Fraunhofer ISI

MODERNISIERUNG DER PRODUKTION

Mitteilungen aus der ISI-Erhebung | September 2018 | Ausgabe 72

Spione in der Produktion

Unterschätzte Risiken führen zu unzureichendem Schutz

Esther Bollhöfer, Angela Jäger

Mittelständische Unternehmen verzeichnen immer wieder erhebliche Schäden durch Fälle von Wirtschaftsspionage und Konkurrenzausspähung. Hinzu kommen viele Vorfälle, die unentdeckt bleiben oder deren Auswirkungen auf andere Ursachen zurückgeführt werden. Das gesamte Ausmaß kann daher nur geschätzt werden.

Gerade im Bereich digital vernetzter Datenbestände und Arbeitsformen sind erhebliche Werte durch ungewollten Wissensabfluss betroffen. Dennoch gelten Wirtschaftsspionage und Konkurrenzausspähung besonders im Mittelstand häufig „nur" als diffuse Bedrohungsszenarien – ohne direkte operative Relevanz. Zudem wird das gestiegene Potenzial, auf digital erfasste und damit verfügbare vertrauliche Informationen zurückzugreifen und dabei in der Menge an Kommunikationsprozessen unentdeckt zu bleiben, unterschätzt.

Vor allem für kleine und mittelständische Unternehmen (KMU) bedeutet das, in Präventionsmaßnahmen zu investieren und Strategien dagegen zu entwickeln. Dazu bedarf es einer systematischen Beobachtung der Bedrohungslage, einer fortlaufenden Information über Präventionsmöglichkeiten und des Anschlusses an ein Experten-Netzwerk, um voneinander Schutzmaßnahmen zu lernen und im Schadensfall richtig und schnell zu reagieren.

Einleitung

Eine der zentralen Fragen im Kontext von Wirtschaftsspionage und Konkurrenzausspähung ist die nach dem Schutz vertraulicher Informationen. Diese Aufgabe ist für Unternehmen nicht neu. Jedoch ist mit der Digitalisierung die Menge an digital erfassten und verfügbaren Informationen gestiegen, zugleich haben sich die Kommunikationsprozesse vervielfältigt.

Gefahr von Ausspähung ist im Zeitalter der Digitalisierung neu zu bewerten

Digitalisierung bringt damit nicht nur große Potenziale mit sich, sondern auch neue Herausforderungen, gerade auf dem Gebiet des Informationsschutzes. Durch die rasante Entwicklung der Informations- und Kommunikationstechnologie (IKT) ist ein schneller Transfer komplexer, technologischer Informationen möglich, der die traditionellen Know-how-Vorsprünge von KMU rascher schwinden lässt als bisher und so zu einem wachsenden Innovationsdruck führt. Schaden durch ungewollten Informationsabfluss kann sowohl direkt als oft auch indirekt entstehen, was dann mit weit größeren Folgen einhergeht. Ein Datenleck kann das ganze Unternehmen ruinieren, so könnte beispielsweise ein Wettbewerber das gleiche Produkt oder die gleiche Dienstleistung schneller und günstiger auf den Markt bringen.

Vor diesem Hintergrund stellt sich die Frage, wo die größten Potenziale für den Schutz betrieblicher Informationen liegen und wie sie gehoben werden können. Im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF) wurden dazu im Rahmen der Expertise „Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WiSKoS)" auf Basis der ISI-Erhebung *Modernisierung der Produktion* 2015 folgende Fragen analysiert:

Leitfragen

- Wie stark sind die Betriebe des Verarbeitenden Gewerbes in Deutschland von Wirtschaftsspionage und Konkurrenzausspähung betroffen?
- Welche Rolle spielen dabei Auslandsaktivitäten der Unternehmen?
- Welche Schutzmaßnahmen treffen Unternehmen gegen ungewollten Wissensabfluss?

Die vorliegende Mitteilung fasst ausgewählte Ergebnisse zusammen. Ergänzend werden Angaben einer Vertiefungsbefragung von kleinen und mittelständischen Unternehmen (KMU) zu ihrem Präventionsverhalten und konkreten Vorfällen, welche im Rahmen der Expertise erhoben wurden, einbezogen. Dies bietet zusätzliche Einblicke in konkrete Bedrohungsszenarien für 166 KMU des Verarbeitenden Gewerbes.

Situation im Verarbeitenden Gewerbe in Deutschland

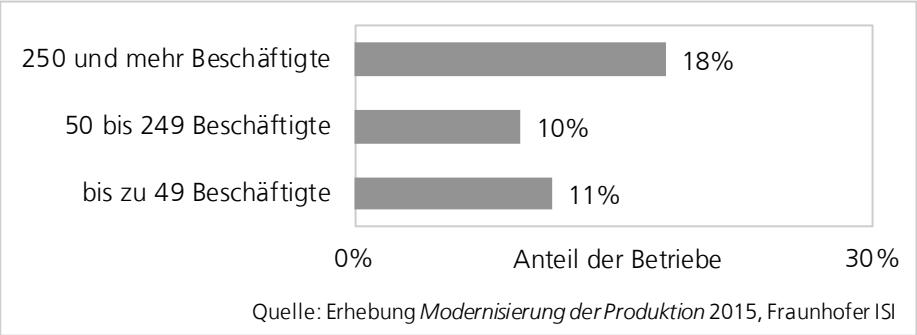
Die Frage nach tatsächlich bekannten Vorfällen oder Verdachtsfällen zur Wirtschaftsspionage und Konkurrenzausspähung in den letzten fünf Jahren bejahten im Durchschnitt elf Prozent der Betriebe des Verarbeitenden Gewerbes. Besonders betroffen

