INSTITUT FÜR ARBEITSMARKT- UND BERUFSFORSCHUNG
Die Forschungseinrichtung der Bundesagentur für Arbeit

IAB-KURZBERICHT

Aktuelle Analysen aus dem Institut für Arbeitsmarkt- und Berufsforschung

2|2025

In aller Kürze

- Industrie- und Wirtschaftsspionage sind nicht zu vernachlässigende Probleme, die zu wirtschaftlichen Belastungen führen können – nicht nur für die betroffenen Betriebe, sondern auch für die Gesamtwirtschaft.
- Neue Befragungsdaten des IAB zeigen, dass in den vergangenen fünf Jahren 9 Prozent aller Betriebe in Deutschland Opfer eines Spionageangriffs wurden. Rund 12 Prozent aller Betriebe berichten über mindestens einen Verdachtsfall oder Angriff auf ihren Betrieb (vgl. Abbildung A1).
- Gut die Hälfte aller berichteten Verdachtsfälle sind Hackerangriffe auf die IT-Systeme, bei den tatsächlichen Angriffen beträgt dieser Anteil sogar fast zwei Drittel.
- In über einem Fünftel der Betriebe, die Angriffen ausgesetzt waren, wurden Daten gestohlen.
- Sowohl Verdachtsfälle als auch Spionageangriffe kommen besonders häufig in den Wirtschaftszweigen Information und Kommunikation sowie im Großhandel vor.
- Innovative und exportierende Betriebe in kompetitiven Märkten sind besonders oft von Wirtschafts- oder Industriespionage betroffen.

Befragung zu Industrie- und Wirtschaftsspionage in Deutschland

Neun Prozent der Betriebe werden ausgespäht

von Albrecht Glitz, Susanne Kohaut und Iris Möller

Industrie- und Wirtschaftsspionage, also das Ausspähen von Betriebsinformationen durch andere Unternehmen oder durch Nachrichtendienste, sind Phänomene, die Betriebe als wachsende Bedrohung sehen. Nun liegen hierzu erstmals repräsentative Befragungsdaten aus dem IAB-Betriebspanel 2023 für Deutschland vor. Sie zeigen, dass rund 12 Prozent der Betriebe über alle Wirtschaftszweige und Größenklassen hinweg angeben, von Industrie- oder Wirtschaftsspionage betroffen zu sein.

Industrie- und Wirtschaftsspionage (vgl. Infobox 1) sind keine neuen Phänomene, sondern lassen sich schon im Altertum und Mittelalter episodisch nachweisen (Norwich 1990; Ben-Atar 2004). Auch heute wird davon ausgegangen, dass Industrie- und Wirtschaftsspionage in vielen Industrie- und Schwellenländern weit verbreitet sind, und dass wir derzeit eine Intensivierung dieser Aktivitäten erleben. So schätzt eine Mehrheit der Unternehmen in Deutschland die von Industriespionage (im weitesten Sinne) ausgehende Bedrohung als groß bis sehr groß ein und

A1

Industrie- oder Wirtschaftsspionage betreffen etwa jeden zehnten Betrieb

Angaben der Betriebe, Anteile in Prozent

Quelle: IAB-Betriebspanel 2023. © IAB

1

Definition

Die Bezeichnungen Wirtschaftsspionage und Industriespionage werden im allgemeinen Sprachgebrauch oft synonym verwendet, beschreiben aber verschiedene Phänomene: Während sich „Industriespionage" auf Aktivitäten einzelner Unternehmen gegen ihre Wettbewerber zu kommerziellen Zwecken bezieht, versteht man unter „Wirtschaftsspionage" solche Aktivitäten, die im wirtschaftlichen Bereich im Auftrag eines ausländischen Nachrichtendienstes und aus nicht ausschließlich kommerziellen Gründen betrieben werden (Nasheri 2005).

rechnet mit einem zukünftig weiteren Anstieg dieser Bedrohung (Bitkom 2023).

Schätzungen zufolge beziffern sich die durch Spionage im weitesten Sinne erwachsenen wirtschaftlichen Schäden pro Jahr in den USA auf rund 400 Milliarden Dollar (IP Commission 2017), das sind etwa 2,1 Prozent des Bruttoinlandsprodukts, und in Deutschland auf rund 200 Milliarden Euro (Bitkom 2023), was etwa 4,8 Prozent des Bruttoinlandsprodukts entspricht. Allerdings variieren diese Schätzungen aufgrund der unsicheren Datenlage und der grundsätzlichen Schwierigkeit der Quantifizierung möglicher Schäden je nach Studie stark (Kasper 2015).

Vor allem China und Russland wird systematische Wirtschaftsspionage in großem Umfang vorgeworfen (IP Commission 2021; Verfassungsschutz 2024). Jedoch ist anzunehmen, dass solche Aktivitäten auch zwischen befreundeten Ländern als Teil der allgemeinen nachrichtendienstlichen Aufklärung stattfinden. Das lassen beispielsweise die WikiLeaks-Enthüllungen im Jahr 2013 über die Überwachungsaktivitäten der National Security Agency (NSA), dem größten Auslandsgeheimdienst der Vereinigten Staaten, in Frankreich, Deutschland und Japan vermuten (Corporate Trust 2017a).

