Wirtschaftsspionage Konkurrenzausspähung

Das Forschungsprojekt WISKOS

Die Ergebnisse im Überblick

WISKOS

Text
Elisa Wallwaey, M.A.
Max-Planck-Institut für ausländisches und internationales Strafrecht
Abteilung Kriminologie

Phänomene der Wirtschaftsspionage und Konkurrenzausspähung sind aufgrund ihrer Komplexität und der vielseitigen möglichen Kombinationen von Angreifern und Tatmustern für Opfer nur schwer zu erkennen und richtig zuzuordnen. Erschwerend kommt hinzu, dass seitens betroffener Unternehmen und Organisationen Vorbehalte bestehen, Vorfälle oder Verdachtsfälle offiziell anzuzeigen.

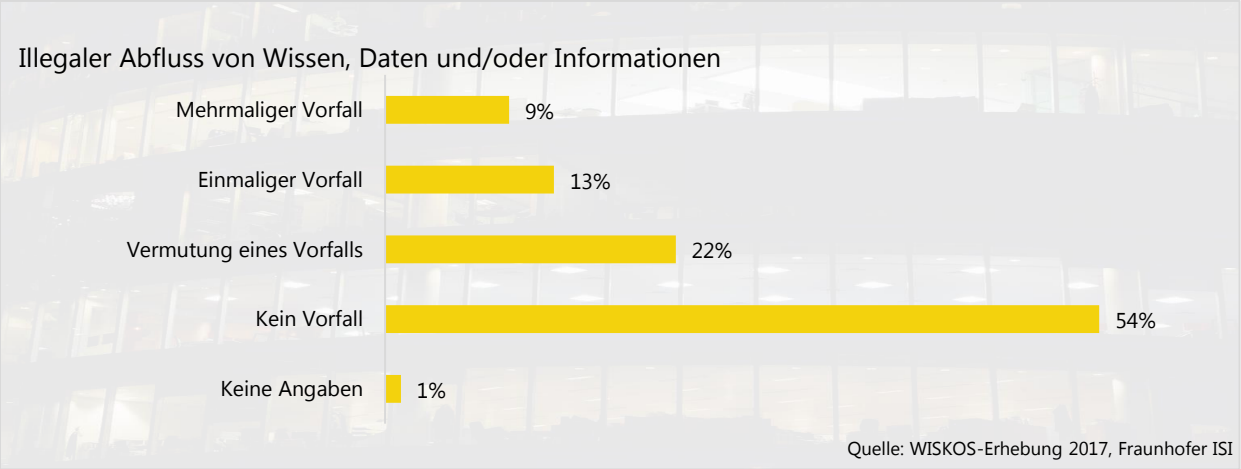
Das Forschungsprojekt WISKOS widmete sich unter Nutzung vielfältiger methodischer Ansätze dem systematisch bislang wenig untersuchten Phänomenbereich der Wirtschaftsspionage und Konkurrenzausspähung in Deutschland, den weiteren EU-Mitgliedstaaten und der Schweiz. Erforscht wurden in einem mehrstufigen Forschungskonzept die rechtlichen und behördlichen Kontrollstrukturen, die Prävalenz der Phänomene im Hell- und Dunkelfeld sowie betriebliche und staatliche Präventionskonzepte. Das Vorhaben konzentrierte sich zunehmend auf die Situation in Deutschland. Neben den spezifischen wissenschaftlichen Interessen verfolgte das Projekt das Ziel, praxisorientierte Empfehlungen für die Optimierung von Präventionsstrategien zu entwickeln und Möglichkeiten für eine verbesserte Kommunikation und Kooperationsbereitschaft von Unternehmen und Wissenschaftsorganisationen mit Behörden aufzuzeigen.

Die entwickelten Informationsmaterialien und Handlungsempfehlungen stehen zum Download bereit.

