Ihre Risiken

- > Materielle Schäden
- > Imageverlust
- > Marktverdrängung

Wirtschaftsspionage Konkurrenzausspähung

Jedes dritte Unternehmen ist betroffen.

Schützen Sie Ihr Know-how!

Ihre Chancen

- > Schadensvermeidung
- > Aufklärung krimineller Vorfälle
- > Regress
- > Optimierung des Sicherheitsmanagements
- > Zukunftssicherung

Hinweis: Aus Gründen der leichten Lesbarkeit wird in der vorliegenden Broschüre die männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Sämtliche Sprachformen gelten gleichermaßen für alle Geschlechter.

Text

Ass. iur. Susanne Knickmeier, M.A.

Max-Planck-Institut für ausländisches und internationales Strafrecht

Impressum:

Herausgeber

Max-Planck-Institut für ausländisches und
internationales Strafrecht

Günterstalstr. 73

79100 Freiburg

Tel. +49 (761) 7081-0

Bildnachweis

Pixabay

WISKOS

© Max-Planck-Institut für ausländisches und internationales Strafrecht
und Fraunhofer-Institut für System-
und Innovationsforschung (ISI)

Druck: Stücker Druck und Verlag, Stücker-Straße 1, 77955 Ettenheim

<https://doi.org/10.30709/2018-005>

Das Projekt WISKOS wurde vom BMBF im Zuge der Bekanntmachung "Zivile Sicherheit - Schutz vor Wirtschaftskriminalität" des BMBF im Rahmen des Programms "Forschung für die zivile Sicherheit" der Bundesregierung unter dem Förderkennzeichen: 13N13410 gefördert.

Vorwort

„Fast ein Fünftel der im WISKOS-Projekt befragten Unternehmen mit weniger als 50 Mitarbeitern verfügt über keine Strategie gegen physische Spionage oder Cyberangriffe.“

So lautet ein Ergebnis aus dem Projekt „Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa“ (WISKOS), in dem das Max-Planck-Institut für ausländisches und internationales Strafrecht und das Fraunhofer-Institut für System-und Innovationsforschung mit dem Bundeskriminalamt, dem Landeskriminalamt Baden-Württemberg und der Sächsischen Hochschule der Polizei als assoziierten Partnern den Phänomenbereich des unerlaubten Informationsabflusses sowie die staatlichen Kontrollstrukturen und die innerbetrieblichen Erkennungs- und Präventionsstrategien untersuchten.

Kleine und mittlere Unternehmen (KMU) stellen in Deutschland die meisten Arbeitsplätze und sind seit vielen Jahren ein Garant für das Wirtschaftswachstum. Der illegale Wissens-, Daten- oder Informationsabfluss kann schwerwiegende Konsequenzen für Unternehmen und auf lange Sicht für die deutsche Volkswirtschaft haben. Durch die Digitalisierung, die Entwicklungspotentiale, aber auch Risiken mit sich bringt, sind auch kleinere Unternehmen (inter-)national präsenter. Dadurch werden bei der Konkurrenz oder anderen Staaten Begehrlichkeiten geweckt und neue Ziele für Angreifer geschaffen mit der Folge, dass viele KMU einen Zuwachs an Angriffen verzeichnen. Wesentlich mehr Fälle bleiben jedoch unentdeckt oder werden von den Unternehmen nicht angezeigt, da Chancen und Nutzen von Strafanzeigen verkannt werden oder Vorbehalte und Unsicherheiten gegenüber der polizeilichen Ermittlungsarbeit bestehen.

Die Broschüre dient der Sensibilisierung für Wirtschaftsspionage und Konkurrenzausspähung und ihren Gefahren. In diesem Kontext werden Handlungsstrategien zur Prävention und für das Vorgehen nach einem erfolgreichen Angriff beschrieben sowie Kooperationsmöglichkeiten mit staatlichen Stellen aufgezeigt.

Dr. Esther Bollhöfer

Fraunhofer-Institut für System-und
Innovationsforschung, Karlsruhe

Dr. Michael Kilchling

Max-Planck-Institut für ausländisches und
internationales Strafrecht, Freiburg i.Br.

Das Projekt WISKOS: Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa

Modul 1: Länder-Screening

- > **Länderberichte** aus allen 28 Mitgliedsstaaten der Europäischen Union und der Schweiz zu den rechtlichen Regelungen, dem verfahrensrechtlichen Rahmen und statistischen Basisdaten

Modul 2: Mehrebenen-Evaluation

- > **Literatur- und Dokumentenanalyse**
- > **Strafaktenanalyse** (n=713 Strafakten zur Konkurrenzausspähung aus Deutschland)
- > **Exemplarische Fallstudien** (n=50 Fallstudien aus Bulgarien, Dänemark, Österreich, der Schweiz und dem Vereinigten Königreich)
- > **Experteninterviews** (n=62 mit Vertretern von Behörden, KMU, Kammern, Verbänden, Wissenschaftsorganisationen in Deutschland sowie Bulgarien, Dänemark, Österreich, der Schweiz und dem Vereinigten Königreich)

Modul 3: Dunkelfeldbefragung

- > **Erhebung** *Modernisierung der Produktion* 2015 (n=1.282 Betriebe)
- > **Erhebung** bei produzierenden Betrieben und industrienahen Dienstleistern bis zu 250 Mitarbeitern 2017 (n=583)

Projektpartner

- > Max-Planck-Institut für ausländisches und internationales Strafrecht
- > Fraunhofer-Institut für System-und Innovationsforschung

