Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie

Studienbericht 2018

www.bitkom.org

bitkom

Herausgeber
Bitkom e.V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner
Teresa Ritter | Bereichsleiterin Sicherheitspolitik und Verteidigung | T 030 27576-203 | t.ritter@bitkom.org

Projektteam
Teresa Ritter | Lukas Gentemann (Bitkom Research GmbH) | Franz Grimm (Bitkom Research GmbH)

Autoren
Michael Bartsch (Deutor Cyber Security Solutions GmbH) | Lukas Gentemann (Bitkom Research GmbH) | Prof. Timo Kob (HiSolutions) | Christoph Krösmann (Bitkom e.V.) | Marco Mille (Siemens AG) | Axel Petri (Telekom) | Teresa Ritter (Bitkom e.V.) | Peter Rost (Rohde & Schwarz Cybersecurity GmbH) | Swantje Schmidt (Capgemini Deutschland) | Marco Schulz (marconcert GmbH) | Dr. Dan Trapp (Bundesamt für Verfassungsschutz) | Lars Wittmaack (QuoScient GmbH) | Torsten Wunderlich (DATEV eG)

Redaktion
Linda van Rennings

Gestaltung
Daniel Vandré

Bildnachweis
Titelbild und Seite 38: © Cherish Bryck – Stocksy United | Seite 51: © Liam Grant – Stocksy United | Seite 56: © Daniel Kim Photography – Stocksy United

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

Vorwort

In Zeiten der zunehmenden Digitalisierung und Vernetzung ist der Wirtschaftsschutz untrennbar mit dem Schutz von Daten, Informationen und IT-Systemen verknüpft. Dadurch erweitern sich die Aufgaben des Wirtschaftsschützers in jedem Unternehmen zusätzlich um die komplexen Fragestellungen der Cyber- und Informationssicherheit. Die Grenzen zwischen der digitalen und der analogen Welt verwischen zunehmend und damit auch die Aufgaben, die immer komplexer werden. Auch werden die jetzt schon knappen Personalressourcen durch die zusätzlichen Aufgaben des Wirtschaftsschutzes im Umfeld der Cybersicherheit belastet.

Der Grad der Digitalisierung in den Unternehmen hat in den letzten Jahren stark zugenommen und dadurch auch Vorfälle im Bereich des Wirtschaftsschutzes, insbesondere durch Datendiebstahl, Industriespionage und Sabotage von Betriebsabläufen. Auch haben diese digitalen IT-Angriffe große Schäden bei den Wirtschaftsunternehmen verursacht. Dazu gehören insbesondere Kosten für Rechtsstreitigkeiten, Imageschäden bei Kunden oder Lieferanten, Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen, Patentrechtsverletzungen und Ausfall, Diebstahl oder Schädigung von Informationssystemen.

Der Täterkreis ist weitreichend und unüberschaubar und reicht vom Innentäter, wie ehemalige Mitarbeiter bis hin zum Außentäter, wie Hacker, konkurrierende Unternehmen, Organisierte Kriminalität (Banden), Kunden und Lieferanten sowie ausländischen Nachrichtendiensten.

Es ist nun zwingend erforderlich, das Zusammenspiel aller Bereiche eines Unternehmens und den Sicherheitsverantwortlichen zu erhöhen, damit der Schutz gegen Cyberspionage, Cybersabotage und Cybercrime nachhaltig erhöht werden kann. Viele Straftaten werden heute digital ausgeführt und somit müssen auch die Lösungen digital sein.

Die Bedeutung und die Abgrenzung der Aufgaben des Wirtschaftsschutzes müssen in Zeiten der Globalisierung, Digitalisierung und Vernetzung neu gedacht oder gar gänzlich neu definiert werden. Wirtschaftsschutz ist Unternehmensschutz und damit sollten die Unternehmen nicht allein gelassen werden. Staatliche Stellen müssen ebenfalls gegen digitale Spionage und Sabotage aufrüsten und Rahmenbedingungen schaffen, die eine Kooperation auf Augenhöhe ermöglicht.

Der Bitkom, als Plattform für die Anbieter der IT-Industrie, der schutzbedürftigen Unternehmen sowie allen relevanten staatlichen Stellen, unterstützt bei der digitalen Transformation des Wirtschaftsschutzes. Alle reden von Kooperation, wir leben diese in den Arbeitskreisen Öffentliche Sicherheit und Wirtschaftsschutz, dem Arbeitskreis Sicherheitspolitik und den technischen Arbeitskreisen zur Cyber- und IT-Sicherheit.

Der digitale Wandel kann nur effektiv sein, wenn er gemeinsam vollzogen wird. Sicherheit, Vertrauen, Lösungswille, ausreichende Budgets und ein starker Kooperationswille sind die Grundlage für eine sichere und vertrauensvolle Zukunft für alle Unternehmensgrößen in Deutschland.

Michael Bartsch
Vorsitzender des AK Öffentliche Sicherheit, Bitkom e.V.

Einleitung

Wir tasten uns gerade in eine neue digitale Ära vor. Allgegenwärtige Konnektivität ist ihr Hauptmerkmal. Intelligente Heizkörper, Kühlschränke und Lampen im Smart-Home-Bereich, vernetzte Autos auf der Straße oder die intelligente Fabrik in der Industrie 4.0: Immer mehr Geräte sind internetfähig. Die Digitalisierung all unserer Lebensbereiche bringt Vorteile für Konsumenten und Chancen für die Wirtschaft. Verbraucher können mehr Lebenskomfort genießen, da sie Zeit und Kosten sparen. Die deutsche und europäische Wirtschaft hat die Chance, das neueste Kapitel der digitalen Transformation mitzugestalten.

Aber nicht nur Verbraucher und Unternehmen profitieren von Vernetzung und Digitalisierung. Vereinfachte Prozesse ermöglichen es auch Kriminellen, Angriffe auf digitale Systeme und Geräte effektiver und erfolgreicher zu gestalten. Cyber-Kriminalität wird dadurch immer lukrativer. Deshalb haben Cyberkriminelle einen finanziellen Anreiz, mehr Brainpower in die Entwicklung von raffinierten Hacking-Methoden zu investieren. Dabei haben Hacker ganz unterschiedliche Motive: Daten werden angegriffen, um das Know-how der Industrie abzuschöpfen oder um Unternehmen durch Erpressungstrojaner zur Auszahlung von Geldsummen zu bewegen. Eindringlinge können gehackte Geräte aber auch dazu missbrauchen, um z. B. DDoS-Angriffe gegen die Internet-Infrastruktur durchzuführen. Somit gerät auch die kritische Infrastruktur in die Schusslinie von Cyberkriminellen. Spektakuläre und medial präsente Fälle, wie beispielsweise WannaCry und NotPetya, sind nur die Spitze des Eisbergs. Unternehmen sowie Behörden und staatliche Einrichtungen werden Opfer von Wirtschaftsspionage, Sabotage und Datendiebstahl und das nahezu täglich.

Aber gerade in der Wirtschaft wird eine große Dunkelziffer darüber vermutet, wie viele Unternehmen tatsächlich Opfer von Hackerangriffen sind. Hierfür gibt es verschiedene Gründe: Zum einen werden Angriffe von den Unternehmen oft erst spät festgestellt und zum anderen wird der Schaden in vielen Fällen gar nicht gemeldet – aus Angst vor Reputationsschäden. Mit der Spezialstudie »Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie« bringt der Bitkom nun zum dritten Mal auf einer validen Datengrundlage Licht ins Dunkle und zieht aus den Ergebnissen Schlüsse für einen umfassenden Wirtschaftsschutz.

Methodik

Der Digitalverband Bitkom untersucht mit der vorliegenden Studie nun zum dritten Mal nach 2016 wie es um die deutsche Industrie beim Thema Wirtschaftsschutz bestellt ist. Welche Unternehmen sind von Spionage, Sabotage und Datendiebstahl betroffen? Wer sind die mutmaßlichen Täter? Und schützt sich die Wirtschaft heute schon ausreichend? Außerdem wurde auch die Höhe der verursachten Schäden ermittelt.

Dafür wurden insgesamt 503 nach Branchen und Größenklassen repräsentativ ausgewählte Industrieunternehmen mit mindestens zehn Mitarbeitern befragt. Die Interviews wurden mit Führungskräften durchgeführt, die in ihrem Unternehmen für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen.

Durch Schichtung der Zufallsstichprobe wurde dabei gewährleistet, dass Unternehmen aus den unterschiedlichen Branchen und Größenklassen in für statistische Auswertungen ausreichender Anzahl vertreten sind. Die Aussagen der Befragungsteilnehmer wurden bei der Analyse gewichtet, sodass die Ergebnisse ein nach Branchengruppen und Größenklassen repräsentatives Bild für alle Industrieunternehmen ab zehn Mitarbeitern in Deutschland ergeben.

Der standardisierte Fragebogen wurde von der Bitkom Research GmbH in Zusammenarbeit mit dem Digitalverband Bitkom konzipiert. Die computergestützten telefonischen Interviews (CATI) wurden im Mai 2018 von im Vorfeld speziell geschulten Telefoninterviewern durchgeführt.

1 Digitalisierungsniveau

Experten-Statement

Marco Mille
Vice President for Security, Siemens AG

Die fortschreitende Digitalisierung schafft nicht nur permanent neue Chancen für die vernetzte Gesellschaft, sondern bietet auch Unternehmen ein enormes Geschäftspotenzial und ein wirksames Mittel zur Steigerung der Wettbewerbsfähigkeit. Bis zum Ende des Jahrzehnts werden rund 50 Milliarden Geräte über das Internet miteinander verbunden sein und unvorstellbare Mengen an Daten liefern. Wir können heute nur ahnen, was künstliche Intelligenz bis dahin leisten können wird. Aber wo Licht ist, ist auch Schatten, wo Chancen sind, gibt es auch Risiken.

So macht uns die zunehmende Digitalisierung abhängiger von Technologien, von Infrastrukturen oder von Dienstleistern, sie kann mitunter einen Kontrollverlust bedingen und sie macht uns anfälliger für gezielte Angriffe oder ungewollte Pannen.

Der Staat, die Unternehmen und jeder einzelne von uns steht daher in der Pflicht, Risiken transparent zu machen und Rahmenbedingungen zu schaffen, um die Digitalisierung sicher zu machen. Dazu gehören z. B. der Schutz kritischer Infrastrukturen und die Schaffung von Regularien für vertrauenswürdige IT und digitale Souveränität, aber auch Unternehmensinitiativen im Bereich Cyber-Sicherheit wie die Charter of Trust. Letztendlich ist es auch die Verpflichtung jedes Einzelnen, sich ein Mindestmaß an Sicherheitsbewusstsein und digitaler Kompetenz anzueignen. Denn bei allen Möglichkeiten, die künstliche Intelligenz vielleicht bieten mag – die Verantwortung tragen letztendlich immer wir Menschen.

1.1 Digitalstrategien der Industrie nach Größenklassen

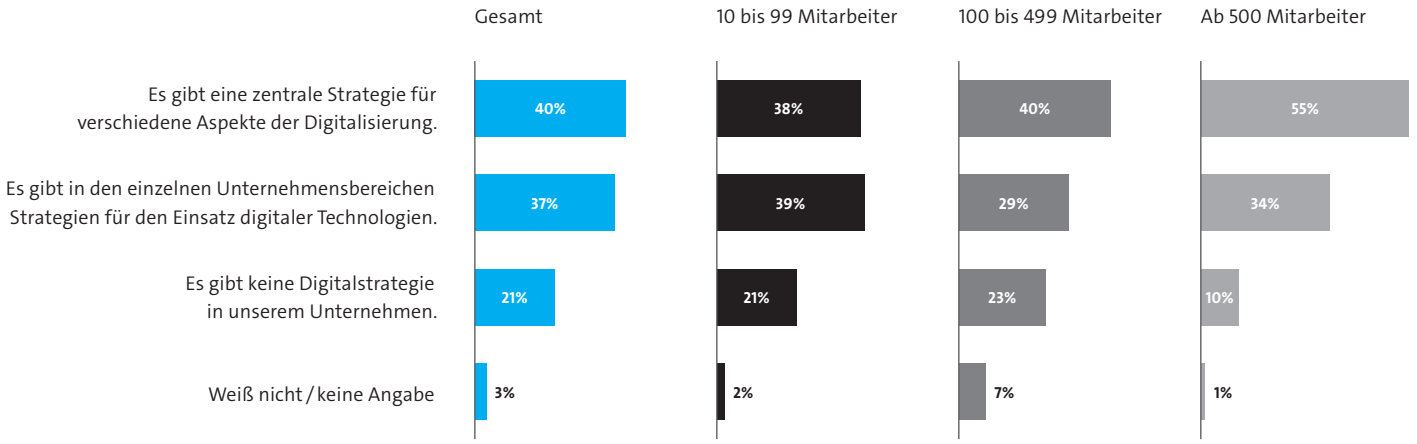
Zu Beginn wurden die Industrieunternehmen gefragt, wie sie die Veränderungen durch den digitalen Wandel aktiv im Unternehmen angehen und ob sie hierfür eine Strategie entwickelt haben bzw. dies in Zukunft tun. Die größeren Industrieunternehmen bereiten sich merklich besser auf die Herausforderungen vor als die kleineren Betriebe.

Noch lange nicht jedes Unternehmen hat eine Digitalstrategie fest in der Unternehmenskultur verankert. Insgesamt haben nur 40 Prozent der befragten Unternehmen eine zentrale Strategie für verschiedene Aspekte der Digitalisierung. Bei den Unternehmen mit mehr als 500 Mitarbeitern wird zumindest in 55 Prozent der Fälle eine Strategie umgesetzt. Bei den kleinen Unternehmen mit 10 bis 99 Mitarbeitern sind es dagegen nur 38 Prozent.

