BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

iv INDUSTRIELLEN VEREINIGUNG

FH CAMPUS WIEN UNIVERSITY OF APPLIED SCIENCES

WKO WIRTSCHAFTSKAMMER ÖSTERREICH

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

in österreichischen Unternehmen 2015

Dezember 2015

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

in österreichischen Unternehmen 2015

Dezember 2015

Diese Broschüre – sowie sonstige aktuelle Publikationen – ist in der Service-GmbH
der Wirtschaftskammer Österreich erhältlich:
Telefon: 0590 900-5050 oder
Fax: 0590 900-236 sowie
E-Mail: mservice@wko.at
Internet: http://webshop.wko.at

IMPRESSUM:

Verfasser
Das vorliegende Handbuch wurde von mehreren Autoren im Auftrag des Bundesministeriums für Inneres/Bundesamt für Verfassungsschutz und Terrorismusbekämpfung durch die FH Campus Wien Forschungs- und Entwicklungs GmbH (verantwortlich: FH Campus Wien – Fachbereich Risiko- und Sicherheitsmanagement) erstellt.
Unterstützt wurde das Projekt durch die Partner Wirtschaftskammer Österreich und Industriellenvereinigung.

Autoren
Mag. Claudia Körmer, FH-Prof. Martin Langer, FH Campus Wien

Abwicklung der Umfrage: Mag. Claudia Körmer, Wirtschaftskammer Österreich, Industriellenvereinigung
Statistische Auswertung: Mag. Christian Steinlechner
Redaktionelle Bearbeitung: DI (FH) Mag. Thomas Goiser MA
Gestaltung: Marion Gaa (www.lucid.at)

Medieninhaber
Bundesministerium für Inneres
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)
Telefon: 01-531 26-4100
E-Mail: wis@bvt.gv.at
Internet: http://www.bmi.gv.at

Hersteller
Gestaltet und gedruckt mit freundlicher Unterstützung der Wirtschaftskammer Österreich.
Wiedner Hauptstraße 75
1045 Wien

Alle Rechte vorbehalten.
Trotz sorgfältiger Prüfung sämtlicher Beiträge in dieser Publikation sind Fehler nicht auszuschließen, und die Richtigkeit des Inhalts ist daher ohne Gewähr. Eine Haftung der Autoren oder des Medieninhabers ist ausgeschlossen.

Hinweis
Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter!
Wien, Dezember 2015

INHALTSVERZEICHNIS

©BMI/Alexander TUMA

Mag.ª Johanna Mikl-Leitner
Bundesministerin für Inneres

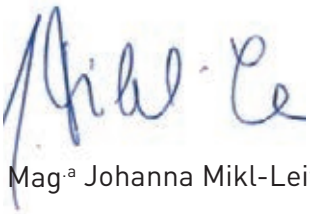
Die Herausforderungen an ein Unternehmen, im nationalen und internationalen Wettbewerb zu bestehen, sind mannigfaltig. Die Verfügbarkeit von Ressourcen einschließlich der erforderlichen Mitarbeiter, förderliche rechtliche Rahmenbedingungen und ein vertrauensvolles Miteinander von Wirtschaft, Wissenschaft und Sicherheitsbehörden sind die Grundvoraussetzungen für einen sicheren Wirtschaftsstandort. Diesen gilt es zu schützen.

Im aktuellen Arbeitsprogramm für die XXV. Gesetzgebungsperiode 2013–2018 setzt sich die österreichische Bundesregierung die Bekämpfung von Wirtschafts- und Industriespionage im Zusammenwirken mit der Wirtschaft zum Ziel. Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) als zuständige Sicherheitsbehörde hat im Rahmen des Präventionsprogramms Wirtschafts- und Industriespionage (WIS) eine Studie über die aktuelle Betroffenheit der österreichischen Unternehmen von Wirtschafts- und Industriespionage durchgeführt, um die Wirkung der bereits gesetzten Initiativen zu evaluieren und neue Handlungsfelder für die Präventionsarbeit zu identifizieren.

Die Kooperation des BMI als Dienstleister im Bereich Sicherheit mit der Wirtschaftskammer Österreich, der Industriellenvereinigung sowie der FH Campus Wien beruht auf dem Verständnis, dass bestmöglicher Schutz vor Wirtschafts- und Industriespionage nur in Teamarbeit mit Wirtschaft und Wissenschaft gewährleistet werden kann.

Denn kurzfristig betrachtet, bedeuten erfolgreiche Angriffe die Schwächung des einzelnen Unternehmens. Langfristig wird jedoch die Attraktivität und Reputation des Wirtschaftsstandortes Österreich geschwächt. Das Bewusstsein für mögliche Bedrohungen des Unternehmens durch die staatlich gelenkte Wirtschaftsspionage sowie durch die unlautere Wettbewerbspraxis der Industriespionage ist die Grundlage für die Entwicklung individueller Sicherheitsmaßnahmen.

Die Aufgabe des BMI ist es, von der Wirtschaft gewünschte Formate im Bereich der Prävention anzubieten. Die vorliegende repräsentative Studie ergänzt die bereits verfügbaren Publikationen und liefert ein objektives Bild hinsichtlich der Selbsteinschätzung der Unternehmen, und zeigt einmal mehr die Relevanz der Identifizierung der tatsächlichen Geschäfts- und Betriebsgeheimnisse auf. Denn in der heutigen Wissensgesellschaft und den ständig wachsenden Möglichkeiten der Vernetzung auf individueller und virtueller Ebene gilt es, Know-how gemeinsam zu schützen.



Mag.ª Johanna Mikl-Leitner

Dr. Christoph Leitl
Präsident der Wirtschaftskammer Österreich

Chancen nützen – auf Sicherheit setzen.

Sehr geehrte Damen und Herren,

die österreichischen Unternehmen nutzen die Chancen der Globalisierung und des EU-Binnenmarktes. So hat sich seit dem EU-Beitritt 1995 bis 2014 die Ausfuhr der Waren aus Österreich von 42 Mrd. Euro auf 128 Mrd. Euro mehr als verdreifacht.

Viele österreichische Betriebe sind Marktführer in Nischenbereichen. Sie sichern mit ihren innovativen Produkten und Dienstleistungen Arbeitsplätze und Einkommen in Österreich. Die global vernetzte und hochrangig digitalisierte Welt stellt uns allerdings vor neue Herausforderungen.

So sind viele österreichische Unternehmen der Gefahr ausgesetzt, Opfer von Wirtschafts- und Industriespionage zu werden. Im Fokus der Täter liegen vor allem Produktionsunternehmen und produktionsnahe Dienstleister sowie Telekommunikations- und IKT-Unternehmen.

Was können die Betriebe selbst tun? Sie können ihre Unternehmens- und Sicherheitsstrategie stärker verknüpfen, Sicherheits-Verantwortliche in Unternehmen bestimmen, den Informationsschutz verstärken und externe Gefahrenquellen systematisch durchleuchten. Wie können die Unternehmen im Bereich der Prävention unterstützt werden?

Die Wirtschaftskammer Österreich wird gemeinsam mit dem Bundesministerium für Inneres die Informationen zum Thema „Schutz vor Wirtschafts- und Industriespionage" weiter ausbauen. So wird sich der „E-Day:16" mit dem Motto „Unternehmen Sicherheit" unter anderem den Themen „IT- und Datensicherheit" sowie „Sicherheitstraining und loyale Mitarbeiter" widmen.

Danke an dieser Stelle den über 1.100 Unternehmen, die – trotz ihres intensiven Alltagsgeschäfts – die Zeit gefunden haben, an der Studie durch Beantwortung des Fragebogens mitzuwirken. Danke auch den Projektpartnern Bundesministerium für Inneres, Industriellenvereinigung und FH Campus Wien für ihre Unterstützung!

Dr. Christoph Leitl

© Andi Bruckner, IV

Ing. Mag. Peter Koren
Vize-Generalsekretär
der Industriellenvereinigung

Im Kontext der Globalisierung nehmen die Anforderungen an die Sicherheit der heimischen Industrie seit Jahren an Komplexität zu. Ein funktionierender Industrie- und Wirtschaftsschutz kann daher nur in einem umfassenden Ansatz verfolgt werden.

Nur gemeinsam können wir durch die Analyse der Bedrohungen für die österreichische Wirtschaft entsprechende Strategien entwickeln und dadurch den Schutz des Industrie- und Wirtschaftsstandortes verbessern. Die Industriellenvereinigung hat daher in einem Kooperationsprojekt mit dem Bundesministerium für Inneres, der Wirtschaftskammer Österreich und der Fachhochschule Campus Wien die aktuelle Situation in Österreich gemeinsam erhoben, um die Wirkung der bereits gesetzten Initiativen zu evaluieren und neue Handlungsfelder zu identifizieren. Die vorliegende Studie bildet die Betroffenheit der österreichischen Unternehmen ab und gibt zugleich einen gemeinsamen Arbeitsauftrag für alle betroffenen Stakeholder zur Stärkung des Standortes.

Die Bedrohung für die österreichische Industrie und Wirtschaft ist sehr real und richtet jährlich einen Milliardenschaden an. In den meisten Fällen richtet sich die Spionage gegen Unternehmen, deren Produkte und Dienstleistungen aufgrund ständiger Innovation und hoher Qualitätsstandards weltweit geschätzt werden. Gütesiegel wie „Made in Austria" sind Ausdruck dieser Qualität und machen es attraktiv, sie zu kopieren. Die Abwehr von Industrie- und Wirtschaftsspionage wird damit immer mehr zu einem entscheidenden Wettbewerbsfaktor.

Aber wo Schatten, da auch Licht: Das Thema Cyber- sowie Industrie- und Wirtschaftssicherheit eröffnet neue Geschäftsmöglichkeiten für innovative Unternehmen in Österreich und Europa. So ist der Weltmarkt für IT-Sicherheit etwa 50 Mrd. Euro groß und ist in den letzten zehn Jahren jährlich im zweistelligen Prozentbereich gewachsen. Österreich und Europa müssen diese Chance nützen und zur Aufholjagd antreten. Viele Innovationen der Zukunft – von selbstfahrenden Autos über Heimautomatisierung – benötigen eine digital vernetzte Wirtschaft. Hier sind neue Denkmuster und Innovationen im Bereich der Sicherheit gefragt. Das sind Herausforderungen, die Staat und Wirtschaft gemeinsam lösen müssen.

Eine sichere Wirtschaft leistet auch einen Beitrag zu sozialer Sicherheit und gesellschaftlicher Stabilität unseres Landes. Wirtschaftsschutz ist damit sowohl Wettbewerbsvorteil als auch Zukunftssicherung. Österreichs Industrie ist bereit und willens, Verantwortung zu tragen und die notwendigen Schritte für mehr Cybersicherheit und effektiven Industrie- und Wirtschaftsschutz aktiv und in enger Abstimmung mit den Behörden voranzutreiben – ohne dass es zu Überregulierung und flächendeckender Überwachung kommt.

Ing. Mag. Peter Koren

FH-Prof. DI Martin Langer
Studiengangsleiter, FH Campus Wien
Fachbereich Risiko- und
Sicherheitsmanagement

Wirtschafts- und Industriespionage:
Ein strategisches Thema

Wir sind täglich über die Medien mit Krisen und Katastrophen konfrontiert und setzen uns sowohl im beruflichen als auch im persönlichen Leben mit den unterschiedlichsten Gefahren auseinander. Eine Gefahr, die wenig in unserem Bewusstsein verankert ist, ist Wirtschafts- und Industriespionage.

In unserer vernetzten Welt sitzen die Täter potenziell überall, im Unternehmen selbst, im Ausland oder am Tisch nebenan im Restaurant. Ihre Angriffsmöglichkeiten sind ebenfalls vielseitig und werden oft kombiniert. Die Gefahr für das Unternehmen wird zumeist nicht bemerkt, es gibt oft statt gerichtsfester Beweise nur Vermutungen, und die Auswirkungen werden erst viel später wahrgenommen.

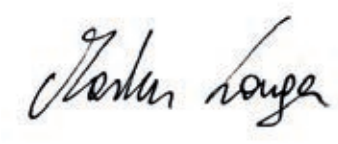
Mit dieser Studie, die wir gemeinsam mit unseren bewährten Partnern BMI, der Wirtschaftskammer Österreich und der Industriellenvereinigung durchführen, wollen wir das tatsächliche Ausmaß und die Hintergründe dieser Problematik beleuchten.

Ich möchte mich persönlich bei allen Unternehmen, die an der Umfrage für dieses Studienprojekt teilgenommen haben, ganz herzlich bedanken. Durch ihre Mithilfe werden geeignete Maßnahmen zur Unterstützung von akademischer und politischer Seite möglich.

