
Austausch zu und Umgang mit etwaigen Vorfällen	Vorab sollten Sie auch regeln, wie mit Zwischenfällen oder Verdachtsmomenten bezüglich illegaler Informationsabflüsse im Rahmen der Kooperation umgegangen werden soll.

Quelle: Eigene Darstellung

Pre-Business-Screening vor Abschluss der Kooperationsvereinbarung

Eine genauere Analyse des Hintergrunds und der Vertrauenswürdigkeit Ihres Gegenübers (Pre-Business-Screening) sollten Sie bei sensiblen Kooperationen vor dem Abschluss der Kooperationsvereinbarung und dem Austausch vertraulicher Informationen durchführen. Holen Sie sich, falls nötig, Hilfe von einem externen Dienstleistungsunternehmen.

Sensibel können Kooperationen unter anderem dann sein, wenn streng vertrauliche Informationen oder eine große Anzahl vertraulicher Informationen ausgetauscht werden muss oder beispielsweise einem Dienstleistungsunternehmen Zugriff auf kritische IT-Systeme des eigenen Unternehmens eingeräumt werden soll. Darüber hinaus können Lieferbeziehungen im Hinblick auf knappe spezielle Rohstoffe oder Zwischenprodukte sowie know-how-relevante Maschinen, Reaktoren oder Anlagen (insbesondere Einzelanfertigungen) kritisch sein. Auf Basis von Verhältnismäßigkeits- und Kosten-Nutzen-Erwägungen sollten sich Breite und Tiefe eines Pre-Business-Screenings nach der Kritikalität der avisierten Geschäftsbeziehung richten.

Mögliche Elemente eines Pre-Business-Screenings

Mögliche Elemente eines Pre-Business-Screenings
• Verifizierung der Geschäftstätigkeit
• Prüfung der Kreditwürdigkeit
• Prüfung der Eigentumsverhältnisse
• Prüfung auf etwaig anhängige Gerichtsverfahren
• Prüfung von Korruptions-, Sanktions- und Watchlisten
• Ausschluss relevanter Hinweise auf mögliche Interessenkonflikte

Quelle: Eigene Darstellung

Was sollte eine Geheimhaltungsvereinbarung grundsätzlich umfassen? Die folgende Liste erhebt keinen Anspruch auf Vollständigkeit; auch hängt es von der geplanten Geschäftsbeziehung ab, welche Punkte im Einzelnen relevant sind:

Mögliche Punkte für eine Geheimhaltungsvereinbarung

Mögliche Punkte, die in einer Geheimhaltungsvereinbarung geregelt werden sollten

- Präambel, die besagt, welches Know-how bereits vor der Kooperation vorhanden ist und weshalb eine Geschäftsbeziehung angestrebt wird
- Festlegung, die festhält, welche kooperationsrelevanten Informationen geheimhaltungswürdig sind
- Festlegung darüber, was unter Geheimhaltung im Sinne der Vereinbarung zu verstehen ist (Verwendung der Informationen ausschließlich für das Projekt und Modus der Handhabung, z. B. „streng vertraulich, keine Weitergabe an Dritte“)
- Vereinbarung von Rückgabe- und Löschpflichten
- Festlegung der Verfügungsrechte über die geteilten Informationen
- Festlegung des Rechts zur Anmeldung von Schutzrechten
- Nennung von Ausnahmen
- Dauer des Offenlegungszeitraums (d. h. Dauer des Informationsaustausches) und der Geheimhaltungsvereinbarung
- Notwendigkeit der schriftlichen Zustimmung von Änderungen der Geheimhaltungsvereinbarung
- Festlegung des geltenden Rechts, Gerichtsstand, ggf. Schiedsgerichtsbarkeit, salvatorische Klausel, ggf. Vereinbarung der Mindestanforderungen an den Informationsschutz und die Vorgaben zum sicheren Austausch der Informationen innerhalb der Kooperationspartnerschaft