Assoziierte Partner

- > Bundeskriminalamt
- > Landeskriminalamt Baden-Württemberg
- > Sächsische Hochschule der Polizei

Inhaltsverzeichnis

1. Wirtschaftsspionage und Konkurrenzausspähung.....	5
🔒 Wer kann Täter sein?	
🔒 Was motiviert die Täter?	
🔒 Wie gehen die Täter vor?	
🔒 Könnte auch Ihr Unternehmen betroffen sein?	
🔒 Welche Unternehmensgeheimnisse interessieren die Täter?	
🔒 Welche Auswirkungen haben Vorfälle auf Unternehmen?	
🔒 Wie gut sind KMU geschützt?	
2. Verdachtsindikatoren.....	11
🔒 In welchem Zusammenhang wurden Vorfälle festgestellt?	
🔒 <i>Übersicht:</i> Welche Verdachtsindikatoren sollten beobachtet werden?	
3. Vorgehen bei einem Vorfall.....	15
🔒 Warum ist eine Strafanzeige wichtig und sinnvoll?	
🔒 <i>Übersicht:</i> Was verstehen Behörden unter Wirtschaftsspionage und Konkurrenzausspähung?	
🔒 An wen können Sie sich bei einem Verdachtsfall wenden?	
🔒 Was erwartet Sie nach der Anzeige einer Straftat?	
🔒 Können Ihre Unternehmensgeheimnisse in einem Strafverfahren geschützt werden?	
🔒 Wie läuft ein Strafverfahren ab?	
🔒 <i>Übersicht:</i> Wie sollten Sie bei einem Vorfall vorgehen?	
4. Prävention und Strafverfolgung.....	21
🔒 <i>Übersicht:</i> Realisierte Schutzmaßnahmen zur Abwehr von Spionage und Ausspähung	
🔒 Best practices aus dem Inland	
🔒 Best practices aus dem Ausland	
🔒 <i>Übersicht:</i> Welche Präventionsmaßnahmen können Sie ohne viel Aufwand umsetzen?	
5. Fazit.....	27
Anhang.....	30
🔒 Kontaktadressen der Landeskriminalämter und des Bundeskriminalamtes	
🔒 Publikationen mit Ergebnissen aus dem Projekt WISKOS

1. Wirtschaftsspionage und Konkurrenzausspähung

Nicht nur global tätige Unternehmen sind Ziel von Wirtschaftsspionage und Konkurrenzausspähung, sondern auch oder gerade die kleinen und mittleren Unternehmen, die wertvolles und begehrtes technisches Know-how entwickeln und deren Geschäfts- und Kundendaten Interesse bei der Konkurrenz oder anderen Staaten hervorrufen.

Wer kann Täter sein?

Die Bedrohung durch einen illegalen Wissens-, Daten- oder Informationsabfluss besteht gleichermaßen von innen und von außen. Angreifer können die Mitarbeiter des Geheimdienstes eines anderen Staates, eines anderen Unternehmens, Dritte oder auch eigene Mitarbeiter sein. Über die Hälfte aller befragten Unternehmen¹ ist sich sicher, dass mindestens ein Wettbewerber illegal beschaffte Daten und Informationen nutzt.

Oft ist der Täter kein Unbekannter, sondern kommt aus dem eigenen unternehmerischen Umfeld. Es können unzufriedene oder ehemalige Mitarbeiter sein, die Informationen bei einem neuen Arbeitgeber verwenden, neu eingestellte Beschäftigte, die nicht unter Sicherheitsgesichtspunkten überprüft wurden, oder Praktikanten und Beschäftigte von Drittunternehmen, die oftmals sorglos Zugang zu schützenswertem Know-how erhalten.

Gerade Innentäter können besonders schweren Schaden anrichten, da sie einen guten Einblick in das Unternehmen und den Wert der geschützten Informationen haben. Innentäter können bewusst vorgehen oder unbewusst Täter werden, indem sie durch einen Außentäter zur Informationsbeschaffung „benutzt“ werden, wie zum Beispiel beim Social Engineering, der manipulativen Beeinflussung von Mitarbeitern mittels zwischenmenschlicher Kontakte, oder der gezielten Kontaktaufnahme über XING oder LinkedIn.

¹ Im Rahmen der Dunkelfeldbefragung im Projekt WISKOS fragte das Fraunhofer-Institut (ISI) n=583 produzierende kleine und mittlere Unternehmen sowie industrienähe Dienstleister, wie sicher Unternehmen seien, dass mind. ein Wettbewerber illegal beschaffte Daten oder Informationen nutze.

Was motiviert die Täter?

Bei der Entwicklung wirksamer Entdeckungs- und Präventionsstrategien sollten die folgenden Beweggründe der Täter bedacht werden:

- 🔒 **Rache oder Unzufriedenheit** durch (ehemalige) Mitarbeiter sind ernstzunehmende Motive.
- 🔒 Der Verkauf von Kundendaten oder Know-how dient dem **finanziellen Profit** der Täter.
- 🔒 Nicht zu unterschätzen sind Konkurrenten oder Mitarbeiter ausländischer Geheimdienste, die geschütztes Know-how abziehen, um **im Ausland ein Konkurrenzprodukt kostengünstiger herstellen** zu lassen, ohne selbst in die Forschung und Entwicklung investieren zu müssen.
- 🔒 Wettbewerber oder Staaten, die ihre eigenen Unternehmen fördern wollen, könnten unternehmensinterne Informationen nutzen, um einen Konkurrenten bei Ausschreibungen zu unterbieten und sich dadurch einen **Wettbewerbsvorteil** zu verschaffen.