Wirtschafts- und Industriespionage ist ein umfassendes und strategisches Thema, das im Gegensatz zur „klassischen" Sicherheit in Märkten, Produkten, Wettbewerbssituationen und Globalisierung gedacht werden muss. Oberstes Ziel ist es, die Werte des Unternehmens zu schützen – Informationen über Unternehmensstrategie, Kunden, Produkte und Verfahren, Lieferanten oder Prototypen.

Das beste Mittel gegen Wirtschafts- und Industriespionage ist die Prävention. Dazu gehören eine umfassende Bewusstseinsbildung und der Umstand, das Problem zu erkennen und zu verstehen. Die Vernetzung und die Integration von kulturellen, organisatorischen, technischen und baulichen Maßnahmen ist dabei zentral, denn eine Kette ist immer nur so stark wie ihr schwächstes Glied. Mit unserem Bachelorstudiengang Integriertes Sicherheitsmanagement bilden wir Fachleute aus, die sowohl Safety als auch Security für die unterschiedlichsten Firmenstandorte gewährleisten können bis hin zum Thema Reisesicherheit oder auch Informationssicherheit. Mit dem Masterstudiengang Integriertes Risikomanagement bilden wir Experten für die strategische Ebene aus, die die Sprache der Wirtschaft sprechen und Risiken und Gefahren adäquat managen können. Dabei setzen wir auf internationale akademische Vernetzung und die Zusammenarbeit mit spezialisierten Unternehmen, vor allem im gesamten deutschsprachigen Raum.

Wir verstehen akademische Ausbildung und angewandte Wissenschaft als die Fähigkeit, Probleme zu verstehen und zu lösen. Wir freuen uns auf weitere Kooperationen und den Informationsaustausch mit Ihnen!



FH-Prof. DI Martin Langer

STUDIENDESIGN

Für die Zusammenstellung der Stichprobe wurde eine Grundgesamtheit von N = 163.872 österreichischen Unternehmen aus dem Datenbestand der Wirtschaftskammer Österreich und der Industriellenvereinigung (IV) herangezogen. Insgesamt wurden 15.000 Unternehmen mittels geschichteter Stichprobe nach Bundesland, Branche und Unternehmensgröße für die Befragung ausgewählt. Diese wurde von 23. Juni bis 31. Juli 2015 mittels standardisiertem Online-Fragebogen abgewickelt.

Die Klassifizierung der Wirtschaftstätigkeiten der untersuchten Unternehmen erfolgte nach ÖNACE 2008, um ein möglichst differenziertes Bild zu erhalten. Die Grundgesamtheit der Studie stellt den gesamten Wirtschaftsstandort Österreich dar. Frühere und internationale Umfragen waren nur auf eine bestimmte Mindest-Unternehmensgröße, Branche oder Mitarbeiterzahl bezogen. Die Ergebnisse der vorliegenden Studie sind daher mit anderen, weniger umfassenden Umfragen nicht vergleichbar, da sich aufgrund der geänderten Stichprobe andere Relationen ergeben.

Der Fragebogen umfasste neben den Angaben zum Unternehmen (z. B. Bundesland, Niederlassungen, Umsatz) die Bereiche Innovationen, mögliche Spionagevorfälle in den vergangenen fünf Jahren, Einschätzung von möglichen Spionagevorfällen in der Zukunft (bei nicht betroffenen Unternehmen), Präventionsmaßnahmen sowie Erwartungen. Durch den längeren Betrachtungszeitraum von fünf Jahren ist, bei der Leitfrage nach der Betroffenheit von Wirtschafts- und Industriespionage, eine höhere Aussagekraft gegeben, insbesondere hinsichtlich der Folgeschäden. Ein besonderer Schwerpunkt lag inhaltlich auf Fragen nach dem Bewusstsein der Unternehmen dafür, dass Mitarbeiter und der Umgang mit ihnen ein zentrales Element für die Sicherheit im Unternehmen sind.

Insgesamt wurden 1.149 Fragebögen vollständig ausgefüllt und ausgewertet. Dies entspricht einer Rücklaufquote von 7,7 %.

ZENTRALE STUDIENERGEBNISSE

1. 5,1 % der befragten Unternehmen gaben an, dass sie in den vergangenen fünf Jahren mindestens einmal Opfer von Wirtschafts- und Industriespionage waren (viele davon mehrfach). Ein Drittel der Vorfälle betraf Industriebetriebe. Auf die verwendete Grundgesamtheit hochgerechnet würde das rund 8.400 betroffene Unternehmen bedeuten.

2. Die Täter kommen aus dem In- und Ausland und greifen (oft kombiniert) mit unterschiedlichsten Mitteln österreichische Unternehmen an ihren Standorten im Inland wie im Ausland an. Unabhängig von den verwendeten Werkzeugen stehen hinter jedem Angriff Menschen. In nahezu der Hälfte der Fälle kommen Mitbewerber als Täter infrage.

3. Betroffene Unternehmen haben bisher nur geringe Erwartungen an die Erfolge einer strafrechtlichen Verfolgung: Lediglich ein Viertel gab an, Behörden eingebunden zu haben; als häufigster Grund werden Beweisprobleme genannt.

4. Neben dem unmittelbaren finanziellen Schaden entstehen aufseiten der Unternehmen eine Reihe weiterer Schäden: 71 % der betroffenen Unternehmen gaben an, unternehmenskritische Folgeschäden erlitten zu haben, etwa durch den Verlust von Aufträgen und/oder Kunden, Reputationsschäden etc.

5. Ein großer Teil der Unternehmen schätzt einen zu hohen Anteil ihrer Information als besonders schutzwürdige Geschäfts- und Betriebsgeheimnisse ein: Nahezu 30 % gaben an, dass mehr als die Hälfte der Informationen im Unternehmen Geschäfts- und Betriebsgeheimnisse darstellen. Dies macht ihren effektiven Schutz in der Praxis schwierig.

6. Es gibt in Bezug auf die Unternehmensgröße keine signifikanten Unterschiede. Jedes Unternehmen ist potenziell betroffen. Große Unternehmen verfügen in der Regel über umfangreichere Mechanismen und spezifischeres Know-how, wie sie ihre Geschäfts- und Betriebsgeheimnisse schützen. In stärker regulierten Branchen wird die Qualität der getroffenen Maßnahmen höher eingeschätzt.

7. Für die Zukunft wünschen sich Unternehmen vor allem gezielte Informationsangebote seitens der Behörden in Form von Online-Informationsplattformen und Broschüren sowie Branchenveranstaltungen.

ZUSAMMENSETZUNG DER UNTERNEHMEN

Branchen

Die Unternehmen verteilen sich nach ihrer Wirtschaftstätigkeit gemäß ÖNACE 2008 folgendermaßen:

Tabelle 1: Branche bzw. Hauptbetätigungsfeld

BRANCHE	ERWARTETE WERTE	BEOBACHTETE WERTE
Handel, Instandhaltung und Reparatur von Kraftfahrzeugen	25,5 %	10,3 %
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen	15,2 %	7,7 %
Bau	10,9 %	10,2 %
Beherbergung und Gastronomie	10,9 %	6,6 %
Herstellung von Waren	8,4 %	15,6 %
Information und Kommunikation	6,5 %	10,5 %
Erbringung von sonstigen wirtschaftlichen Dienstleistungen	4,2 %	7,2 %
Erbringung von sonstigen Dienstleistungen	4,1 %	12,1 %
Verkehr und Lagerei	3,6 %	3,7 %
Erbringung von Finanz- und Versicherungsdienstleistungen	2,8 %	4,5 %
Grundstücks- und Wohnungswesen	2,3 %	1,6 %
Gesundheits- und Sozialwesen	1,9 %	3 %
Kunst, Unterhaltung und Erholung	1,4 %	1,7 %
Erziehung und Unterricht	1,1 %	0,7 %
Land- und Forstwirtschaft, Fischerei	0,6 %	1,2 %
Wasserversorgung, Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen	0,3 %	0,6 %
Bergbau und Gewinnung von Steinen und Erden	0,1 %	1 %
Energieversorgung	0,1 %	1,8 %

n = 1.149

Unternehmensgröße

Die Gliederung der Unternehmen erfolgte nach der Mitarbeiterzahl gemäß der gängigen Definition von kleinen und mittleren Unternehmen: Kleinstunternehmer bis 9 Mitarbeiter, Kleinunternehmen 10–49 Mitarbeiter, mittlere Unternehmen 50–249 Mitarbeiter, Großunternehmen ab 250 Mitarbeiter (die ihrerseits in weitere Kategorien unterteilt wurden).

Tabelle 2: Unternehmensgröße

MITARBEITER	ERWARTETE WERTE	BEOBACHTETE WERTE
0 bis 9	82,0 %	63,2 %
10 bis 49	15,2 %	16,6 %
50 bis 249	2,4 %	8,2 %
250 bis 999	0,2 %	6,4 %
1.000 bis 9.999	0,1 %	4,5 %
10.000 und mehr	0,1 %	1,0 %

n = 1.149

Standorte und Auslandsniederlassungen

Die 1.149 Unternehmen verteilen sich nach Bundesländern bezüglich ihres Hauptsitzes vorwiegend auf die Bundesländer Wien und Niederösterreich (jeweils rund 20 %), gefolgt von der Steiermark (13 %), Oberösterreich (12 %), Tirol (9 %), Salzburg (9 %), Kärnten (7 %), Vorarlberg (4 %) und dem Burgenland (3 %). Bei rund 2 % befindet sich der Hauptsitz nicht in Österreich.[1]

255 der 1.149 befragten Unternehmen verfügen über Niederlassungen im Ausland, sie gaben durchschnittlich drei Niederlassungen an.[2]

Geschäftsbeziehungen

Nahezu alle (über 94 %) befragten Unternehmen unterhalten ständig oder häufig Geschäftsbeziehungen im Inland, knapp die Hälfte in Westeuropa und knapp mehr als ein Viertel in Zentral- und Osteuropa. Jeweils rund 10 bis 14 % der Unternehmen unterhalten ständig oder häufig Geschäftsbeziehungen zu den GUS-Staaten, Nordamerika und Asien. Zum Mittleren und Nahen Osten, Mittel- und Südamerika sowie Afrika unterhalten weniger als 10 % der österreichischen Unternehmen ständig oder häufig Geschäftsbeziehungen.

Jahresumsatz

7 von 10 Unternehmen erzielten in ihrem letzten Geschäftsjahr einen Jahresumsatz von maximal 2 Mio. Euro, rund 10 % maximal 10 Mio. Euro. Rund 5 % der Unternehmen setzten maximal 50 Mio. Euro um, 4 % bis zu 100 Mio. Euro. Rund 10 % verzeichneten schließlich einen Umsatz von mehr als 100 Mio. Euro.

Forschungs- und Entwicklungsarbeit, Innovationen

Ein Drittel der befragten Unternehmen gab an, Forschungs- und/oder Entwicklungsarbeit zu betreiben.
61 % der Unternehmen (702 insgesamt) brachten in den letzten fünf Jahren keine neuen Produkte und Verfahren auf den Markt. Von den restlichen 39 % (447 Unternehmen) brachten nahezu drei Viertel bis zu zehn neue Innovationen auf den Markt.

1 Dies deckt sich von den Größenordnungen her mit der Verteilung der Unternehmen in den österreichischen Bundesländern: Wien 18 %, Niederösterreich 17 %, Steiermark 15 %, Tirol 12 %, Oberösterreich 11 %, Salzburg 10 %, Kärnten 8 %, Vorarlberg 6 % und Burgenland knapp 3 %.

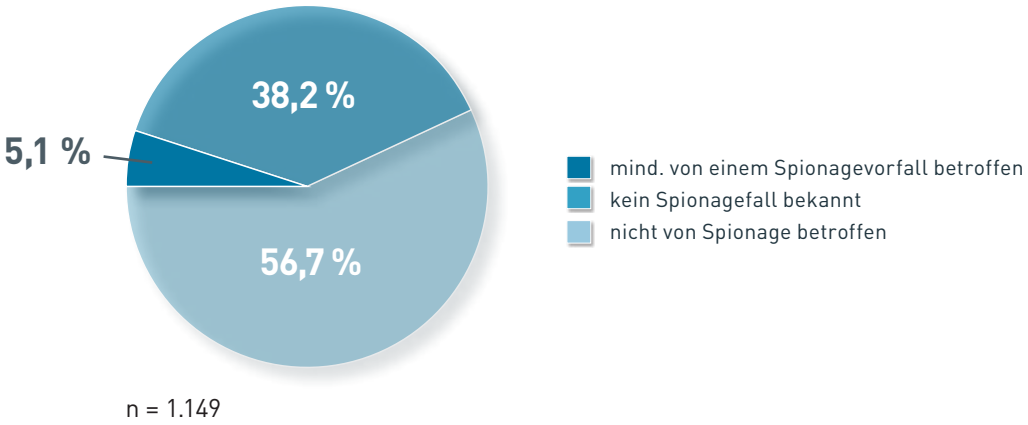
2 Die meisten dieser Niederlassungen befinden sich mit über 43 % in Europa (25,8 % in Westeuropa und 17,4 % in Zentral- und Osteuropa), gefolgt von Asien und Nordamerika (mit jeweils etwas über 11 %). Das restliche Drittel verteilt sich auf die GUS-Staaten, Mittel- und Nordamerika, den Mittleren und Nahen Osten, Australien, Ozeanien und Afrika.