Dagegen stimmten der Frage, ob es keine Digitalstrategie im Unternehmen gäbe, nur 21 Prozent der befragten Unternehmen zu. Bei den Unternehmen mit mehr als 500 Mitarbeitern stimmten dieser Frage sogar nur 10 Prozent zu. Das Gefühl, dass Digitalisierung im Unternehmen angekommen sei, spiegelt sich nicht in einer umfassenden Strategie wider. Aber genau das ist enorm wichtig, um das Unternehmen erfolgreich in das digitale Zeitalter zu führen.

Abbildung 1: Digitalstrategie

Verfolgt Ihr Unternehmen eine Strategie zur Bewältigung des digitalen Wandels?
Basis: Alle befragten Industrieunternehmen (n=503) | Abweichungen von 100 Prozent sind rundungsbedingt
Quelle: Bitkom Research



Experten-Statement

Torsten Wunderlich
Leiter Innovationsbüro Berlin, DATEV eG

Die Transformation hin zu einer Plattformökonomie bedingt, dass sich auch KMU in einer Phase befinden, in der sie ebenfalls Teil eines »Plattform-Ökosystems« werden. Zahlreiche Prozesse sind vollständig – zahlreiche andere aber noch gar nicht digitalisiert oder müssen individuell vor Ort (On-Premise) gesteuert werden. Dieses Stadium der Digitalisierung bedeutet oft eher Zusatzaufwand und noch nicht eine Reduktion von Aufwand und ineffizienten Prozessen und schon gar nicht eine Zunahme sicherer IT-Infrastrukturen. Vielmehr sind die KMU oft noch einer Zunahme an Komplexität ausgesetzt, die durch verschiedenste Standards, Vorgaben und Regelungen, auch im Bereich der IT-Sicherheit, eher noch steigt. KMU sind besonders häufig Angriffen ausgesetzt, sie müssen sich aber momentan weitgehend allein um die Sicherheit ihrer Systeme kümmern.

Setzt sich aber der Trend fort, wonach diejenigen Prozesse und Tätigkeiten, die nicht den unbedingten Kern eines Unternehmens darstellen, zunehmend in Richtung der Partner des Ökosystems verlagert werden, so bieten sich zahlreiche Vorteile gegenüber selbstständig betriebenen On-Premise-Lösungen an. Eine mögliche Entlastung der KMU läge darin, dass IT- und Datensicherheit in der Verantwortung des Partners wären. Die Sicherheit von On-Premise-Lösungen ist mit hohem Aufwand (auf Seiten des Unternehmers) verbunden, während der IT-Support bspw. eines Plattformbetreibers breiter unterstützen, Updates automatisch laufen lassen und insgesamt seine Lösung durch den Einsatz viel größerer Ressourcen sicherer machen kann. Auch Verantwortungen im Zusammenhang mit Archivierungs- und weiteren Compliancepflichten könnten dann auf Plattformbetreiber übergehen und so den Unternehmer vor Datenverlusten schützen. Rechenzentren bieten im Gegensatz zu lokalen Speichermedien eine zuverlässige Langzeitarchivierung. Unternehmen können somit Daten »einfach« in Rechenzentren laden und müssen nicht selbst auf Speichermedien sicherstellen, dass sie sich an regulatorische Archivierungspflichten von mehreren Jahren halten. Ihre Daten sind bei spezialisierten Partnern oft besser gegen Diebstahl, Verlust und Zerstörung geschützt. Und das ist aktiver Wirtschaftsschutz.

1.2 Kleinere Unternehmen weiterhin weniger digital

Ein Überblick über die Betriebsgrößenklassen zeigt, dass die kleineren Industrieunternehmen den Grad ihrer Digitalisierung am geringsten einschätzen. Nur 16 Prozent der Industrieunternehmen mit 10 bis 99 Mitarbeitern stufen den Digitalisierungsgrad ihres Unternehmens als sehr hoch ein, weitere 21 Prozent schätzen ihr Unternehmen als eher hoch digitalisiert ein. Der größte Anteil (37 Prozent), bewertet den Stand der Digitalisierung als sehr niedrig.

Unternehmen mit 100 bis 499 Mitarbeitern sind nach eigenen Angaben zu 18 Prozent hoch digitalisiert, 30 Prozent schätzen ihren Digitalisierungsgrad eher hoch ein. Hier sind es 20 Prozent, die sich als sehr niedrig digitalisiert einschätzen.

Bei den Unternehmen mit mehr als 500 Mitarbeitern ist der Anteil der sich sehr hoch digital einschätzenden Unternehmen mit 36 Prozent am höchsten. Weitere 24 Prozent meinen, eher hoch digitalisiert zu sein. 5 Prozent der Unternehmen schätzen ihren Digitalisierungsgrad als sehr niedrig ein.

Dieser Unterschied zwischen den Größenklassen macht einmal mehr deutlich, dass große Unternehmen die Digitalisierung bereits in der Unternehmenskultur verankert haben. Durch ihre Größe fällt es ihnen leichter genügend Personal auf dieses Thema anzusetzen. Kleine Unternehmen haben in vielen Fällen nicht einmal eine eigene IT-Abteilung, geschweige denn Personal, das sich strategisch um die Digitalisierung des Unternehmens kümmert.

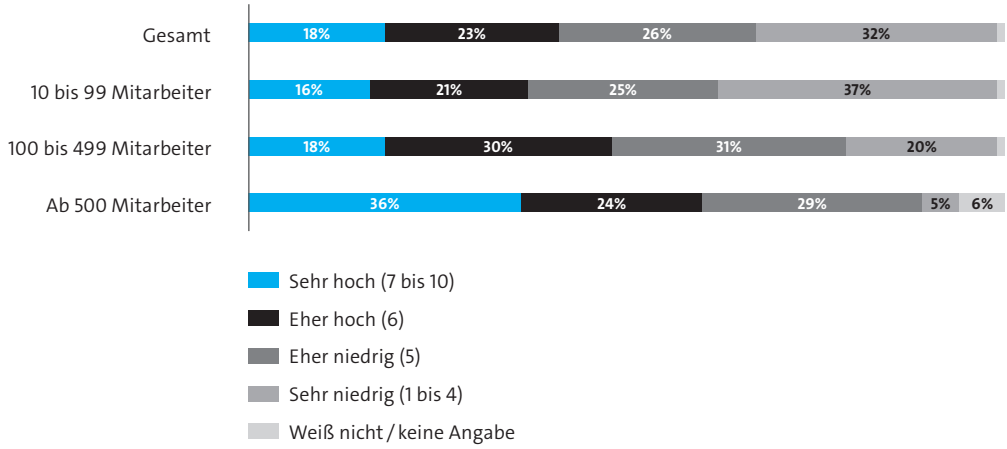


Abbildung 2: Grad der Digitalisierung Gesamt und nach Betriebsgrößenklasse

Wie hoch würden Sie den Grad der Digitalisierung Ihres Unternehmens einstufen?
Basis: Alle befragten Industrieunternehmen (n=503) | Abweichungen von 100 Prozent sind rundungsbedingt
Quelle: Bitkom Research

2 Betroffene Industrieunternehmen

»Mit ihren Weltmarktführern ist die deutsche Industrie besonders interessant für Kriminelle. Wer nicht in IT-Sicherheit investiert, handelt fahrlässig und gefährdet sein Unternehmen.«

Achim Berg, Bitkom-Präsident, Berlin 2018

Experten-Statement

Peter Rost
Director Business Development and Strategy,
Rohde & Schwarz Cybersecurity GmbH

Digitalisierung bedeutet für die Wirtschaft heute vorwiegend die Einführung von vernetzten Maschinen, Sensoren und Steuerungen. Oft werden vorhandene Maschinen internetfähig nachgerüstet. Den massiven Produktivitäts- und Flexibilitätsvorteilen des industriellen Internet of Things steht allerdings die kaum nachvollziehbare Komplexität solcher Systeme aus Endgeräten, Netzwerken, Anwendungen und Nutzern gegenüber. Mit dem Ansatz »Functionality first, Cybersecurity later« haben schon einige Vorreiter schlechte Erfahrungen gemacht.

Über die gehackte Webcam in die Robotersteuerung eingedrungene Angreifer können enormen materiellen Schaden anrichten. Über die Einbeziehung des »Security by Design«-Gedankens entstehen resiliente Digitalisierungskonzepte, sodass digitale Wertschöpfungsprozesse von Anfang an hochverfügbar sind und Datenschutz zu rentablen Kosten möglich wird. Ergänzt durch ein laufendes Netzwerkmonitoring und ein konsequentes Patch-Management gehen digital transformierte Unternehmen den meisten Problemen aus dem Wege.

7 von 10 Unternehmen sind Opfer geworden

Der überwiegende Teil aller Industrieunternehmen in Deutschland ist von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen oder vermutet betroffen zu sein. 68 Prozent der Industrieunternehmen gaben an in den vergangenen zwei Jahren Opfer von Datendiebstahl, Industriespionage oder Sabotage gewesen zu sein. Weitere 19 Prozent waren vermutlich betroffen – denn nicht immer lässt sich zweifelsfrei feststellen, ob wirklich Daten abgeflossen sind oder ein Angriff nicht entdeckt wurde.

Mittelstand weiterhin im Fokus der Angreifer

Drei von vier Unternehmen (73 Prozent) in der Größe von 100 bis unter 500 Mitarbeitern waren betroffen. Der Mittelstand in Deutschland ist besonders innovativ und stark in die Lieferketten von großen Konzernen eingebunden. Insofern liegt es nahe, dass es Angreifer zum einen auf das Spezialwissen der KMU abgesehen haben. Und zum anderen KMU als Einfallstore nutzen, um an die Daten großer Konzerne zu kommen. In der Regel schützen sich Großkonzerne besser. Bei Unternehmen mit mehr als 500 Mitarbeitern sind deutlich weniger Unternehmen angegriffen worden – 60 Prozent der Unternehmen gaben an, betroffen gewesen zu sein, weitere 28 waren vermutlich betroffen. 68 Prozent der Unternehmen mit 10 bis 99 Mitarbeiter waren Opfer von Spionage, Sabotage und Datendiebstahl.

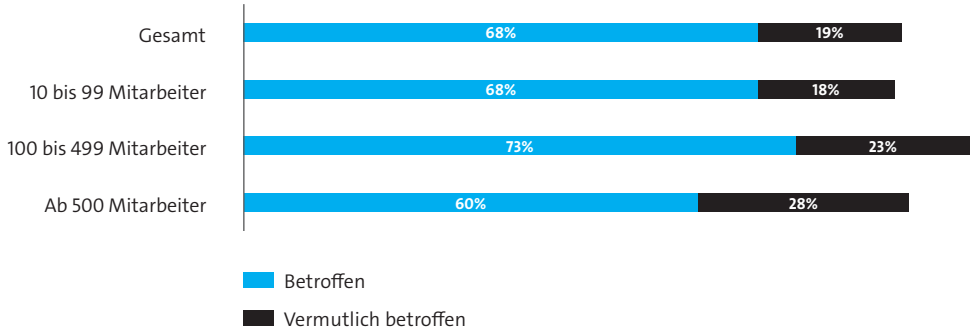


Abbildung 3: Betroffene Unternehmen nach Betriebsgrößenklasse

War Ihr Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen bzw. vermutlich betroffen?

Basis: Alle befragten Industrieunternehmen (n=503) | zu 100 Prozent fehlende Prozente entfallen auf »Nicht betroffen« & »Weiß nicht / keine Angabe«
Quelle: Bitkom Research

2.1 Diebstahl von Daten und Datenträgern ist häufigster Vorfall

Nachdem festgestellt wurde, welche Unternehmen von Attacken betroffen waren, wurden diese zu den jeweiligen Delikten befragt. Am häufigsten wurden in den letzten zwei Jahren IT- und Telekommunikationsgeräte gestohlen, wie etwa Notebooks oder Smartphones. 32 Prozent der befragten Industrieunternehmen waren davon betroffen. Die Täter können es hierbei auf die Hardware oder auf die Daten, die sich auf der Hardware befinden, abgesehen haben.

Vom Diebstahl sensibler digitaler Daten waren 23 Prozent der Unternehmen betroffen. Sensible physische Dokumente, Muster, Bauteile oder sogar Maschinen wurden bei jedem fünften der betroffenen Industrieunternehmen (21 Prozent) gestohlen. Dies zeigt, dass die Verbindung von physischer Sicherheit und Cybersicherheit ein wesentliches Thema für die Unternehmenssicherheit ist. Jedes dritte Unternehmen berichtet von der Sabotage ihrer IT-Systeme oder Betriebsabläufe. Der Anteil der vermuteten Angriffe ist hier am höchsten. Immerhin über ein Viertel der Industrieunternehmen (28 Prozent) vermuten, sabotiert worden zu sein.