Quelle: Eigene Darstellung

Besonderes Augenmerk bei Kooperationen gilt den Informationsschutzmaßnahmen

Bei Kooperationen, bei denen die Geheimhaltung eine besonders wichtige Rolle spielt, sollten Sie im Vorfeld der Zusammenarbeit bereits das Niveau von Informationsschutzmaßnahmen thematisieren. Es ist auch nicht unüblich, dass Mindeststandards des Informationsschutzes durch eine Partei vorgeschrieben und im Kooperationsvertrag bzw. der Geheimhaltungsvereinbarung aufgenommen werden und ggf. auch auditiert werden können. Als Mindeststandards können allgemeingültige Normen zum Informationsschutz angewendet werden (z. B. ISO 27000). Wichtig ist auch, dass ein sicherer Weg gefunden wird, auf welche Weise (streng) vertrauliche Informationen ausgetauscht werden können.

Beispielhafte Mindestanforderungen an den Informationsschutz

Die folgende Liste bietet einen Überblick über mögliche, relativ abstrakt gehaltene Schutzmaßnahmen. Diese können Sie auch innerhalb Ihrer Kooperation noch weiter konkretisieren.

Beispielhafte Mindestanforderungen an den Informationsschutz im Rahmen externer Kooperationen	
√	Das Unternehmen verfügt über eine Informationsschutzrichtlinie.
√	Personen, die sich auf sicherheitsrelevante Funktionen bewerben, werden einem legalen Background-Check unterzogen.
√	Allen Beteiligten wird durch Ausbildung und Schulung ein angemessenes Sicherheitsbewusstsein vermittelt.
√	Regeln für den zulässigen Gebrauch von Informationen und Werten sind aufgestellt, dokumentiert und werden angewendet, z. B. eine durchgängige Informationsklassifizierung einschließlich verbindlicher Regeln je Informationsklasse.
√	Verfahren für die Handhabung von Wechseldatenträgern sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt.
√	Nicht mehr benötigte Datenträger werden sicher und unter Anwendung formaler Verfahren entsorgt.
√	Eine Zugangssteuerungsrichtlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft.
√	Benutzerinnen und Benutzer haben ausschließlich Zugang zu den Netzwerken und Netzwerkdiensten, zu deren Nutzung sie ausdrücklich befugt sind.
√	Die Zugangs- und Zugriffsrechte aller externen Personen zu Informationen und informationsverarbeitenden Einrichtungen werden bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst.
√	Die physische Sicherheit für Büros, Räume und Einrichtungen ist konzipiert und wird angewendet.
√	Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren für informationsverarbeitende Einrichtungen werden angewendet.
√	Netzwerke werden aktiv verwaltet und gesteuert, um Informationen in Systemen und Anwendungen zu schützen.
√	Informationssicherheitsereignisse werden von Betroffenen so schnell wie möglich über geeignete Kanäle zu ihrer Handhabung den jeweiligen Sicherheitsbeauftragten gemeldet.
√	Aufzeichnungen sind gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt.

Quelle: Eigene Darstellung

Ein effektiver Informationsschutz ist im Rahmen von Kooperationen immer nur bis zu einem gewissen Grad möglich:
Wenn die Informationen erst einmal die Grenzen des eigenen Unternehmens verlassen haben, sind Sie auf den „Goodwill“ des Gegenübers angewiesen.

Daher ist es erfahrungsgemäß wichtig, eine vertrauensvolle Kooperation zu etablieren, die durch wiederkehrende Projekttreffen, gegenseitige Besuche und regelmäßige Besprechungen gekennzeichnet ist.