KMU

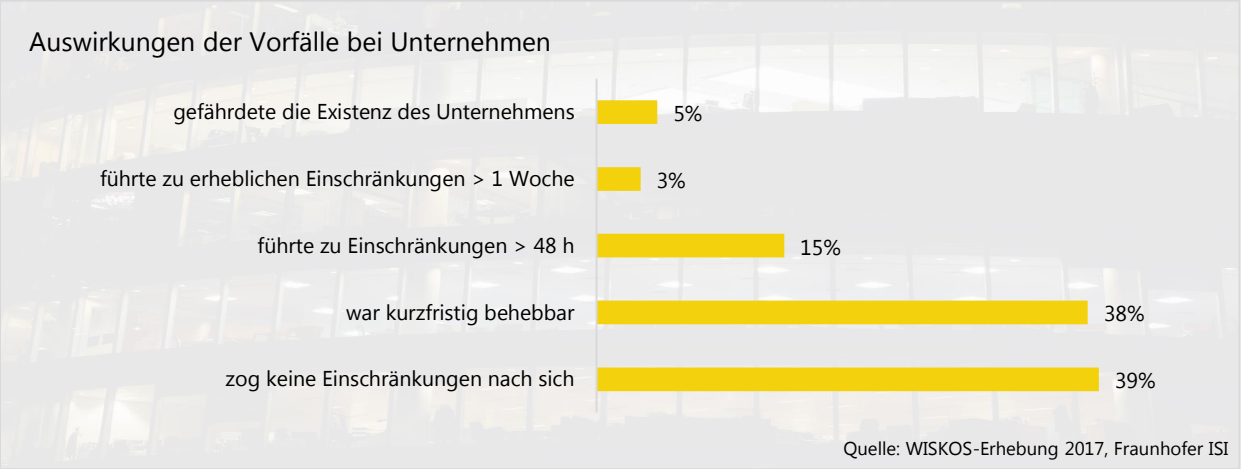
Kleine und mittlere Unternehmen (KMU) in Deutschland sind in gleichem Maße von Wirtschaftsspionage und Konkurrenzausspähung bedroht wie Großunternehmen oder international agierende Konzerne, denn der rapide technische Fortschritt und die Digitalisierung der Gesellschaft bedingen die national wie international zunehmende Wahrnehmbarkeit auch dieser Unternehmensgruppe. Im Gegensatz zu letzteren verfügen KMU jedoch i.d.R. nicht über die finanziellen und personellen Ressourcen für einen umfassenden Unternehmensschutz. Ein solcher wird jedoch benötigt, denn **KMU hatten in den letzten fünf Jahren einen Vorfall oder konkreten Verdachtsfall zu verzeichnen**.

Abbildung 1: Vorliegen eines Vorfalls oder Verdachtsfalls



Schadenssummen sind schwer zu ermitteln oder zu schätzen, betrachtet man jedoch die Dauer der sich aus einem Vorfall oder Verdachtsfall ergebenden Betriebseinschränkungen wird das enorme Schadenspotenzial deutlich: **Für fast ein Viertel der betroffenen Unternehmen bedeutete der Vorfall eine Einschränkung von mindestens 48 Stunden Dauer; 5% davon stuften den Vorfall gar als existenzbedrohend für das Unternehmen ein.**

Abbildung 2: Betriebseinschränkungen



Wissenschaftsorganisationen

Dem deutschen Wissenschaftssektor kommt seit langem in der internationalen Forschungslandschaft große Aufmerksamkeit zu. Doch nicht jede Form von Aufmerksamkeit ist willkommen, denn neben der Forschungslandschaft selbst ziehen auch Forschungsergebnisse Interesse auf sich und wecken Begehrlichkeiten bei ausländischen Staaten, anderen Wissenschaftsorganisationen aber auch Unternehmen, denen sie mit nicht immer legalen Mitteln nachgehen.

Auch hier kann der Schaden, der durch Spionage entsteht, nur schwerlich beziffert werden, denn **belastbare Daten fehlen** und der **Wert von Forschungsergebnissen lässt sich häufig nicht in Zahlen ausdrücken**.