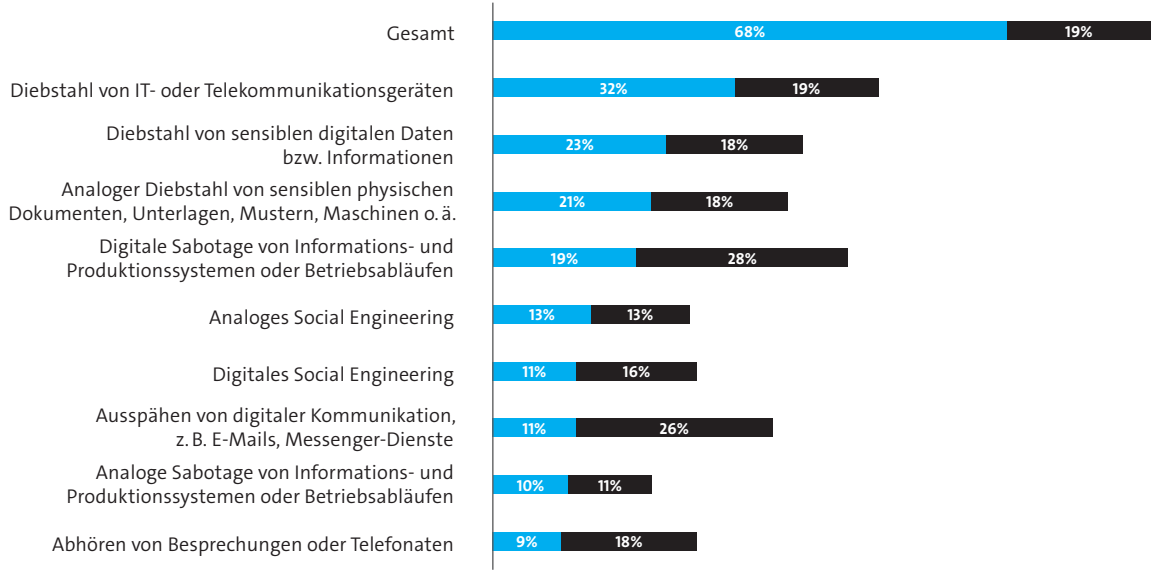


Abbildung 4: Vorfälle im Bereich Wirtschaftsschutz

Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der letzten 2 Jahre betroffen bzw. vermutlich betroffen?
Basis: Alle befragten Industrieunternehmen (n=503) | zu 100 Prozent fehlende Prozente entfallen auf »Nicht betroffen« & »Weiß nicht / keine Angabe«
Quelle: Bitkom Research

13 Prozent der Industrieunternehmen registrierten in den vergangenen zwei Jahren Fälle von analogem, 11 Prozent von digitalem Social Engineering. Bei dieser Methode werden Mitarbeiter manipuliert, um an bestimmte Informationen zu gelangen. Gezielte Hacking- oder Phishing-Angriffe sind meist die Vorläufer des Social Engineerings. Mithilfe von Informationen aus dem Umfeld der Mitarbeiter werden dann beispielsweise täuschend echte E-Mails von vermeintlichen Bekannten, oftmals Mitgliedern der Unternehmensführung, verfasst. Der Anhang dieser Mails ist meist mit Schadstoff infiziert. Durch das Öffnen des Anhangs gelangen beispielsweise Trojaner auf die Computer, die in der Folge Passwörter und andere Daten auslesen.

Das Ausspähen elektronischer Kommunikation trat in 11 Prozent der Fälle auf. Das Abhören von Telefonaten oder Besprechungen gehört eher zu den selteneren Fällen der Wirtschaftsspionage. Neun Prozent der Industrieunternehmen haben nach eigenen Angaben in den vergangenen zwei Jahren solche Angriffe festgestellt und weitere 18 Prozent vermuten dies.

Sabotage, Spionage und Datendiebstahl zielen im wirtschaftlichen Umfeld auf digitale Daten oder die Informations- und Kommunikationsinfrastruktur der Industrieunternehmen ab. Durch die fortgeschrittene Digitalisierung fällt es Kriminellen zunehmend leicht, an diese Daten zu gelangen.

2.2 Chemie- und Pharmabranche am stärksten betroffen

Besonders betroffen waren in den vergangenen zwei Jahren die Chemie- und Pharmabranche sowie der Automobilbau. 74 Prozent der befragten Unternehmen aus der Chemie- und Pharmabranche waren betroffen, zusätzliche 22 Prozent vermutlich betroffen. Im Automobilbau gaben 68 Prozent der Unternehmen an, Opfer von Angriffen gewesen zu sein und weitere 22 Prozent vermuten dies. Aber auch der Maschinen- und Anlagenbau sowie die Hersteller von Kommunikations- und Elektrotechnik sahen sich einer Vielzahl an Attacken ausgesetzt. Die produzierende Wirtschaft in Deutschland ist besonders innovativ und in vielen Bereichen Weltmarktführer. Damit rückt dieser Teil der Wirtschaft immer wieder besonders stark in den Fokus von Hackern.

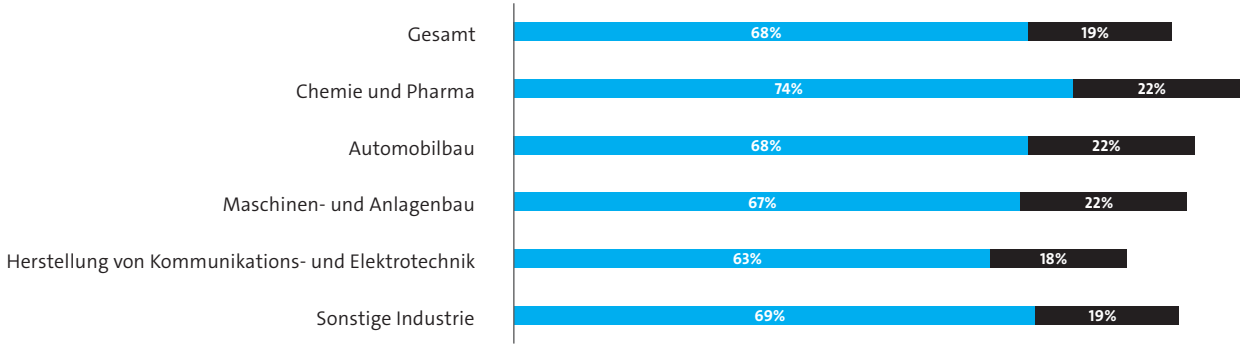


Abbildung 5: Betroffene Unternehmen nach Branchen

War Ihr Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen bzw. vermutlich betroffen?
Basis: Alle befragten Unternehmen (n=503) | zu 100 Prozent fehlende Prozente entfallen auf »Nicht betroffen« & »Weiß nicht / keine Angabe«
Quelle: Bitkom Research

2.3 Höher digitalisiert – geringer betroffen

Ein besonderes Augenmerk wurde bei der Befragung auf die Betroffenheit von Unternehmen im Zusammenhang zu ihrem Digitalisierungsniveau gelegt. Experten gehen eigentlich davon aus, dass die zunehmende Vernetzung auch zu steigenden Sicherheitsrisiken führt. Damit müssten stärker digitalisierte Unternehmen auch stärker von Cyberkriminalität betroffen sein.

Die Ergebnisse jedoch zeigen, dass das Gegenteil der Fall ist. Der Anteil betroffener Industrieunternehmen, die ihren Digitalisierungsgrad hoch einschätzen, ist um 7 Prozentpunkte geringer als bei den Unternehmen, die ihr Digitalisierungsniveau niedrig einschätzen. Dies deckt sich in etwa mit den Ergebnissen aus dem Jahr 2016.

Unternehmen, die sich verstärkt mit der Digitalisierung auseinandersetzen und beispielsweise Strategien etablieren, sind automatisch auch für das Thema IT-Sicherheit sensibilisiert. Offenbar ist denjenigen Unternehmen, die sich stärker digitalisieren, die damit wachsende Angriffsfläche bewusst. Deshalb werden Sicherheitsstandards etabliert und ein effektiver Schutz gegen IT-Angriffe garantiert.

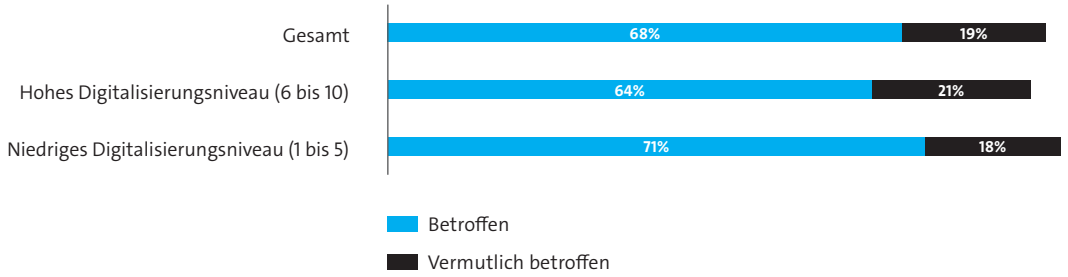


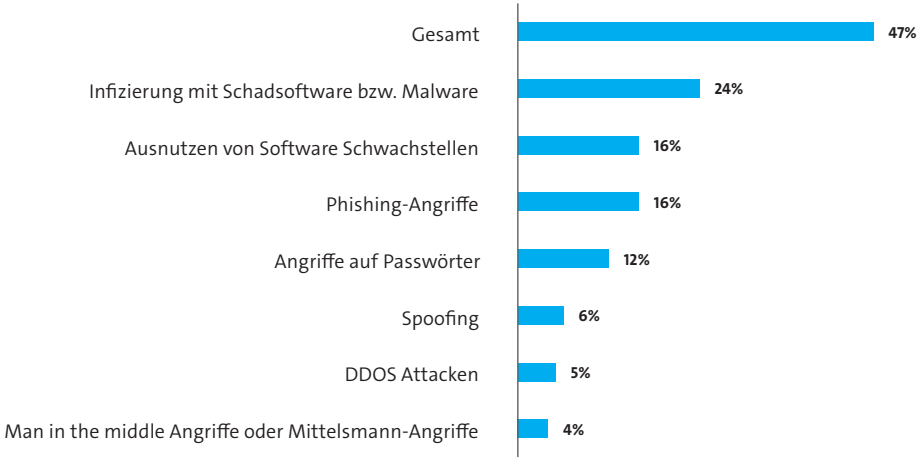
Abbildung 6: Betroffene Unternehmen nach Digitalisierungsniveau

War Ihr Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen bzw. vermutlich betroffen?

Basis: Alle befragten Industrieunternehmen (n=503) | zu 100 Prozent fehlende Prozente entfallen auf »Nicht betroffen« & »Weiß nicht / keine Angabe«
Quelle: Bitkom Research

2.4 Fast die Hälfte erleidet Schäden durch digitale Angriffe

Digitale IT-Angriffe sind für sehr viele Industrieunternehmen ein Problem. Fast die Hälfte von ihnen ist dadurch in den vergangenen zwei Jahren zu Schaden gekommen. Ein Viertel berichtet von der Infizierung mit Schadsoftware, jedes sechste Unternehmen kam jeweils zu Schaden aufgrund von ausgenutzten Software-Schwachstellen oder Phishing-Angriffen. Das sogenannte Spoofing führte bei 6 Prozent zu Schäden. Das sind jene Methoden, mit denen sich Authentifizierungs- und Identifikationsverfahren untergraben lassen, etwa indem IP-Pakete beim Datentransfer manipuliert werden und falsche Absenderinformationen tragen.
Auch bei digitalen Angriffen zeigt sich, dass Mittelständler häufiger zu Schäden kommen als kleine oder große Industrieunternehmen.



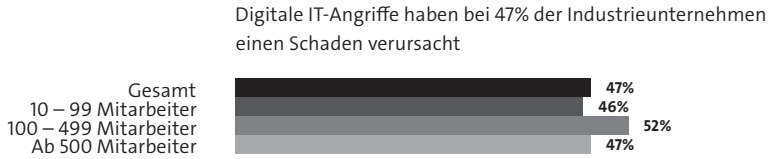


Abbildung 7: Schäden durch IT-Angriffe

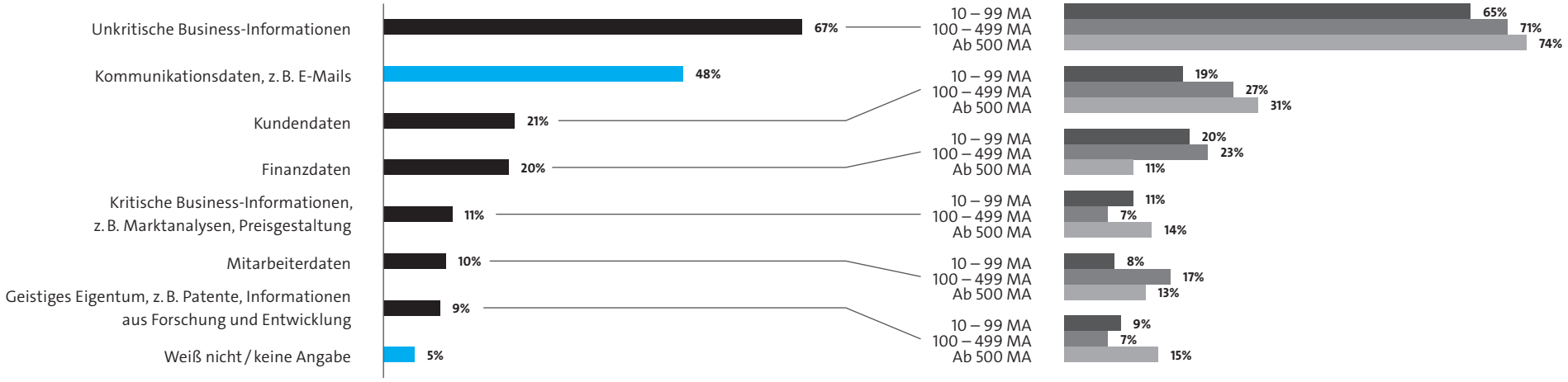
Welche der folgenden Arten von digitalen IT-Angriffen haben innerhalb der letzten 2 Jahre in Ihrem Unternehmen einen Schaden verursacht?
Basis: Alle befragten Industrieunternehmen (n=503) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

2.5 Vor allem Mails, Kunden- und Finanzdaten fließen ab

Datendiebstahl war eins der häufigsten Delikte, von denen die befragten Unternehmen in den letzten zwei Jahren betroffen waren. Deshalb widmete sich die Studie auch der Frage, welche Daten entwendet wurden. Sehr häufig sind es unkritische Geschäftsinformationen gewesen, mit denen die Angreifer vermutlich wenig anfangen konnten. Bei 48 Prozent der Unternehmen, wurden Kommunikationsdaten wie E-Mails entwendet. Kunden- und Finanzdaten flossen in ca. 20 Prozent der Fälle ab. 11 Prozent der Unternehmen meldeten den Verlust von Kritischen Business-Informationen, z. B. Marktanalysen und Informationen zur Preisgestaltung. Mitarbeiterdaten und geistiges Eigentum flossen bei ca. 10 Prozent der betroffenen Unternehmen ab. Damit sollte jedem Verantwortlichen klar werden, dass der Schutz digitaler Daten höchste Priorität verdient.