III. Detektion

Beides gehört zusammen: Detektion und Reaktion

Zwei Dinge sind beim Informationsschutz elementar: Sie müssen in der Lage sein, sicherheitsrelevante Ereignisse rechtzeitig zu erkennen, und Sie müssen schnell auf Vorfälle reagieren können. Laut einer Statistik des Wirtschaftsberatungsunternehmens Pricewaterhouse-Coopers (PwC) erfolgt bei mehr als jedem dritten Fall eine Erstaufdeckung durch einen internen Hinweis (35 %), gefolgt durch die interne Revision (9 %), die Datenanalyse (3 %) und die Unternehmenssicherheit (6 %).[17]

Eine frühzeitige Detektion ermöglicht eine schnelle Reaktion

Eine frühzeitige Detektion ist nicht nur eine Präventionsmaßnahme, sondern erlaubt auch eine angemessene Reaktion auf Informationsabflüsse. Die folgenden Maßnahmen unterstützen Sie dabei:

- organisatorische Maßnahmen: Sicherheitsrichtlinie, Informationsklassifikation, Meldewege sowie Informationen von Behörden und Verbänden
- personelle Maßnahmen: Aufgabenteilung, Awareness-Trainings für Beschäftigte
- technische Maßnahmen: Barrieren, individuelle Zuteilung von Zugriffsrechten und Detektionssystemen

In einer Sicherheitsrichtlinie sollten Sie die verschiedenen Mittel zur Detektion von Informationsabflüssen für die Beschäftigten gut verständlich darlegen.

Im Folgenden finden Sie eine Liste möglicher Detektionsmittel:

Festlegung von Meldewegen für Informationsabflüsse

Melde- und Alarmierungswege müssen bekannt sein

Legen Sie geeignete, unternehmensweite Melde- und Alarmierungswege fest und stellen Sie sicher, dass diese allen Firmenangehörigen bekannt sind. Ein Meldesystem ermöglicht es, dass Mitarbeiterinnen und Mitarbeiter Verstöße gegen interne oder gesetzliche Regelungen anzeigen können. Bei internen Meldewegen ist es empfehlenswert, den Hinweisgebenden Vertraulichkeit bzw. Anonymität und Schutz vor negativen Konsequenzen zuzusichern - im gesetzlich zulässigen Rahmen.

Beispiele für verschiedene Meldewege sind:

- Compliance-/Hinweisgeber-Hotline
- Anruf, E-Mail oder Ticket an die IT- oder Sicherheitsabteilung des Unternehmens

Die Effizienz dieser Präventionsmaßnahme lässt sich durch die Sensibilisierung der Beschäftigten zu Themen des Informationsschutzes deutlich erhöhen.

[17] PwC (2016): Wirtschaftskriminalität in der analogen und digitalen Welt.

Einrichtung von technischen Analyseverfahren (UBA, NBA)

Technische Verfahren unterstützen die Detektion

Durch verschiedene technische Einrichtungen können Sie den Schutz vor einem ungewollten Informationsabfluss weiter erhöhen: So können Bedrohungen und Anomalien im IT-User-Verhalten frühzeitig durch softwaregestützte UBA (User Behavior Analytics) erkannt werden. Ziel ist es hierbei, Attacken auf IT-Systeme und den Diebstahl von Informationen zu detektieren und zu unterbinden. UBA-Lösungen nutzen spezielle Algorithmen und sogenannte Machine-Learning-Verfahren, die typische Verhaltensmuster von IT-Nutzenden anhand ihrer Position innerhalb eines Unternehmens ermitteln und analysieren.
In Kombination mit der netzwerkbasierten Systemverhaltensanalyse (NBA) werden Profile erstellt, anhand derer sich zum Beispiel abschätzen lässt, ob es sich um einen legitimen oder illegitimen Zugriff auf Systeme, Daten, Applikationen oder Informationen handelt.