Von besonderem Interesse im Bereich der Wirtschaftsspionage durch ausländische Nachrichtendienste ist traditionell jede Art von Militär- und Verteidigungstechnologie. Jedoch werden häufig auch andere Bereiche wie die Luft- und Raumfahrt, Hochtechnologie-Elektronik, Telekommunikation, Nanotechnologie, Biotechnologie, Energie oder Finanzdienstleistungen ausgespäht (Corporate Trust 2017a). Diese Bereiche sind vermutlich auch in besonderem Maße das Ziel von Industriespionage durch Wettbewerber, da es sich um technologie- und innovationsintensive Sektoren handelt, in denen Betriebs- und Geschäftsgeheimnisse eine wichtige Rolle spielen.

Trotz der ökonomischen Bedeutung der Industrie- und Wirtschaftsspionage ist es schwierig, sich ein genaues Bild dieser Phänomene zu verschaffen, da hierzu kaum verlässliche Daten vorliegen. Zum einen werden viele Spionageangriffe – sei es von Wettbewerbern oder ausländischen Nachrichtendiensten – von den betroffenen Unternehmen und Institutionen nicht bemerkt. Zum anderen werden viele der Angriffe, die bemerkt werden, nicht öffentlich gemacht, da dadurch wirtschaftliche Nachteile – insbesondere eine Rufschädigung gegenüber Investoren, Kunden und Mitarbeitenden – befürchtet werden (Office of the National Counterintelligence Executive 2011).

Die empirischen Daten, die für Deutschland bislang vorliegen, stammen zum großen Teil von Studien privater Beratungs- und Sicherheitsfirmen wie Ernst & Young, KPMG, PricewaterhouseCoopers und Corporate Trust. Ein großes Problem

2

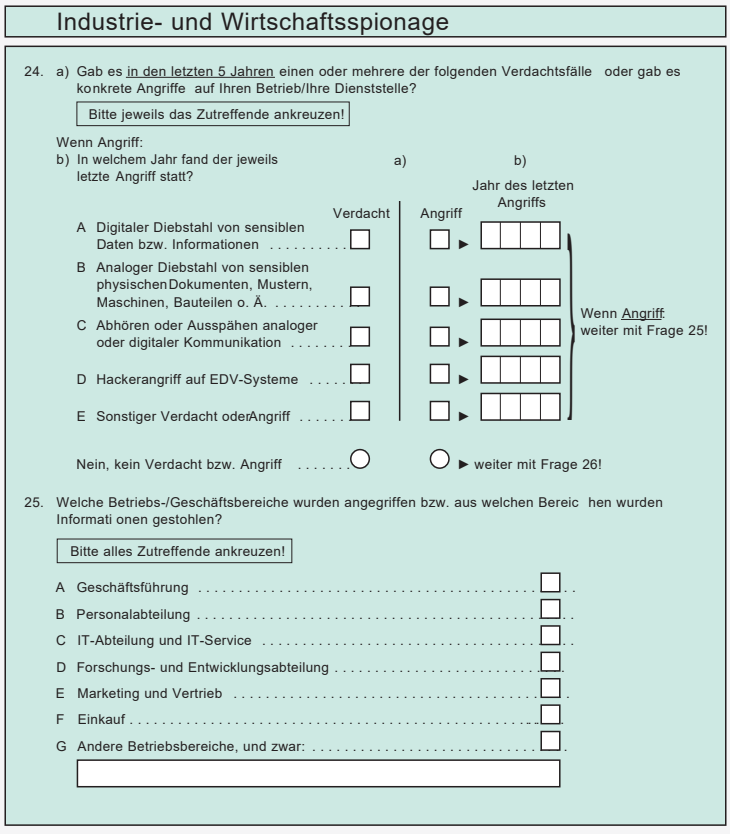
Das IAB-Betriebspanel

ist eine repräsentative Arbeitgeberbefragung zu betrieblichen Bestimmungsgrößen der Wirtschaft. Jährlich werden rund 15.000 Betriebe aller Betriebsgrößen und Wirtschaftszweige befragt. Grundgesamtheit sind Betriebe mit mindestens einem sozialversicherungspflichtig Beschäftigten. Die Befragung existiert seit 1993 in den westdeutschen und seit 1996 in den ostdeutschen Bundesländern und stellt als umfassender Längsschnittdatensatz die Grundlage für die Erforschung der Nachfrageseite des Arbeitsmarktes dar. Die Rücklaufquoten im Jahr 2023 lagen bei rund 70 Prozent der wiederholt befragten und bei rund 11 Prozent der erstbefragten Betriebe.

Mehr zum IAB-Betriebspanel findet sich bei Ellguth et al. (2014) oder auf der Internetseite des IAB (http://www.iab.de/de/erhebungen/iab-betriebspanel.aspx/).

Datenzugang zum IAB-Betriebspanel: https://fdz.iab.de/betriebsdaten/iab-betriebspanel-iab-bp-version-9321-v1/ (doi.org/10.5164/IAB.FDZD.2316.de.v1).