sind dabei die größeren Unternehmen mit mehr als 250 Beschäftigten (Abbildung 1), unter denen jeder fünfte Betrieb (18 Prozent) von Ausspähung betroffen war oder einen konkreten Verdachtsfall hatte. Aber auch jeder zehnte kleinere Betrieb (11 Prozent) verzeichnete in den letzten fünf Jahren einen konkreten Verdachtsfall bzw. einen konkreten Vorfall von Ausspähung.

Große Unternehmen stärker betroffen

Der höhere Anteil gefährdeter Betrieben unter den großen Unternehmen resultiert zum Teil daraus, dass diese auch auf den Märkten sichtbarer sind und dadurch eher Aufmerksamkeit auf sich lenken. Weiterhin haben auch organisatorische Maßnahmen wie z.B. Frühwarnsysteme einen Anteil daran, dass Betriebe Angriffe auf vertrauliche Informationen überhaupt bemerken. Solche Kontrollverfahren werden bei kleineren Unternehmen wesentlich seltener eingesetzt. Zahlreiche Vorfälle bleiben unbemerkt und Auffälligkeiten werden aufgrund fehlender Weiterverfolgung(-smöglichkeiten) nicht als Verdachtsfälle eingestuft. Daher ist zu vermuten, dass bei diesen der Anteil der unentdeckten Angriffe höher einzuschätzen ist als bei größeren Unternehmen mit entsprechenden Präventionsmaßnahmen.

Abbildung 1: Vorfälle und Verdachtsfälle bei Unternehmen



Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI

Gefährdung ist in Verbindung mit doppeltem Dunkelfeld zu bewerten

Die in Abbildung 1 berichteten Anteile von Vorfällen bzw. Verdachtsfällen von ungewolltem Wissensabfluss vermögen auf den ersten Blick nicht zu alarmieren. Allerdings ist zu beachten, dass es sich hierbei nur um die *tatsächlich bekannten Fälle* von Wirtschaftsspionage bzw. Konkurrenzausspähung in den Unternehmen handelt. Außen vor bleiben Vorfälle, die Betrieben erst gar nicht bekannt werden oder nicht als Schadensfall registriert wurden. Dies wird als sogenanntes *doppeltes Dunkelfeld* bezeichnet und umfasst den Anteil an Vorfällen, die für Betriebe nicht erkennbar waren. Hinzu kommt dann noch das sogenannte *Dunkelfeld*, also der Anteil an Vorfällen, der aus diversen Gründen bewusst verschwiegen und nicht gemeldet wird.

Mindestens jeder zehnte Betrieb betroffen

Insgesamt ist festzuhalten, dass nicht nur global agierende Konzerne, sondern auch KMU von illegalem Wissensabfluss betroffen sind und unter den Folgen leiden. Der beobachtbare durchschnittliche Anteil von elf Prozent ist die Spitze des Eisbergs. Er

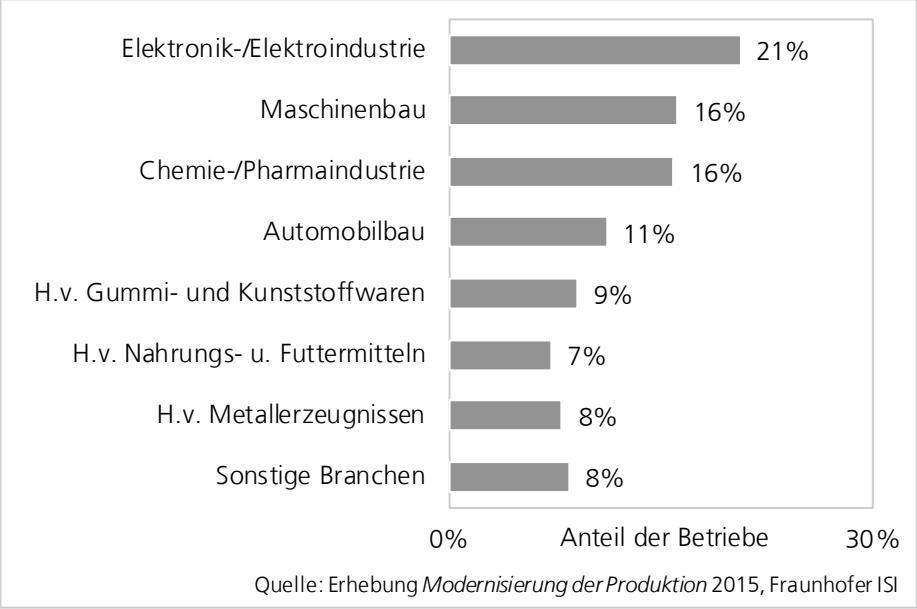
stellt nur den offensichtlich erkennbaren Anteil dar und ist daher als Mindestanteil anzusehen. In anderen Studien, welche noch beispielsweise nach Datenlecks bzw. ungewolltem Informationsabfluss an Dritte fragten, wurden teilweise höhere Anteile festgestellt. Verschiedener Wortgebrauch bzw. die unterschiedlichen Assoziationen erklären die stark schwankenden Zahlen zur Betroffenheit der deutschen Wirtschaft durch Wirtschaftsspionage und Konkurrenzausspähung in diversen Studien der letzten Jahre.