STUDIENERGEBNISSE IM DETAIL

BETROFFENHEIT DER UNTERNEHMEN

Auf die Frage, ob sie in den vergangenen fünf Jahren von Spionage betroffen waren, gaben 5,1 % (59) der 1.149 Unternehmen an, von mindestens einem Spionagevorfall betroffen gewesen zu sein. 38,2 % antworteten, dass ihnen kein Spionagefall in ihrem Unternehmen bekannt geworden ist, 56,7 % erklärten, dass sie nicht von Spionage betroffen waren.[3]

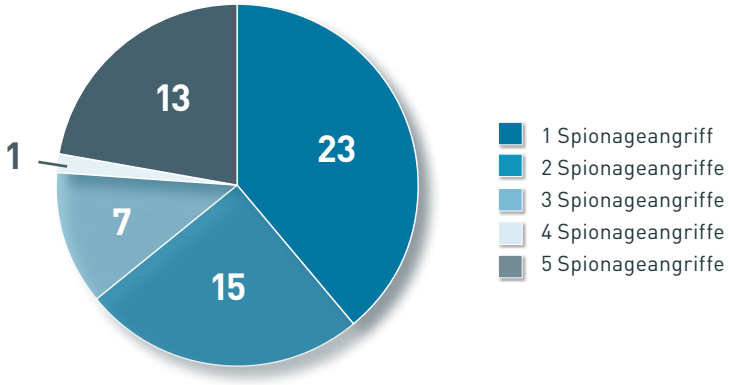
Abbildung 1: Betroffene Unternehmen



n = 1.149

Von den 59 betroffenen Unternehmen verzeichneten 23 nach Eigenangaben einen, 15 zwei, 7 drei, ein Unternehmen vier und 13 Unternehmen fünf oder mehr Spionageangriffe.

Abbildung 2: Anzahl der Vorfälle bei den betroffenen Unternehmen



n = 59

3 2010 gab nahezu jedes dritte der befragten österreichischen Unternehmen (31 %) an, in der Vergangenheit bereits Opfer gewesen zu sein. Ein direkter Vergleich ist allerdings aufgrund unterschiedlicher Studiendesigns, Fragestellungen und Schwerpunkte nicht möglich.

Betroffenheit nach Branche und Bundesland

In einem Drittel der Vorfälle waren Industriebetriebe von Wirtschafts- und Industriespionage betroffen. Die Top 5 der betroffenen Branchen sind „Herstellung von Waren", gefolgt von „Information und Kommunikation", „Beherbergung und Gastronomie", „Erbringung von sonstigen wirtschaftlichen Dienstleistungen" und „sonstigen Dienstleistungen".

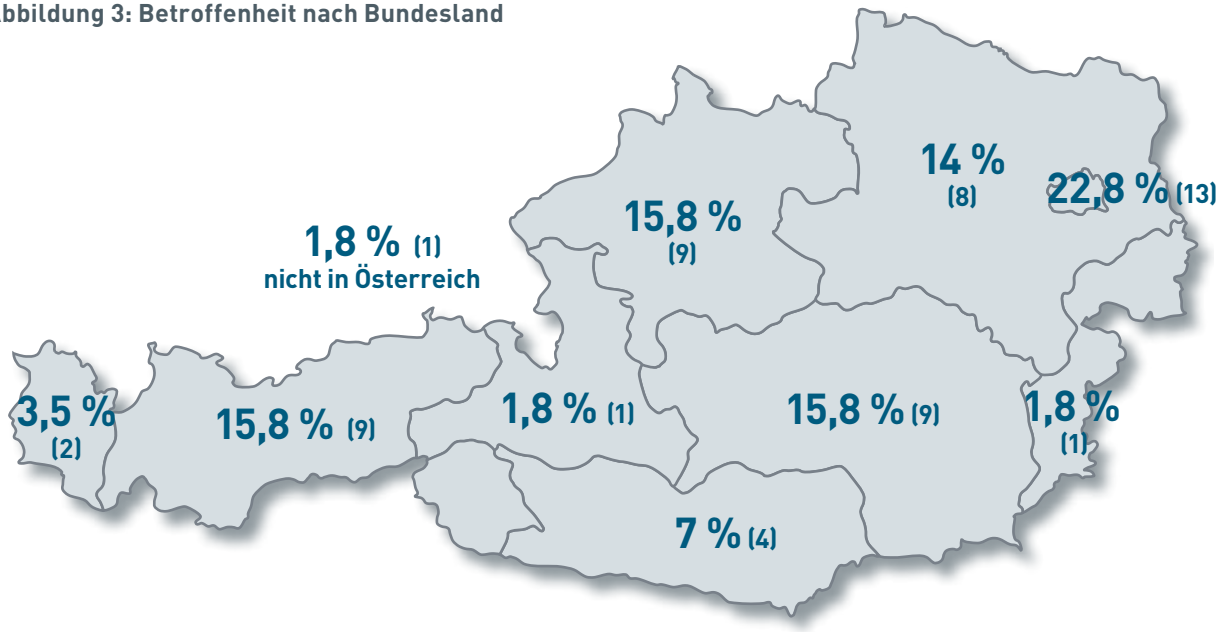
Dies deckt sich mit anderen Umfragen und der öffentlichen Diskussion; hier sind die großen internationalen Industrieunternehmen ebenso erfasst wie Telekommunikations- und IKT-Unternehmen.

Tabelle 3: Betroffenheit nach Branche

BRANCHE	HÄUFIGKEIT	PROZENT
Herstellung von Waren	**14**	**26,4 %**
Information und Kommunikation	**10**	**17,5 %**
Erbringung von sonstigen Dienstleistungen	**5**	**8,8 %**
Erbringung von sonstigen wirtschaftlichen Dienstleistungen	**5**	**8,8 %**
Beherbergung und Gastronomie	**5**	**8,8 %**
Handel; Instandhaltung und Reparatur von Kraftfahrzeugen	3	5,3 %
Verkehr und Lagerei	3	5,3 %
Bau	2	3,5 %
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen	2	3,5 %
Erziehung und Unterricht	2	3,5 %
Erbringen von Finanz- und Versicherungsdienstleistungen	1	1,8 %
Energieversorgung	1	1,8 %
Kunst, Unterhaltung und Erholung	1	1,8 %
Grundstücks- und Wohnungswesen	1	1,8 %
Bergbau und Gewinnung von Steinen und Erden	1	1,8 %

n = 53; keine Angabe von 6 Unternehmen

Abbildung 3: Betroffenheit nach Bundesland

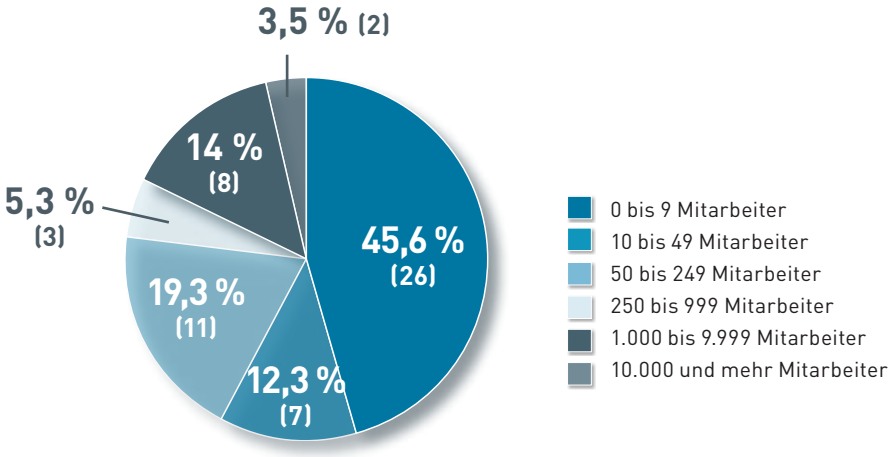


n = 57; keine Angabe von 2 Unternehmen

Betroffenheit nach Unternehmensgröße und Umsatz

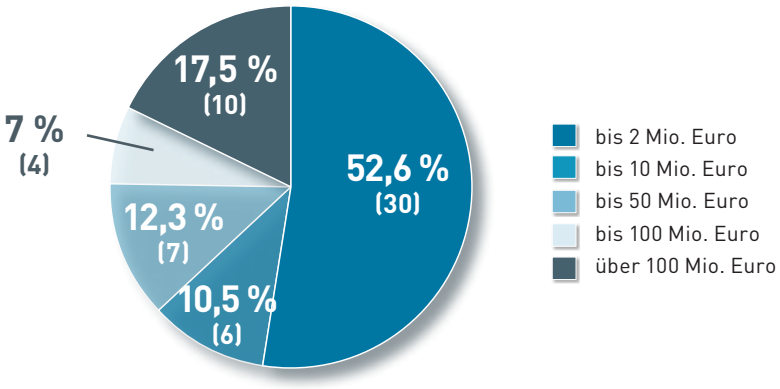
In Zusammenschau mit der Gesamtzahl der Unternehmen, gegliedert nach der Zahl der Mitarbeiter, welche an der Umfrage teilnahmen, bestätigen die Ergebnisse weiters, dass insbesondere klein- und mittelständische Unternehmen von Spionagevorfällen betroffen sind.
Mehr als die Hälfte der betroffenen Unternehmen setzen weniger als zwei Millionen Euro jährlich um.

Abbildung 4: Betroffenheit nach Unternehmensgröße



n = 57; keine Angabe von 2 Unternehmen

Abbildung 5: Betroffene Unternehmen nach Umsatz



n = 57; keine Angabe von 2 Unternehmen

Niederlassungen

29 der betroffenen Unternehmen verfügen über Niederlassungen im Ausland[4], 30 über keine. Von jenen Unternehmen, die Niederlassungen unterhalten, sind in allen Regionen jene aus der Branche „Herstellung von Waren" am stärksten von Spionageangriffen betroffen, gefolgt von Dienstleistungsbranchen und der Branche „Information und Kommunikation".

Häufigkeit der Spionagevorfälle

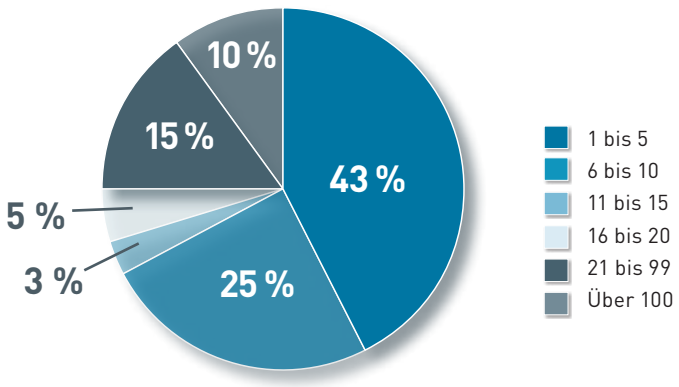
In den vergangenen fünf Jahren waren eher Kleinst- und Kleinunternehmen von fünf oder mehr bekannt gewordenen Spionagevorfällen betroffen. Rein statistisch betrachtet lässt sich aus den Daten allerdings keine Aussage darüber treffen, ob die Größe eines Unternehmens Auswirkungen auf die Anzahl von Spionagevorfällen hat.

Innovationen, Forschung und Entwicklung

Beinahe die Hälfte der betroffenen Unternehmen betreibt Forschungs- und Entwicklungsarbeit. Die Ergebnisse zeigen, dass die Industrieunternehmen hier die Hauptrolle spielen und insbesondere die Branche „verarbeitendes Gewerbe" im Regelfall mehr als eine marktfähige Innovation pro Jahr entwickelt.

Insgesamt haben knapp drei Viertel der von Wirtschafts- und Industriespionage betroffenen Unternehmen innerhalb der vergangenen fünf Jahre neue Produkte oder Verfahren auf den Markt gebracht. Zumeist wurden bis zu fünf Innovationen generiert.

Abbildung 6: Anzahl der Innovationen bei betroffenen Unternehmen, die Forschung und Entwicklungsarbeit betreiben, in den vergangenen fünf Jahren



n = 57; keine Angabe von 2 Unternehmen

4 Überwiegend in Westeuropa, Zentral- und Osteuropa sowie Asien und Nordamerika.