Konkrete Fragestellung zum Themenschwerpunkt „Industrie- und Wirtschaftsspionage“ im IAB-Betriebspanel 2023:


Industrie- und Wirtschaftsspionage

24. a) Gab es in den letzten 5 Jahren einen oder mehrere der folgenden Verdachtsfälle oder gab es konkrete Angriffe auf Ihren Betrieb/Ihre Dienststelle?

Bitte jeweils das Zutreffende ankreuzen!

Wenn Angriff:
b) In welchem Jahr fand der jeweils letzte Angriff statt?

	a) Verdacht	a) Angriff	b) Jahr des letzten Angriffs
A Digitaler Diebstahl von sensiblen Daten bzw. Informationen	☐	☐ ▶	☐☐☐☐
B Analoger Diebstahl von sensiblen physischen Dokumenten, Mustern, Maschinen, Bauteilen o. Ä.	☐	☐ ▶	☐☐☐☐
C Abhören oder Ausspähen analoger oder digitaler Kommunikation	☐	☐ ▶	☐☐☐☐
D Hackerangriff auf EDV-Systeme	☐	☐ ▶	☐☐☐☐
E Sonstiger Verdacht oder Angriff	☐	☐ ▶	☐☐☐☐

Wenn Angriff: weiter mit Frage 25!

Nein, kein Verdacht bzw. Angriff ○ ○ ▶ weiter mit Frage 26!

25. Welche Betriebs-/Geschäftsbereiche wurden angegriffen bzw. aus welchen Bereichen wurden Informationen gestohlen?

Bitte alles Zutreffende ankreuzen!

A Geschäftsführung ☐
B Personalabteilung ☐
C IT-Abteilung und IT-Service ☐
D Forschungs- und Entwicklungsabteilung ☐
E Marketing und Vertrieb ☐
F Einkauf ☐
G Andere Betriebsbereiche, und zwar: ☐

dieser Studien ist, wie in vielen anderen Ländern auch (European Commission 2018), deren oft geringer Umfang und unklare Repräsentativität. Meistens liegt die Zahl der erfolgreich befragten Unternehmen im mittleren dreistelligen Bereich, mit Rücklaufquoten von oft weniger als 10 Prozent (Kasper 2015). Auf einer solchen Datenbasis lassen sich nur schwer aussagekräftige Rückschlüsse über Gegenstand und Ausmaß von Industrie- und Wirtschaftsspionage ziehen.

Um diese Datenlage zu verbessern und neue Einblicke in den komplexen Themenbereich der Industrie- und Wirtschaftsspionage zu liefern, wurde im IAB-Betriebspanel 2023 ein entsprechendes Fragemodul eingefügt (vgl. Infobox 2). Das IAB-Betriebspanel erfasst Betriebe aller Größen und Wirtschaftszweige in Deutschland. Es werden also auch kleinere Betriebe befragt, was eine große Stärke im Vergleich zu bisherigen Befragungen darstellt.

9 Prozent aller Betriebe in Deutschland berichten von Spionageangriffen

Im IAB-Betriebspanel 2023 wurde danach gefragt, ob es in den vergangenen fünf Jahren Verdachtsfälle und/oder konkrete Spionageangriffe in den befragten Betrieben gab (vgl. Infobox 2). Insgesamt berichten 12 Prozent der befragten Verantwortlichen über einen oder mehrere Verdachtsfälle oder Angriffe auf ihren Betrieb oder ihre Dienststelle (vgl. Abbildung A1). In diesen Betrieben arbeiten rund 22 Prozent aller Beschäftigten.

Der Anteil der Spionageangriffe ist dabei mit 8,9 Prozent etwas höher als der Anteil der Verdachtsfälle mit 7,3 Prozent. Diese Zahlen liegen damit deutlich unter den Ergebnissen des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom), der seit 2015 regelmäßig Befragungen zum Thema Wirtschaftsschutz in Deutschland durchführt.

In der letzten Bitkom-Erhebung (Bitkom 2024) gaben 81 Prozent der befragten Industrieunternehmen an, in den letzten zwölf Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen gewesen zu sein. Ein Teil der beträchtlichen Diskrepanz ist sicherlich auf die breitere Fragestellung in der Bitkom-Studie zurückführen. Aber auch die Tatsache, dass diese lediglich Industrieunternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von einer Million Euro oder mehr umfasst (N=1.002), dürfte zu einem insgesamt höheren Anteil an betroffenen Unternehmen beitragen.

Eher vergleichbar mit den Zahlen aus dem IAB-Betriebspanel sind diejenigen der letzten Kurzstudie zum Thema Industriespionage der international tätigen Sicherheitsberatung Corporate Trust. In dieser gaben 29,1 Prozent der befragten Unternehmen an, in den letzten drei Jahren Opfer von Spionage oder sonstigem Informationsabfluss geworden zu sein (Corporate Trust 2017b). Auch hier wurden nur Unternehmen mit mindestens zehn Beschäftigten und einem Umsatz von mindestens einer Million Euro berücksichtigt (N = 356). Sowohl bei der Bitkom- als auch der Corporate-Trust-Studie ist eine systematische Selektion der an der Befragung teilnehmenden Unternehmen nicht auszuschließen.