Größere Betroffenheit bei einzelnen Branchen und Produzentengruppen

Besondere Gefährdung in drei Branchen

Erwartungsgemäß war festzustellen, dass der Anteil an Betrieben mit konkreten Vorfällen und Verdachtsfällen in den verschiedenen Branchen sehr unterschiedlich ausfällt: Besonders betroffen sind die Elektronik- bzw. Elektroindustrie mit fast 21 Prozent an betroffenen Betrieben, gefolgt vom Maschinenbau (16 %) und der Chemie-/Pharmaindustrie (ebenfalls 16 %), wie Abbildung 2 deutlich zeigt. Gründe für diese besondere Betroffenheit liegen sicher in der globalen Marktpräsenz, der großen Bedeutung von Produkt- und Prozessinnovationen in den betroffenen Branchen sowie der hohen Forschungsintensität, den langen Forschungs- bzw. Vorlaufzeiten bis zur Produktreife sowie der Komplexität der Produkte. Entsprechend zeigen Detailanalysen, dass jeder fünfte Betrieb mit mittlerer und hoher Forschungs- und Entwicklungsintensität (FuE) betroffen ist, wohingegen Betriebe mit weniger FuE-Ausgaben deutlich seltener Angriffen ausgesetzt sind.

Abbildung 2: Vorfälle und nach Branchen

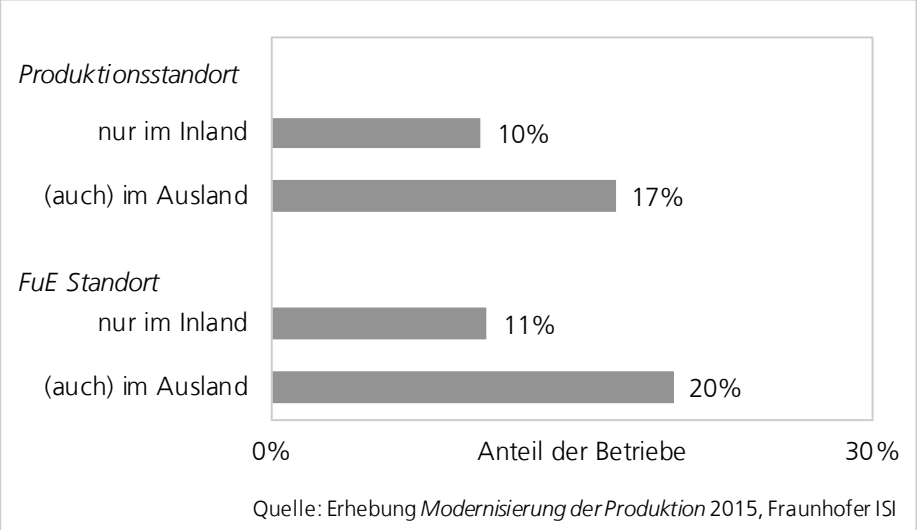


Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI

Demgegenüber sind die anderen Branchengruppen nur zu etwas geringeren Anteilen als der Durchschnitt betroffen. Es bleibt daher festzuhalten, dass alle Branchen von ungewolltem Wissensabfluss bedroht sind. Auch unter den Herstellern von Gummi- und Kunststoffwaren, von Nahrungs- und Futtermitteln oder von Metallerzeugnissen berichteten etwa acht Prozent der Betriebe von bekannten Vorfällen oder Verdachtsfällen von Wirtschaftsspionage und Konkurrenzausspähung in den letzten fünf Jahren.

Dennoch: Betroffenheit besteht bei allen Branchen

Inwieweit eine globale Marktpräsenz in der Tat eine größere Angriffsfläche für Konkurrenzausspähung oder Spionage bietet, verdeutlicht Abbildung 3. Demnach rückt die Verflechtung eines Betriebs mit dem Ausland das Unternehmen stärker ins Visier der Spione: Unternehmen mit einer Produktionsstätte im Ausland berichten mit einem Anteil von 17 Prozent deutlich häufiger von Vorfällen bzw. konkreten Verdachtsfällen, als solche ohne einen Auslandsbezug (10 %). Ebenso meldet jedes fünfte Unternehmen, welches eine Forschungs- und Entwicklungsabteilung im Ausland unterhält, mindestens einen Vorfall oder Verdachtsfall. Bei Unternehmen, welche nur über FuE-Abteilungen im Inland verfügen, liegt dieser Anteil bei nur 11 Prozent.



Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI

Abbildung 3: Vorfälle und Verdachtsfälle bei Unternehmen mit Auslandsbezug für die Produktion bzw. FuE

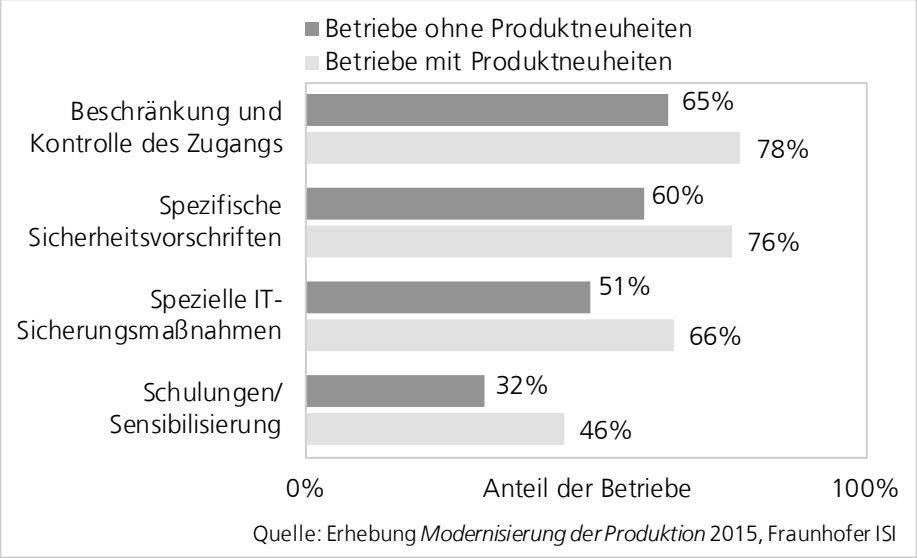
Schutzmaßnahmen und ihre Verbreitung

Angesichts dieser Situation stellt sich die Frage, in welchem Umfang sich Unternehmen schützen und welche Maßnahmen ergriffen werden, um Ausspähung und ungewolltem Wissensabfluss vorzubeugen. Von Interesse sind hier vier Bereiche: Der Schutz vor physischem Zugang zu Produktionsstätten, das Vorhandensein von Sicherheitsvorschriften zum Schutz gegen den unerlaubten Abfluss von Informationen (z.B. Regelungen zum Umgang mit sensiblen Daten gegenüber Dritten), die Existenz von speziellen IT-Sicherheitsmaßnahmen (wie z.B. Verschlüsselung von Dokumenten, Nutzungsverbot von fremden Cloud-Diensten oder portablen Datenträgern) sowie die Schulung

Schutzmaßnahmen können auf verschiedenen Ebenen ansetzen

bzw. Sensibilisierung von Beschäftigten zu den Gefahren durch Wirtschaftsspionage und Konkurrenzausspähung.

Abbildung 4: Realisierte Schutzmaßnahmen zur Abwehr von Spionage bzw. Ausspähung



Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI

Abbildung 4 gibt einen Überblick über die Verbreitung dieser Art von Maßnahmen in diesen vier Bereichen im Verarbeitenden Gewerbe. Dabei wird differenziert zwischen Betrieben, welche in den letzten drei Jahren Produktneuheit(en) auf den Markt brachten und jenen Betrieben, die in den letzten drei Jahren keine Produktinnovation realisierten. Insgesamt lässt sich ein verstärktes Bewusstsein für die Gefahrenlage und daraus resultierend, ein größerer Umfang an realisierten Schutzmaßnahmen bei solchen Unternehmen feststellen, die in den letzten Jahren neue Produkte auf den Markt brachten.

Zugangskontrolle und Sicherheitsvorschriften weit verbreitet …

Bei den einzelnen Handlungsbereichen sind jedoch große Unterschiede festzustellen: Die Kontrolle und Beschränkung des Zugangs zum Betriebsgelände, zu Gebäuden oder Räumen wird von einer Mehrheit der Betriebe praktiziert. Drei Viertel der Produktinnovatoren bzw. zwei Drittel der anderen Betriebe praktizieren diese Art von Kontrolle. Die damit offensichtlich weitverbreitete Praxis bedeutet dennoch, dass mindestens ein Viertel der Betriebe über keine organisatorische Zugangsregelung verfügt und Lieferanten und betriebsfremde Dienstleister damit einen relativ ungehinderten Zugang zum Gelände haben. Für kleinere Betriebe mit weniger als 50 Beschäftigten mag dies weniger problematisch sein, da strikte Zutrittsbeschränkungen und entsprechende Organisationsanweisungen sich möglicherweise erübrigen, wenn sich alle zutrittsberechtigten Personen untereinander persönlich kennen. Für Betriebe mit mehr als 250 Beschäftigten hingegen ist dieser Mangel an formeller Beschränkung überraschend.

Vergleichbar häufig sind spezifische Sicherheitsvorschriften zum unerlaubten Abgriff von Informationen verbreitet. Dazu gehören beispielsweise Regelungen zum Umgang mit sensiblen Daten gegenüber Dritten, Beschränkung des Zugriffs auf betriebsinterne Netzwerke, Einschränkung des unkontrollierten Kopierens und Übertragens auf private Geräte, aber auch Regelungen für (Auslands-) Reisen oder für die Begleitung von externen Dienstleistern auf dem Firmengelände. Diese Art von Sicherheitsmaßnahmen wird ebenfalls von über zwei Dritteln der Betriebe praktiziert. Überraschend ist, dass immerhin ein Viertel der Produktinnovatoren und sogar 40 Prozent der anderen Betriebe keine dieser Sicherheitsvorschriften oder Kontrollen implementiert hat.