Abbildung 8: Gestohlene digitale Daten

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Diebstahl von sensiblen digitalen Daten betroffen waren (n=205) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research



2.6 Häufigstes Angriffsziel: Die IT (Administration oder Service)

Häufigstes Angriffsziel war in den letzten zwei Jahren die IT (Administration oder Service) der Unternehmen. Bei mehr als einem Drittel der betroffenen Unternehmen (37 Prozent) war die IT befallen. An zweiter Stelle steht der Lager- und Logistikbereich. Er wurde in 29 Prozent der Fälle angegriffen. Auch die Produktion und Fertigung sowie die Geschäftsführung bzw. das Management waren ein beliebtes Ziel der Attacken (jeweils 27 Prozent). Im Hinblick auf die zunehmende Vernetzung der Produktion und Fertigung im Rahmen von Industrie 4.0 ist zu erwarten, dass die Angriffe zukünftig steigen werden. Durch die Vernetzung wächst die Angriffsfläche für Kriminelle.

Es folgen weiter die Bereiche Finanz- und Rechnungswesen (24 Prozent), Marketing und Vertrieb (18 Prozent) sowie Personalwesen und Human Resources (17 Prozent). Weniger betroffen sind Forschung und Entwicklung (15 Prozent) und Einkauf (11 Prozent).

Dass der Bereich Forschung und Entwicklung mit 15 Prozent fast an letzter Stelle liegt, mag überraschen. Da die meisten kleinen Industrieunternehmen aber oft über keine eigenen Forschungs- und Entwicklungsabteilungen verfügen, können diese auch nicht angegriffen werden. Deshalb wundert es nicht, dass mehr als ein Drittel (22 Prozent) der großen Industrieunternehmen ab 500 Mitarbeitern Angriffe auf ihre F&E-Bereiche verzeichneten. Im Vergleich zur letzten Studie aus dem Jahr 2016 ist das allerdings ein starker Rückgang. Dies könnte daran liegen, dass große Unternehmen ihre F&E-Bereiche aufgrund der zahlreichen Attacken in den Jahren 2014/2015 mittlerweile stärker schützen.

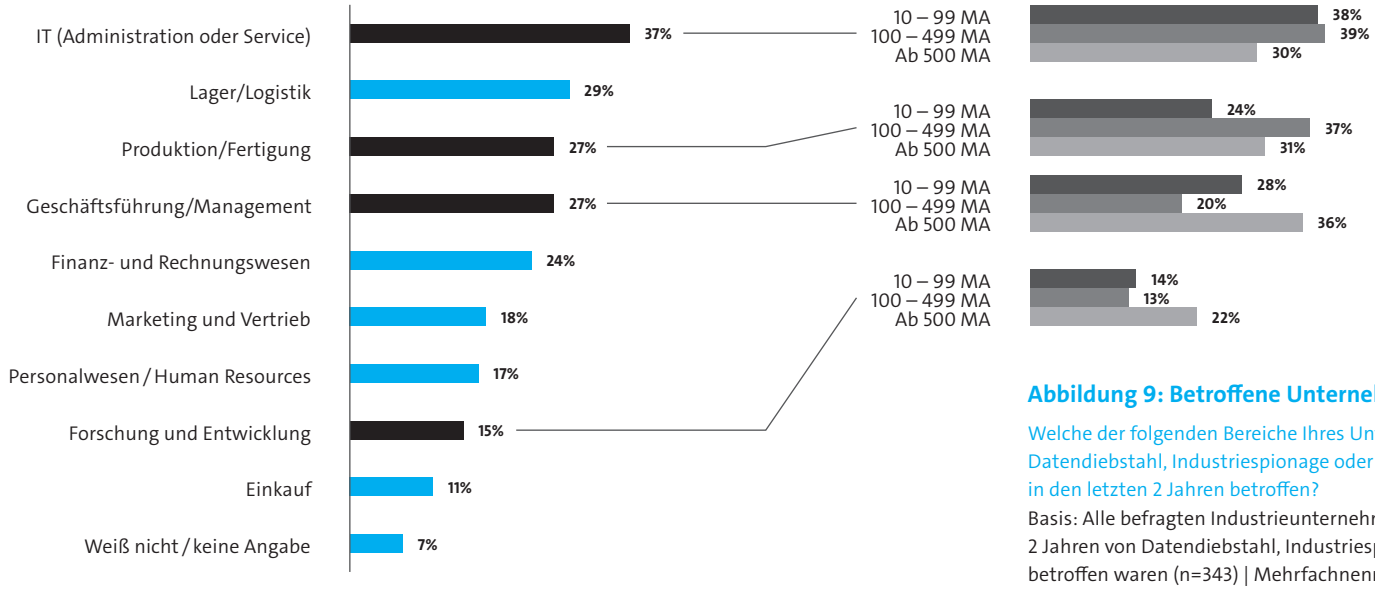


Abbildung 9: Betroffene Unternehmensbereiche

Welche der folgenden Bereiche Ihres Unternehmens waren von Datendiebstahl, Industriespionage oder Sabotage (vermutlich) in den letzten 2 Jahren betroffen?

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

2.7 Imageschäden bei Kunden und Lieferanten ist größter Kostenverursacher

Die Schäden der betroffenen Unternehmen sind hoch. Dabei ist es besonders interessant zu sehen, welche Arten von Schäden es gibt und zu welchen Anteilen sie Kosten bei den betroffenen Unternehmen verursachen.

An erster Stelle liegen dabei Reputationsschäden bei Kunden oder Lieferanten. Das berichteten 41 Prozent der betroffenen Unternehmen. Datenschutzrechtliche Maßnahmen, die nach einem Angriff durchgeführt werden müssen, verursachten bei 40 Prozent der betroffenen Unternehmen Kosten. Ausfall oder Schädigung von Informationssystemen sind bei über einem Viertel (27 Prozent) angefallen, ebenso wie Kosten für Rechtsstreitigkeiten (27 Prozent). Rechtsstreitigkeiten sind insbesondere für Unternehmen mit mehr als 100 Mitarbeitern ein Kostentreiber (100–499 Mitarbeiter: 44 Prozent, 500 + Mitarbeiter: 41 Prozent). Fast jedes zwölfte Unternehmen verzeichnete Umsatzeinbußen (8 Prozent) als direkte Konsequenz. Dazu kommen Patentrechtsverletzungen (18 Prozent) und allgemeine Kosten für die Aufklärung der Angriffe (16 Prozent).

Hervorzuheben ist auch, dass die entstandenen Kosten für Ausfall, Diebstahl oder Schädigung von Informationssystemen insbesondere bei Unternehmen mit mehr als 500 Mitarbeitern aufgetreten sind. 40 Prozent der Unternehmen dieser Größenklasse gaben das an.

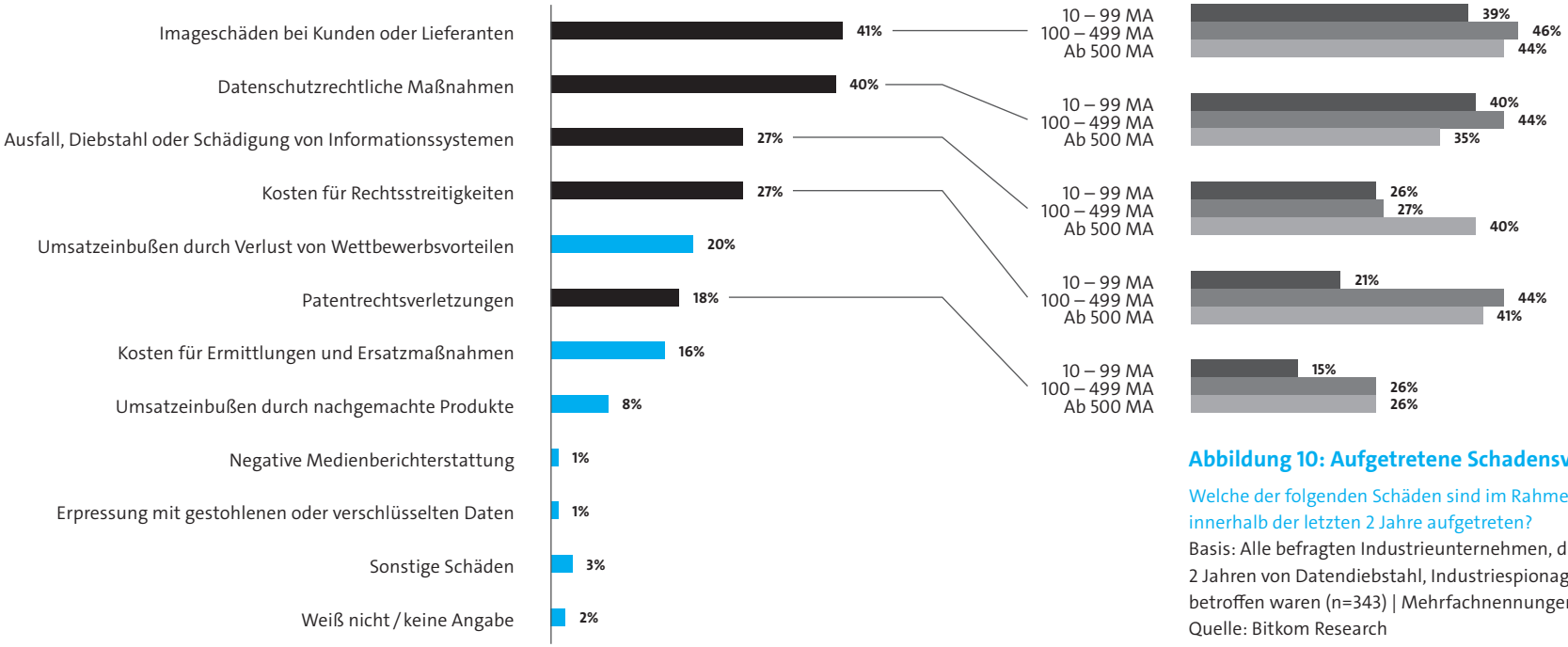


Abbildung 10: Aufgetretene Schadensvorfälle 2018

Welche der folgenden Schäden sind im Rahmen dieser Handlungen innerhalb der letzten 2 Jahre aufgetreten?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

3 Aufgetretene Schäden

»Illegaler Wissens- und Technologie-transfer, Social Engineering und auch Wirtschaftssabotage sind keine seltenen Einzelfälle, sondern ein Massenphänomen.«

Thomas Haldenwang, Vizepräsident des Bundesamtes für Verfassungsschutz (BfV), Berlin 2018

3.1 Schadenrechnungsmodell

Das zentrale Ziel dieser Studie ist die Bestimmung des Gesamtschadens, der durch Wirtschaftsspionage, Sabotage oder Datendiebstahl in der deutschen Industrie in den zurückliegenden zwei Jahren entstanden ist. Um die Vergleichbarkeit der vorliegenden Studie zu gewährleisten, wurden Fragebogen und Vorgehensweise vergleichbar zu ihrem Vorgänger, der Spezialstudie Wirtschaftsschutz 2016, gestaltet und die Methode nicht verändert.

Allen befragten Unternehmen wurde der Fragebogen vor dem Telefoninterview zur Verfügung gestellt. Zu Beginn des Gesprächs wurden die Unternehmen gefragt, von welchen Handlungen, wie z. B. Diebstahl von IT-Geräten oder sensiblen Dokumenten, diese innerhalb der letzten zwei Jahre betroffen waren. Dann wurde ermittelt, welche Schadensdelikte überhaupt innerhalb der letzten zwei Jahre aus diesen Handlungen aufgetreten sind. In einem weiteren Schritt wurden dann die Schadenssummen für die einzelnen aufgetretenen Delikte abgefragt. Die genannten Summen wurden während des Telefoninterviews automatisch aufaddiert und dem befragten Unternehmen bei der abschließenden Frage nach dem Gesamtschaden genannt. Damit hatte jeder Teilnehmer die Möglichkeit, die Teilschadenssummen sowie die Summe des Gesamtschadens abschließend zu verifizieren.