Hackerangriffe auf IT-Systeme sind die häufigste Form von Spionage

Spionage kann in Form unterschiedlicher Aktivitäten stattfinden. Am häufigsten wird von Hackerangriffen[1] auf IT-Systeme berichtet: Die Hälfte aller Betriebe, die einen Spionageverdacht äußern, berichten von Hackerangriffen (50,8 %, vgl. Tabelle T1 auf Seite 4). 61,5 Prozent der von einem tatsächlichen Angriff betroffenen Betriebe geben an, dass dieser in Form eines Hackerangriffs auf IT-Systeme stattgefunden hat. Das bedeutet, dass in 5,5 Prozent aller Betriebe in Deutschland Hackerangriffe verübt wurden und 3,7 Prozent den Verdacht haben, dass solche auf ihren Betrieb verübt wurden.

Über ein Drittel der Betriebe mit Verdachtsfällen vermutet, dass ihnen sensible digitale Daten beziehungsweise Informationen gestohlen wurden (36,1 %); das entspricht 2,6 Prozent aller Betriebe in Deutschland. Über ein Fünftel der Betriebe, die tatsächlichen Angriffen ausgesetzt waren, wurde Opfer digitalen Datendiebstahls (21,4 %); bezogen

[1] Es ist nicht auszuschließen, dass die Befragten zu „Hackerangriffe auf EDV-Systeme“ auch Ransomware zählen, obwohl es sich dabei nicht um Spionage im eigentlichen Sinn handelt. Unter Ransomware versteht man Schadprogramme, die den Zugriff auf Daten und Systeme einschränken oder unterbinden und für dessen Freigabe ein Lösegeld verlangt wird.

auf alle Betriebe in Deutschland sind dies 1,9 Prozent. Ob es sich dabei immer um Wirtschafts- oder Industriespionage im engeren Sinne handelt, lässt sich nicht mit Sicherheit sagen.

Deutlich seltener berichten Betriebe vom Abhören oder Ausspähen analoger oder digitaler Kommunikation. 17,3 Prozent der von Spionageverdacht betroffenen Betriebe und 9,4 Prozent der Betriebe, die tatsächlichen Angriffen ausgesetzt waren, wurden abgehört oder äußerten einen entsprechenden Verdacht. Bezieht man diese Angaben auf alle Betriebe, so berichten 1,3 Prozent über Abhör- oder Ausspähverdachtsfälle und 0,8 Prozent über entsprechende Angriffe.

Etwas häufiger sind Betriebe dem analogen Diebstahl, etwa von sensiblen physischen Dokumenten, Mustern, Maschinen oder Bauteilen, ausgesetzt und äußern demgegenüber etwas seltener einen entsprechenden Verdacht: Jeder zehnte Betrieb mit Spionageverdacht vermutet, dass er bestohlen wurde und fast jeder fünfte von einem tatsächlichen Angriff betroffene Betrieb wurde tatsächlich bestohlen. Den Verdacht eines solchen Diebstahls äußerten 1,3 Prozent aller Betriebe und den tatsächlichen Diebstahl 1,7 Prozent.

Die Kategorie „Sonstiger Verdacht“ wird mit 31 Prozent von Betrieben mit Spionageverdacht am dritthäufigsten genannt (vgl. Tabelle T1). Es gibt also eine Reihe von Verdachtsfällen, die sich nicht unter die abgefragten Kategorien subsumieren lassen. Der Anteil der angegriffenen Betriebe, die „Sonstigen Angriff“ angekreuzt haben, liegt mit 16,8 Prozent deutlich darunter. Um welche Vorfälle es sich konkret handelt, bleibt an dieser Stelle unklar. Bezogen auf die gesamte Betriebslandschaft fallen unter die Kategorie „Sonstiger Verdacht oder Angriff“ 2,3 Prozent (Spionageverdacht) beziehungsweise 1,5 Prozent (Spionageangriff).

Die Ergebnisse zeigen insgesamt, dass Industrie- und Wirtschaftsspionage vor allem digital, beispielweise durch Cyberattacken oder digitales Ausspähen, stattfinden.

T1

Art und Weise des Spionageverdachts oder des Spionageangriffs

Angaben der Betriebe, Anteile in Prozent

	Verdacht		Angriff	
	Anteil an ...		Anteil an ...	
	... Betrieben mit Verdacht	... allen Betrieben	... Betrieben mit Angriff	... allen Betrieben
Hackerangriff auf IT-Systeme	50,8	3,7	61,5	5,5
Digitaler Diebstahl von sensiblen Daten oder Informationen	36,1	2,6	21,4	1,9
Abhören oder Ausspähen analoger oder digitaler Kommunikation	17,3	1,3	9,4	0,8
Analoger Diebstahl von sensiblen physischen Dokumenten, Mustern, Maschinen, Bauteilen o. Ä.	10,3	1,3	18,4	1,7
Sonstiger Verdacht oder Angriff	31,0	2,3	16,8	1,5