Noch überraschender ist, dass nur zwei Drittel der Produktinnovatoren und gerade nur die Hälfte aller anderen Betriebe des Verarbeitenden Gewerbes über spezielle IT-Sicherheitsmaßnahmen verfügen. Im Umkehrschluss sind für knapp die Hälfte aller Industriebetriebe die Einschränkung der Nutzung von Cloud-Diensten oder Social Media, das Verschlüsseln von Dokumenten, Regelungen für den Umgang mit Passwörtern in mobilen Geräten oder programmierbaren CNC-Maschinen, das Verbot der Nutzung portabler Datenträger keine etablierte Praxis. Gerade im Zuge einer zunehmenden Verbreitung digitaler Anwendungen sollten der Einsatz bekannter IT-Sicherheitsstandards besonders in der Produktion gängige Praxis sein.

… jedoch noch viel Nachholbedarf bei Schulung und Sensibilisierung der Beschäftigten

Hinsichtlich der Verbreitung von Schulung bzw. Sensibilisierung von Beschäftigten zu den Gefahren durch Wirtschaftsspionage und Konkurrenzausspähung muss festgehalten werden, dass in der Mehrheit der Betriebe die Beschäftigten nicht mitgenommen werden. Nur durchschnittlich zwei von fünf Unternehmen bieten den Beschäftigten Möglichkeiten der Schulung bzw. führen Sensibilisierungsmaßnahmen durch. Gerade der letzte Bereich wäre durch einfache Mittel wie das Anbringen von Postern, das Informieren am schwarzen Brett über aktuelle Fälle von Ausspähung oder den Einsatz von Bildschirmschonern mit Warnhinweisen in ersten Ansätzen leicht umsetzbar und würde relevante Schwachstellen schließen. Die Ergebnisse zeigen, dass einige Unternehmen die Schulung bzw. Sensibilisierung ihrer Beschäftigten nicht für nötig erachten, da sie das bei den Mitarbeitern vorhandene Wissen als nicht relevant für Wirtschaftsspionage bzw. Konkurrenzausspähung halten. Diese Fehleinschätzung wird durch Vertreter verschiedener Unternehmen bestätigt, die im Rahmen der WiSKoS-Studie interviewt wurden. Um Schäden zu vermeiden, sollten viele Betriebe eine höhere Sensibilität für diese Risiken entwickeln.

Fokus IT-Sicherheitsmaßnahmen

IT Sicherheitsmaßnahmen sind noch kein Standard

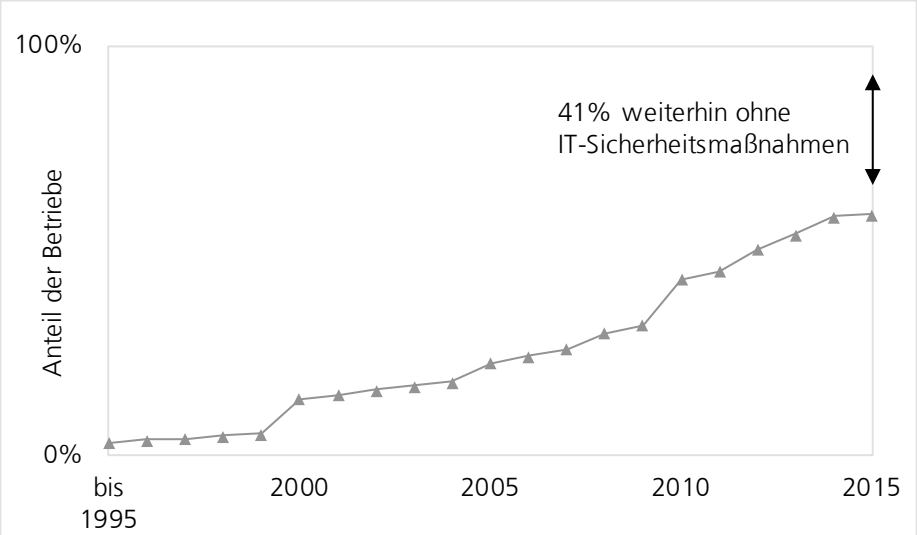
Obwohl sich die meisten Unternehmen der Gefahren in Grundzügen bewusst sind, werden trotzdem E-Mails unverschlüsselt verschickt, USB-Sticks ungeprüft in den Laptop gesteckt und unsichere Apps auf Geschäftsgeräten installiert. Durch die rasante Entwicklung der Informations- und Kommunikationstechnologie (IKT) ist ein schneller

Transfer auch sehr komplexer, technologischer Informationen möglich, der die traditionellen Know-how-Vorsprünge von KMU rascher schwinden lässt als bisher und so zu einem wachsenden Innovationsdruck führt. Der Abfluss von Betriebsgeheimnissen kann das ganze Unternehmen ruinieren oder den Verlust des eigenen Informationsvorsprungs gegenüber Wettbewerben bedeuten.

Weniger als zwei Drittel der Betriebe setzt IT-Sicherheitsmaßnahmen ein

Diese Handlungsnotwendigkeiten werden auch mit genauerem Blick auf den Einsatz von IT-Sicherheitsmaßnahmen deutlich: 2015 trafen 41 Prozent der Unternehmen überhaupt keine(!) Schutzmaßnahmen gegen ungewollten Informationsabfluss (Abbildung 5). Angesichts der besonderen Bedrohung, die Cyber-Angriffe darstellen – sei es durch das Ausnutzen von Sicherheitslücken im IKT-Bereich, den direkten Angriff auf Maschinen und Anlagen mit Netzwerkeinbindung, die Schadsoftware-Infiltration per Internetnutzung (Drive-by-Exploits) oder die gezielten Angriffe auf Sicherheits-Hardware (Router) und Firewalls –, ist dies unverständlich.