Wie gehen die Täter vor?

Die Täter versuchen auf vielfältige Weise an die geschützten Informationen zu gelangen: sie kopieren Daten auf USB-Sticks, senden sich Geschäfts- und Betriebsgeheimnisse aus dem Unternehmensnetzwerk per E-Mail zu, kopieren, fotografieren Skizzen oder stehlen Datenträger oder Modelle. Mit Handycameras oder mithilfe von Drohnen können Prototypen oder Produktionsanlagen aufgenommen werden.

Auch wenn der Faktor Mensch nicht unterschätzt werden darf, stellen Cyberangriffe eine immer größere Bedrohung dar, sei es durch das Ausnutzen von Sicherheitslücken im Informations- und Kommunikationstechnologie-Bereich, Phishing-E-Mails, Bot-Netze, direkte Angriff auf Maschinen und Anlagen mit Netzwerkeinbindung oder eine Schadsoftware-Infiltration per Internetnutzung (Drive-by-Exploits). Teilweise haben die Täter über Monate hinweg Zugriff auf geschützte Informationen, bis der Angriff entdeckt wird. Strategien gegen Cyberangriffe sind daher unabdingbar.

Wie gehen die Täter vor (ohne Cyberdelikte)?	
Versenden von Daten (z.B. als E-Mail)	43
Speicherung auf Datenträger	66
Mitnahme in Papierform	27
kopierte oder fotografierte Dokumente	29
nicht feststellbar	28
Quelle: Analyse von Straftaten zu §§ 17 ff. UWG, MPI für Strafrecht, n=170 Fälle, Mehrfachnennung möglich	

Könnte auch Ihr Unternehmen betroffen sein?

„Ich bin nicht betroffen“ – **doch!**

Wirtschaftsspionage und Konkurrenzausspähung können jedes Unternehmen unabhängig von der Branche oder der Unternehmensgröße treffen. Von den im WISKOS-Projekt befragten Unternehmen berichtete fast ein Viertel von mindestens einem Vorfall des illegalen Abflusses von Wissen, Daten oder Informationen innerhalb der letzten fünf Jahre.

Abhängig von der Branche gab es bei 46% bis 63% der befragten KMU mit weniger als 50 Mitarbeitern einen Vorfall oder konkreten Verdachtsfall. Bei den Unternehmen mit mehr als 50 Mitarbeitern lag die Betroffenheit zwischen 35% und 45%.² Die hohe Zahl der Verdachtsfälle ist ein Hinweis darauf, dass Wirtschaftsspionage und Konkurrenzausspähung oft schwer festzustellen sind und der eventuelle Abfluss geschützter Informationen, zum Beispiel bei einem Einbruchsdiebstahl, erst viel später in einem anderen Zusammenhang bemerkt wird.

Welche Unternehmensgeheimnisse interessieren die Täter?

Von besonderem Interesse für die Konkurrenz sind vor allem die folgenden Unternehmensgeheimnisse:

- 🔒 Kundendaten
- 🔒 Informationen über den Vertragsgegenstand, z.B. Preislisten, Verträge mit Lieferanten oder Dritten
- 🔒 Unternehmensstrategien
- 🔒 technische Daten, z.B. Maschinendaten, Softwarecodes, Informationen über die Materialzusammensetzung oder Daten zur Produktentwicklung
- 🔒 interne Unternehmensdaten, z.B. Mitarbeiterverträge, Passwörter.

Was ist ein Geschäfts- oder Betriebsgeheimnis?

Nach der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen der Europäischen Union umfasst ein Geschäfts- oder Betriebsgeheimnis **jede im Zusammenhang mit einem Betrieb stehende Tatsache**, die **nicht offenkundig**, sondern nur einem, vom Betriebsinhaber bestimmten, **eng begrenzten Personenkreis bekannt** ist und nach dem **Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheim** gehalten werden soll. Der Inhaber des Geheimnisses muss **angemessene Maßnahmen zur Geheimhaltung** der Information unternehmen.

² Im Rahmen der Dunkelfeldbefragung im Projekt WISKOS fragte das Fraunhofer-Institut (ISI) n=583 produzierende kleine und mittlere Unternehmen sowie industrienähe Dienstleister nach einem oder mehreren Vorfällen und Verdachtsfällen.

Welche Auswirkungen haben Vorfälle auf Unternehmen?

Der illegale Wissens-, Daten- oder Informationsabfluss kann schwerwiegende Konsequenzen für die KMU haben. Neben materiellen Schäden verlieren die Unternehmen Betriebs- und Geschäftsgeheimnisse, die die Grundlage für ihre wirtschaftliche Tätigkeit sind. Dadurch besteht die Gefahr der Marktverdrängung und des Vertrauensverlustes bei Kunden. Wirtschaftsspionage und Konkurrenzausspähung sind eine Bedrohung für den Innovationsvorsprung deutscher Unternehmen. Sie können zu nachhaltigen Wettbewerbsnachteilen führen und langfristig zum Verlust von Arbeitsplätzen.

Schäden durch den illegalen Informationsabfluss sind schwer zuzuordnen und zu beziffern. Im WISKOS-Projekt wurde daher auf die wahrgenommenen Einschränkungen im Geschäftsbetrieb, die ein Angriff bzw. ein versuchter Angriff mit sich brachten, abgestellt. Fünf Prozent der Unternehmen, die bereits einen Angriff oder Versuch wahrgenommen hatten, gaben an, diesen in einer Form erlebt zu haben, die existenzbedrohliche Auswirkungen hatte. Insgesamt musste knapp ein Viertel der bereits angegriffenen Unternehmen Einschränkungen im Geschäftsbetrieb hinnehmen, die mehr als 48 Stunden andauerten.