Quelle: IAB-Betriebspanel 2023, gewichtete Werte. © IAB

Betriebe der Informations- und Kommunikationsbranche werden am häufigsten ausspioniert

Am häufigsten findet Spionage im Wirtschaftsbereich Information und Kommunikation statt: 13,7 Prozent der Betriebe dieser Branche berichten über Verdachts- und 15,5 Prozent über Angriffsfälle (vgl. Abbildung A2 auf Seite 5). Verdachts- und Angriffsfälle lassen sich auch häufig im Bereich Großhandel, KfZ-Handel und -reparatur (11 % Verdachts- und 13,1 % Angriffsfälle) sowie bei den Interessensvertretungen (jeweils rund 11 %) feststellen.

Überdurchschnittlich häufig wurden Angriffe auf Betriebe der Wirtschaftszweige Verkehr und Lagerei mit 14 Prozent, öffentliche Verwaltung (12,1 %) sowie Finanz- und Versicherungsdienstleistungen (10,7 %) verübt. Im verarbeitenden Gewerbe gibt es mit 9,2 beziehungsweise 9,0 Prozent ähnlich viele Verdachtsfälle wie Angriffe.

Grundsätzlich scheint es keine Wirtschaftsbereiche zu geben, die von der Industrie- und Wirtschaftsspionage völlig verschont bleiben. Interessanterweise ist es nicht ausschließlich das verarbeitende Gewerbe, das von Spionage betroffen ist. Viele Branchen im Dienstleistungs- und Servicebereich werden ebenso ausgespäht wie die öffentliche Verwaltung. Dies deckt sich mit den Ergebnissen der Bitkom-Umfragen, die ebenfalls Spionage, Sabotage und Datendiebstahl in Unternehmen aller Branchen aufzeigen.

Die Größe eines Betriebs spielt eine Rolle

Neben der Branche hat auch die Betriebsgröße einen starken Einfluss darauf, ob ein Betrieb von Spionageaktivitäten betroffen ist. Kleinstbetriebe

mit bis zu neun Beschäftigten sind mit 6,3 Prozent Verdachts- und 7,3 Prozent Angriffsfällen seltener betroffen, während bei den Großbetrieben mit 200 und mehr Beschäftigten fast jeder fünfte Betrieb einen Angriff erlebt hat (19,9 %) oder von Verdachtsfällen betroffen ist (17,7 %; vgl. Abbildung A2). Grundsätzlich scheint zu gelten, dass das Risiko, von Industrie- und Wirtschaftsspionage betroffen zu sein, mit der Betriebsgröße steigt.

Innovative, exportierende und forschende Betriebe in kompetitiven Märkten sind besonders betroffen

Nicht alle Betriebe werden gleichermaßen Opfer von Spionageaktivitäten. Es ist davon auszugehen, dass vor allem dann spioniert wird, wenn der Spionagegegenstand einen strategischen Wettbewerbsvorteil darstellt. Dies ist insbesondere in innovativen, forschenden Betrieben, die im Wettbewerb stehen, der Fall. So äußern Betriebe, die sich mit Forschung und Entwicklung befassen, mit 17,8 Prozent wesentlich häufiger einen Spionageverdacht und mit 22 Prozent einen Spionageangriff als Betriebe, die nicht auf diesem Gebiet tätig sind (6,8 % bzw. 8,3 %, vgl. Tabelle T2 auf Seite 6).