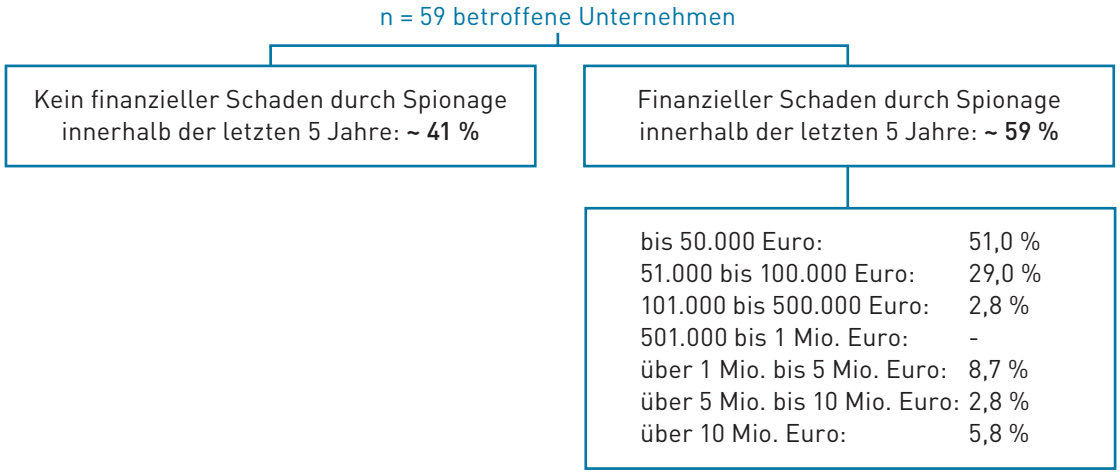
Schadensausmaß

Im Folgenden werden sowohl die finanziellen Schäden als auch die sonstigen Schäden der betroffenen Unternehmen dargestellt. Dies stellt auf die mittel- und langfristige Perspektive der Folgen ab. Dabei zeigt sich, dass ein Großteil der Unternehmen ebenfalls weitere Schäden erleiden musste, von Umsatzrückgängen über Auftragsverluste bis hin zum Abbau von Mitarbeitern.

Finanzieller Schaden

Von den 59 betroffenen Unternehmen gaben **35 (59 %) an, einen finanziellen Schaden erlitten zu haben**, bei 24 Unternehmen (41 %) konnte kein unmittelbarer finanzieller Schaden festgestellt werden.

Abbildung 7: Finanzieller Schaden bei den betroffenen Unternehmen



Verteilung nach Branchen

Unternehmen aus nahezu allen Branchen hatten durch zumindest einen Spionagevorfall einen finanziellen Schaden verzeichnet. Aus den Branchen „Bau, Verkehr und Lagerei", „Finanz- und Versicherungsdienstleistungen" sowie „Grundstücks- und Wohnungswesen" waren Unternehmen nach Eigenangaben zwar von Spionage betroffen, aber nicht von einem finanziellen Schaden.

Überwiegend waren finanzielle Schäden bis zu 100.000 Euro zu verzeichnen. Schäden zwischen 1 Mio. und 5 Mio. Euro betreffen zwei Unternehmen der Branche „Herstellung von Waren" und jeweils ein Unternehmen aus der Branche „Beherbergung und Gastronomie" bzw. „Erbringung von sonstigen wirtschaftlichen Dienstleistungen". Schäden über 5 Mio. Euro konnten in der Branche „Beherbergung und Gastronomie" festgestellt werden. Insgesamt wurden bei drei Industrieunternehmen Schäden über 10 Mio. Euro identifiziert – zwei Unternehmen kommen aus dem Bereich „Herstellung von Waren" und ein Unternehmen aus der „Energieversorgung".

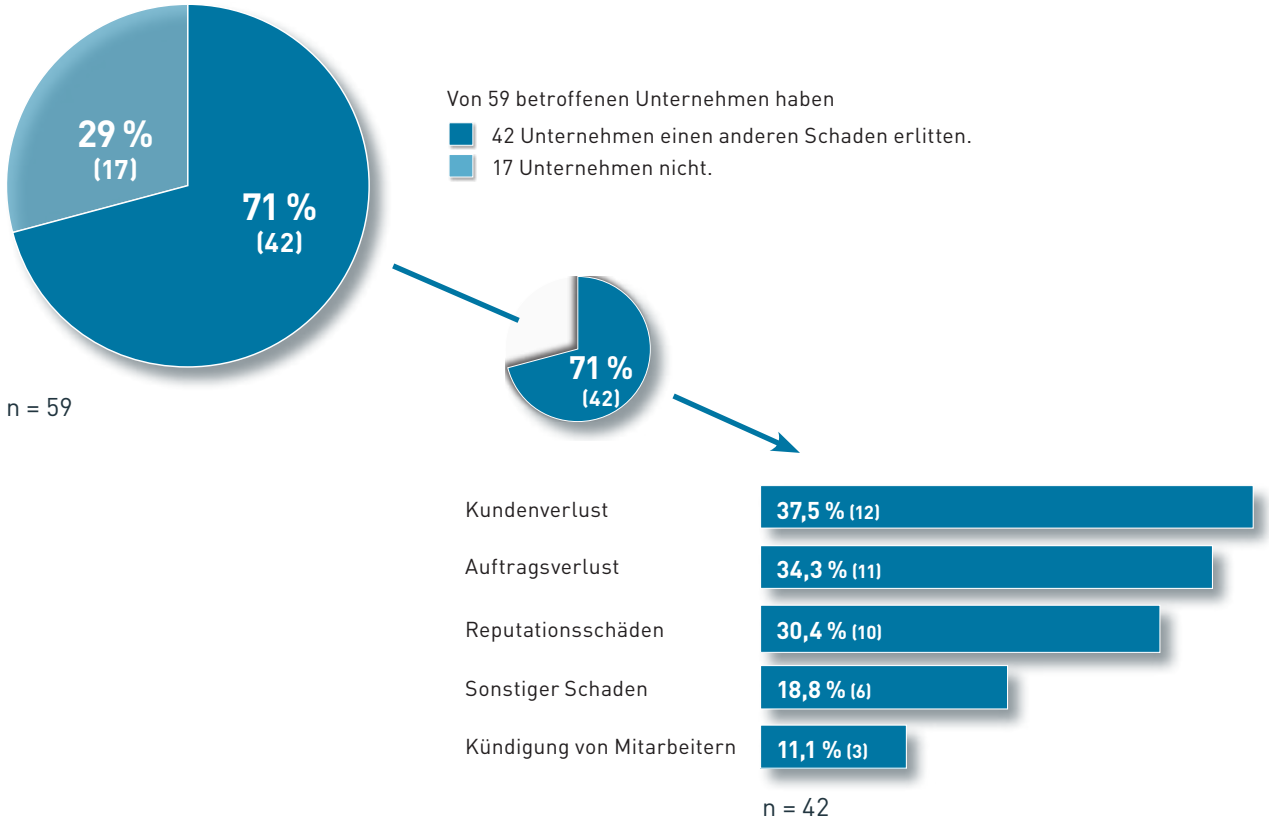
Verteilung nach Unternehmensgröße

- Bei den 16 betroffenen **Kleinstunternehmen** (bis zu 9 Mitarbeiter) sind die größten finanziellen Schäden bis zu 100.000 Euro zu beziffern (14 Unternehmen bis 50.000 und 2 Unternehmen bis 100.000 Euro).
- Bei **Kleinunternehmen** mit bis zu 49 Mitarbeitern sind bei insgesamt 4 Unternehmen Schäden bis zu 500.000 Euro entstanden (2 Unternehmen bis 50.000 Euro und jeweils ein Unternehmen bis 100.000 bzw. 500.000 Euro).
- Die finanziellen Schäden bei betroffenen **mittleren Unternehmen** (bis zu 249 Mitarbeiter) verteilen sich folgendermaßen: Bei 4 von 9 mittleren Unternehmen entstanden finanzielle Schäden von bis zu 50.000 Euro, bei zwei Unternehmen bis zu 100.000 Euro und in jeweils einem Unternehmen in der Höhe von bis zu 500.000, bis zu 5 Mio. und über 10 Mio. Euro.
- Sechs betroffene **Großunternehmen** ab 250 Mitarbeitern sind eher bei größeren finanziellen Schäden zu finden. Ein betroffenes Unternehmen beziffert die Summe des finanziellen Schadens auf 50.000, zwei auf bis zu 100.000 Euro, zwei weitere auf bis zu 5 Mio. Euro, ein Unternehmen auf bis zu 10 Mio. Euro und eines auf über 10 Mio. Euro.

Mögliche Folge: Unternehmenskritischer Schaden

Neben den finanziellen Einbußen kommt es oftmals zu anderen Schäden; dies bestätigten 42 von 59 betroffenen Unternehmen (71 %) aus eigener Erfahrung: Sie waren vor allem durch den Verlust von Kunden (38 %), den Auftragsverlust (34 %) und die Schädigung des Rufs bzw. des Ansehens des Unternehmens (30 %) betroffen.

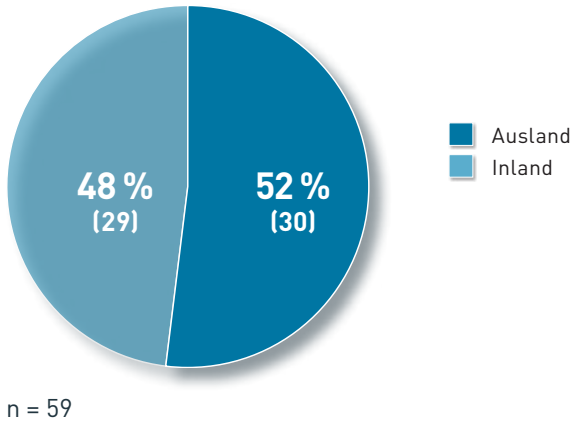
Abbildung 8: Unternehmenskritische Schäden betroffener Unternehmen



Inland und Ausland als Ausgangspunkt gleichauf

Knapp mehr als die Hälfte der betroffenen Unternehmen vermuten, dass der Spionageangriff aus dem Ausland stattgefunden hat. Annähernd die Hälfte der betroffenen Unternehmen geht davon aus, dass die Spionage im Inland ihren Ausgangspunkt hatte.

Abbildung 9: Vermuteter Ausgangspunkt des Spionageangriffs



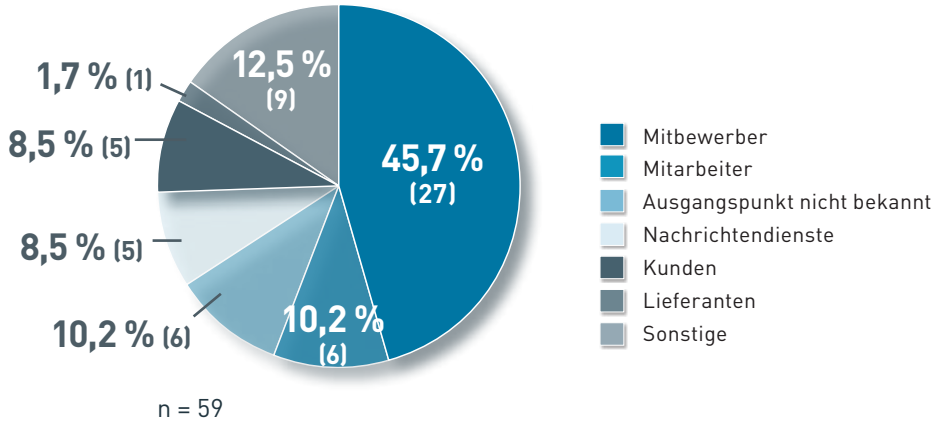
Entsprechend der Arbeitsdefinition des .BVT bezeichnet Wirtschaftsspionage die gezielte Ausforschung von Geschäfts- und Betriebsgeheimnissen (Wirtschaftsgeheimnissen) inländischer Unternehmen und Forschungseinrichtungen zur Stärkung der Wirtschaft anderer Staaten. In Zusammenschau mit der Interpretation des § 124 StGB (österr. Strafgesetzbuch) – Auskundschaftung von Geschäfts- und Betriebsgeheimnissen zugunsten des Auslandes, als „wirtschaftlicher Landesverrat" stellen Spionageangriffe aus dem Ausland bzw. durch ausländische Täter nicht nur eine Gefahr für die Wettbewerbsfähigkeit des einzelnen betroffenen Unternehmens dar, sondern für den gesamten Wirtschaftsstandort Österreich.

Demgegenüber sind Spionageangriffe auf ein österreichisches Unternehmen aus dem Inland vor allem aus der wettbewerbsrechtlichen Perspektive zu betrachten. Denn die klassische Konkurrenzspionage (Industriespionage oder Werksspionage) eines österreichischen Mitbewerbers mindert die Wettbewerbsfähigkeit des betroffenen Unternehmens und kann bis zur vollständigen Marktverdrängung führen.