Wie gut sind KMU geschützt?

Trotz der potenziellen Betroffenheit und möglichen schweren Folgen fehlen nahezu jedem fünften Unternehmen mit weniger als 50 Mitarbeitern Präventionskonzepte und hinreichende Sicherungsmechanismen gegen physische Spionage oder Cyberangriffe. Bei den Unternehmen mit über 50 Mitarbeitern fehlten bei 6% Strategien gegen Cyberangriffe und bei 9% gegen physische Spionage.³ Zwar sahen die Unternehmen, wie sich aus den im WISKOS-Projekt geführten Experteninterviews ergab, grundsätzlich Handlungsbedarf, stellten die zweckmäßigen Präventionsmaßnahmen aber, oft aus Kapazitätsgründen, hinten an.

³ Im Rahmen der Dunkelfeldbefragung im Projekt WISKOS fragte das Fraunhofer-Institut (ISI) n=583 produzierende kleine und mittlere Unternehmen sowie industrienähe Dienstleister nach ihren Präventionsstrategien.

2. Verdachtsindikatoren

Aufgrund der vielfältigen Behebungsmöglichkeiten sind Delikte der Wirtschaftsspionage und Konkurrenzausspähung gerade bei Cyberangriffen oft nur schwer als solche zu erkennen. Die Sensibilisierung und Schulung der eigenen Mitarbeiter für den Kontext von Vorfällen, die Implementierung von Präventionsstrategien und die regelmäßige Beobachtung von Verdachtsindikatoren sind sinnvolle Maßnahmen, um Vorfälle und Verdachtsfälle zeitnah zu identifizieren und Abwehrmaßnahmen einzuleiten.

In welchen Zusammenhängen wurden Vorfälle festgestellt?

Über 66%⁴ der befragten Unternehmen gaben an, dass der unerlaubte Daten-, Wissens-, oder Informationsabfluss im Zusammenhang mit der Öffnung von E-Mails mit kritischem Inhalt stand. Auch der Einsatz privater Geräte (24%), Besucher im Unternehmen (21%), die Ankündigung von Produkten (10%) oder Auslandsreisen (7%) bergen Gefahren für Angriffe auf geschützte Informationen. Aufgedeckt wurden die Angriffe bei den im WISKOS-Projekt untersuchten Strafverfahren vor allem durch Mitarbeiter, die interne Vorgänge genau beobachteten und Hinweise gaben oder Dritte (Kunden, Lieferanten, externe Mitarbeiter), die in Kontakt zu dem betroffenen Unternehmen standen. Cyberangriffe konnten zum Beispiel durch eine routinemäßige Kontrolle der Datenströme und Rechneraktivitäten festgestellt werden.

Präventiv sollten Sie eine besondere Aufmerksamkeit auf den grundsätzlichen Umgang mit Daten im Unternehmen, aber auch auf Dienstreisen sowie eine regelmäßige Sensibilisierung der Mitarbeiter auf E-Mails mit kritischem Inhalt (Anhänge, Links) legen. Gerade Phishing-E-Mails, die ohne viel Aufwand schnell und flächendeckend versendet werden können, sind von einer hohen Qualität und schwer als solche erkennbar.

„In der E-Mail war ein Link [...] Der Link ging auf ein Paper bei Springer, für das man sich über die örtliche Bibliotheksmaske anmelden musste. Darüber sollte das Passwort abgegriffen werden. Die Maske war nachgebaut und in der URL war ein kleiner Buchstabe geändert. Die LMU hat die Adresse „@uni-muenchen.de“. In der nachgebauten Adresse war bei „München“ das letzte „e“ durch ein „i“ ersetzt. [...] Das war richtig gut gemacht [...]“

Quelle: Experteninterview Wissenschaftsorganisation, MPI für Strafrecht

⁴ Im Rahmen der Dunkelfeldbefragung im Projekt WISKOS fragte das Fraunhofer-Institut (ISI) n=583 produzierende kleine und mittlere Unternehmen sowie industrienähe Dienstleister nach einem Zusammenhang von Vorfällen mit anderen Aktivitäten. Eine Mehrfachnennung war bei der Beantwortung der Frage möglich.

Welche Verdachtsindikatoren sollten beobachtet werden?

Vorsicht bei....

-
- 🔒 einem scheinbar belanglosen Einbruch
 - 🔒 Auffälligkeiten in der IT und großen Datentransfers
 - 🔒 Diebstahl/Verlust von Datenträgern
 - 🔒 Anwesenheit von Mitarbeitern/Mitarbeiterinnen zu ungewöhnlichen Zeiten
 - 🔒 Bewerbungen von Studierenden oder Praktikanten/Praktikantinnen aus einschlägigen Ländern
 - 🔒 eigenen Reisen in einschlägige Länder
 - 🔒 auffälligem Interesse auf/nach internationalen Messen
 - 🔒 Auftauchen von (Teil-) Informationen außerhalb des eigenen Unternehmens
 - 🔒 unerwarteten Kunden- oder Auftragsverlusten
 - 🔒 Social Engineering (manipulative Beeinflussung durch zwischenmenschliche Kontakte)
 - 🔒 der gezielten Kontaktaufnahme zu Mitarbeitern/Mitarbeiterinnen, z.B. über soziale Netzwerke (XING, LinkedIn)

Auszug aus dem Faltblatt: Wirtschaftsspionage und Konkurrenzausspähung: Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how.