Charakteristika der Spionage

Ungeachtet dessen, ob gegen ein Unternehmen oder eine Wissenschaftsorganisation spioniert wird, das Ziel ist das gleiche. Es geht um geschützte Informationen, seien es Produktskizzen, Prototypen, Kundendaten, Herstellungsformeln, Forschungsergebnisse oder dergleichen mehr.

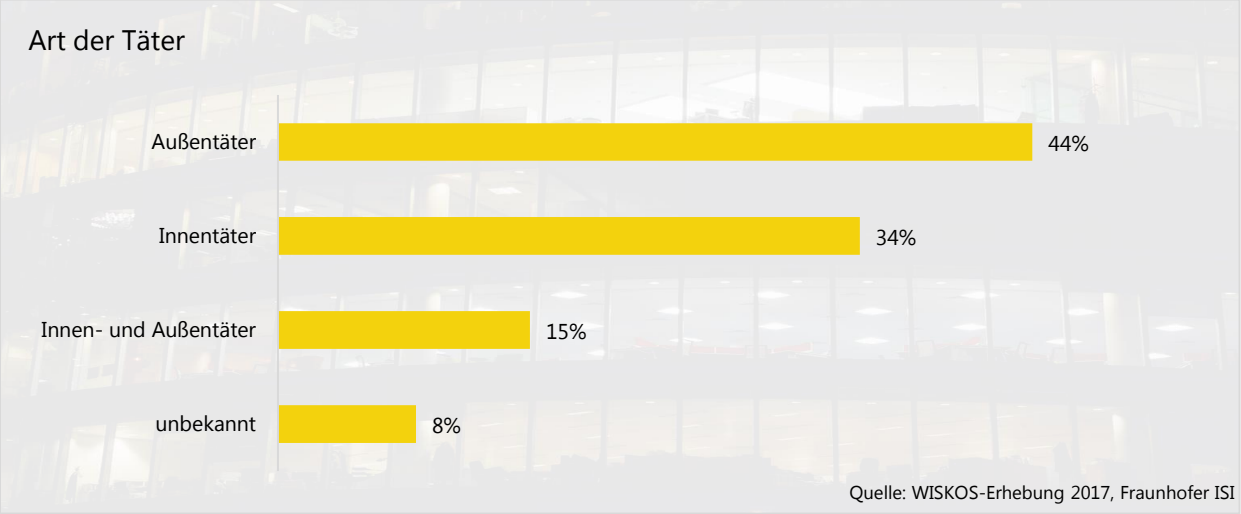
Auch die potenziellen Tätergruppen, ihre konkreten Handlungsweisen und ihre Motive sind gleich.

Die Täter und ihre Handlungsweisen

Die größte potenzielle Gefahr geht von Innentätern aus, denn aufgrund ihres Wissens über z. B. interne Abläufe, Produkte, Kunden oder Investitionen können sie den Wert geschützter Informationen einschätzen und somit gezielt stehlen. Aber auch von externen Akteuren, die im Auftrag von Konkurrenzunternehmen oder ausländischen Geheimdiensten arbeiten oder den

eigenen Profit zum Ziel haben, gehen erhebliche Gefahren aus. Eine weitere Möglichkeit besteht in der Kombination von externer und interner Täterschaft bspw. mittels des sogenannten **Social Engineering**, der zweckgebundenen Manipulation einer Person, um sie zu einer bestimmten Handlung, wie beispielsweise der Weitergabe von geschützten Informationen, zu motivieren.