Schließlich wurden die durchschnittlichen Schadenssummen für die einzelnen Delikte auf die deutsche Industrie hochgerechnet. Bei der Berechnung der Durchschnittswerte bzw. Mittelwerte wurde das sogenannte »5 Prozent getrimmte Mittel« verwendet. Hierbei werden 2,5 Prozent der kleinsten und 2,5 Prozent der größten Werte ausgeblendet und der Mittelwert über die verbliebenen Werte berechnet. Die durchschnittlichen Schadenssummen sind somit um Ausreißer nach oben und unten bereinigt. Folglich kann man von einer eher konservativen Berechnung der Schadenssummen sprechen. Die Hochrechnung erfolgte auf der Grundlage der Umsatzsteuerstatistik des Statistischen Bundesamtes, die aktuell rund 66.000 Industrieunternehmen ab 10 Mitarbeitern ausweist. Basis für die Hochrechnung sind alle betroffenen Industrieunternehmen mit einem nachweislichen finanziellen Schaden. Das sind 68 Prozent der befragten Unternehmen und entspricht rund 45.000 Unternehmen.

3.2 43,4 Milliarden Euro Schaden in den letzten zwei Jahren

Der Schaden als Folge digitaler Wirtschaftsspionage, Sabotage und Datendiebstahls liegt nach konservativen Berechnungen bei rund 43,4 Mrd. Euro in den letzten zwei Jahren. Jeweils mehr als ein Fünftel dieser Summe geht auf Imageschäden bei Kunden oder Lieferanten bzw. negative Medienberichterstattung (8,8 Mrd. Euro pro Jahr) sowie auf Patentrechtsverletzung (8,5 Mrd. Euro) zurück. Ein solcher Reputationsverlust kann im schlimmsten Fall ein Unternehmen in seiner Existenz gefährden.

An dritter Stelle liegen Umsatzeinbußen durch Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen. Hier wurden 6,7 Milliarden Euro in den letzten beiden Jahren verursacht. Hohe Kosten verursachten außerdem Ermittlungen und Ersatzmaßnahmen. Geschätzt wird der Schaden hier auf 5,7 Milliarden. Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen (4,0 Mrd. Euro pro Jahr), Umsatzeinbußen durch nachgemachte Produkte (3,7 Mrd. Euro pro Jahr) und Kosten für Rechtsstreitigkeiten (3,7 Mrd. Euro) sind weitere große Faktoren, die Kosten verursachten. Datenschutzrechtliche Maßnahmen, die nach einem Angriff ergriffen werden müssen, sind in ihren Kosten ebenfalls nicht zu unterschätzen. Sie liegen bei 1,4 Milliarden Euro. Eher weniger ins Gewicht fallen die Kosten für die Erpressung mit gestohlenen oder verschlüsselten Daten. Sie verursachten in den letzten zwei Jahren weniger als eine halbe Milliarde Euro Schaden (0,3 Mrd. Euro). Das man im Falle einer Erpressung auf keinen Fall zahlen sollte, scheint mittlerweile weit verbreitet und unter den betroffenen Unternehmen angekommen zu sein.

Delikttyp	Schadenssummen innerhalb der letzten 2 Jahre in Mrd. Euro
Imageschaden bei Kunden oder Lieferanten / Negative Medienberichterstattung	8,8
Patentrechtsverletzungen (auch schon vor der Anmeldung)	8,5
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	6,7
Kosten für Ermittlungen und Ersatzmaßnahmen	5,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	4,0
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	3,7
Kosten für Rechtsstreitigkeiten	3,7
Datenschutzrechtliche Maßnahmen (z. B. Information von Kunden)	1,4
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	0,3
Sonstige Schäden	0,6
Gesamtschaden innerhalb der letzten zwei Jahre	**43,4**

Tabelle 1: Aufgetretene Schadensvorfälle: rund 43,4 Mrd. Euro in den letzten 2 Jahren

Bitte schätzen Sie den Schaden Ihres Unternehmens in Deutschland innerhalb der letzten 2 Jahre durch den jeweiligen aufgetretenen Delikttyp ein?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343)
Quelle: Bitkom Research

4 Täterkreis und Aufklärung

Experten-Statement

Lars Wittmaack
Manager, Quoscient GmbH

Täterkreis und Aufklärung
Wirtschaftsschutz ist mehr als „nur“ Schutz des einzelnen Unternehmens. Für den effektiven Wirtschaftsschutz ist „Aufklärung“ in seinen verschiedenen begrifflichen Ausprägungen ein wesentlicher Faktor:

1. Im Sinne von Bewusstmachung über Bedrohungen und die Notwendigkeit zur Betrachtung aus der Perspektive des Unternehmens- sowie des Wirtschaftsschutzes.
2. Im Sinne von Informationsbeschaffung über Täter, Motivationen, Ziele, Fähigkeiten und Vorgehensweise zum Zwecke der Abwehr, Erkennung und Nachverfolgung.
3. Im Sinne von Aufarbeitung von Sicherheitsvorfällen zur Minimierung von Schäden, Erlangung von Erkenntnissen und Strafverfolgung.

Im Rahmen der Aufklärung (in allen drei Sinnen) lassen sich Täterkreis und Taten mit den Merkmalen Motiv, Bestrebung, Fähigkeiten, Modus Operandi und Gelegenheit umschreiben:

Motiv – als der eigentliche Beweggrund, wie reine Neugier, Ablenkung, finanzieller Gewinn, politische Aussagen respektive Einflussnahme bis hin zur Erlangung von Macht oder als Druckmittel.

Bestrebung – als die Absichten zur Erfüllung des Motivs, wie finanzieller Gewinn mittels digitaler Erpressung oder Verkauf erbeuteter Daten.

Modus Operandi – als die Vorgehensweise in der konkreten organisatorischen und technischen Ausführung, inklusive dem Grad an Versiertheit, wie Aktualisierung der schadhaften Software im laufenden Betrieb.

Gelegenheit – als die verfügbaren bzw. ausgenutzten Möglichkeiten zur Begehung einer Tat, wie Identifizierung bislang unbekannter technischer Schwachstellen oder Ausnutzung der Wirtschaftsbeziehungen durch zum Beispiel Manipulation in der Lieferkette des eigentlichen Ziels.

Die Beschreibung digitaler Täter und digitaler Taten hilft, Erkenntnisse zu gewinnen, die für den nachhaltigen Schutz einzelner Unternehmen aber auch der gesamten Wirtschaft bedeutend sind. Geringes Bewusstsein, die Unterschätzung digitaler Bedrohungen und verhaltene Investitionen in Fachkräfte und Sicherheitsausstattung, bei gleichzeitiger Intensivierung der Digitalisierung lässt erahnen, dass wir über kurz oder lang mit intensiveren Auswirkungen von Cybercrime zu rechnen haben. Denn letztendlich schaffen wir damit selbst die Gelegenheiten, die digitale Täter benötigen, um erfolgreich zu sein.

Die Quintessenz ist: ein nachhaltiger Schutz von Gesellschaft, Unternehmen und Wirtschaft kann alleine kaum gelingen.

4.1 Mitarbeiter werden zu Tätern

Wer sind die Verursacher dieser Schäden? Auch diese Frage wurde den betroffenen Unternehmen gestellt. Die immer noch erschreckende, aber mittlerweile weit verbreitete Antwort: Sehr häufig ehemalige Mitarbeiter. Fast zwei Drittel der betroffenen Industrieunternehmen gaben an, durch ehemalige Mitarbeiter geschädigt worden zu sein. Damit bleibt der mit Abstand größte Täterkreis im eigenen Hause. Hierbei ist zu beachten, dass die Gelegenheit, zum Täter zu werden überwiegend während der aktiven Mitarbeit geschaffen wird. Besonders betroffen sind hiervon Unternehmen mit 100 bis 499 Mitarbeitern, in 74 Prozent der Fälle waren hier ehemalige Mitarbeiter die Täter.

An zweiter Stelle folgen Privatpersonen bzw. Hobby-Hacker. Diese scheinen es besonders auf Unternehmen mit mehr als 500 Mitarbeitern abgesehen zu haben. Immerhin 47 Prozent dieser Unternehmen waren betroffen. Aber auch konkurrierende Unternehmen sind ein ernstzunehmender Täterkreis. 22 Prozent der befragten Unternehmen führen ihre Angriffe auf konkurrierende Unternehmen zurück. Organisierte Kriminalität (17 Prozent), Kunden (14 Prozent) und Lieferanten (14 Prozent) folgen auf Platz vier, fünf und sechs. Dienstleister, Lieferanten und Kunden haben in vielen Fällen direkten Zugang zu einer Organisation und kennen sich mit den Gegebenheiten aus. Das erleichtert es den Tätern, einen Angriff auszuführen.

Ausländische Nachrichtendienste werden in 11 Prozent der Fälle für den Angriff verantwortlich gemacht. Auf den letzten Plätzen befinden sich externe Dienstleister bzw. Berater (9 Prozent) und eigene derzeitige Mitarbeiter (7 Prozent). Insbesondere in Bezug auf Mitarbeiter, darf nicht immer von einer bösen Absicht ausgegangen werden. Unzureichende Sensibilisierung gepaart mit unvorsichtigem Verhalten ist das größte Problem. Sind sich Unternehmen darüber erst einmal bewusst, können sie bei den eigenen Mitarbeitern ansetzen, um die Sicherheit zu erhöhen.

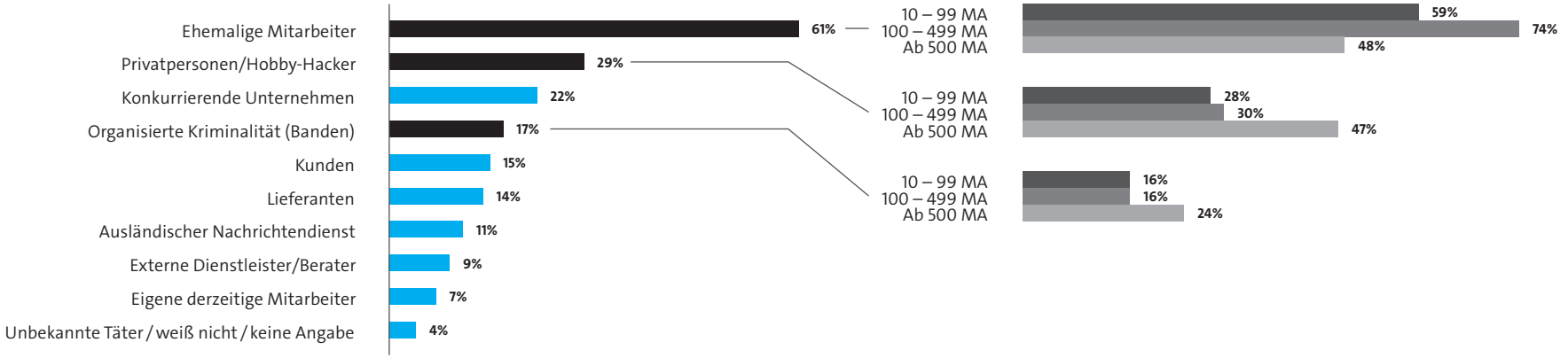


Abbildung 11: Täterkreis

Von welchem Täterkreis gingen diese Handlungen (vermutlich) in den letzten 2 Jahren aus?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

4.2 Herkunft: Region und Land

In der Studie wurde auch die Herkunftsregion bzw. das Herkunftsland der Angriffe abgefragt. Demnach kamen 36 Prozent der Angriffe aus Deutschland. An zweiter Stelle folgte Russland, 24 Prozent der Betroffenen ordnen die Angriffe diesem Herkunftsland zu. China, Japan und Osteuropa (ohne Russland) waren in jeweils knapp 17 Prozent bzw. 18 Prozent der Fälle der Ausgangspunkt der Attacken. Danach folgen die USA mit 15 Prozent und Westeuropa (ohne Deutschland) mit 10 Prozent. Die Attribution von Angriffen ist äußerst schwierig, weshalb nicht verwunderlich ist, dass in 13 Prozent der Fälle unklar war, aus welcher Region die Angriffe tatsächlich kamen.

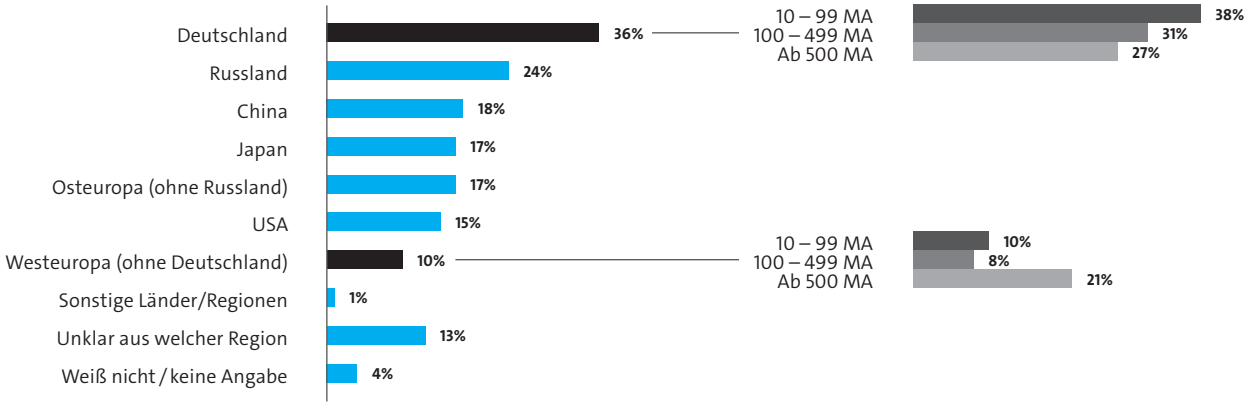


Abbildung 12: Region bzw. Land

Konnten Sie feststellen, von wo aus bzw. aus welcher Region diese Handlungen (vermutlich) vorgenommen wurden?