Die Abgrenzung zwischen Wirtschafts- und Industriespionage ist für das betroffene Unternehmen hinsichtlich des eingetretenen Schadens unerheblich, jedoch bezüglich der Möglichkeiten einer (straf-)rechtlichen Verfolgung von Relevanz. Damit verbunden sind die Behördenzuständigkeiten, die Beweislast und der Ressourcenaufwand des Unternehmens. Allerdings ist bei Bekanntwerden eines Spionagevorfalls im Unternehmen der Ausgangspunkt der Spionage oftmals nicht unmittelbar lokalisierbar.

Mitbewerber kommen in nahezu der Hälfte der Fälle als Täter infrage

Abbildung 10: Täter bei den betroffenen Unternehmen



n = 59

Tathandlungen

Durchschnittlich wurden ein bis zwei Tathandlungen pro betroffenem Unternehmen angegeben. Am häufigsten wurden Hackerangriffe auf IT oder sonstige Geräte genannt. Ebenfalls wurde von rund einem Drittel der betroffenen Unternehmen der Informationsfluss (Kunden/Lieferanten) erwähnt, gefolgt von der Informationsweitergabe durch Mitarbeiter.

Zu beachten ist, dass die meisten Tathandlungen nicht technikbasiert sind, sondern das unmittelbare Agieren von Menschen erfordern (in insgesamt **71,2 %** gegenüber **58,2 % der Fälle**).

Tabelle 4: Durchgeführte Tathandlungen in den betroffenen Unternehmen

	PROZENT	
Informationsfluss (Kunden/Lieferanten)	33,2 %	
Informationsweitergabe durch Mitarbeiter	14,4 %	
Social-Engineering-Attacken	12,8 %	
Diebstahl von Informationsmedien	10,8 %	**71,2 %**
Abhören oder Abfangen von Kommunikation	13,6 %	
Hackerangriff auf IT oder sonstige Geräte	44,6 %	**58,2 %**
Sonstiges	12,8 %	
Anzahl der Tathandlungen (ø)	1,4	

n = 59, Mehrfachnennungen möglich

Besonderheiten: Tathandlungen nach Unternehmensgröße

Tabelle 5: Durchgeführte Tathandlungen nach Unternehmensgröße

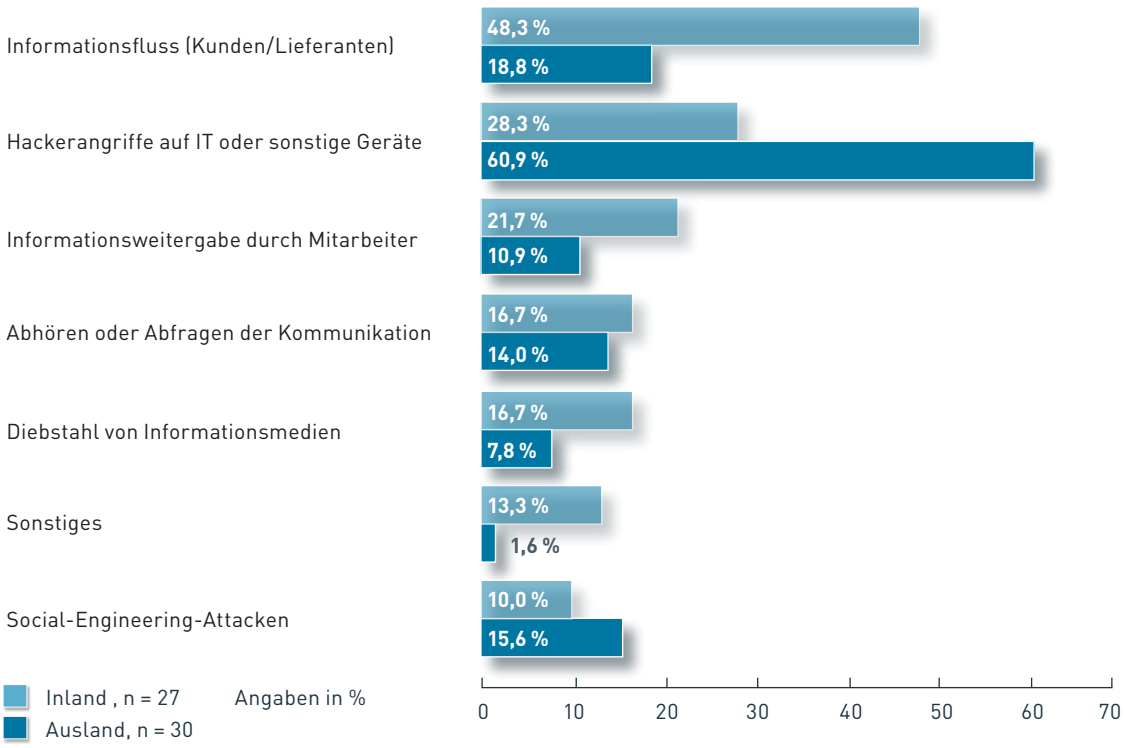
MITARBEITER / TATHANDLUNG	0 BIS 9	10 BIS 49	50 BIS 249	250 BIS 999	1.000 BIS 9.999	10.000 UND MEHR
Hackerangriffe auf IT oder sonstige Geräte	19,1 %	7,8 %	4,5 %	10,1 %	19,7 %	38,8 %
Abhören oder Abfragen der Kommunikation	29,8 %	13,1 %	8,0 %	36,8 %	5,4 %	6,9 %
Diebstahl von Informationsmedien	14,2 %	0 %	12,7 %	23,9 %	25,2 %	16,8 %
Social-Engineering-Attacken	2,6 %	25,6 %	4,1 %	2,8 %	33,2 %	31,7 %
Informationsweitergabe durch Mitarbeiter	2,0 %	21,7 %	25,2 %	24,8 %	13,6 %	12,7 %
Informationsfluss (Kunden/Lieferanten)	26,7 %	11,1 %	16,8 %	21,4 %	11,3 %	12,7 %

n = 59 Unternehmen insgesamt; Daten gewichtet, Mehrfachnennungen möglich

In- oder Ausland als Ausgangspunkt des Spionageangriffs

Die Auswertung der genannten Spionageangriffe nach dem Ausgangspunkt der Tathandlung ergab, dass Angriffe auf ein österreichisches Unternehmen aus dem Ausland signifikant öfter durch Hackerangriffe auf IT oder sonstige Geräte erfolgen. Tathandlungen, welche ihren Ausgangspunkt nach Angaben der Unternehmen im Inland haben, sind hingegen zumeist der Informationsfluss (Kunden/Lieferanten). Zudem zeigt sich durch die Möglichkeit der Mehrfachnennung, dass bei gezielten Angriffen oft mehrere Tathandlungen kombiniert werden (im Inland durchschnittlich 1,55, im Ausland 1,3).

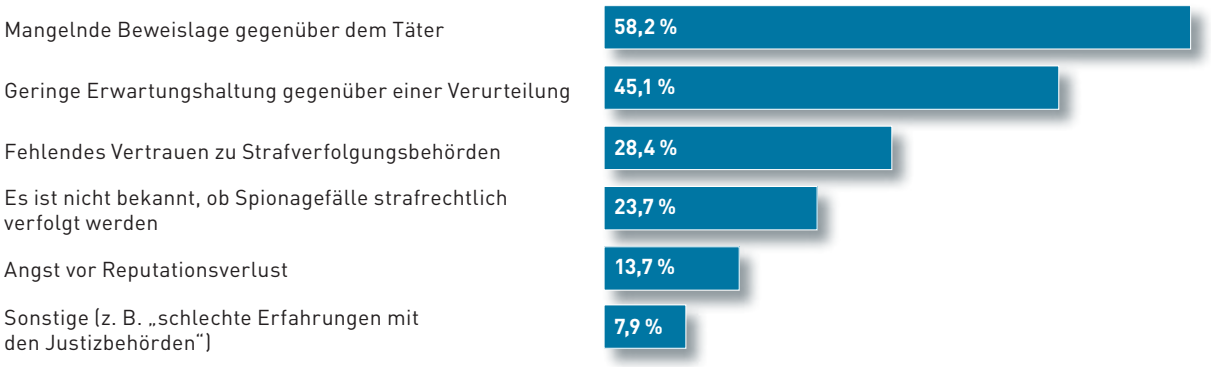
Abbildung 11: Stattgefundene Tathandlungen aus dem In- bzw. Ausland



Behördenverständigung und Folgemaßnahmen

Rund drei Viertel der betroffenen Unternehmen verständigten nach einem vorgefallenen Spionageangriff keine Behörde. Lediglich knapp ein Viertel der Unternehmen hat eine Behörde kontaktiert. In sechs Fällen wurde eine Polizeidienststelle[5] kontaktiert, in vier die Staatsanwaltschaft, in drei Fällen das Bundes- oder Landeskriminalamt, in zwei Fällen das .BVT direkt. In fünf Fällen wurden „andere Stellen" benachrichtigt[6]. Durchschnittlich wurden pro Spionagevorfall eine bis zwei unterschiedliche Behörden verständigt.

Abbildung 12: Gründe, warum nach einem Spionagevorfall keine Behörde verständigt wurde



n = 59, Mehrfachnennungen möglich

Hier zeigt sich deutlich, dass nicht die immer wieder kolportierte Angst vor Reputationsverlust entscheidend ist, keine Behörde zu verständigen. Stattdessen stellen die geringe Erwartungshaltung bezüglich der (straf-) rechtlichen Verfolgung sowie die mangelnde Beweislage gegenüber dem Täter die wichtigsten Gründe dar, warum keine Behörde kontaktiert wird. Offenbar nehmen die betroffenen Unternehmen den Behördenkontakt als wenig zielführend wahr, da die aktuellen rechtlichen Rahmenbedingungen in manchen Fällen unzureichende Möglichkeiten bieten.

Je öfter ein Unternehmen von Spionage betroffen ist, desto eher wird keine Behörde mehr verständigt. Bereits ab dem zweiten Vorfall sinkt die Bereitschaft der betroffenen Unternehmen, eine Behörde zu verständigen, deutlich. Dies kann mit den Angaben hinsichtlich der generell geringen Erwartungshaltung gegenüber einer Verurteilung und der mangelnden Beweislage gegenüber dem Täter begründet werden.

Meist werden nach wenigen Vorfällen organisatorische Maßnahmen gesetzt, bei wiederholten Angriffen steigt die Bereitschaft zur Umsetzung technischer Maßnahmen.

5 In der Praxis werden Anzeigen von der Polizeidienststelle, die oft den ersten Kontaktpunkt für die Unternehmen darstellt, entsprechend der Zuständigkeit an das BVT weitergeleitet.

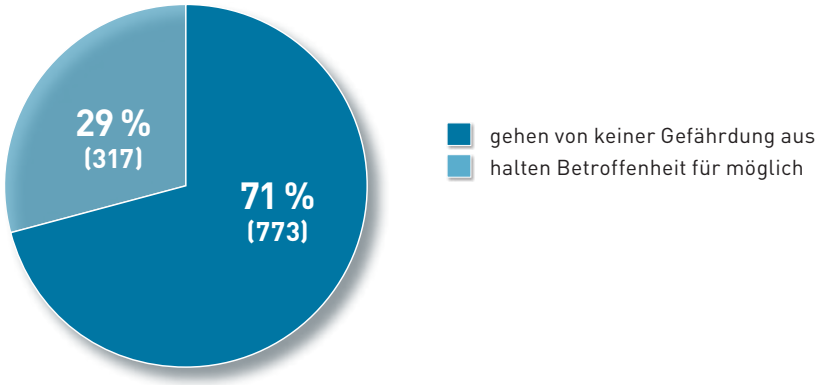
6 Genannt wurden Wirtschaftskammer, Rechtsanwalt, Telekommunikationsbehörde; das Abwehramt des Österreichischen Bundesheeres wurde von keinem betroffenen Unternehmen genannt.

RISIKOEINSCHÄTZUNG VON NICHT BETROFFENEN UNTERNEHMEN

Sehr unterschiedliche Erwartung der künftigen Betroffenheit

Von den 1.090 nicht betroffenen Unternehmen in der Umfrage sind fast drei Viertel (773) der Meinung, dass sie in den kommenden fünf Jahren weiterhin nicht von Spionage betroffen sein werden.