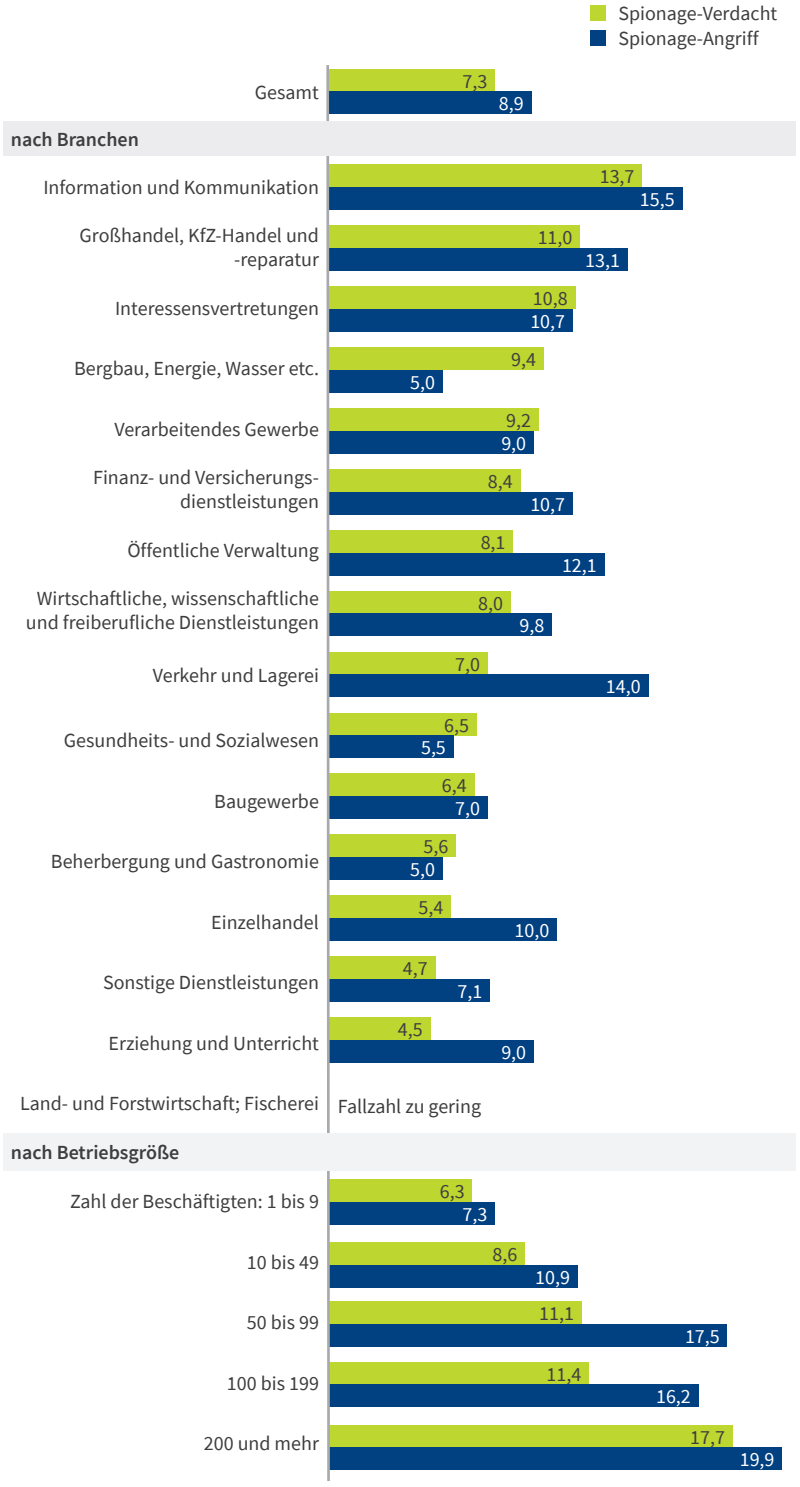
Betriebe, die exportieren, sind ebenfalls häufiger von Spionageaktivitäten betroffen: Einen Spionageverdacht äußern 12,2 Prozent der exportierenden Betriebe, bei nicht exportierenden Betrieben ist der Anteil nur noch etwa halb so hoch. Noch häufiger sind exportierende Betriebe mit 14,4 Prozent tatsächlichen Spionageangriffen ausgesetzt. Bei nicht exportierenden Betrieben sind es lediglich 7,9 Prozent. Dieses Muster ist nachvollziehbar, da exportierende Betriebe typischerweise produktiver und innovativer sind als nicht exportierende Betriebe, und damit ein attraktiveres Ziel für Spionagetätigkeiten darstellen.

Ein zentrales Ergebnis der Befragung ist, dass innovative Betriebe deutlich häufiger ausspioniert werden. Das betrifft vor allem Spionageangriffe in Betrieben mit Produktinnovationen[2] (13,5 %) gegenüber solchen ohne Produktinnovationen mit 5,7 Prozent. Noch deutlicher sind die Unterschie-

A2

Betriebe sind je nach Branche und Größe unterschiedlich von Spionage betroffen

Angaben der Betriebe, Anteile in Prozent



Quelle: IAB-Betriebspanel 2023, gewichtete Werte. © IAB

[2] Als innovative Betriebe werden Betriebe mit Produkt- oder Verfahrensinnovationen bezeichnet. Hat ein Betrieb im letzten Geschäftsjahr eine vorher bereits angebotene Leistung oder ein Produkt verbessert oder weiterentwickelt, eine Leistung oder ein Produkt, das bereits vorher auf dem Markt vorhanden war, neu in das Angebot aufgenommen oder eine völlig neue Leistung oder ein neues Produkt, für das ein neuer Markt geschaffen werden muss, in das Angebot aufgenommen, gilt dieser Betrieb als produktinnovativ.

de bei Betrieben mit Verfahrensinnovationen[3]: Sowohl Verdachtsfälle als auch Spionageangriffe sind in diesen Betrieben mehr als doppelt so hoch wie in Betrieben ohne solche Innovationen (14,2 % versus 6,4 % und 16,7 % versus 7,7 %).

Betriebe, die unter Konkurrenz- und Wettbewerbsdruck stehen, sind ebenfalls häufiger Spionageangriffen ausgesetzt (vgl. Tabelle T2). Mit steigendem Konkurrenz- und Wettbewerbsdruck nimmt der Anteil der Betriebe zu, die einen Spionageverdacht oder einen Spionageangriff angeben.

[3] Betriebe, die neue Verfahren entwickelt oder eingeführt haben, die den Produktionsprozess oder das Bereitstellen von Dienstleistungen merklich verbessern, gelten als verfahrensinnovativ.