Abbildung 5: Entwicklung der Nutzung von IT-Sicherheitsmaßnahmen



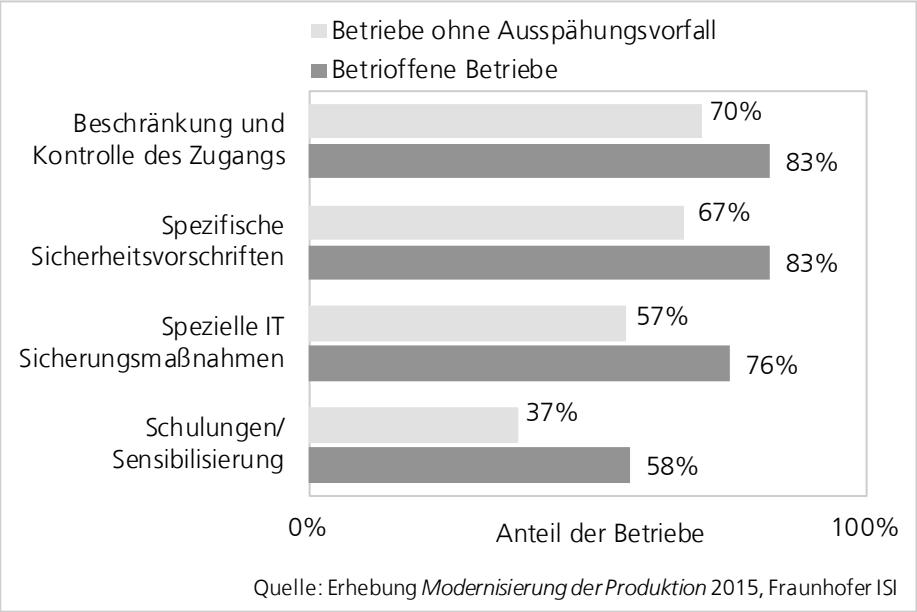
Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI

Große Diskrepanz zwischen Techniknutzung und Einsatz von Schutzmaßnahmen im IT-Bereich

Bemerkenswert ist dabei, dass viele der befragten Unternehmen erst in den letzten Jahren überhaupt IT-Sicherheitsmaßnahmen getroffen haben. Hingegen gehört die Nutzung von Hardware mit Internetzugang bereits seit den neunziger Jahren zum Standard. Hier besteht offensichtlich ein immenser Nachholbedarf. Dabei verdeutlicht der Blick auf die Einführungsdynamik, dass in den letzten Jahren keine herausragende Dynamik bei der Einführung von IT-Sicherheitsmaßnahmen festzustellen war.

Die große Diskrepanz hat unterschiedliche Begründungszusammenhänge, wie in Experteninterviews mit Unternehmensvertretern deutlich wurde: Grundsätzlich scheint

eine große Bereitschaft zu bestehen, sich des Themas anzunehmen. Viele Unternehmen fühlen sich jedoch bei der Auswahl der geeigneten Maßnahmen überfordert, da das Thema IT-Sicherheit inzwischen sehr komplex geworden ist und spezifisches und umfassendes Know-how erfordert. Vielen fehlt zudem der Überblick und damit eine Entscheidungsgrundlage, um die Effektivität und Aktualität solcher Technologien einschätzen zu können. Hinzu kommt die Schnelllebigkeit mancher Lösung: Kaum ist ein wirksamer Schutz verfügbar, wird er schon wieder umgangen. Daher kapitulieren einige Unternehmen regelrecht vor diesem Thema.



Quelle: Erhebung *Modernisierung der Produktion* 2015, Fraunhofer ISI

Abbildung 6: Präventionsverhalten in Abhängigkeit der Betroffenheit

Der Vergleich von betroffenen Unternehmen und Unternehmen, die in den letzten Jahren keinen Vorfall oder konkreten Verdachtsfall zu verzeichnen hatten, macht allerdings deutlich, dass viele Betriebe die notwendigen Aufwendungen an Zeit und Ressourcen zunächst scheuen, da sie die konkrete Gefährdung lediglich als gering einschätzen. Abbildung 6 zeigt, dass Betriebe mit Gefährdungserfahrung eher bereit sind, in entsprechende Schutzmaßnahmen zu investieren. Gerade im Bereich IT-Sicherheitsmaßnahmen und bei der Einbindung der Beschäftigten in Sicherheitskonzepte wird von betroffenen Unternehmen mehr unternommen.