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

4.3 Aufdeckung der Vorfälle

Aufmerksame Mitarbeiter sind der beste Schutz
Wie werden Unternehmen auf die Angriffe aufmerksam? Auch hier stehen die Mitarbeiter an erster Stelle. In 61 Prozent der Fälle wurden Mitarbeiter auf die Handlungen aufmerksam. Damit lässt sich festhalten: Der effektivste Schutz vor Spionage, Diebstahl oder Sabotage sind motivierte, gut geschulte und aufmerksame Mitarbeiter. Wer hier investiert, sorgt am besten vor.

Doch auch die eigenen IT-Sicherheitssysteme liefern Hinweise. Für vier von zehn Betroffenen (40 Prozent) waren sie erster Indikator für Angriffe. Durch interne Ermittlungseinheiten sind ähnlich viele Unternehmen auf Attacken aufmerksam geworden (38 Prozent). Doch auch der Zufall ist ein wichtiger Faktor bei der Aufdeckung der Vorfälle. Fast ein Viertel (23 Prozent) ist zufällig auf Sabotage oder Diebstahl aufmerksam geworden. Anonyme Hinweise gingen bei 18 Prozent der betroffenen Unternehmen ein. Hinweise durch unternehmensexterne Einzelpersonen sowie durch die Jahresabschlussprüfung bzw. durch interne Kontrollsysteme deckten in ca. 15 Prozent bzw. 14 Prozent der Fälle einen Angriff auf. Nur in seltenen Fällen kommt der erste Impuls von Strafverfolgungs- oder Aufsichtsbehörden (3 Prozent), wenn es um Delikte im Bereich Cybercrime geht.

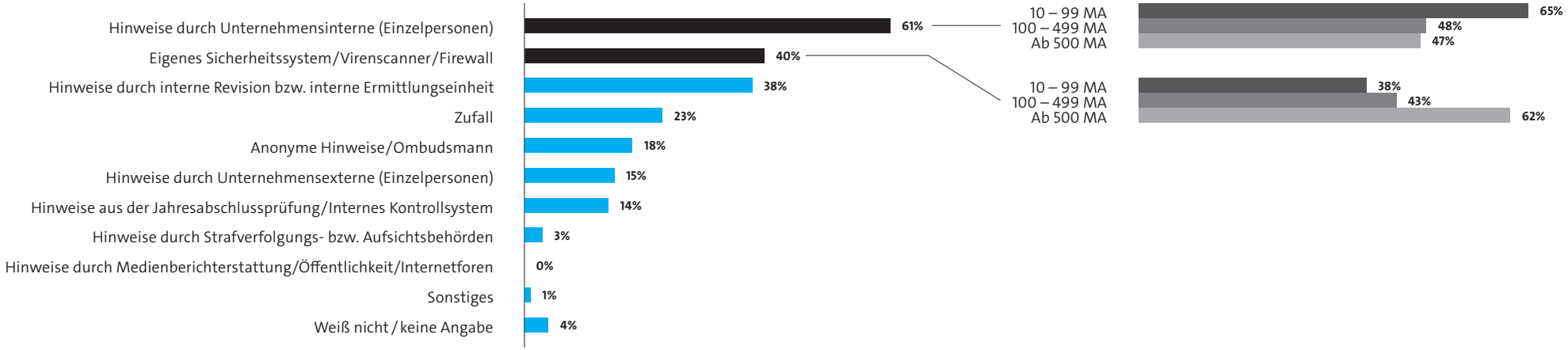


Abbildung 13: Aufklärung der Vorfälle

Wie ist Ihr Unternehmen auf diese Handlungen erstmalig aufmerksam geworden?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

Experten-Statement

Swantje Schmidt
Account Executive Innere Sicherheit,
Capgemini Deutschland

»Um auf IT-Angriffe adäquat zu reagieren und zukunftsorientierte Abwehrstrategien realitätsnah zu entwickeln, ist eine vertrauensvolle Zusammenarbeit zwischen Unternehmen und zuständigen Sicherheitsbehörden wesentlich.«

Die zunehmende Digitalisierung von Unternehmen erhöht die Wirtschaftsleistung, ermöglicht innovative Geschäftsmodelle und effizientere Geschäftsprozesse. Eine damit einhergehende einfachere Verfügbarkeit einer wachsenden Menge geschäftsrelevanter Daten vergrößert gleichzeitig aber auch die potenzielle Angriffsfläche für Wirtschaftsspionage, Sabotage und Datendiebstahl.

Der vorliegenden Studie zufolge werden IT-Angriffe zumeist durch ehemalige Mitarbeiter und zunehmend durch »Hobby-Hacker« oder konkurrierende Unternehmen verübt. Eine Aufklärung wird hierbei insbesondere durch unternehmensinterne Einzelpersonen, IT-Sicherheitssysteme und interne Revisions-/Ermittlungseinheiten unterstützt und in einer Mehrzahl der Vorfälle als Strafanzeige bei Polizei oder Staatsanwaltschaft gemeldet. Unternehmen, die auf eine Einbeziehung staatlicher Stellen bisher verzichten, nennen zumeist Imageschäden oder sonstige negative Konsequenzen als Gründe, aber auch den damit verbundenen Aufwand oder die vermuteten geringen Erfolgsaussichten hinsichtlich der Täterermittlung.

Wie können Unternehmen von den Erkenntnissen zu Täterkreis und Aufklärung der Studie konkret profitieren?
Sowohl die Betrachtung des Täterkreises als auch die unterschiedlichen Perspektiven zur Fallaufklärung im Unternehmen können dabei unterstützen, das Gefahrenbewusstsein zu schärfen, bereits gelebte Prozesse zur Gefahrenminimierung weiterzuentwickeln und diese in eine unternehmensbezogene integrative Sicherheitsstrategie einzubringen. Da IT-Angriffe auf Unternehmen verschiedenster Branchen unabhängig der Unternehmensgröße erfolgen, ist die Gefahr, Ziel von Spionage- oder Sabotageangriffen oder Opfer von Datendiebstahl zu werden auch für jedes Unternehmen vorhanden. Es muss also im ureigenen Interesse eines jeden Unternehmens sein, sich begleitend zum jeweiligen Grad der Digitalisierung beziehungsweise zur jeweiligen Digitalisierungsstrategie durch risikominimierende Maßnahmen proaktiv mit dem Schutz vor IT-Angriffen zu befassen. Sollte ein konkreter IT-Angriff vermutet oder entdeckt worden sein, stellen definierte Prozesse der unternehmenseigenen Sicherheitsstrategie die Basis dar, die kurzfristig erforderliche vertrauensvolle Zusammenarbeit zwischen Unternehmen und zuständigen Sicherheitsbehörden zu initiieren. Nur durch eine wachsende Zusammenarbeit zwischen Unternehmen und Sicherheitsbehörden besteht bei zunehmender Digitalisierung und Veränderung von Arbeits- und Wertschöpfungskulturen in den Unternehmen die Möglichkeit auf konkrete IT-Angriffe adäquat zu reagieren und zukunftsorientierte Abwehrstrategien realitätsnah zu entwickeln.

4.4 Sicherheitsvorfälle führen meist zu Strafanzeigen

Erfreulich ist, dass nur 2 Prozent der Unternehmen, die angegriffen wurden, darauf verzichtet haben, ihre Sicherheitsvorfälle staatlichen Stellen zu melden. Die überwiegende Mehrheit der Betroffenen hat Strafanzeige gestellt (78 Prozent), 29 Prozent als freiwillige Meldung. Verpflichtende Meldungen nach dem IT-Sicherheitsgesetz haben 13 Prozent der betroffenen Unternehmen vorgenommen. Dieser Pflicht unterliegen die Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung. Das klassische produzierende Gewerbe zählt demnach nicht dazu. 8 Prozent der befragten Unternehmen waren im Rahmen des Bundesdatenschutzgesetzes verpflichtet, die Vorfälle an staatliche Stellen zu melden.

Es ist wichtig, dass sich Betroffene grundsätzlich an Ermittlungsbehörden wenden. Diese können nur dann erfolgreich arbeiten, wenn sie auch Kenntnis von den Delikten haben. Zwar ist es für Unternehmen möglich, den Schaden aus eigener Kraft oder mit Unterstützung von Spezialisten einzudämmen. Aber nur durch die Zusammenarbeit mit staatlichen Stellen kann ein realistisches Lagebild erstellt, neue Angriffswege rechtzeitig erkannt und andere Unternehmen gewarnt und geschützt werden. Umgekehrt müssen aber auch die Behörden aktiver werden, um das Vertrauen der Wirtschaft zu gewinnen.

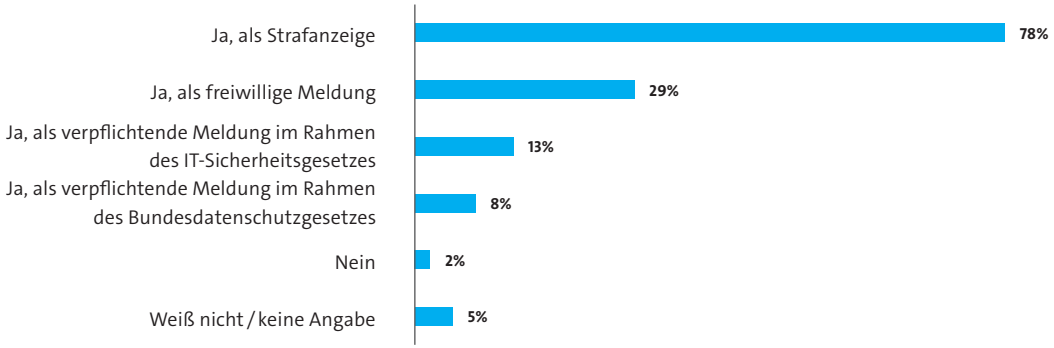


Abbildung 14: Meldung der Vorfälle an staatliche Stellen I

Haben Sie diese Vorfälle staatlichen Stellen gemeldet?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

Wem haben betroffene Industrieunternehmen die Vorfälle gemeldet? Vor allem der Polizei. 90 Prozent derjenigen, die betroffen waren und den Vorfall gemeldet haben, sind damit zur Polizei gegangen. Dieses Bild zeichnet sich durch alle Größenklassen ab. Ein Grund für diese hohe Prozentzahl könnten die in einigen Landeskriminalämtern eingerichteten Zentralen Anlaufstellen Cybercrime (ZAC) sein. Gerade für mittelständische Unternehmen sind sie ein wichtiger Ansprechpartner – sowohl für präventive Maßnahmen, als auch im Ernstfall.

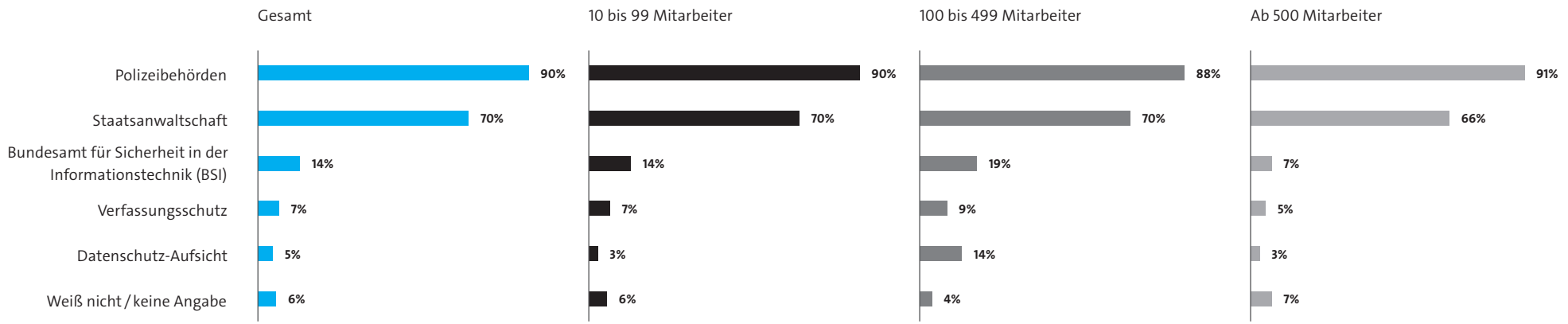
Häufig wurde auch die Staatsanwaltschaft eingeschaltet (70 Prozent). Bundesbehörden wie das BSI oder das Bundesamt für Verfassungsschutz hingegen eher selten. Dies könnte daran liegen, dass das BSI insbesondere dann eingeschaltet wird, wenn es sich um eine verpflichtende Maßnahme im Rahmen des IT-Sicherheitsgesetzes handelt, dies ist in nur 13 Prozent der Fälle relevant gewesen. Die Tatsache, dass nur in wenigen Fällen das Bundesamt für Verfassungsschutz benachrichtigt wurde, könnte darauf zurückzuführen sein, dass eine geringe Prozentzahl der Angriffe von ausländischen Nachrichtendiensten durchgeführt wurde.

Abbildung 15: Meldung der Vorfälle an staatliche Stellen II

An welche der folgenden staatlichen Stellen haben Sie diese Vorfälle gemeldet?

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und diese Vorfälle an staatliche Stellen gemeldet haben (n=321) | Mehrfachnennungen in Prozent

Quelle: Bitkom Research



Warum wird auf das Einschalten von staatlichen Stellen verzichtet?!