„Data Loss Prevention Software“ schützt vor Datenverlust

Verschiedene Softwarelösungen nutzen die Analyseverfahren UBA und NBA und können dabei unterstützen, den Verlust von Daten möglichst zu verhindern: Bei der sogenannten DLP (Data Loss Prevention)-Software lassen sich grundsätzlich drei Varianten unterscheiden:

- **Netzwerk-DLP** verfolgt, überwacht und meldet alle Anomalien in Verbindung mit Informationen, die über Ports, Schnittstellen und Protokolle eines Unternehmensnetzwerks fließen,
- **Speicher-DLP** bietet Kontrolle über Informationen, die Beschäftigte speichern oder teilen (Cloud, Datenbanken etc.), und warnt vor einfach für Externe zugänglichen Informationen,
- **Endpunkt-DLP** überwacht und verhindert mithilfe von Agenten, die auf allen Workstations und Endgeräten (Laptops, Smartphones, Tablets sowie eigenständigen Speichergeräten - USBs und externen Festplatten) eines Unternehmens installiert sind, Transferaktionen vertraulicher Informationen mit Endgeräten, Sharing-Applikationen und Clipboards.

Die DLP-Software-Lösung warnt bei einem detektierten mutmaßlichen Richtlinienverstoß definierte Personen innerhalb des Unternehmens. Je nach Einstufung des Schweregrades des potenziellen Informationsverlustes kann auch eine sofortige Verschlüsselung der Daten eingeleitet werden. Die Effizienz eines solchen Systems hängt weitgehend davon ab, wie gut das Regelwerk durchdacht ist. Die richtige Konfiguration durch im System hinterlegte Regeln ergibt ein Gleichgewicht an Warnungen aller verdächtigen Aktionen und Fehlalarme. Die jeweiligen Schwellenwerte und Konfigurationen sind dabei unternehmensindividuell festzulegen.

Physische Detektion

Klassische Zutritts- und Taschenkontrollen als Detektionsmittel

Sie sollten ebenfalls prüfen, ob auch Zutrittskontrollen zum Firmengelände oder zu besonders sensiblen Bereichen umgesetzt werden können. Auch stichprobenweise Taschenkontrollen ermöglichen die Aufdeckung einer nicht erlaubten Mitnahme von Firmeninformationen, z. B. auf Dokumenten, USB-Sticks oder Laptops. Damit für alle Unternehmensangehörigen Klarheit besteht, sollten Sie vorher schriftlich festhalten, ob und welche Daten das Unternehmensgelände verlassen dürfen. Wird ein ungewollter Informationsabfluss festgestellt, kann die Analyse von außerplanmäßigen Zutritten und ungewöhnlichen Arbeitszeiten Hinweise auf die Person geben. So können Sie Abflusskanäle identifizieren und größeren Schaden verhindern.

Detektion sonstiger Verhaltensauffälligkeiten

Die Detektion auffälliger Verhaltensweisen steht in einem Spannungsverhältnis zwischen der Vertrauenskultur auf der einen Seite und einem berechtigten Misstrauen auf der anderen. Viele Hinweise auf Informationsabflüsse erfolgen aufgrund beobachteter auffälliger Verhaltensweisen und nicht auf eindeutigen Tatnachweisen. Daher sollten Sie Ihre Beschäftigten zu typischen Verhaltensweisen im Zusammenhang mit Informationsabflüssen sensibilisieren.

Beispiele für auffällige Verhaltensweisen

Beispiele für auffällige Verhaltensweisen
• Ungewöhnliche Kontakte zu Konkurrenzunternehmen, ausländischen staatlichen Akteuren etc.
• Suche nach Zugängen zu streng vertraulichen Informationen, z. B. durch Ausfragen von Kolleginnen und Kollegen
• Umgehung des Unternehmens beim Umgang mit Informationen (d. h. Verwendung privater Telefonnummern, Mailadressen, Visitenkarten, IT-Equipment, Lagerung von Dokumenten)
• Beteiligung an Regelverstößen oder illegalen Handlungen
• Wiederholte ungewöhnliche Parteinahme für eine sich bewerbende Person, ein Dienstleistungs- oder ein Konkurrenzunternehmen
• Weigerung, Urlaub zu nehmen oder Einblick in die Arbeitsgebiete zu gewähren

Quelle: Eigene Darstellung

Detektion abgeflossener Informationen – Darknet-Monitoring

Mit dem Darknet bzw. Dark Web verbinden viele einen Platz für alle Formen von Kriminalität. Doch auch die New York Times und Facebook sind im Darknet präsent und bieten dort ihre Dienste an. Was also ist das Darknet und was hat es mit Unternehmen und Informationsschutz zu tun?