Abbildung 3: Täterkategorien

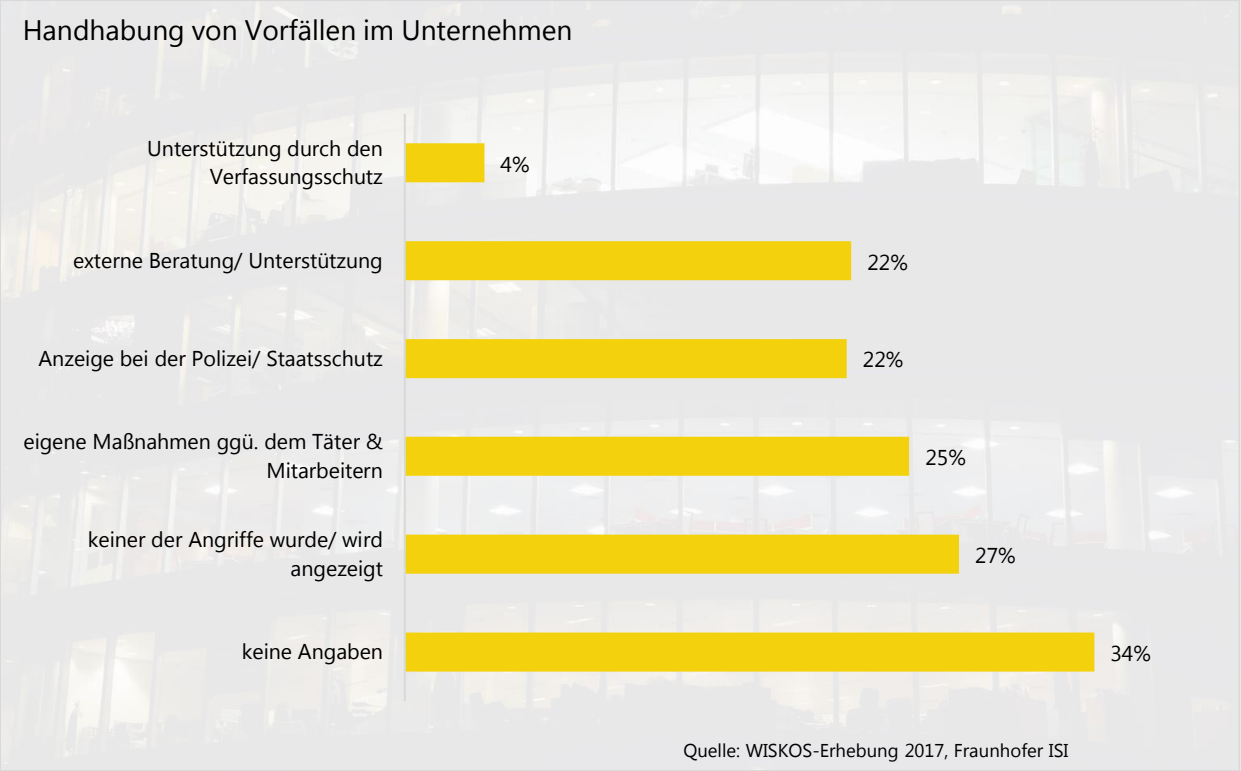


Das konkrete Vorgehen der Täter hängt von der Stellung gegenüber dem Unternehmen bzw. der Organisation ab. Handelt es sich um Innentäter, können diese aufgrund ihres Wissen wertvolle Informationen identifizieren und diese anschließend bspw. kopieren, abfotografieren oder per E-Mail versenden.
Obwohl Externe nicht auf diese Art des Wissens zurückgreifen können, sind ihre möglichen Vorgehensweisen vielfältig. Sie können z.B. bei Werksbesichtigungen und Messeauftritten Produktionsanlagen oder Prototypen abfotografieren oder über Cyberangriffswege auf das Netzwerk des Unternehmens/der Organisation oder Maschinen und Anlagen zugreifen.