3. Vorgehen bei einem Vorfall

Wenn Sie einen Angriff aufdecken, stellt sich die Frage, wie mit dem Vorfall umgegangen werden sollte. Neben eigenen Maßnahmen gegenüber dem Täter und der Unterstützung durch externe Beratung steht den Unternehmen die Möglichkeit einer Strafanzeige zur Verfügung. Von dieser Möglichkeit machen jedoch nur wenige KMU Gebrauch, da Unklarheiten über behördliche Zuständigkeiten, den Aufwand von Strafverfahren und Unsicherheiten über den Schutz von Unternehmensgeheimnissen bestehen.

Warum ist eine Strafanzeige wichtig und sinnvoll?

Eine Strafanzeige dient nicht nur der Verfolgung und Aufklärung eines individuellen Einzelfalles und der Kriminalitätsbekämpfung, sondern auch dem Erkenntnisgewinn über das tatsächliche Ausmaß im Deliktsbereich, Täter und Tätergruppen sowie neue Modi Operandi. Auch wenn ein Täter nicht ermittelt werden kann, fließen die Informationen aus jedem Fall in die Maßnahmen und Präventionsstrategien der Strafverfolgungsbehörden ein. Andere Unternehmen können somit sensibilisiert und informiert sowie weitere Straftaten und Schäden verhindert werden. Nur wenn bekannt ist, welchen Umfang der Phänomenbereich hat, können die Behörden ihre Präventions- und Strafverfolgungsmaßnahmen, auch mit der Zurverfügungstellung finanzieller Mittel, daran ausrichten. Durch Schweigen überlassen Sie den Aktivitäten der Täter freien Lauf. Die Höhe des Schadens spielt für eine Strafanzeige keine Rolle.

Was verstehen Behörden unter Wirtschaftsspionage und Konkurrenzausspähung?		
	Wirtschaftsspionage	Konkurrenzausspähung
Definition	Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von Nachrichtendiensten fremder Staaten ausgehende Ausforschung von Unternehmen	Konkurrenzausspähung ist die private Ausforschung konkurrierender Unternehmen
Ziel	Förderung der Wirtschaft eines fremden Staates	Verfolgung (eigener) kommerzieller Interessen
Für wen handelt der Täter?	Geheimdienst eines anderen Staates	ein anderes Unternehmen oder sich selber
Wichtige Strafvorschriften	geheimdienstliche Agententätigkeit (§ 99 StGB)	Verrat von Geschäfts- und Betriebsgeheimnissen (§ 17 UWG)
Zuständigkeit	Generalbundesanwalt (§§ 74a, 142a GVG)	Staatsanwaltschaft (ggf. Schwerpunkt-Staatsanwaltschaft Wirtschaftskriminalität)

An wen können Sie sich bei einem Verdachtsfall wenden?

Die Zuständigkeiten für die Verfolgung von Straftaten liegen bei der Polizei und den Staatsanwaltschaften. Mit dem Verdacht eines Vorfalls können Sie sich an jede Polizeidienststelle oder an die im Anhang aufgeführten Experten der Landeskriminalämter und des Bundeskriminalamtes wenden, die Sie an die für Sie zuständige Dienststelle vermitteln, sofern sie nicht selbst zuständig sind. Damit bei einem Cyberangriff weitere Schäden verhindert und die Ermittlungen umgehend begonnen werden können, sollten Sie möglichst frühzeitig die Experten Ihres Landeskriminalamtes oder das Bundeskriminalamt informieren.⁵

Was erwartet Sie nach der Anzeige einer Straftat?

Im Ermittlungsverfahren versuchen die Strafverfolgungsbehörden mit den gesetzlich zulässigen Maßnahmen den von Ihnen berichteten Vorfall aufzuklären, strafrechtlich zu prüfen und Beweise zu sichern. Zu einer Anklage durch die Staatsanwaltschaft kommt es, wenn die Verurteilung des Beschuldigten wahrscheinlich ist.

Die polizeilichen Ermittlungen können verschiedene Maßnahmen beinhalten und einige Zeit in Anspruch nehmen. Gerade die Auswertung einer großen Datenmenge, grenzüberschreitende Ermittlungen und das Zusammenwirken mehrerer Behörden kosten Zeit. Bei Ihrem polizeilichen Ansprechpartner können Sie sich jederzeit nach dem Stand des Verfahrens erkundigen.

Soweit es sich vermeiden lässt, was der Normalfall ist, wird der laufende Betrieb Ihres Unternehmens durch die Ermittlungen nicht behindert. Sollte zum Beispiel die Sicherung von Firmendaten nötig sein, können diese auf Festplatten, die die Polizei mitbringt, kopiert werden. Da die Polizei rund um die Uhr im Dienst ist, sind Gesprächstermine auch außerhalb der normalen Geschäftszeiten möglich. Sie können individuelle Absprachen treffen.

Können Ihre Unternehmensgeheimnisse in einem Strafverfahren geschützt werden?

Bei einem Strafverfahren, in dem es um eine Verletzung von geschützten Informationen geht, besteht die Gefahr, dass der Täter erst durch das Strafverfahren (über die Akteneinsicht oder eine öffentliche Hauptverhandlung) alle für ihn notwendigen Informationen erhält. Während des Strafverfahrens besteht die Möglichkeit des Geheimnisschutzes, indem dem Anwalt des Beschuldigten die Einsicht in Akten oder Teile der Akten gemäß

⁵ Die Adressen, Telefonnummern und E-Mail-Adressen der polizeilichen Ansprechpartner finden Sie auf Seite 30 dieser Broschüre.