Open Web, Deep Web und Darknet sind Teile des WWW

Stellen Sie sich einmal das gesamte Internet als Eisberg vor: Der an der Oberfläche sichtbare Teil ist das sogenannte Surface- oder Open-Web und repräsentiert den frei zugänglichen Teil des WWW. Man geht übrigens von einem Anteil im einstelligen Prozentbereich aus. Über 90 % des Internets werden mittlerweile dem Deep Web zugerechnet. Das sind die Bereiche des Internets, zu denen Sie Zugangsdaten benötigen, z. B. Buch- und Zeitschriftenbestände, Datenbanken, E-Mail- und Social-Media-Accounts und vieles mehr. Das Darknet nun ist ein spezieller Teil des Internets, der nur mit bestimmten Browsern zugänglich ist – der bekannteste ist der Tor-Browser. Anders als im offen zugänglichen Bereich verläuft der Datenverkehr hierbei verschlüsselt zwischen privaten Computern.

Das Darknet als Tummelplatz für Kriminelle

Die Anonymität des Darknets bietet z. B. für Oppositionelle oder investigativ arbeitende Journalistinnen und Journalisten Schutz vor Verfolgung und Repressionen. Aber: Das Darknet ist aufgrund dieser Anonymität auch Tummelplatz für Kriminelle. Neben anderen illegalen Aktivitäten werden auf verschiedenen elektronischen Marktplätzen und Foren Firmeninterna, vertrauliche Dokumente, Nutzungsdaten, Bilanzen, Rezepturen oder Formeln zum Verkauf angeboten.

Unternehmensdaten aufspüren durch Darknet-Monitoring

Unternehmen haben jedoch die Möglichkeit, mithilfe eines Darknet-Monitorings abgeflossene Informationen zu finden. Dabei werden einschlägige Marktplätze und Foren mithilfe von unternehmensspezifischen Stichworten durchsucht und es erfolgt eine Alarmierung, sobald relevante Daten gefunden wurden. Handelt es sich dabei um sensible Unternehmensdaten, können entsprechende Gegenmaßnahmen eingeleitet werden, z. B. eine strafrechtliche Verfolgung, das Abschalten von Seiten oder eine Sensibilisierung der Beschäftigten.

Indirekte Detektionsmechanismen

Offen über Probleme und Fehler sprechen zu können unterstützt den Informationsschutz

Oftmals wird in der Belegschaft dem Thema Informationsschutz keine große Beachtung geschenkt. Dem muss mit einem entsprechenden Kulturwandel hin zu einer sogenannten „Speak-up-Kultur“ entgegengetreten werden. Eine „Speak-up-Kultur“ ist dadurch gekennzeichnet, dass Mitarbeitende Probleme, Konflikte und Fehlverhalten offen ansprechen können, ohne Angst vor Konsequenzen haben zu müssen. Ist dieser offene Umgang mit Fehlern etabliert, lassen sich durch gezielte Kampagnen und Umfragen Schwachstellen und Anomalien zum gewünschten Verhalten der Unternehmensangehörigen ermitteln. Ihre Inhalte können sich u. a. auf den Bekanntheitsgrad und die Umsetzung von Richtlinien und Präventionsmaßnahmen beziehen.