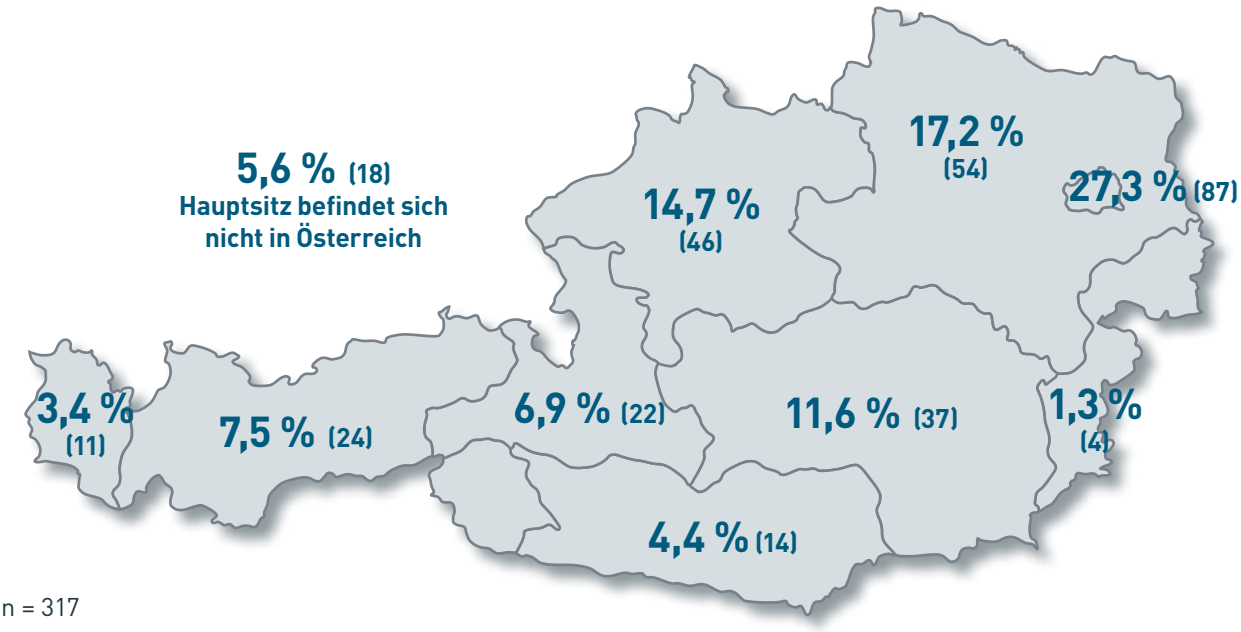
Abbildung 13: Einschätzung der Betroffenheit in den kommenden fünf Jahren



n = 1090

Die restlichen 317 Unternehmen (29 %) gehen von einem diesbezüglichen Risiko aus, von diesen wiederum rechnen knapp die Hälfte mit einem Spionagevorfall im Unternehmen, mehr als ein Drittel der Unternehmen denken, dass sie fünfmal oder öfter betroffen sein werden.

Abbildung 14: Risikoeinschätzung (Betroffenheit in den nächsten fünf Jahren) nach Bundesland



n = 317

Bedrohungspotenzial: 60 % der bisher nicht betroffenen Unternehmen vermuten, dass das größte Bedrohungspotenzial vom Mitbewerb ausgeht, rund 13 % nennen die eigenen Mitarbeiter, nahezu 8 % Nachrichtendienste, gefolgt von Kunden, Lieferanten und sonstigen Personen (insbesondere IT/Hacker, ehemalige Mitarbeiter, Terrorismus, Lieferanten).

Immerhin 5,5 % (60 Nennungen) meinten, es gebe überhaupt kein Bedrohungspotenzial.

Möglicher Ausgangspunkt eher im In- oder Ausland? Zwei Drittel der bisher nicht betroffenen Unternehmen würden einen Spionageangriff eher aus dem Inland, ein Drittel dagegen eher aus dem Ausland erwarten.[7]

Erwartete Tathandlungen: Von den 1.090 nicht betroffenen Unternehmen sind jeweils mehr als 20 % der Meinung, dass sie am ehesten von einem Hackerangriff auf IT oder sonstige Geräte oder durch den Informationsfluss (Kunden/Lieferanten) betroffen sein könnten. Jeweils rund 15 % vermuten, dass durch Informationsweitergabe der eigenen Mitarbeiter, Abhören oder Abfragen der Kommunikation und durch Diebstahl von Informationsmedien ihr Unternehmen betroffen sein würde. Nahezu 12 % schätzen, von Social-Engineering-Attacken betroffen sein zu können.

Geschätztes Schadensausmaß

Finanzieller Schaden: Knapp 60 % der befragten nicht betroffenen Unternehmen sind der Meinung, dass bei einem möglichen Spionageangriff in ihrem Unternehmen kein finanzieller Schaden entstehen würde; dagegen würden mehr als 40 % einen finanziellen Schaden erwarten.

Von jenen Unternehmen, die einen finanziellen Schaden durch einen möglichen Spionageangriff erwarten, beziffern rund zwei Drittel diesen auf bis zu 100.000 Euro, rund 16 % bis zu 500.000 Euro, etwa 7 % bis zu 1.000.000 Euro, 8 % bis zu 5.000.000 Euro und jeweils rund 2 % bis zu oder über 10.000.000 Euro.

Unternehmenskritischer Schaden: Von den 1.090 nicht betroffenen Unternehmen sind 763 (70 %) der Meinung, dass sie durch einen Spionagevorfall von mindestens einem unternehmenskritischen Schaden betroffen sein würden. Sie erwarten vor allem den Verlust von Kunden und Aufträgen sowie Reputationsschäden. Die Kündigung von Mitarbeitern und sonstige Schäden, wie Vertrauensmissbrauch und andere zwischenmenschliche Konflikte, werden dagegen kaum genannt.

Mögliche Verständigung von Behörden

Auf die Frage an die bisher nicht betroffenen Unternehmen, ob sie im Falle eines Spionageangriffs eine Behörde verständigen würden, antworteten drei Viertel mit „eher ja". Von diesen würden die meisten die nächste Polizeidienststelle bzw. das Landes- oder Bundeskriminalamt informieren. Weniger Unternehmen würden die Staatsanwaltschaft einschalten, das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung oder das Abwehramt des Österreichischen Bundesheeres sowie sonstige Stellen, wie beispielsweise die Wirtschafts- oder Arbeiterkammer, das Gesundheitsministerium, die Finanzmarktaufsicht oder Rechtsanwälte.

Von den Unternehmen, die im Falle eines Spionageangriffs keine Behörden verständigen würden, gaben knapp 40 % als Grund an, dass sie voraussichtlich über nicht genügend Beweise gegenüber möglichen Tätern verfügen. Etwa ein Drittel hat eine geringe Erwartungshaltung gegenüber einer Verurteilung. Diese Einschätzungen treffen sich grundsätzlich mit den Angaben der Unternehmen, die tatsächlich von Spionagevorfällen betroffen waren (siehe Seite 23).

Des Weiteren wurden „fehlendes Vertrauen zu den Strafverfolgungsbehörden", die Unklarheit darüber, ob Spionagefälle strafrechtlich verfolgt werden, und die Angst vor einem möglichen Reputationsverlust genannt. In zwei Fällen gaben Unternehmen an, keine passende Behörde für die Meldung von Spionagefällen zu kennen.

7 Insgesamt gingen auf diese Frage 678 Antworten ein.

PRÄVENTIONSMASSNAHMEN

Behördenkenntnis und Kooperation

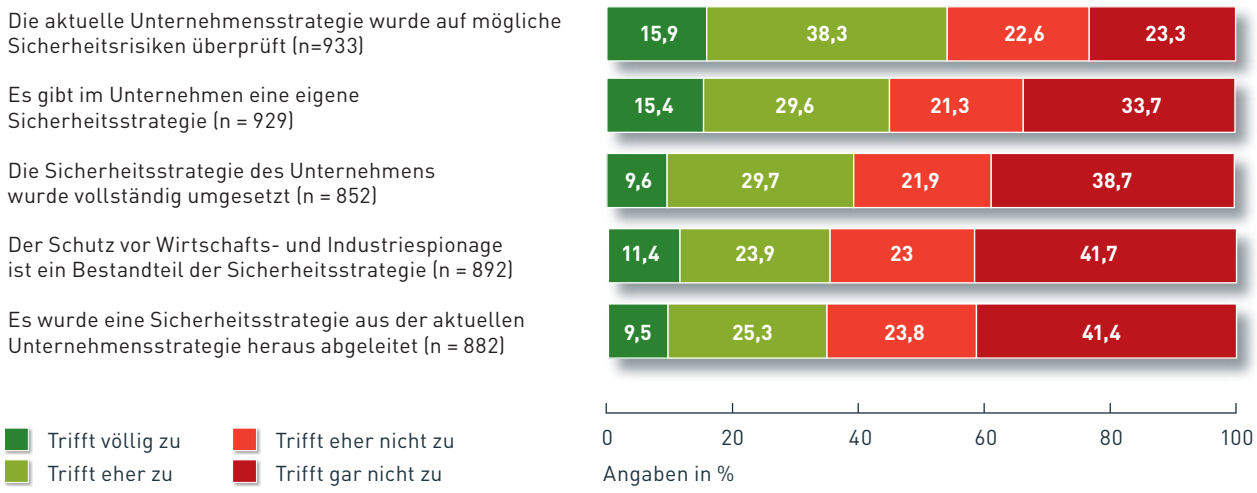
Derzeit unterhalten nach Angaben der befragten Unternehmen nur 4 % eine Kooperation bzw. stehen in Kontakt mit Behörden, die für Wirtschafts- und Industriespionage zuständig sind (36 Nennungen). Von diesen zeigen sich nahezu alle mit der Zusammenarbeit zufrieden. Die restlichen 96 % der befragten Unternehmen haben dagegen keine Kooperation oder laufenden Kontakt zu Behörden.[8]

Neun von zehn Unternehmen gaben an, dass sie keine Behörden kennen, die proaktive Unterstützungsmöglichkeiten zum Schutz vor Wirtschafts- und Industriespionage anbieten.

Unternehmens- und Sicherheitsstrategie

Nach den Eigenangaben der befragten Unternehmen bestehen im Bereich der Verknüpfung von Unternehmens- und Sicherheitsstrategie noch Möglichkeiten zur Weiterentwicklung. Ein deutlicher Anteil von Unternehmen antwortete in diesem Bereich nicht, was darauf schließen lässt, dass in diesen Unternehmen keine Strategie vorhanden ist. Dies legt eine mögliche Verwundbarkeit der Unternehmen für künftige Spionageangriffe offen. Als einzige Teilfrage wurde überwiegend positiv beantwortet, dass die aktuelle Unternehmensstrategie auf Sicherheitsrisiken überprüft wurde.