Vorgehen im Schadensfall

Ist es zu spät, präventiv tätig zu werden, da bereits ein Vorfall zu verzeichnen ist, herrscht meistens große Unsicherheit über das Vorgehen, um diesen zu bearbeiten. Neben eigenen Maßnahmen gegenüber dem Täter werden häufig **externe Spezialisten** zurate gezogen. Die Möglichkeit der **Erstattung einer Strafanzeige** wird derzeit nur von gut einem **Fünftel der Opfer** wahrgenommen, während **mehr als ein Viertel eine Anzeigeerstattung explizit ausschließt**. Dieser Sachverhalt lässt seitens der Betroffenen Unklarheiten über die behördlichen Zuständigkeiten und den Schutz von Unternehmensgeheimnissen im Strafverfahren vermuten. Auf Basis eines Kosten-Nutzen-Kalküls wird der mit dem Strafverfahren einhergehende Aufwand als zu hoch und der Nutzen als gering eingestuft, sodass regelmäßig von einer Anzeige abgesehen wird.
Welche zusätzlichen Maßnahmen nach Erkennung eines Vorfalls eingeleitet wurden zeigt sich bei einem Blick auf die Befragungsergebnisse der WISKOS-Erhebung.

Abbildung 4: Vorgehen bei einem Vorfall

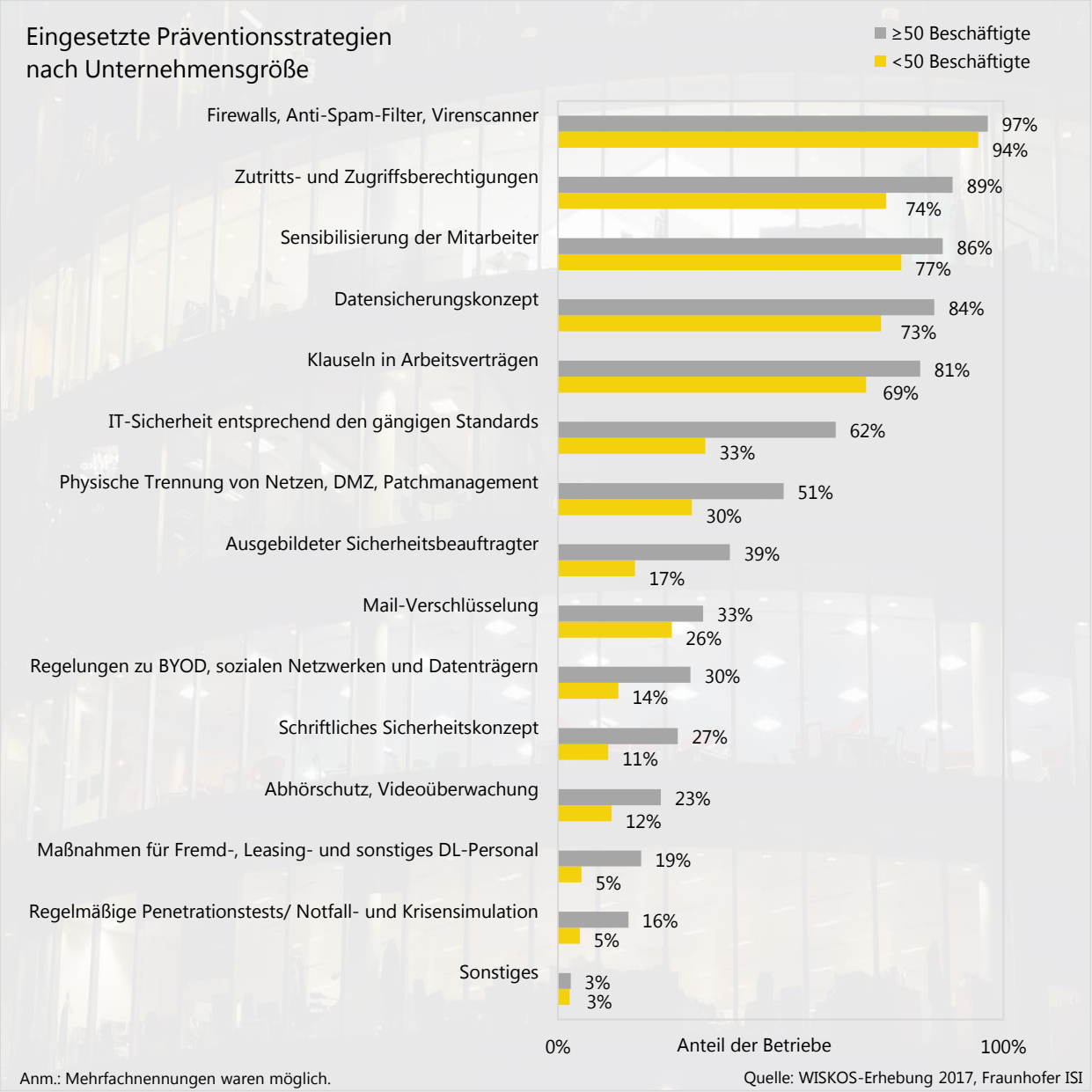


Prävention

Nicht nur die Tatmodalitäten sind die gleichen, sondern auch Möglichkeiten zur Tatprävention und dem Schutz von Know-how sind für Unternehmen wie Wissenschaftsorganisationen gleichermaßen wichtig und umsetzbar. Doch sowohl KMU als auch Wissenschaftsorganisationen sind sich des Wertes ihres Wissens sowie der materiellen und immateriellen Folgen eines Know-how-Diebstahls oft nicht ausreichend bewusst. Deshalb kommt Schutzvorkehrungen sowie der systematischen Beobachtung von Verdachtsindikatoren häufig nicht die gebührende Aufmerksamkeit zu; mit der Folge, dass viele Angriffe unentdeckt bleiben.

Die Möglichkeiten zur Prävention von Know-how-Verlusten sind vielfältig und häufig ohne großen Aufwand umsetzbar; seien es Maßnahmen des IT-Schutzes, Zugangs- und Zutrittskontrollen, Mitarbeiterschulungen, Datenschutzregeln, etc. Diese und weitere Maßnahmen wurden hinsichtlich ihres Verbreitungsgrades in KMU untersucht.