Die Angst vor Imageschäden hindert in 38 Prozent der Fälle Unternehmen daran, staatliche Stellen einzuschalten. Gleich auf liegt die Befürchtung, dass der oder die Täter sowieso nie gefasst würden (38 Prozent). Hier ist ein starker Anstieg im Vergleich zum Vorjahr zu verzeichnen, damals waren die Unternehmen noch optimistischer gestimmt und lediglich 22 Prozent gingen davon aus, dass die Täter ohnehin nicht gefasst werden.

Für viele Unternehmen ist aber auch der große Aufwand ein Hindernis, um staatliche Stellen einzuschalten. 37 Prozent der Unternehmen gaben an, aus diesem Grund auf das Einschalten von staatlichen Stellen verzichtet zu haben. Weitere 36 Prozent befürchteten negative Konsequenzen. 4 Prozent der betroffenen Unternehmen gehen davon aus, dass staatliche Stellen sich in diesem Umfeld nicht auskennen und melden deshalb die Vorfälle nicht.

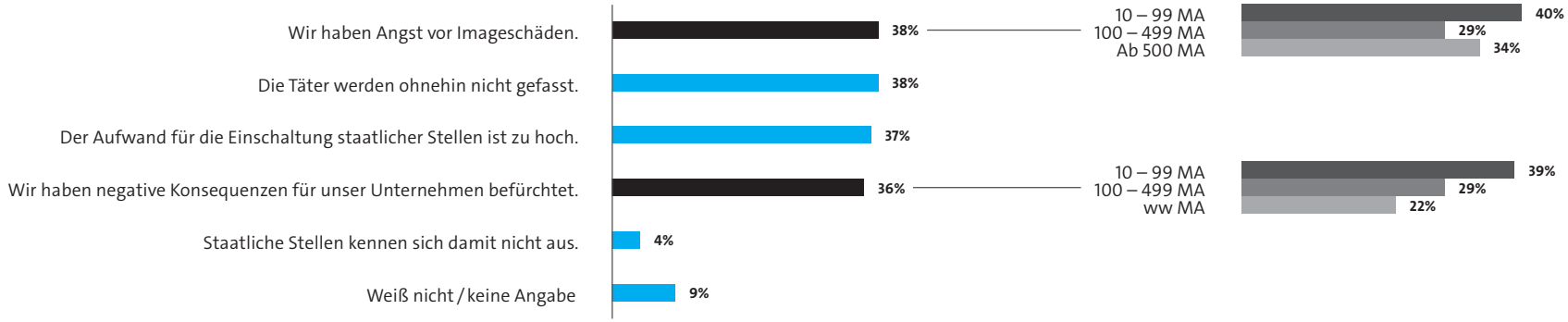


Abbildung 16: Aufklärung der Vorfälle I

Aus welchen der folgenden Gründe hat Ihr Unternehmen keine staatlichen Stellen zur Untersuchung der Vorfälle eingeschaltet?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und keine staatlichen Stellen bei der Untersuchung eingeschaltet haben (n=212) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

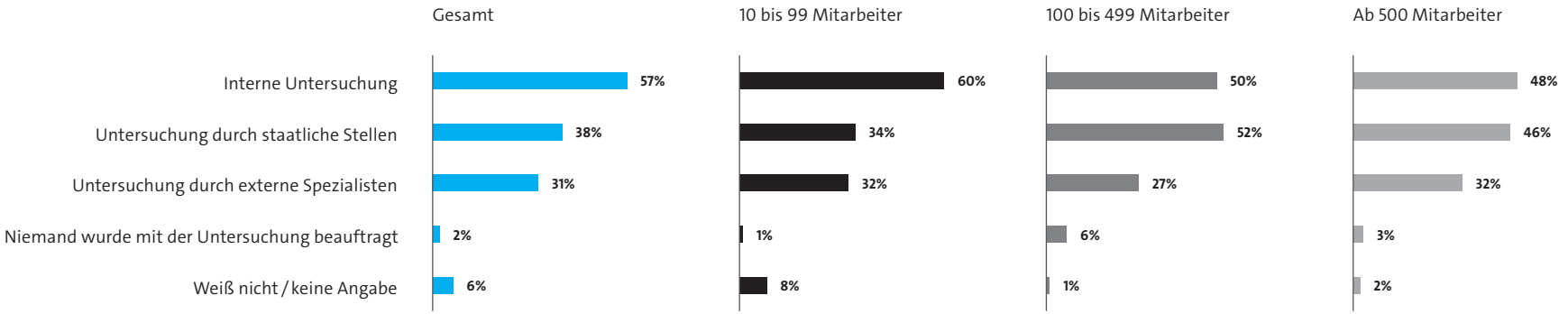
4.5 Aufklärung und Untersuchung der Vorfälle

Noch immer verlassen sich viele Unternehmen auf interne Untersuchungen, um Angriffe im Bereich Wirtschaftsspionage, Sabotage und Datendiebstahl aufzuklären (57 Prozent). An zweiter Stelle werden die Untersuchungen staatlichen Institutionen (38 Prozent) anvertraut. Das ist ein deutlicher Anstieg im Vergleich zu den Ergebnissen aus den Jahren 2014/2015, damals waren es nur knapp 25 Prozent. Dies könnte auf die gute Aufklärungsarbeit der Polizei zurückzuführen sein. Wie bereits erwähnt sind durch die ZAC zentrale Ansprechpartner definiert.

Externe Spezialisten werden von 31 Prozent der betroffenen Unternehmen mit den Untersuchungen betraut. Nur in 2 Prozent der Fälle wurde niemand mit der Untersuchung beauftragt. Bei Unternehmen mit 100 bis 499 Mitarbeitern sind es 6 Prozent. Hier ist im Vergleich zum Vorjahr ein deutlicher Rückgang zu verzeichnen. Die Unternehmen scheinen realisiert zu haben, dass zum einen die Meldung als auch die Aufklärung wichtiger Bestandteil eines umfassenden Schutzes sind.

Abbildung 17: Aufklärung der Vorfälle II

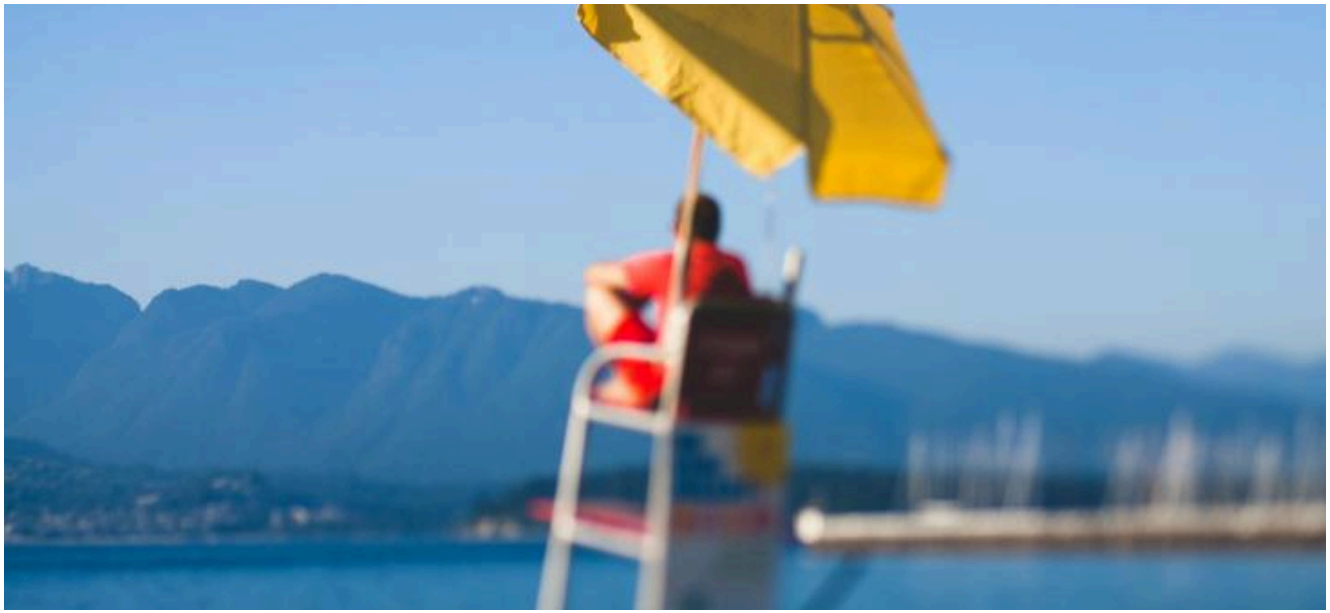
Wer hat diese Vorfälle untersucht?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research



»Viele Unternehmen nehmen das Thema Sicherheit noch zu sehr auf die leichte Schulter, auch weil ihnen das entsprechende Know-how fehlt. Erster und wichtigster Schritt ist, IT-Sicherheit im Unternehmen zur Chefsache zu machen.«

Achim Berg, Bitkom-Präsident, Berlin 2018

Die Industrieunternehmen haben im Bereich der Prävention in den letzten Jahren einiges getan. So bestätigten alle befragten Industrieunternehmen, dass sie über einen technischen Basisschutz vor Cyberangriffen verfügen. Allerdings ist das nicht genug. Zum einen sind weitere Maßnahmen bei der Angriffserkennung notwendig. Zum anderen sollten sich Organisationen für den Fall der Fälle vorbereiten. Bisher verfügt nur knapp jedes zweite Industrieunternehmen über ein Notfallmanagement.



5.1 Technische Sicherheitsmaßnahmen

Über einen technischen Basisschutz verfügen nahezu alle befragten Unternehmen. Flächendeckend setzen Industrieunternehmen beispielsweise Passwortschutz, Virenscanner und Firewalls auf allen Geräten ein. Außerdem führen alle Unternehmen regelmäßige Backups für Daten durch. Gängige Betriebssysteme enthalten in den meisten Fällen derartige Funktionen. Da Schadstoffsoftware aber immer komplexer wird und in vielen Fällen unerkannt bleibt, reichen diese Methoden nicht mehr aus.

Eine Verschlüsselung von Netzwerkverbindungen setzen immerhin 91 Prozent der befragten Unternehmen ein. Elektronische Zugangskontrollen (74 Prozent), Protokollierung von Zugriffen (67 Prozent) und eine abhörsichere Sprachkommunikation (59 Prozent) sind bei deutlich über der Hälfte der Industrieunternehmen angekommen. Das Thema Verschlüsselung dagegen spielt nur bei rund jedem dritten Unternehmen eine Rolle. Auf Penetrationstests (24 Prozent) und Intrusion Detection Systeme (20 Prozent) setzen bisher noch nicht allzu viele Unternehmen. Diese Anwendungen analysieren die Datenströme in einer Organisation und melden verdächtige Aktivitäten. Sie kommen vor allem dann zum Tragen, wenn Firewall und Virenscanner den Angriff nicht stoppen konnten.

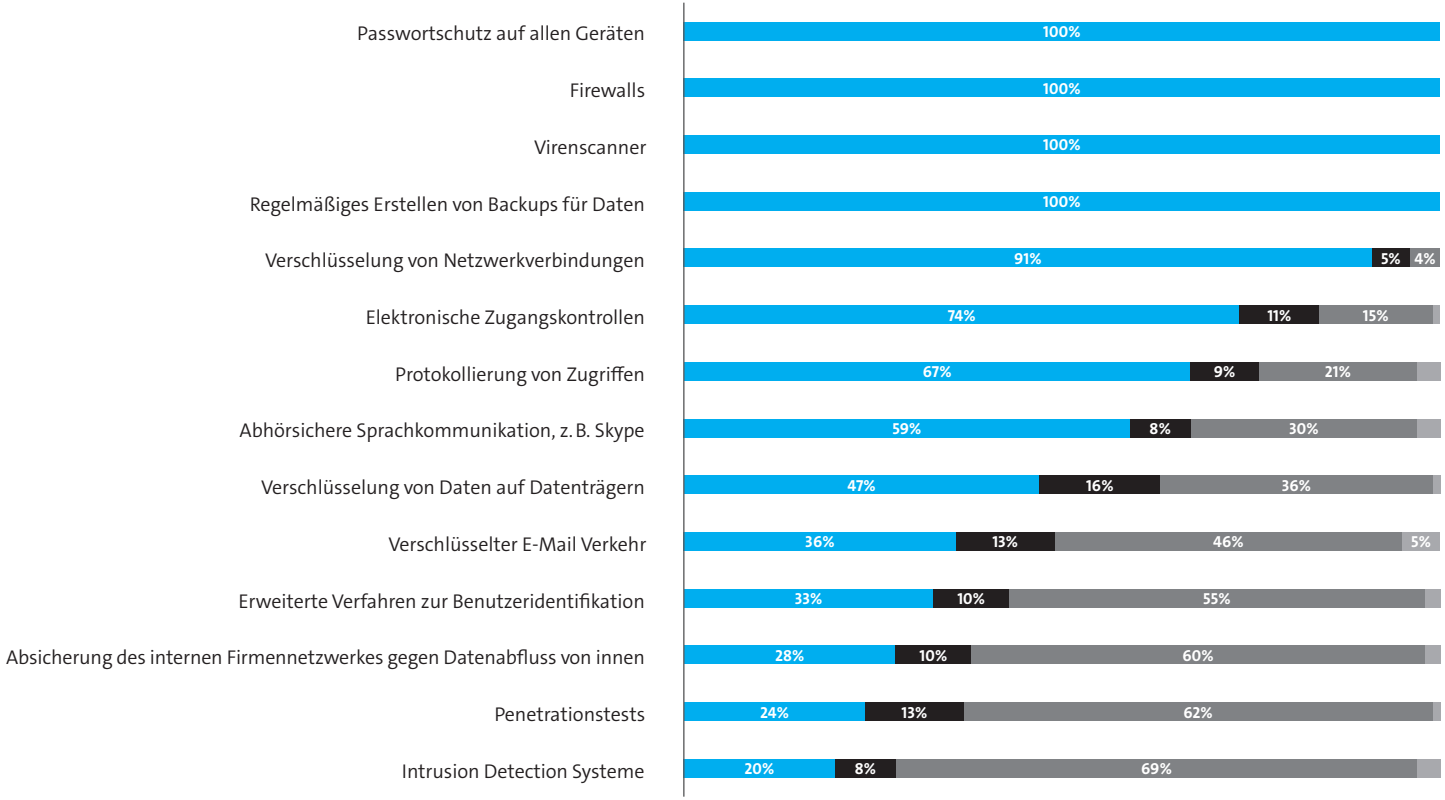


Abbildung 18: Technische IT-Sicherheitsmaßnahmen 2018

Welche der folgenden technischen IT-Sicherheitsmaßnahmen kommen in Ihrem Unternehmen bereits zum Einsatz bzw. plant Ihr Unternehmen in Zukunft einzusetzen?