§ 406e Abs. 2 StPO verwehrt werden kann, wenn überwiegend schutzwürdige Interessen anderer Personen der Akteneinsicht entgegenstehen.

Wie läuft ein Strafverfahren ab?

In der folgenden Übersicht finden Sie einen kurzen Überblick über den Ablauf eines Strafverfahrens, das abhängig vom Sachverhalt, den rechtlichen Voraussetzungen und besonderen Begleitumständen unterschiedlich ablaufen kann. Nach der Anzeigenerstattung bei der Polizei wird das Verfahren an die zuständige Staatsanwaltschaft weitergeleitet, die nach Abschluss ihrer Ermittlungen entweder Anklage erhebt, den Erlass eines Strafbefehls beantragt oder das Verfahren einstellt. Bei Fällen der Konkurrenzausspähung kann die Staatsanwaltschaft unter Umständen das öffentliche Interesse verneinen und auf den Privatklageweg verweisen. Der Erlass eines Strafbefehls obliegt wie ein Urteil der Entscheidung des zuständigen Gerichts. Als Betroffener einer Straftat erhalten Sie auf Wunsch Informationen über den Stand und den Ausgang des Verfahrens.

Wie sollten Sie bei einem Vorfall vorgehen?

Vorgehen bei einem Vorfall

- 🔒 Sie leiten sofort Abwehr- und Schutzmaßnahmen ein, auch bei einem scheinbar geringen Schaden.
- 🔒 Sie kontaktieren sofort Ihre Ansprechperson bei der Polizei oder die Fachdienststelle des Landes- oder Bundeskriminalamts.
- 🔒 Ihr Anliegen wird dort sofort vertrauensvoll und diskret behandelt.
- 🔒 Die Ermittlungen dauern unter Umständen lange. Sie können sich bei Ihrer polizeilichen Ansprechperson jederzeit nach dem aktuellen Status erkundigen.
- 🔒 Sie profitieren vom Erfahrungswissen der Experten/Expertinnen und werden im Hinblick auf das Vorgehen und Präventionsmaßnahmen schnell beraten.

Auszug aus dem Faltblatt: Wirtschaftsspionage und Konkurrenzausspähung: Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how.

4. Prävention und Strafverfolgung

Praktizierte Informationssicherheit ist ein Wettbewerbsvorteil. Allerdings unterschätzen KMU oft den Wert der eigenen Daten sowie die materiellen und immateriellen Folgen, wenn ein Wettbewerber oder ein fremder Staat ihre geschützten Informationen erlangen. Unzureichende Schutzvorkehrungen sowie eine fehlende Wahrnehmung und Beobachtung von Verdachtsindikatoren haben zur Folge, dass viele Angriffe unentdeckt bzw. die (Folge-)Schäden scheinbar unerklärlich bleiben.

Ein umfassendes Schutzkonzept sollte neben technischen und personellen Sicherungsmechanismen, internen Kontrollmaßnahmen und Schulungen für Mitarbeiter die eigene Fortbildung sowie die Teilnahme an informellen Gesprächsrunden, Tagungen oder Workshops der Unternehmensverbände beinhalten. Zudem sollten die Kooperationsmöglichkeiten zwischen KMU, Verbänden und Behörden einbezogen werden.

Best practices aus dem Inland

Initiative Wirtschaftsschutz

Mit der Initiative Wirtschaftsschutz haben sich Staat und Wirtschaft zum Ziel gesetzt, zentrale Unternehmenswerte und die Wirtschaft in Deutschland besser zu schützen. Auf der Internetplattform www.wirtschaftsschutz.info bündeln die Sicherheitsbehörden (Bundesamt für Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik, Bundeskriminalamt und Bundesnachrichtendienst) ihre Informationen und stellen sie kostenfrei zur Verfügung.

In einem **offenen Bereich** erhalten Sie allgemeine Informationen zu den Themen Spionage/Sabotage, Proliferation, Wirtschaftsschutz international und Wirtschaftskriminalität, Cyberabwehr/IT-Sicherheit und Cybercrime, internationale Sicherheitslage, Sicherheit auf Geschäftsreisen, PMK/Extremismus/Terrorismus. Neben dem regelmäßig erscheinenden Sonderbericht Wirtschaftsschutz können Publikationen, Veranstaltungshinweise, Pressemitteilungen oder Warnhinweise der beteiligten Behörden zum Thema Wirtschaftsschutz eingesehen werden.

Vertiefende Informationen zu den zuvor genannten Themen werden registrierten Nutzern im **geschlossenen Nutzerbereich** zur Verfügung gestellt. Das Internet kennt keine Öffnungs- bzw. Bürodienstzeiten und für alle Beteiligten ist es von Vorteil, im Schadensfall Informationen abrufen und zeitnah handeln zu können. Daher besteht die Möglichkeit, Sachverhalte zu vermuteten Ausspähvorfällen/Cyberangriffen per Kontaktformular zu übermitteln, die im weiteren Verlauf bewertet und an die zuständigen sachbearbeitenden Behörden zur Bearbeitung übermittelt werden.

Angebote von Verbänden

Die Branchen- und Dachverbände auf Bundes- und Landesebene sowie die Industrie- und Handelskammern (IHK) spielen bei der Bündelung von Interessen, der Selbststeuerung von Unternehmen und der Entwicklung optimaler Rahmenbedingungen für ihre Mitglieder eine wichtige Rolle. Sie kennen die Bedürfnisse ihrer Mitgliedsunternehmen sowie die Anforderungen, die in Bezug auf die Informationssicherheit in der jeweiligen Branche gestellt werden und können branchenspezifische Informationen zu Prävention und Strafverfolgung verbreiten.