Abbildung 15: Unternehmens- und Sicherheitsstrategie

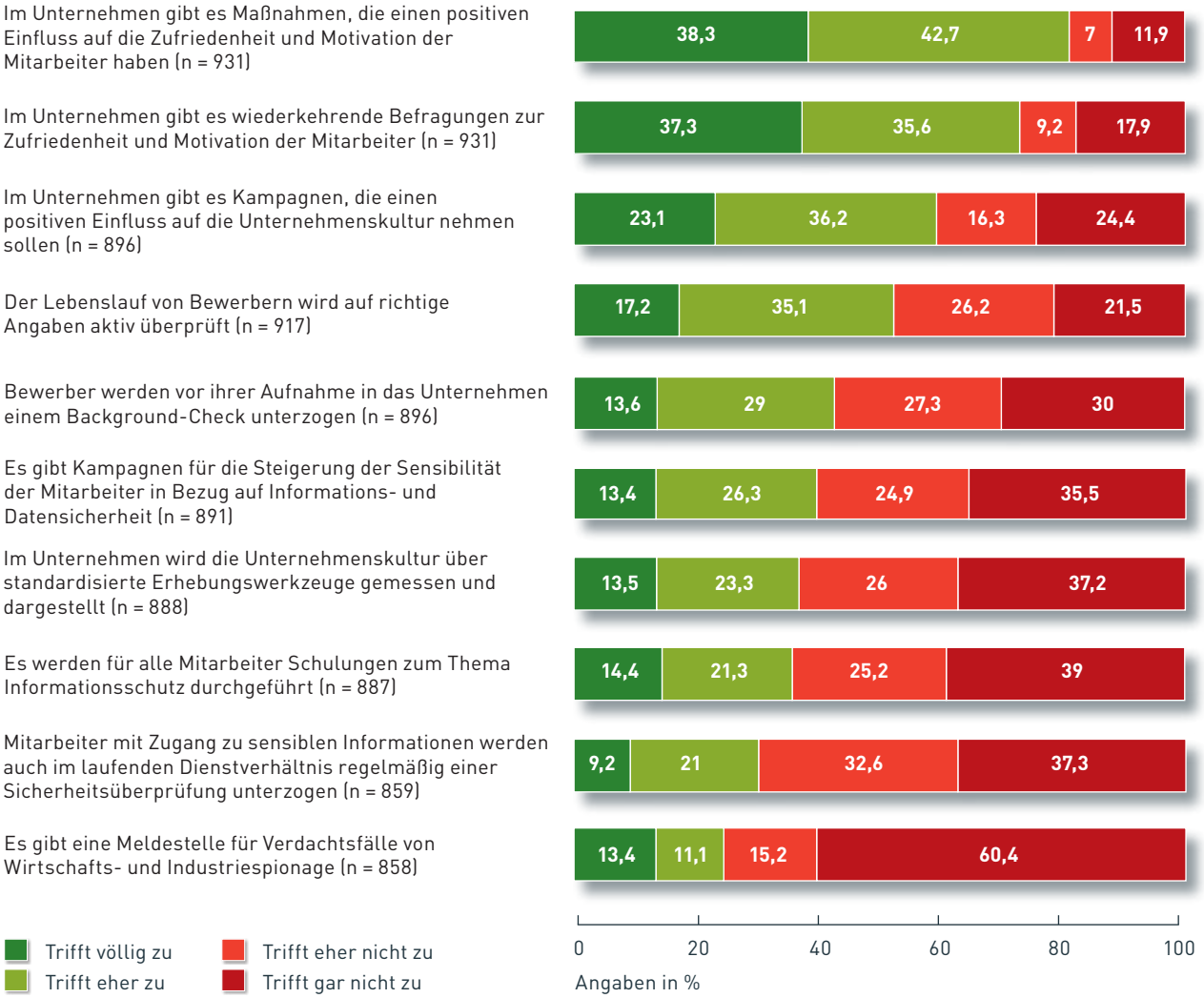


Aktivitäten in den Unternehmen

Möglichst hohe Sicherheit im Unternehmen kann nur mit den Beschäftigten gemeinsam verwirklicht werden. Zahlreiche Maßnahmen, die in Unternehmen heute bereits umgesetzt werden, sind sicherheitsrelevant. Dies bezieht sich auf die Unternehmenskultur generell, Zufriedenheit und Motivation, Kampagnen und Schulungen, die Aufnahme und Überprüfung von neuen Mitarbeitern bis hin zur Einrichtung geeigneter Meldestellen für Wirtschafts- und Industriespionage. In der folgenden Übersicht sind einige Maßnahmen und ihre Umsetzung dargestellt.

8 n = 1.015; 134 Unternehmen gaben hier keine Antwort.

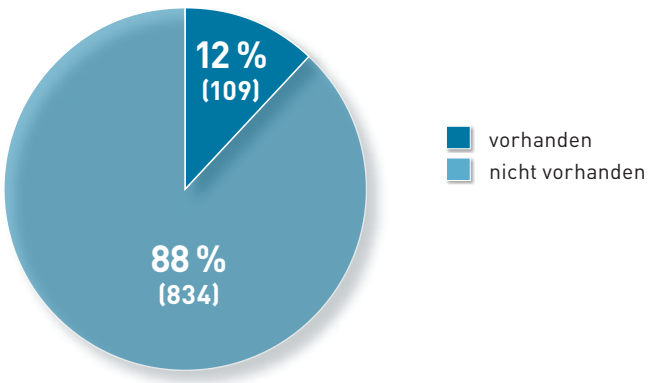
Abbildung 16: Personalmanagement – Maßnahmen



Verantwortliche für Wirtschafts- und Industriespionage

Bei fast 90 % der befragten Unternehmen gibt es keine verantwortliche Person für Wirtschafts- und Industriespionage; rund 12 % der Unternehmen verfügen über eine eigene zuständige Person.

Abbildung 17: Verantwortliche in Unternehmen



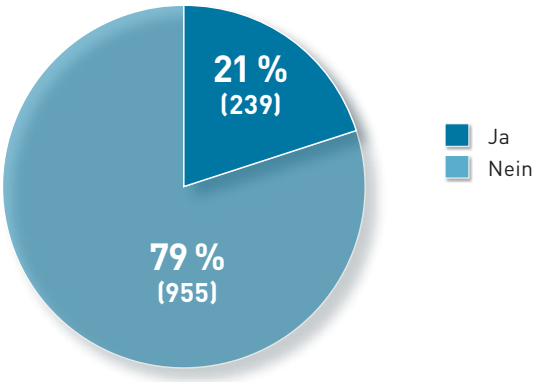
n = 943; keine Angabe: 206 Unternehmen

Bei diesen wiederum zeigt sich ein deutlicher Unterschied nach Unternehmensgröße: Rund ein Viertel aller Großunternehmen hat eine eigene verantwortliche Person für Wirtschafts- und Industriespionage. Nur rund ein Achtel der mittleren Unternehmen beschäftigt eigene Verantwortliche oder Beauftragte dafür, und weniger als ein Zehntel der Klein- und Kleinstunternehmen.

Eingesetzte Systeme und Zertifizierungsmodelle

Für das Management von Risiken und sicherheitsrelevanten Fragen ist eine Reihe von Systemen verbreitet. Wichtige Gründe dafür sind beispielsweise Anforderungen von Kunden, die Steigerung der Wettbewerbsfähigkeit oder die bessere Steuerbarkeit des Unternehmens. Von den befragten Unternehmen setzt etwa jedes fünfte Systeme oder Zertifizierungsmodelle ein.

Abbildung 18: Einsatz von Systemen bzw. Zertifizierungsmodellen



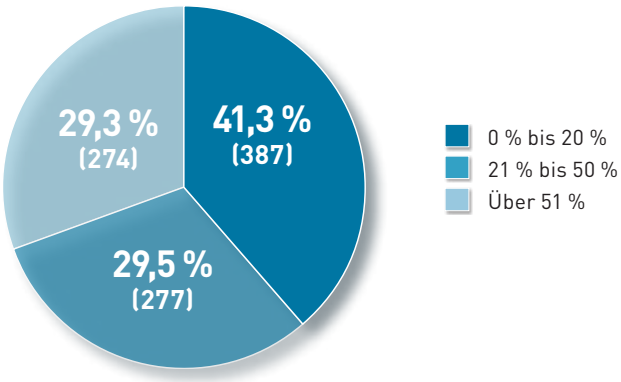
n = 938; keine Angabe: 211

Von jenen Unternehmen, die Systeme bzw. Zertifizierungsmodelle einsetzen, sind in ca. einem Fünftel der Fälle die ISO 31000 Risikomanagement, etwas weniger die 27001 Informationssicherheitssysteme sowie der IT-Grundschutz des deutschen BSI verbreitet. Außerdem verwendet werden die ONR 49000 Risikomanagement, die IT Infrastructure Library, COSO ERM – Enterprise Risk Management und die ISO 9001 sowie weitere Systeme.

Streng vertrauliche Geschäftsgeheimnisse und Informationsschutz

Nahezu 30 % der befragten Unternehmen vertreten die Ansicht, dass 21 bis 50 % ihrer Informationen streng vertrauliche Geschäftsgeheimnisse sind; ebenso viele nehmen an, dass über 51 % der Informationen als streng vertraulich gelten.

Abbildung 19: Einschätzung zum Anteil von streng vertraulichen Geschäftsgeheimnissen an den gesamten Informationen im Unternehmen



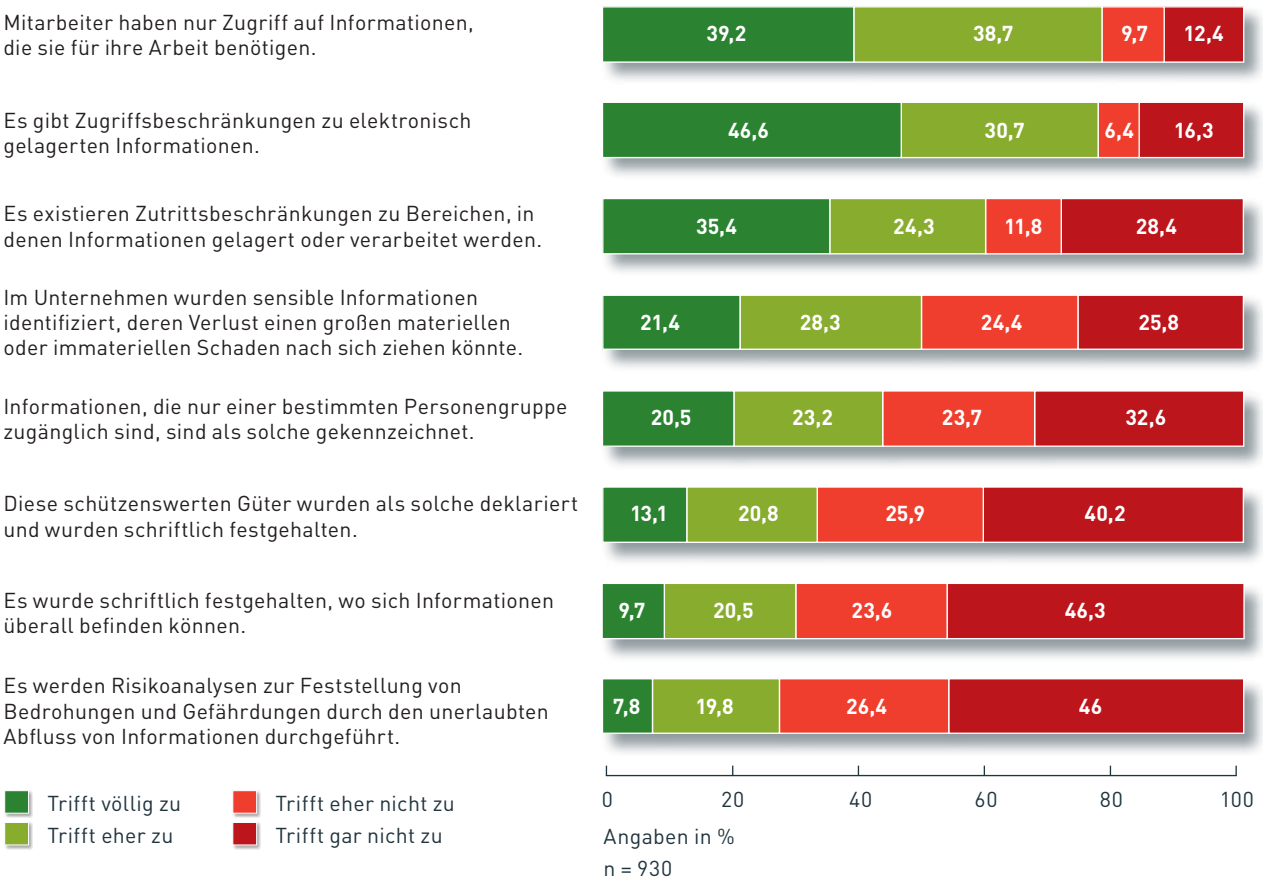
n = 938

In der Praxis ist meist ein viel geringerer Anteil wirklich als Geschäfts- oder Betriebsgeheimnis anzusehen, der entsprechend geschützt werden kann, denn folgende Fragen drängen sich auf: Wie könnte etwa bei einem Anteil von 50 % Geschäftsgeheimnissen ein „Need-to-know"-Prinzip organisiert und aufrechterhalten werden? Oder wie ließe sich beispielsweise der Schutz vor unerlaubtem Zugriff (physisch oder technisch) wirksam umsetzen?

Mangelhafter Informationsschutz?

Die Unternehmen wurden gefragt, inwiefern sie ihre Daten schützen, Zutritte für Mitarbeiter freigeben oder wie sie die Identifizierung von sensiblen Daten im Unternehmen vornehmen. So werden in mehr als drei Viertel der Unternehmen die Zugriffe auf Informationen nach dem „Need-to-know"-Prinzip beschränkt bzw. existieren Zugriffsbeschränkungen auf elektronische Daten. In etwa 60 % der Unternehmen existieren bauliche Zutrittsbeschränkungen, und in ca. der Hälfte der Unternehmen wurden sensible Daten identifiziert, deren Verlust zu einem großen Schaden für das Unternehmen führen könnte.