T2

Spionageverdacht und -angriff nach betrieblichen Kriterien

Angaben der Betriebe, Anteile in Prozent

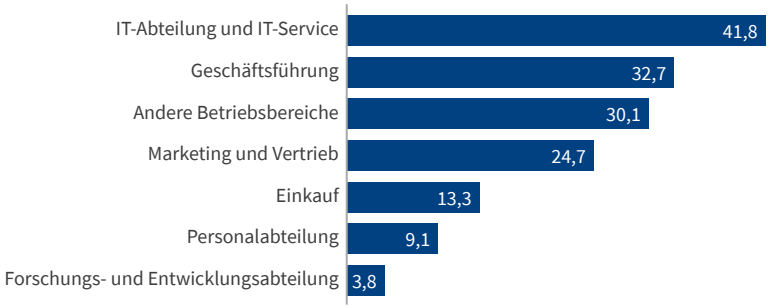
		Spionage	
		Verdacht	Angriff
Forschung und Entwicklung	ja	17,8	22,0
	nein	6,8	8,3
Exportierender Betrieb	ja	12,2	14,4
	nein	6,4	7,9
Produktinnovationen	ja	9,5	13,5
	nein	5,8	5,7
Verfahrensinnovationen	ja	14,2	16,7
	nein	6,4	7,7
Wettbewerbsdruck	ohne	5,6	5,7
	gering	5,8	6,9
	mittel	8,2	9,6
	hoch	8,8	12,6
Insgesamt		7,3	8,9

Anmerkung: In Probit-Schätzungen zeigen sich für die Variablen in dieser Tabelle signifikante Unterschiede.
Quelle: IAB-Betriebspanel 2023, gewichtete Werte. © IAB

A3

Spionageangriffe zielen am häufigsten auf IT-Abteilungen der Betriebe ab

Angaben der Betriebe, Anteile in Prozent



Quelle: IAB-Betriebspanel 2023, gewichtete Werte. © IAB

Betriebe mit hohem Wettbewerbsdruck berichteten mehr als doppelt so häufig von Spionageangriffen (12,6 %) im Vergleich zu Betrieben, die unter keinem Wettbewerbsdruck stehen (5,7 %). Die naheliegende Erklärung ist, dass in Märkten mit hohem Wettbewerbsdruck die Anreize insbesondere für Industriespionage unter Wettbewerbern stärker ausgeprägt sind. In solchen Märkten kann durch Spionage erlangtes Wissen entscheidend zum Überleben einzelner Betriebe beitragen, oder ihnen zumindest erlauben, mit den Marktführern Schritt zu halten.

Diese Befunde zeigen deutlich, dass Industrie- und Wirtschaftsspionage zielgerichtet sind und insbesondere solche Betriebe betreffen, die technologisch weit entwickelt sind und im internationalen Wettbewerb Fuß gefasst haben.

Angriffe zielen meistens auf IT-Abteilungen

Innerhalb der von Spionageangriffen betroffenen Betriebe sind nicht alle Bereiche beziehungsweise Abteilungen gleichermaßen Angriffsziel. Die Betriebe nannten mit 41,8 Prozent am häufigsten die IT-Abteilung und den IT-Service (vgl. Abbildung A3). Fast ein Drittel der Betriebe gab an, dass auf die Geschäftsführung Spionageangriffe verübt wurden (32,7 %). Die Kategorie „Andere Betriebsbereiche“ kam mit 30,1 Prozent am dritthäufigsten vor. Bei einem Viertel der Betriebe war die Marketing- und Vertriebsabteilung Ziel der Angriffe (24,7 %). Eine untergeordnete Rolle spielten der Einkauf und die Personalabteilung (13,3 % und 9,1 %).

Die seltene Nennung von Forschung- und Entwicklungsabteilungen (3,8 %) ist zum Teil darauf zurückzuführen, dass sich nur 5 Prozent der Betriebe mit Forschung und Entwicklung befassen. Bezieht man sich nur auf diese Betriebe, geben 13,4 Prozent von ihnen an, dass die entsprechende Abteilung angegriffen wurde.

Fazit

Industrie- und Wirtschaftsspionage können sowohl auf betrieblicher als auch auf gesamtwirtschaftlicher Ebene zu erheblichen Schäden führen. Trotz der ökonomischen Bedeutung war es bislang

schwierig, sich ein verlässliches Bild über diese Phänomene zu machen, da es keine repräsentativen Daten dazu gab.

Mit dem IAB-Betriebspanel 2023 wird diese Lücke geschlossen: Die neuen Daten geben einen Überblick über die Verbreitung von Spionageaktivitäten in Deutschland, denen Betriebe in den letzten Jahren ausgesetzt waren. Insgesamt berichten 12 Prozent aller Betriebe von Verdachtsfällen oder tatsächlichen Angriffen. Industrie- und Wirtschaftsspionage finden dabei vor allem digital statt, beispielweise durch Cyberattacken oder digitales Ausspähen. Es ist allerdings von einer hohen Dunkelziffer auszugehen, da sich nicht alle Betriebe darüber bewusst sind, Opfer von Spionageaktivitäten geworden zu sein.