Erfolgreiche Detektion erhöht die Wirksamkeit anderer Präventionsmaßnahmen

Die Herausforderung für Ihr Unternehmen ist, dass die einzelnen, ausgewählten Detektionsmittel ineinandergreifen müssen. Doch der Aufwand lohnt sich: Es wird nicht nur die Entdeckungswahrscheinlichkeit erhöht, auch die Wirksamkeit anderer Präventionsmaßnahmen wird durch eine erfolgreiche Detektion verstärkt. In der Kriminologie ist allgemein bekannt, dass eine hohe Entdeckungswahrscheinlichkeit einer Tatdurchführung entgegenwirkt. Die frühzeitige Detektion eines potenziellen Informationsabflusses führt schließlich nicht nur zu einer verkürzten Reaktionszeit und damit im günstigsten Fall zur Verhinderung des Informationsverlustes, sondern langfristig auch zu einer nachhaltigen Analyse von Ursachen, Risikopositionen und Angriffspunkten innerhalb eines Unternehmens. Schlussendlich schließt sich der Kreis durch diese Analyse, die wiederum als Grundlage für notwendige Präventionsmaßnahmen dient.

III. Detektion

IV. Reaktion

1. Erstanalyse, Aufklärung

Zielgerichtete Fragen erleichtern die Reaktion

Haben Sie einen Verdacht auf einen Informationsabfluss, erleichtern Ihnen folgende Fragen eine angemessene Reaktion:

- Wo und unter welchen Umständen sind die Informationen aufgetaucht?
- Liegen konkrete Hinweise auf Informationsdiebstahl vor (z. B. Logfiles von Downloads, die bei IT-Monitoring aufgefallen sind)?
- Sind die Informationen hochspezifisch oder ist es auch möglich, dass z. B. ein konkurrierendes Unternehmen auf die „gleiche Idee“ gekommen ist?
- Ist es plausibel, dass ein Konkurrenzunternehmen durch Maßnahmen der Competitive Intelligence (d. h. durch intelligentes Zusammenfügen einzelner Informationen) auf die brisante Information gestoßen ist?

2. Erstuntersuchung

Im Rahmen der Erstuntersuchung sind folgende Fragen zu beantworten und ihre Antworten zu dokumentieren:

- Wo sind die Informationen im eigenen Unternehmen gespeichert bzw. wo werden sie aufbewahrt?
- Gibt es Hinweise darauf, wann der Informationsabfluss stattgefunden hat?
- Wer hat/hatte Zugang zu den relevanten Informationen?
  - Haben Externe im Zuge von Kooperationen solche Informationen auch erhalten?
  - Gab es in der infrage kommenden Zeit Kündigungen von Beschäftigten, die Zugang zu relevanten Informationen hatten?
  - Gab es IT-Lecks in der infrage kommenden Zeit?

Hinweis

- Sollte es bereits einen Verdachtsmoment gegen eine Person geben, ist diese zunächst nicht mit dem Sachverhalt zu konfrontieren.
- Führungskräfte und Teammitglieder der verdächtigen Person sollten zunächst ebenfalls nicht involviert werden, da Loyalitäten zwischen diesen bestehen könnten.

3. Response

Eine Entscheidung zur jeweiligen Handlung hängt von dem verfolgten Ziel ab:

a) sofortiger Stopp des Informationsabflusses

- personenbezogene Zugänge abstellen (Zugang von Verdächtigen zum Gelände, IT-Rechte etc.)
- IT-Untersuchung bzgl. Malware-Detektion
- physischen Schutz verbessern
- Kappen von Geschäftsverbindungen
- Freistellung der verdächtigen Person

b) vertiefende unternehmensinterne Untersuchung

Soll die Ermittlung durch unternehmensinterne Fachkräfte oder durch ein externes Dienstleistungsunternehmen stattfinden?

- Auswertung von Logfiles
- Auswertung der dienstlichen Mailbox
- Auswertung von dienstlichen Kalender- und Kontaktdaten
- Befragungen von Personen etc.