Konkrete Gefährdungssituationen

Weiterführende Untersuchungen haben gezeigt, dass die Gefahren für ungewollten Wissensabfluss oft aus dem Innern der Betriebe stammen. Die WiSKoS-Studie untersuchte auch, im Zusammenhang mit welchen Aktivitäten Betriebe Vorfälle an ungewolltem Abfluss von Wissen, Informationen oder Daten bemerkten. Mit Referenz auf

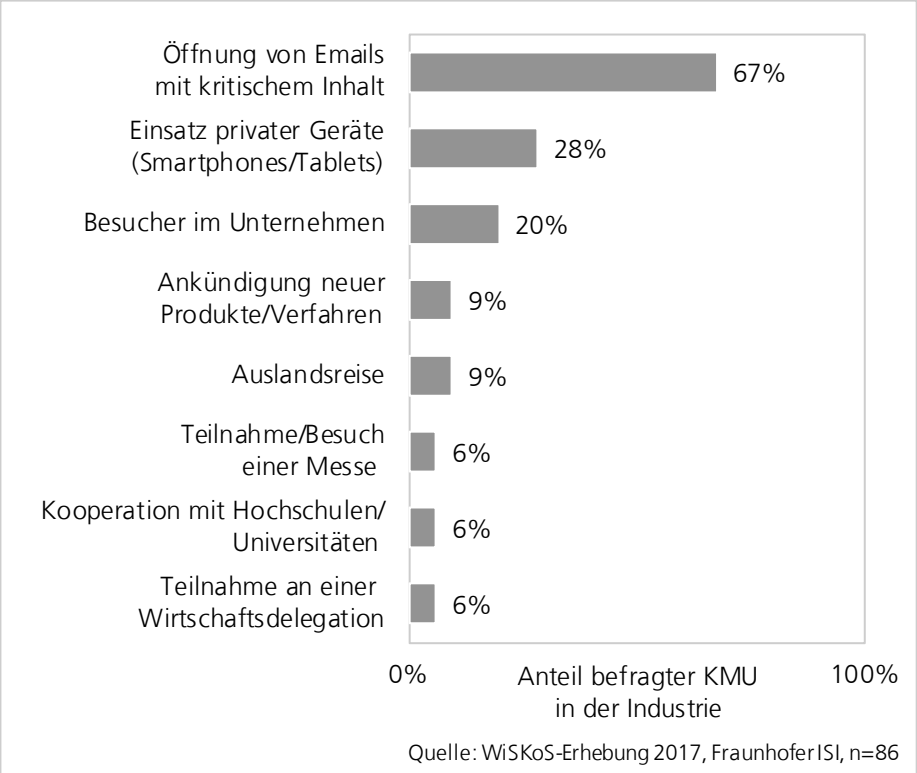
einen erlebten Vorfall wurden Betriebe um Auskunft zu ihren konkreten Erfahrungen gebeten.

Nur etwa die Hälfte der betroffenen Unternehmen berichten von Außentätern

Bemerkenswert war das Ergebnis, dass neben betriebsfremden Personen bei gut der Hälfte der betroffenen Betriebe auch betriebsinterne Personen an der Ausspähung beteiligt waren. Ein Drittel der betroffenen Betriebe gab an, dass es sich ausschließlich um einen Innentäter handelte. Dabei ist zu beachten, dass Vorfälle mit Beteiligung von Innentätern längst nicht immer mit böser Absicht erfolgen. Eine Beteiligung kann auch durch Unvorsichtigkeit, Fahrlässigkeit und Unwissen entstehen. Gerade hieran anknüpfend sollten Unternehmen ihre Präventionsmaßnahmen ausbauen und justieren, um die Informationssicherheit im Unternehmen zu erhöhen.

Ein weiterer Anhaltspunkt für die Entwicklung von Präventionsmaßnahmen in KMU ist der inhaltliche Zusammenhang mit anderen Aktivitäten, wie er von den befragten Unternehmen festgestellt wurde (Abbildung 7). Anders als landläufig angenommen, standen die entdeckten Vorfälle bei den KMU nur selten im Zusammenhang mit Messebesuchen, Auslandsreisen oder der Teilnahme an Wirtschaftsdelegationen. Auch die Ankündigung von Innovationen stand nur in neun Prozent der beobachteten Fälle in direktem Zusammenhang mit einem Vorfall.

Abbildung 7: Betriebsaktivitäten, die mit konkreten Vorfällen in Verbindung standen



Quelle: WiSKoS-Erhebung 2017, Fraunhofer ISI, n=86

Vielmehr mussten 28 Prozent der KMU einen Zusammenhang des Angriffs mit dem Einsatz privater Mobilfunkgeräte wie Smartphones oder Tablets feststellen. Sogar zwei Drittel der befragten Betriebe konnte einen Zusammenhang zum Öffnen von E-Mails mit kritischem Inhalt beobachten. Dieses Ergebnis bestätigt einerseits das allgemeine Bewusstsein um die Gefährdung, die von Emails und privaten mobilen Endgeräten ausgeht, andererseits bedeutet dieser Befund aber auch eine positive Botschaft: Bei diesen Themen kann mit relativ einfachen Mitteln ein höherer Schutz erreicht werden. Betriebsinterne Maßnahmen im Bereich der IT-Sicherheit, der organisatorischen Regelungen sowie bei der Schulung und Sensibilisierung aller Beschäftigten würden diesen beiden Gefährdungsarten entgegenwirken.