Nicht alle Betriebe sind in gleichem Maße betroffen: Große Betriebe mit 200 und mehr Beschäftigten sind deutlich häufiger das Ziel von Industrie- und Wirtschaftsspionage. Darüber hinaus sind insbesondere innovative Betriebe, die unter hohem Wettbewerbsdruck stehen, mit einer höheren Wahrscheinlichkeit Spionageaktivitäten ausgesetzt. Eine naheliegende Erklärung ist, dass in Märkten mit hohem Wettbewerbsdruck die Anreize für Industrie- und Wirtschaftsspionage unter Wettbewerbern stärker ausgeprägt sind. In solchen Märkten kann durch Spionage erlangtes Wissen entscheidend zum Überleben einzelner Betriebe beitragen, oder ihnen zumindest erlauben, mit den Marktführern Schritt zu halten. Die Ergebnisse deuten darauf hin, dass Industrie- und Wirtschaftsspionage nicht nur umfangreich, sondern auch zielgerichtet ist.

Angesichts der zunehmenden geopolitischen Spannungen in der Welt und des rasanten technologischen Fortschritts – etwa in den Bereichen Künstliche Intelligenz, Bioengineering, Robotik und Nanotechnologie – dürften die Anreize für Industrie- und Wirtschaftsspionage steigen. Für den Wirtschaftsstandort Deutschland wird es daher künftig noch wichtiger sein, die Entwicklungen in diesem Bereich genau zu verfolgen und effektive Gegenmaßnahmen zu ergreifen, um den gesamtwirtschaftlichen Schaden zu minimieren.

Literatur

Ben-Atar, Doron S. (2004): Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power. Yale University Press.

Bitkom (2023): Wirtschaftsschutz 2023. Studienabruf unter http://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf am 15.1.2025.

Bitkom (2024): Wirtschaftsschutz 2024. Studienabruf unter http://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf am 15.1.2025.

Corporate Trust (2017a): NSA Report. Systemische Analyse der Snowden-Dokumente zum Schutz der deutschen Wirtschaft. Studienabruf unter www.corporate-trust.de/wp-content/uploads/2023/11/NSA-Report.pdf am 15.1.2025.

Corporate Trust (2017b): Future Report. Weltweite Mega-Trends und Ihre Sicherheitsherausforderungen. Studienabruf unter www.corporate-trust.de/wp-content/uploads/2023/11/Future_report_2017.pdf am 15.1.2025.

Ellguth, Peter; Kohaut, Susanne; Möller, Iris (2014): The IAB Establishment Panel – methodological essentials and data quality. Journal for Labour Market Research, 47, S. 27–41.

European Commission (2018): The Scale and Impact of Industrial Espionage and Theft of Trade Secrets Through Cyber. Studienabruf unter https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1 am 15.1.2025.

IP Commission (2017): Update to the IP Commission Report – The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy.

IP Commission (2021): The IP Commission 2021 – Updated Recommendations.

Kasper, Karsten (2015): Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse, Bundeskriminalamt 2015.

Nasheri, Hedieh (2005): Economic Espionage and Industrial Spying. Cambridge University Press.

Norwich, John Julius (1990): Byzantium – The Early Centuries. Penguin Books.

Office of the National Counterintelligence Executive (2011): Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage. Studienabruf unter https://nsarchive.gwu.edu/document/21451-document-55 am 15.1.2025.

Verfassungsschutz (2024): Verfassungsschutzbericht 2023.

Albrecht Glitz*), PhD

ist Associate Professor an der Universitat Pompeu Fabra und affiliiert mit der Barcelona School of Economics, IPEG und RFBerlin.

albrecht.glitz@upf.ed

Dr. Susanne Kohaut

ist Mitarbeiterin im Bereich „Betriebe und Beschäftigung" am IAB.

Susanne.Kohaut@iab.de

Dr. Iris Möller

ist Mitarbeiterin im Bereich „Betriebe und Beschäftigung" am IAB.

Iris.Moeller@iab.de

*) Albrecht Glitz dankt der ROCKWOOL Foundation Berlin (Projektnummer 2006, „Economic Espionage, Globalization and Welfare") für ihre finanzielle Unterstützung.

Impressum | IAB-Kurzbericht Nr. 2, 11.3.2025 | Herausgeber: Institut für Arbeitsmarkt- und Berufsforschung (IAB) der Bundesagentur für Arbeit, 90327 Nürnberg | Redaktion: Elfriede Sonntag | Grafik & Gestaltung: Nicola Brendel | Foto: Wolfram Murr, Fotofabrik Nürnberg und privat | Druck: MKL Druck GmbH & Co. KG, Ostbevern | Rechte: Diese Publikation ist unter folgender Creative-Commons-Lizenz veröffentlicht: Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0) https://creativecommons.org/licenses/by-sa/4.0/deed.de | IAB im Internet: www.iab.de. Dort finden Sie unter anderem diesen Kurzbericht zum kostenlosen Download | Kontakt: IAB.Kurzbericht@iab.de | ISSN 0942-167X | DOI 10.48720/IAB.KB.2502