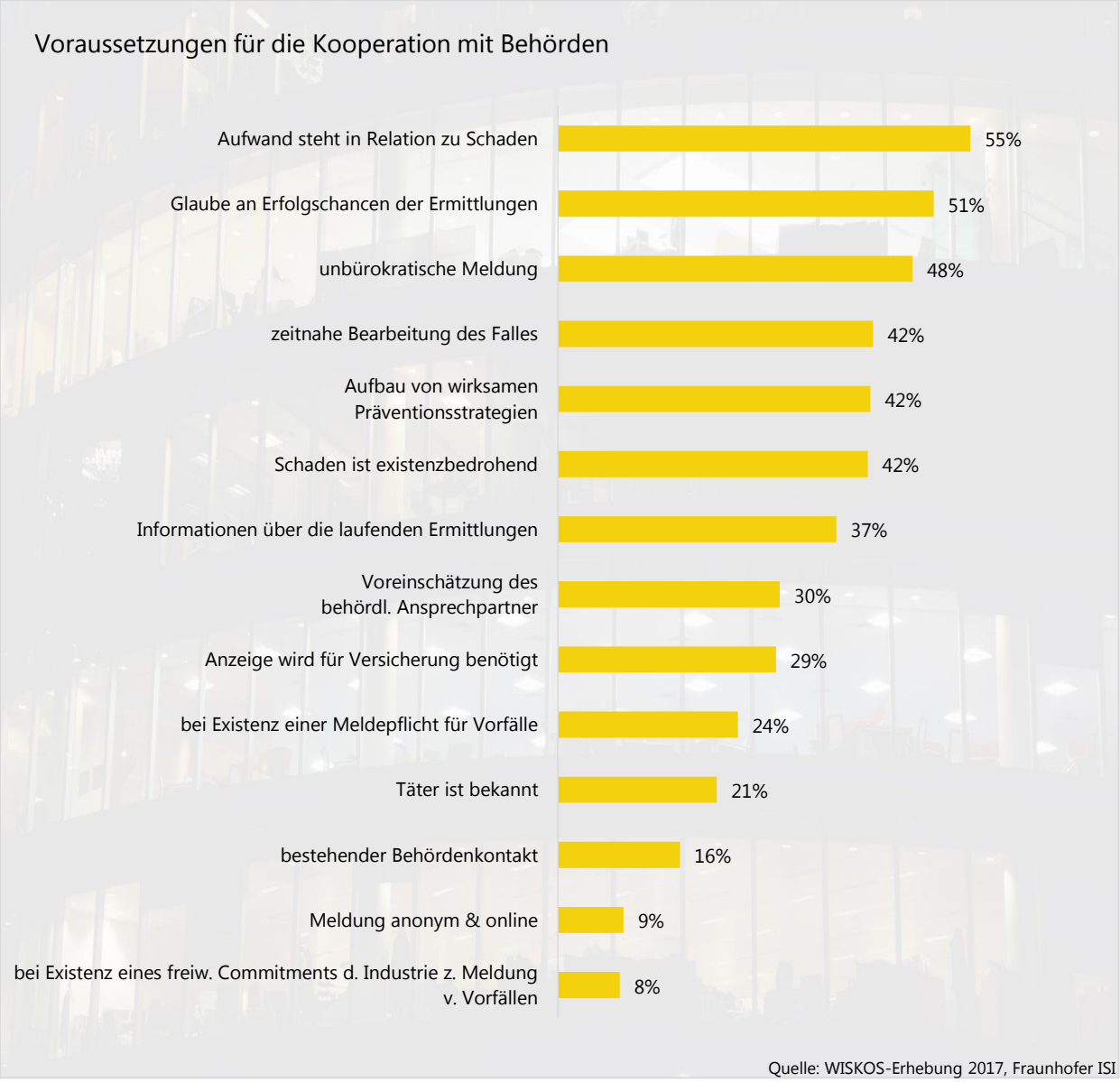
Abbildung 5: Genutzte Präventionsmaßnahmen



Darüber hinaus ist auch die Zusammenarbeit mit den Strafverfolgungsbehörden ein wichtiges Element eines umfassenden Schutzkonzepts. Dies umfasst nicht nur die Anzeige von Vorfällen, sondern setzt bereits viel früher, beim Aufbau von Vertrauen zwischen den Akteuren und der Bekanntmachung von staatlicherseits angebotenen Präventionsangeboten, an.

Hinsichtlich der Kooperationsbereitschaft von KMU mit Behörden zeigt sich, dass lediglich 2% keinesfalls zur Kooperation bereit wären, gut ein Viertel nach eigenen Angaben hingegen in jedem Fall. Wieder andere knüpfen diese Bereitschaft an bestimmte Voraussetzungen.

Abbildung 5: Kooperationsbereitschaft



Fazit

Spionage bedroht Unternehmen gleich welcher Größe und Wissenschaftsorganisationen gleichermaßen. Obwohl keine belastbaren Schadenssummen ermittelt werden konnten, kann davon ausgegangen werden, dass das Schadenspotenzial enorm ist und unter Umständen gar existenzbedrohend sein kann, sodass deutlicher Bedarf an umfassenden Schutzkonzepten besteht. Hier ist das Engagement der potenziell Betroffenen und der Polizei gleichermaßen gefordert. In einem ersten Schritt sind die Unklarheiten bei KMU wie auch Wissenschaftsorganisationen hinsichtlich der zuständigen Ansprechpartner und des Verfahrensablaufs nach einer Anzeigeerstattung abzubauen, um eine breitere Vertrauensbasis zu schaffen, die langfristige Zusammenarbeit zu ermöglichen und so nachhaltig die Anzeigebereitschaft zu erhöhen.