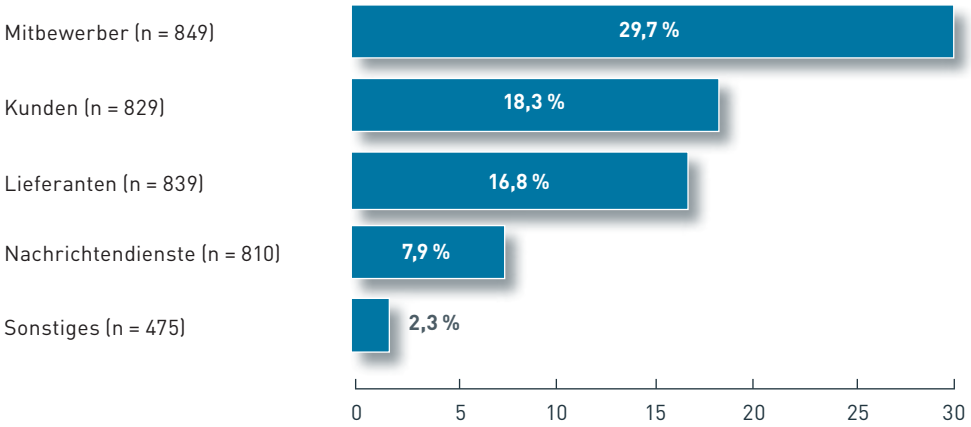
Abbildung 20: Informationsschutz und Zugriffsbeschränkungen in den Unternehmen



Analyse externer Gefahrenquellen

Wesentlich geringer ist der Anteil der Unternehmen, die sich mit ihrer Außenwelt in Bezug auf Wirtschafts- und Industriespionage auseinandersetzen: Nahezu 30 % der befragten Unternehmen analysieren Mitbewerber, knapp 20 % analysieren Kunden, mehr als 15 % Lieferanten und weniger als 10 % Nachrichtendienste. Etwas mehr als zwei Prozent der Unternehmen gaben an, einzelne weitere Gefahrenquellen zu analysieren, wie den IT-Bereich (Hacker, Viren und Netzwerke), ehemalige und aktuelle Mitarbeiter.

Abbildung 21: Analyse von externen Gefahrenquellen



Durchwegs über alle Unternehmensgrößen hinweg wird vor allem der Mitbewerb analysiert. In Großunternehmen ab 1.000 Mitarbeiter werden zusätzlich verstärkt Lieferanten, Kunden, Nachrichtendienste und sonstige Gefahrenquellen analysiert.

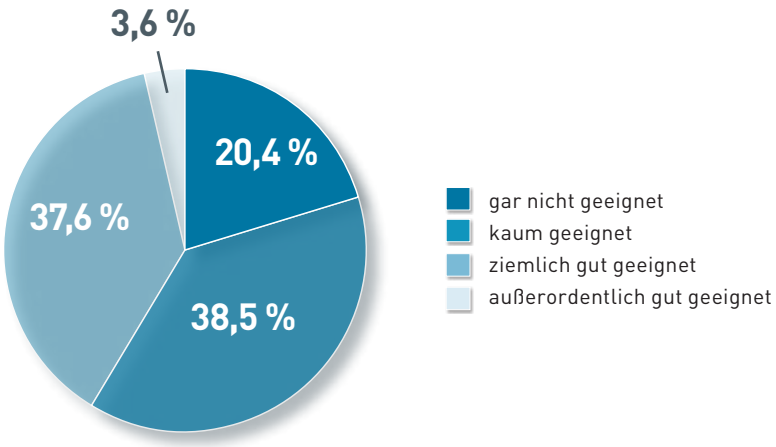
Bereits betroffene Unternehmen beobachten Umwelt aufmerksamer

Bei jenen 59 Unternehmen, die bereits von Spionageangriffen betroffen waren, ist die Analyse externer Gefahrenquellen deutlich stärker ausgeprägt: Sie analysieren jeweils zu rund 48 % ihre Kunden sowie Mitbewerber. Lieferanten und sonstige Gefahrenquellen (IT-Bereich, aktuelle/ehemalige Mitarbeiter) werden jeweils in etwa rund einem Drittel der Unternehmen analysiert, und Nachrichtendienste zu rund 18 %. Durchschnittlich analysieren die betroffenen Unternehmen ein bis zwei externe Gefahrenquellen.

Qualität der umgesetzten Sicherheitsmaßnahmen oft kritisch

In der Beurteilung der bisherigen Bemühungen sind die Unternehmen sehr selbstkritisch. Im Alltag ist der Schutz vor Wirtschafts- und Industriespionage weiterhin meist ein Stiefkind. Knapp 60 % der 1.149 befragten Unternehmen sind der Meinung, dass die umgesetzten Sicherheitsmaßnahmen im eigenen Unternehmen gar nicht oder kaum geeignet sind.

Abbildung 22: Einschätzung der Eignung der getroffenen Maßnahmen



Bezüglich der Größe der Unternehmen zeigten sich hier deutliche Unterschiede: In Kleinst-, Klein- und mittleren Unternehmen sind die Sicherheitsmaßnahmen (laut Eigenangaben) zu mehr als 60 % gar nicht oder kaum geeignet. In größeren Unternehmen (ab 250 Mitarbeitern) dagegen werden die Sicherheitsmaßnahmen zu fast 70 % als „ziemlich“ oder „außerordentlich gut geeignet“ beurteilt.

Differenzierung nach Branchen

Es zeigt sich, dass spezielle branchenbezogene Regulierungen, die Anforderungen von Kunden, frühere Betroffenheit und hohe öffentliche Aufmerksamkeit starke Treiber für die Einführung von Schutzmaßnahmen sein können. Damit einher geht ein höheres Bewusstsein der Mitarbeiter. In fünf Branchen werden die getroffenen Sicherheitsmaßnahmen überwiegend als ziemlich bzw. außerordentlich gut geeignet eingeschätzt: „Finanz- und Versicherungsdienstleistungen“ (zwei Drittel), „Gesundheits- und Sozialwesen“, „Energieversorgung“, „Freiberufliche, wissenschaftliche und technische Dienstleistungen“ (jeweils nahezu etwa 60 %), „Information und Kommunikation“ (etwas mehr als die Hälfte). In den anderen Branchen werden die Sicherheitsmaßnahmen als weniger gut geeignet eingeschätzt.

ERWARTUNGEN DER UNTERNEHMEN

Bevorzugte Informationsquellen

Interessenvertretungen haben in den vergangenen Jahren auf den Bedarf mit Informations- und Beratungsangeboten reagiert, ebenfalls in Kooperation mit Behörden. 80 % der befragten Unternehmen (915) wünschen sich, weitere Informationen über Gefahren durch Wirtschafts- und Industriespionage und mögliche Schutzmaßnahmen von Behörden zu erhalten. Von den folgenden Institutionen wird erwartet, dass sie diese Bereiche abdecken: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, Bundesministerium für Inneres, Industriellenvereinigung, Wirtschaftskammer Österreich, Landespolizeidirektion, Bundes- bzw. Landeskriminalamt sowie Staatsanwaltschaft.

Als Informationsmittel wünschen sich jeweils ca. 40 % Online-Informationsplattformen und Broschüren, außerdem werden Branchenveranstaltungen von mehr als 25 % und die persönliche Beratung von mehr als 18 % genannt. Informationen bei Messen und Kongressen rangieren mit 6 % am Ende der Skala. Kleinst- und Kleinunternehmen wünschen sich am ehesten Informationen via Broschüren oder Online-Informationsplattformen. Mittlere Unternehmen nennen vor allem Broschüren, Branchenveranstaltungen oder Online-Informationsplattformen, größere Unternehmen ebenso, zusätzlich erwarten diese verstärkt persönliche Beratung.

Wunsch nach weiterer Forschung

Auf die Frage, wo die Unternehmen aus ihrer Sicht einen weiteren Forschungsbedarf im Bereich Wirtschafts- und Industriespionage[9] sehen, wurden hauptsächlich zwei unterschiedliche Dimensionen erwähnt: Technologie und organisatorischer Bereich.

Die Aussagen, gereiht nach den meisten Nennungen, sind:

Organisation

- Information der Mitarbeiter
- Psychologische Schulungen für Mitarbeiter/Beschäftigte, die unter Stress stehen
- Urheberrechtsschutz/Patentschutzrechte
- Buchhaltung und Bilanzbuchhaltung
- Bessere Zusammenarbeit zwischen Justiz und Unternehmen

Technologie

- Verhinderung/Abwehr von Hackerangriffen (inkl. Trojaner, Spam-Mails und Phishing)
- IT-Verschlüsselungsmaßnahmen/Schutzmöglichkeiten (insbesondere im Ausland)
- Datenspeicherung
- IT-Richtlinien
- Frühwarnsysteme
- Eigenes europäisches Betriebssystem

9 Vgl. hierzu das Arbeitsprogramm der österreichischen Bundesregierung, Kapitel 06 Sicherheit und Rechtsstaat (S. 79–81).

AUSBLICK: STÄRKERE VERNETZUNG GEFRAGT

Wie die Ergebnisse dieser Studie zeigen, ist das Thema sehr vielschichtig und umfasst Unternehmenskultur, Organisation und Führung sowie Technologie. Unternehmerisches Handeln trifft auf staatliche Unterstützung, die – aus verschiedenen Gründen – oft noch nicht ausreichend angenommen wird. Aufgrund des höheren Bewusstseins durch die öffentliche Diskussion des Themas und der teilweise konkreten Betroffenheit ist für die Zukunft mehr Vorbeugung in den Unternehmen und eine stärkere Zusammenarbeit mit Behörden und öffentlichen Stellen zu erwarten. Dazu werden eine stärkere Vernetzung der Unternehmen untereinander und die Vernetzung mit den Sicherheitsbehörden auf speziellen Plattformen beitragen.

Weiter heruntergebrochen bedarf es zudem einer intensiven Zusammenarbeit von Unternehmen im B2B-Bereich. Denn hoch spezialisierte Dienstleistungsunternehmen, in denen viel (technisches) Know-how ihrer Kunden liegt, und die etwa in Forschungs- und Entwicklungsprojekte großer Unternehmen eingebunden sind, können vermehrt ins Zentrum von Wirtschafts- und Industriespionageaktivitäten rücken. Die Verständigung auf einheitliche Vorgehensweisen im Rahmen von Kooperationen und der Austausch über aktuelle Vorgehensweisen von Akteuren der Wirtschafts- und Industriespionage innerhalb der Wirtschaft können den Schutz des einzelnen Unternehmens wesentlich erhöhen.

Geistiges Eigentum und menschliche Intelligenz sind der Innovationsmotor. Für die nächsten Jahre ist eine noch stärkere Digitalisierung, Automatisierung und Vernetzung der Unternehmen zu erwarten. Damit verbunden steigt die Abhängigkeit der Unternehmen von entsprechendem Know-how zur Aufrechterhaltung ihrer Wettbewerbsfähigkeit und somit die mögliche Bedrohung durch Wirtschafts- und Industriespionage. Die Entwicklung hin zur „Industrie 4.0“ ist ebenfalls in diesem Zusammenhang zu sehen.

Die geplante EU-Richtlinie bezüglich eines einheitlichen Begriffsverständnisses von Geschäftsgeheimnissen wird dazu beitragen, den Schutz der immateriellen Vermögenswerte der in der EU (als übergeordneter Wirtschaftsstandort) ansässigen Unternehmen zu stärken. Dies ist eine Grundlage für soziale Sicherheit.

BEZEICHNUNGEN DER BRANCHEN NACH ÖNACE 2008

Land- und Forstwirtschaft, Fischerei

Bergbau und Gewinnung von Steinen und Erden

Herstellung von Waren

Energieversorgung

Wasserversorgung, Abwasser- und Abfallentsorgung und

Beseitigung von Umweltverschmutzungen

Bau

INDUSTRIE

Handel, Instandhaltung und Reparatur von Fahrzeugen

Verkehr und Lagerei

Beherbergung und Gastronomie

Information und Kommunikation

Erbringung von Finanz- und Versicherungsdienstleistungen

Grundstücks- und Wohnungswesen

Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen

Erbringung von sonstigen wirtschaftlichen Dienstleistungen

Erziehung und Unterricht

Gesundheits- und Sozialwesen

Kunst, Unterhaltung und Erholung

Erbringung von sonstigen Dienstleistungen

LITERATURVERZEICHNIS

Verfassungsschutzbericht 2014
www.bmi.gv.at/cms/bmi_verfassungsschutz

Sicherheitsbericht 2014
www.bmi.gv.at/cms/bmi_service

Arbeitsprogramm der Österreichischen Bundesregierung
www.bundeskanzleramt.at/site/3354/default.aspx

Handbuch WIS
www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis

Struktur ÖNACE 2008:
http://wko.at/statistik/oenace/oenace2008.pdf

Definition von kleinen und mittleren Unternehmen;
Empfehlung der EU-Kommission 2003/361/EG, zusammengefasst in:
https://www.wko.at/Content.Node/Interessenvertretung/ZahlenDatenFakten/KMU_Definition.html

Diese Broschüre – sowie sonstige aktuelle Publikationen –
ist in der Service-GmbH der Wirtschaftskammer Österreich erhältlich:
Telefon: 0590 900-5050 oder
Fax: 0590 900-236 sowie
E-Mail: mservice@wko.at
Internet: http://webshop.wko.at

Online abrufbar unter:
http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES
iv INDUSTRIELLEN VEREINIGUNG
FH CAMPUS WIEN UNIVERSITY OF APPLIED SCIENCES
WKO WIRTSCHAFTSKAMMER ÖSTERREICH