An dieser Stelle bietet sich bei einer möglichen Verbindung der unter Verdacht stehenden Person zu einem fremden Staat die Involvierung des Bundesamtes für Verfassungsschutz sowie der jeweils zuständigen Landesämter an.[18]

Der Verfassungsschutzverbund steht als vertraulicher Ansprechpartner zur Verfügung, um Verdachtsfälle im Hintergrund zu analysieren.

Hinweis

Diese Ermittlungsschritte unterliegen immer dem Vorbehalt datenschutzrechtlicher, persönlichkeitsrechtlicher und mitbestimmungsrechtlicher – ggf. auch unternehmensindividueller Regelungen.

Insbesondere ist das Verhältnismäßigkeitsprinzip zu wahren:- Schützenswerte Rechte der Beschäftigten müssen gegen das Ermittlungsrecht aufgrund eines hinreichenden Tatverdachts des Unternehmens abgewogen werden.

[18] Die Kontaktdaten finden Sie unter https://www.verfassungsschutz.de

Erwägen Sie die Einschaltung der örtlichen Strafverfolgungsbehörden

c) Strafverfolgung

Legen unternehmensinterne Untersuchungen nahe, dass die Person eine Straftat begangen haben könnte, ist die Einschaltung der örtlich zuständigen Strafverfolgungsbehörden (Polizei/Staatsanwaltschaft) zu erwägen bzw. die Kontaktaufnahme zu empfehlen. Diese wiederum involvieren anlassbezogen oft weitere zuständige Polizeidienststellen in Bund (z. B. BKA) und Ländern (LKA), weil diese in bestimmten Deliktfeldern mit einer größeren Fallexpertise aufwarten können. Die Strafverfolgungsbehörden sind sich dabei auch bewusst, dass Unternehmen Sorgen vor einem möglichen Reputationsschaden haben.

Die Verfolgung von Straftaten hat abschreckende Wirkung

Nach Abschluss der Ermittlungen durch die Polizei und Vorlage der Akten bei der Staatsanwaltschaft erhebt diese bei einem hinreichenden Tatverdacht Anklage beim zuständigen Gericht oder stellt das Verfahren – ggf. auch unter Auflagen – ein. Die Verfolgung von Straftaten kann auch eine abschreckende Wirkung haben und vor Nachahmungs- oder Wiederholungstaten schützen, außerdem lassen sich möglicherweise wichtige Informationen für die Entwicklung von behördlichen Bekämpfungsstrategien ableiten. Dabei stehen ihnen weiterführende Ermittlungsmaßnahmen als etwa privat Ermittelnden zur Verfügung, beispielsweise im Bereich der Sicherung von Daten.

Mögliche Maßnahmen der Strafverfolgungsbehörden

Mögliche Maßnahmen der Strafverfolgungsbehörden (offen und verdeckt)

- Durchsuchungen vor Ort, um potenziell beweisrelevante Daten auf Firmenrechnern und -servern wie E-Mail-Accounts, Logfiles, Netzwerkprofile etc. möglicher verdächtiger Personen aufzufinden und anschließend auszuwerten
- Sicherstellung/Beschlagnahmung von Gegenständen
- Befragungen/Vernehmungen von anderen Beschäftigten
- Die StPO ermöglicht grundsätzlich aber auch die Durchführung sogenannter verdeckter Maßnahmen wie Telekommunikationsüberwachung, E-Mail-Überwachung etc.