Fazit

Mindestens jeder zehnte Betrieb von ungewollter Ausspähung betroffen

Im Rahmen der Expertise zu Wirtschaftsspionage und Konkurrenzausspähung wurden erstmals repräsentative Zahlen zu Spionagefällen bzw. Verdachtsfällen in Unternehmen des Verarbeitenden Gewerbes in Deutschland vorgelegt. Dabei musste festgestellt werden, dass selbst innovative Unternehmen das Thema Gefahrenabwehr nicht umfassend adressiert haben. Gleichzeitig wurde deutlich, dass Betriebe aller Branchen potenziell bedroht sind. Im Durchschnitt hatte jeder zehnte Betrieb in den letzten drei Jahren einen Vorfall oder konkreten Verdachtsfall zu verzeichnen. Das doppelte Dunkelfeld dürfte um ein Vielfaches größer sein.

Für Industrieunternehmen ist es von essenzieller Bedeutung, die zum Wettbewerbsvorteil beitragenden Informationen und vertraulichen Unterlagen in den eigenen Geschäftsräumen zu verwahren und Dritten nicht zugänglich zu machen. Besonders wenn Innovationskraft die Basis für den Geschäftserfolg darstellt, ist es wichtig, Frühwarnsignale drohender Angriffe zu erkennen und ernst zu nehmen. Immer stärker vernetzte Abläufe und automatisierte Prozesse – besonders im Rahmen von Industrie 4.0 – verlangen die Implementierung eines umfassenden Sicherheitssystems.

Schutz vor ungewolltem Wissensabfluss ist auf vielen Ebenen notwendig

Vor allem bei kleinen und mittelständischen Unternehmen besteht ein großer Nachholbedarf im Bereich des Schutzes von Unternehmensdaten. Die KMU sind daher gut beraten, das Thema ungewollter Wissensabfluss und Ausspähung nicht auf die leichte Schulter zu nehmen. Gerade die Einbindung der Beschäftigten sowie die Anwendung von Sicherheitsstandards sind einfache und wirksame Wege, um Sicherheitslücken zu schließen. Unternehmen müssen dabei in Fragen der Sicherheit nicht allein auf die eigenen Ressourcen vertrauen. Es gibt umfangreiche Informationsangebote, die helfen, wirksame Maßnahmen zu identifizieren. Erster Ansprechpartner in allen Angelegenheiten des Schutzes vor ungewolltem Informationsabfluss sind die Landespolizeibehörden sowie die Landesämter für Verfassungsschutz. Auch das BSI sowie die Branchenverbände haben Angebote, um die Unternehmen im Bereich der Prävention zu unterstützen und zu informieren.

Die ISI-Erhebung
Modernisierung der Produktion 2015

Das Fraunhofer-Institut für System- und Innovationsforschung ISI führt seit 1993 regelmäßig Erhebungen zur *Modernisierung der Produktion* durch. Die Erhebung deckt alle Branchen des Verarbeitenden Gewerbes ab. Untersuchungsgegenstand sind die Produktionsstrategien, der Einsatz innovativer Organisations- und Technikkonzepte in der Produktion, Fragen des Personaleinsatzes sowie Fragen zur Wahl des Produktionsstandorts. Daneben werden Leistungsindikatoren wie Produktivität, Flexibilität und Qualität erhoben. Mit diesen Informationen erlaubt die Umfrage detaillierte Analysen zur Modernität und Leistungskraft der Betriebe des Verarbeitenden Gewerbes.

Die vorliegende Mitteilung stützt sich auf Daten der Erhebungsrunde 2015, für die 15 720 Betriebe des Verarbeitenden Gewerbes in Deutschland angeschrieben wurden. Bis August 2015 schickten 1 282 Firmen einen verwertbar ausgefüllten Fragebogen zurück (Rücklaufquote 8 Prozent). Die antwortenden Betriebe decken das gesamte Verarbeitende Gewerbe umfassend ab. Unter anderem sind Betriebe des Maschinenbaus und der Metallverarbeitenden Industrie zu 17 bzw. 20 Prozent vertreten, die Elektroindustrie zu 12 Prozent, die Gummi- und Kunststoffverarbeitende Industrie zu acht Prozent, das Ernährungsgewerbe zu acht Prozent und das Papier-, Verlags- und Druckgewerbe zu fünf Prozent. Betriebe mit weniger als 100 Beschäftigten stellen 66 Prozent, mittelgroße Betriebe 31 Prozent und große Betriebe (mit mehr als 1 000 Beschäftigten) drei Prozent der antwortenden Firmen.

Die bisher erschienenen Mitteilungen finden sich im Internet unter der Adresse:
http://isi.fraunhofer.de/i/mitteilung.php

Wenn Sie an speziellen Auswertungen der Datenbasis interessiert sind, wenden Sie sich bitte an:
Spomenka Maloca, Fraunhofer ISI
Tel.: 0721/6809-328
E-Mail: spomenka.maloca@isi.fraunhofer.de

WISKOS

Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa – WiSKoS

Die Studie entstand im Rahmen eines vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts, an dem das Fraunhofer-Institut für System- und Innovationsforschung ISI (Karlsruhe) gemeinsam mit dem Max-Planck-Institut für ausländisches und internationales Strafrecht (Freiburg) und weiteren, assoziierten Partnern arbeitet.

Mehr Informationen zum Projekt:
http://wiskos.de/de/home.html

Impressum

Modernisierung der Produktion
Mitteilung aus der ISI-Erhebung

Herausgeber
Fraunhofer-Institut für
System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe
www.isi.fraunhofer.de

Autoren
Esther Bollhöfer, Angela Jäger