Auf Messen, Workshops, Ausstellungen und weiteren Veranstaltungen der IHK und der Verbände können Sie sich zielgerichtet über Themen rund um den Bereich Wirtschaftsschutz, Wirtschaftsspionage und Konkurrenzausspähung, Cyberangriffe zur Ausspähung, Sabotage oder das Schulen und Sensibilisieren der eigenen Mitarbeiter informieren. Durch die Teilnahme an Tagungen, an denen auch Behördenvertreter teilnehmen oder die von Behörden angeboten werden, kann zu einem frühen Zeitpunkt ein Kontakt zwischen Behörden und KMU im Bereich des Informationsaustausches, auch mit dem Ziel einer langfristigen Zusammenarbeit, aufgebaut werden.

Da die Wirtschaft immer häufiger Ziel von Angriffen ist, bietet der bei Tagungen oder informellen Gesprächsrunden stattfindende Erfahrungsaustausch die Chance zur Kooperation und zur Stärkung geschaffener Netzwerke.

Best practices aus dem Ausland

Die im Rahmen der Experteninterviews geäußerten Erfahrungen von Unternehmen aus dem Ausland sind den zuständigen Entscheidungsträgern von Polizeibehörden zur Entwicklung weiterer Maßnahmen zur Verfügung gestellt worden, z.B. der Wunsch nach einem Online-Meldesystem für angegriffene Unternehmen. Schon heute können die Behörden einiger Bundesländer im Ausland erfolgreich praktizierte Maßnahmen, wie den Einsatz von hochqualifizierten Fachkräften oder Risikoanalysen durch staatliche Stellen, in einem begrenzten Umfang anbieten.

ICT-Engineers – Verfügbarkeit hochqualifizierter Fachkräfte

Mit diesem, bereits in Dänemark, aber auch einigen deutschen Bundesländern etablierten Modell, wird die schnelle Verfügbarkeit hochqualifizierter Experten gefördert. Die Experten können von Behörden angefordert werden, um die Strafverfolgung zu unterstützen und bieten den Unternehmen bei sich fortwährend weiterentwickelnden Angriffsformen und Bedrohungen zeitnah direkte Hilfe und professionelle Unterstützung an.

Risikoanalysen durch staatliche Stellen

Polizeidienststellen sollen langfristig die KMU bei der Auswahl angemessener Präventionsmaßnahmen beraten können. Ein implementiertes Informationssicherheitskonzept sollte eine Risikoanalyse - vor Ort oder mithilfe eines online verfügbaren Tools - einschließen. Auf diese Weise kann dem Unternehmen widerspiegelt werden, wie gut es gegen Angriffe auf sein geschütztes Know-how gesichert ist. Zudem sollte die Möglichkeit einer Zertifizierung durch staatliche oder staatlich beauftragte Stellen angeboten und mit der Bereitstellung von Informationen kombiniert werden, so dass die KMU einen praktischen Nutzen und Wettbewerbsvorteil aus der Risikoanalyse und der Zertifizierung ziehen können.

Welche Präventionsmaßnahmen können Sie ohne viel Aufwand umsetzen?

Wichtige Maßnahmen zur Prävention

- 🔒 regelmäßige Aktualisierung Ihrer (IT-)Schutzmaßnahmen
- 🔒 Nutzung der Alert-Services und Informationsmaterialien der Behörden (z.B. das Bürger-CERT (Computer Emergency Response Team) vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) oder der Cyber-Brief vom Bundesamt für Verfassungsschutz (BfV)
- 🔒 Sensibilisierung und Training kritischer Situationen mit Ihrer Mitarbeiterschaft
- 🔒 Verhaltensregeln für den Umgang mit Daten und sensiblen Informationen in Ihrem Unternehmen oder auf Dienstreisen
- 🔒 Begutachtung Ihrer Schutzmaßnahmen von (externen) Experten
- 🔒 Zugangskontrollen und interne Kontrollmaßnahmen

Auszug aus dem Faltblatt: Wirtschaftsspionage und Konkurrenzausspähung: Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how.

5. Fazit

Wirtschaftsspionage und Konkurrenzausspähung sind ein wachsendes Kriminalitätsfeld, das in unterschiedlicher Ausprägung in nahezu allen Ländern zu finden ist. Eine besondere und schwer aufzudeckende Bedrohung stellen Cyberangriffe dar. Die Untersuchungen im Projekt WISKOS haben gezeigt, dass KMU ebenso wie große Unternehmen gefährdet sind und ähnlich oft angegriffen werden. Der Wert der eigenen Informationen sowie möglicherweise entstehende Schäden werden von den KMU regelmäßig unterschätzt, so dass bei der Entwicklung umfassender Schutzstrategien Nachholbedarf besteht.

Handeln Sie jetzt

Das Thema Prävention von Wirtschaftsspionage und Konkurrenzausspähung muss zur Chefsache gemacht und nachdrücklich kommuniziert werden. Treffen Sie neben technischen Sicherheitsmaßnahmen aufeinander abgestimmte organisatorische und personelle Vorkehrungen. Beziehen Sie bei der Informationssicherheit und dem Informationsschutz Ihre Beschäftigten ein und sensibilisieren Sie sie im Hinblick auf die Verdachtsindikatoren. Ein gesteigertes Bewusstsein für Sicherheitsaspekte und der bewusste Einsatz von Präventionsmaßnahmen können den Schutz Ihres Unternehmens verbessern.