→ **Diese Maßnahmen dienen alle der Feststellung tatrelevanter Spuren sowie der Gewinnung weiterer Beweismittel bzw. der Identifizierung oder Entlastung weiterer Tatverdächtiger.**

Über die Strafverfolgung hinaus können durch die Arbeit der Behörden im Einzelfall auch abstrakte Warnmeldungen für andere Unternehmen generiert werden.

d) Schadensbegrenzung

Den Schaden durch verschiedene Maßnahmen begrenzen

Unternehmen haben verschiedene Möglichkeiten, einen Schaden zu begrenzen:

- Freiwillige Rückgabe der entwendeten Daten mit schriftlicher Zusicherung, dass Datenkopien nicht bestehen und die Daten auch anderweitig nicht eingesetzt bzw. verwendet werden (eine strafbewehrte Unterlassungs- und Verpflichtungserklärung kann hierbei das richtige Mittel sein)
- Sicherstellung und Beschlagnahmung durch die Polizei (Datenträger, Dokumente, Computer)
- Zivilrechtliches Vorgehen, wie die Klage auf Herausgabe der entwendeten Datenträger und Unterlassung auf Nutzung/Weitergabe oder Schadensersatz
- Patentrechtliches Vorgehen: Feststellung einer widerrechtlichen Entnahme, Einspruch gegen erteilte Patente von Konkurrenzunternehmen, die diese auf Basis gestohlener Ideen/F&E-Arbeit angemeldet haben
- Arbeitsrechtliches Vorgehen, wie das Aussprechen einer Kündigung oder Abmahnung

4. Nachbereitung

Ursachenanalyse und konkrete Verbesserung der Prävention und Detektion, siehe entsprechende Kapitel

Schlusswort

Informationen und Daten sind das Gold des 21. Jahrhunderts: Jedes Unternehmen verfügt über sensible Daten und Informationen, die für Dritte interessant sein können. Unternehmensdaten haben entscheidenden Einfluss auf den Unternehmenserfolg. Ihr angemessener Schutz gehört daher heutzutage zu einer ordnungsgemäßen Geschäftsführung.

Von Innentätern geht eine erhebliche Gefahr für Unternehmen oder Forschungseinrichtungen aus. Die Motive, die dem kriminellen Handeln zugrunde liegen, sind dabei überaus vielfältig: Teils handeln Unternehmensangehörige aus ideologischen, teils aus individuellen, egoistischen Beweggründen; und manchmal werden sie selbst zu Opfern gezielter Manipulationsversuche. Aber auch in der Unternehmensorganisation selbst liegen Ursachen, die unternehmensschädigendes Verhalten fördern, z. B. im Verhalten der Führungskräfte oder in der Ausgestaltung von Beförderungen. Wie ein Unternehmen mit den eigenen Beschäftigten umgeht, beeinflusst die Loyalität der Beschäftigten gegenüber dem Unternehmen und hat Einfluss auf eine mögliche Innentäterschaft.

Neben diesen eher „weichen“ Faktoren gibt es verschiedene andere Maßnahmen, die im Unternehmen angegangen werden können, um die Informationssicherheit zu erhöhen: von Taschenkontrollen über die Klassifizierung von Informationen bis hin zu einem Darknet-Monitoring. Auf Basis einer Risikoanalyse können Sie ableiten, welche Maßnahmen für Ihr Unternehmen passend sind.

Die Informationssicherheit lässt sich mit teils einfachen Mitteln wesentlich erhöhen. Schützen Sie sensible Unternehmensdaten und damit die Beschäftigten und den Unternehmenserfolg:

- Bestimmen und kennzeichnen Sie schützenswerte Informationen.
- Definieren Sie Verwendungsregeln und kontrollieren Sie ihre Einhaltung.
- Limitieren und kontrollieren Sie den Zugang zu diesen Informationen.
- Prüfen Sie Angaben und Referenzen von sich bewerbenden Personen.
- Machen Sie Ihre Beschäftigten auf die Gefahren aufmerksam.
- Holen Sie sich im Verdachtsfall professionelle Unterstützung von den Behörden.

Wirtschafskriminalität ist keine Bagatelle – nutzen Sie die dargestellten effektiven Maßnahmen und handeln Sie im Verdachtsfall schnell. Wir hoffen, Ihnen hierzu mit dieser Broschüre wertvolle Hinweise und Anregungen zur Verfügung zu stellen.