Unter <http://wiskos.de> finden Sie neben den Ergebnissen aus dem WISKOS-Projekt verschiedene Produkte zum kostenlosen Download, u.a. ein Informationsfaltblatt für KMU mit den Verdachtsindikatoren und Präventionsmaßnahmen sowie Warnhinweise zum Verlinken auf Ihrer Unternehmenshomepage.

Staatliche Behörden können nur dann wirkungsvoll arbeiten, wenn sie Kenntnis von möglichen Vorfällen und Verdachtsfällen erhalten. Hier sind beide Seiten zur Mitwirkung aufgerufen: Die Unternehmen tragen mit der Meldung von Vorfällen zur Verbreiterung der Informationsbasis und damit zur Entwicklung von übergreifenden Konzepten zu Prävention und Strafverfolgung bei; die Behörden schätzen Vorfälle und Angriffswellen im Kontext ein und unterstützen die Unternehmen bei der Aufklärung und bei der Implementierung von Sicherheitsmaßnahmen. Mittel- bis langfristig profitieren so beide Seiten.

Kontaktadressen der Landeskriminalämter und des Bundeskriminalamtes im Bereich Wirtschaftsschutz

LKA Baden-Württemberg

Inspektion 610
0711 / 5401-2610
stuttgart.lka.abt6.i610@polizei.bwl.de

LKA Bayern

SG 422-EK3
089 / 1212-3469
blka.spionage-
ansprechstelle@polizei.bayern.de

LKA Berlin

LKA 524, SG 2
030 / 4664-952420
lka524@polizei.berlin.de

LKA Brandenburg

LKA 300
03334 / 388-3001
zentraler.staatsschutz.fdlka@polizei.
brandenburg.de

LKA Bremen

K 63
0421 / 362-3863
k63@polizei.bremen.de

LKA Hamburg

LKA 72
040 / 4286-77200
lkahh72@polizei.hamburg.de

LKA Hessen

Hauptsachgebiet 53, SG 533
0611 / 83-53000
hsg53.hlka@polizei.hessen.de

LKA Mecklenburg-Vorpommern

Dez. 32
03866 / 64-3250
dez32.lka@lka-mv.de

LKA Niedersachsen

Dez. 42
0511 / 26262-4244
abteilung4@lka.polizei.niedersachsen.de

LKA Nordrhein-Westfalen

Dez. 23
Tel.: 0211 / 939-2320
33-Sachgebiet232.LKA@polizei.nrw.de

LKA Rheinland-Pfalz

Dez. 53
06131 / 65-2364
lka.53.l@polizei.rlp.de

LKA Saarland

Dez. LPP 233
0681 / 962-2660
lpp233@polizei.slpol.de

LKA Sachsen

Dez. 52
0351 855-3522
ermittlungen.pst.lka@polizei.sachsen.de

LKA Sachsen – Anhalt

Dez. 53
0391 / 250-2530
dl53.lka@polizei.sachsen-anhalt.de

LKA Schleswig-Holstein

SG 321
0431 / 160-4302
kiel.lka3@polizei.landsh.de

LKA Thüringen

Dez. 23
0361 / 341-1166
abteilung2.lka@polizei.thueringen.de

Bundeskriminalamt

Referat ST 23
02225 / 89-23286
st23@bka.bund.de

Publikationen mit Ergebnissen aus dem Projekt WISKOS

Praxisorientierte Informationsmaterialien

Für KMU

- > **Faltblatt** „Wirtschaftsspionage und Konkurrenzausspähung: Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how!“
- > **Bildergalerie** „Wirtschaftsspionage und Konkurrenzausspähung“ Warnhinweise zur Verwendung als Startbildschirm, Sperrbildschirm oder Pop-up-Fenster
- > **Broschüre** „Wirtschaftsspionage und Konkurrenzausspähung: Jedes dritte Unternehmen ist betroffen. Schützen Sie Ihr Know-how!“

Für Wissenschaftsorganisationen

- > **Faltblatt** „Wissenschaftsspionage: Schützen Sie Ihre Forschungsdaten!“
- > **Bildergalerie** „Wissenschaftsspionage“ Warnhinweise zur Verwendung als Startbildschirm, Sperrbildschirm oder Pop-up-Fenster
- > **Handlungsleitfaden** „Risiken für den deutschen Forschungsstandort“

Für Polizeibehörden

- > **Faltblatt** „Wirtschaftsspionage und Konkurrenzausspähung: Was ist zu tun, wenn sich ein Unternehmen an Sie wendet?“
- > **Broschüre** „Wirtschaftsspionage und Konkurrenzausspähung: Was ist zu tun, wenn sich ein Unternehmen an Sie wendet?“
- > **Poster** „Wirtschaftsspionage und Konkurrenzausspähung: Was ist zu tun, wenn sich ein Unternehmen an Sie wendet?“

Wissenschaftliche Publikationen

- > *Carl, S. & Kilchling, M. (Hrsg.): Economic and Industrial Espionage in Germany and Europe: History, Developments and Present Legislative Frameworks in a Comparative Perspective. Berlin 2018.*
- > *Wallwaey, E., Bollhöfer, E. & Knickmeier, S. (Hrsg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten europäischen Ländern. Berlin 2018.*
- > *Bollhöfer, E. & Jäger, A.: Wirtschaftsspionage und Konkurrenzausspähung: Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Freiburg i.Br. 2018.*

Die Informationsmaterialien für KMU und Wissenschaftsorganisationen finden Sie kostenlos zum Download unter:

<http://wiskos.de>

WISKOS