Basis: Alle befragten Industrieunternehmen (n=503)
Quelle: Bitkom Research

Künstliche Intelligenz heute selten im Einsatz

Künstliche Intelligenz kann zum Beispiel beim Erkennen von Anomalien eingesetzt werden. Das Potenzial, welches diese Technologie auch im Bereich Cybercrime bietet, ist enorm. Dennoch wird sie heute noch bei keinem Unternehmen eingesetzt. Immerhin konkret geplant wird ein Einsatz bei rund drei Prozent und diskutiert bei rund acht Prozent der Unternehmen. Für 84 Prozent spielt diese Technologie zum Schutz gegen Angriffe heute noch keine Rolle.

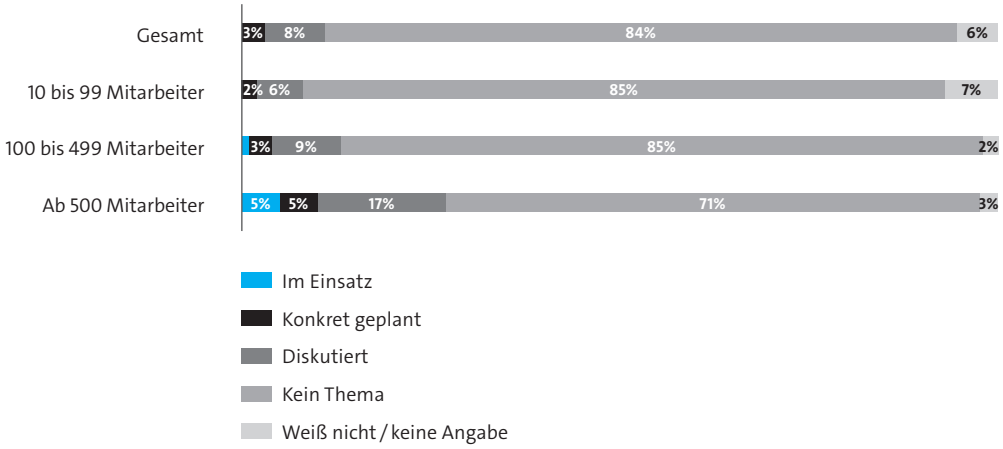


Abbildung 19: Technische IT-Sicherheitsmaßnahmen 2018: KI oder ML

Kommen in Ihrem Unternehmen bereits Anwendungen mit KI oder Maschinelles Lernen zum Einsatz um sich gegen Datendiebstahl, Spionage oder Sabotage zu schützen?

Basis: Alle befragten Industrieunternehmen (n=503) | Abweichungen von 100 Prozent sind rundungsbedingt

Quelle: Bitkom Research

5.2 Organisatorische Sicherheitsvorkehrungen

Zu einem umfassenden Schutz gegen Cyberangriffe zählen auch die organisatorischen Sicherheitsvorkehrungen. Hierzu gehört z. B. die Festlegung von Zugriffsrechten auf bestimmte Informationen. Alle befragten Unternehmen haben solche Zugriffsrechte bestimmt und in ihrer Organisation etabliert. Nur rund 77 Prozent sorgen aber für den physischen Schutz, zum Beispiel in Form von Zutrittskontrollen oder der Sicherung von Gebäuden.

Eine eindeutige Klassifizierung bzw. Kennzeichnung von Betriebsgeheimnissen haben immerhin 84 Prozent eingeführt. 80 Prozent der Unternehmen stellen klare Regeln für den Umgang mit schützenswerten Informationen auf.

Zwei Drittel (66 Prozent) der Unternehmen etablierten bestimmte Regelungen für die Mitnahme von IT- und TK-Equipment bei Geschäftsreisen.

Ein Sonderfall sind Sicherheitszertifizierungen, die nur 49 Prozent der Befragten durchführen. Im Rahmen einer Zertifizierung lassen die Industrieunternehmen ihr Sicherheitskonzept von einer externen Organisation wie dem TÜV oder dem BSI überprüfen. Die Einführung von Informationssicherheits-Managementsystemen (ISMS) sowie die Durchführung von regelmäßigen Sicherheitsaudits finden nur bei rund 35 Prozent bzw. 34 Prozent der Unternehmen statt.

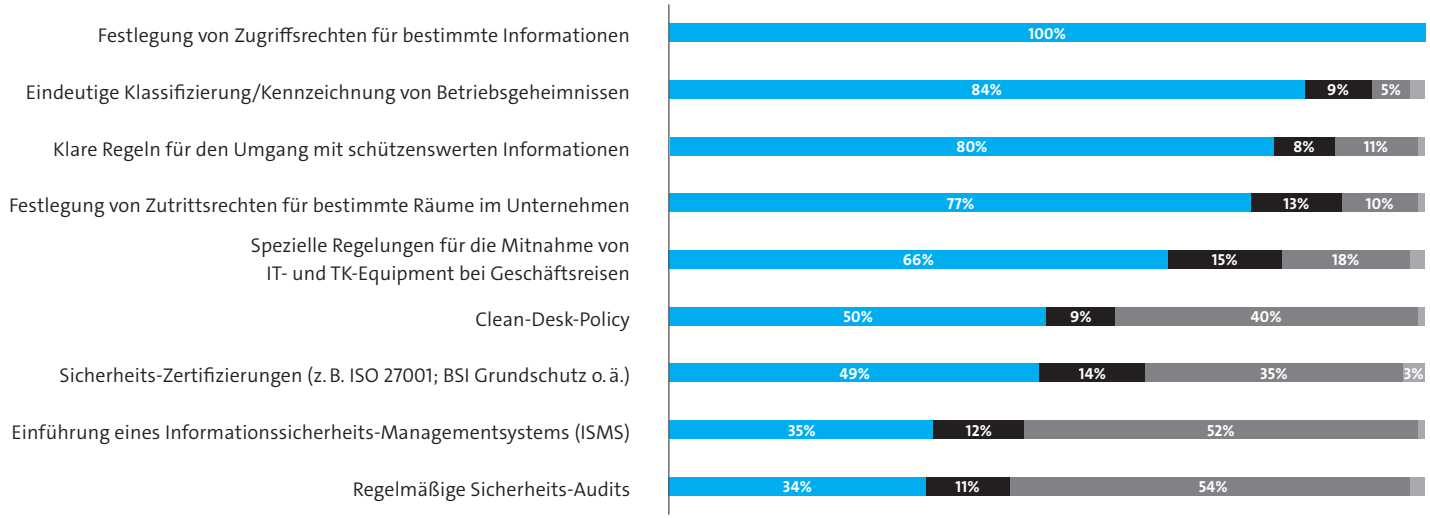


Abbildung 20: Organisatorische Sicherheitsvorkehrungen 2018

Welche der folgenden organisatorischen bzw. prozesstechnischen Sicherheitsvorkehrungen kommen in Ihrem Unternehmen bereits zum Einsatz bzw. plant Ihr Unternehmen in Zukunft einzusetzen?
Basis: Alle befragten Industrieunternehmen (n=503) | Abweichungen von 100 Prozent sind rundungsbedingt
Quelle: Bitkom Research

Notfallmanagement noch nicht ausreichend etabliert

Weniger als die Hälfte (44 Prozent) aller Industrieunternehmen in Deutschland verfügt über ein Notfallmanagement, das im Ernstfall zum Tragen kommt. Hier besteht eine deutliche Diskrepanz zwischen kleinen und größeren Industrieunternehmen. Während Unternehmen mit mehr als 500 Mitarbeitern in 67 Prozent der Fälle ein Notfallmanagement etabliert haben, sind es bei Unternehmen mit 10 bis 99 Mitarbeitern lediglich 40 Prozent. Damit sind größere Industrieunternehmen inzwischen auch in diesem Bereich schon wesentlich besser gerüstet als kleinere.

Ein betriebliches Notfallmanagement umfasst schriftlich geregelte Abläufe und Sofortmaßnahmen im Falle von Datendiebstahl, Spionage oder Sabotage. Wenn erkannt wird, dass eine Cyberattacke stattgefunden hat, muss analysiert werden, welche Unternehmensdaten betroffen sind und wie kritisch der Angriff ist. Im Anschluss sind mögliche Betroffene sowie Strafverfolgungsbehörden zu informieren. Zu den Zielen des Notfallmanagements gehören zum Beispiel auch, den Datenabfluss zu stoppen oder beim Ausfall wichtiger Systeme die Arbeitsfähigkeit des Unternehmens so schnell wie möglich wiederherzustellen.

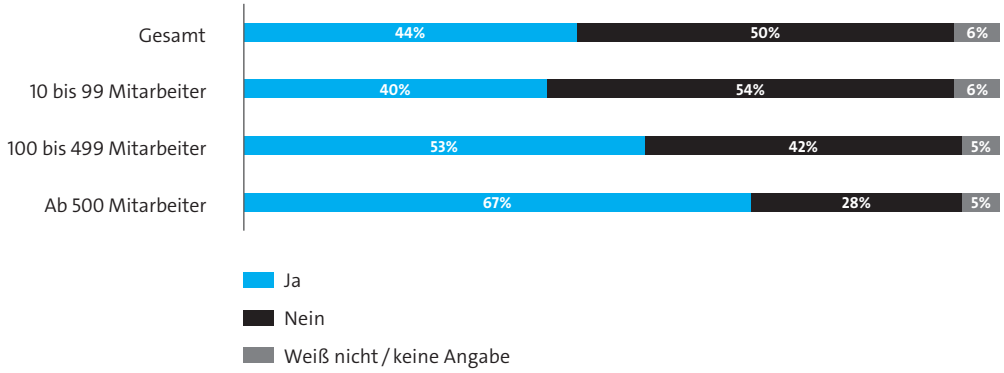


Abbildung 21: Notfallmanagement

Verfügt Ihr Unternehmen über schriftlich geregelte Abläufe und Ad-hoc-Maßnahmen, also ein Notfallmanagement, für den Fall des Auftretens von Datendiebstahl, Industriespionage oder Sabotage?
Basis: Alle befragten Industrieunternehmen (n=503)
Quelle: Bitkom Research

Experten-Statement

Dr. Dan Bastian Trapp
Leiter Prävention, Wirtschaftsschutz
Bundesamt für Verfassungsschutz

Die vorliegende Studie zeigt im Hinblick auf Prävention eines ganz klar: Der Ansatzpunkt für mehr Sicherheit ist der Mensch!

Es ist erfreulich, wenn alle Befragten der Studie angeben, Passwortschutz, Firewalls, Virenscanner und Backups im Einsatz zu haben. Alarmieren muss die Tatsache, dass nur knapp 60 Prozent der Unternehmen ihre Mitarbeiterinnen und Mitarbeiter in Sachen Sicherheit schulen! Ein Virenscanner, eine Firewall und auch Passwortschutz scheitern vielfach in der konkreten Anwendung. Selbst hochspezialisierte APT-Angriffe arbeiten z. B. mit Spear-Phishing-Mails, die auf einen unaufmerksamen Anwender setzen. Notwendig sind hier Sensibilisierung und Schulung. Nur ein sensibilisierter und praxistauglich geschulter Mitarbeiter kann den Gefahren z. B. des Social Engineering entgehen, vor denen auch die beste Firewall nicht schützen kann.

Sensibilisierung und Schulung sind zwei Komponenten einer Präventionsstrategie, die nicht einfach »aufgespielt« werden kann wie ein Update. Erforderlich ist ein Umdenken, das sich in der Unternehmenskultur auswirkt. Es ist nicht damit getan, im Unternehmensintranet aktualisierte Sicherheitsanweisungen abrufbar zu halten. Die Frage muss beantwortet werden: Wie verhält sich jeder Mitarbeiter in seiner Arbeitswirklichkeit effektiv sicher? Hier praxisgerechte Lösungen zu finden ist keine einfache Aufgabe. Wer sich ihr stellt, schafft damit aber eine wesentliche Voraussetzung für ein angemessenes Sicherheitsniveau. Oder anders ausgedrückt: Ohne sensibilisierte und sinnvoll geschulte Mitarbeiterinnen und Mitarbeiter versagen auch die teuersten technischen Sicherheitsfeatures.

Das Bundesamt für Verfassungsschutz informiert im Rahmen der Prävention über eigene Erkenntnisse und Analysen, die dazu beitragen, dass Unternehmen sich effektiv gegen Ausforschung, Sabotage und Bedrohungen durch Extremismus und Terrorismus schützen können. Sprechen Sie uns gerne an.

5.3 Sicherheitsvorkehrungen im Bereich Personal

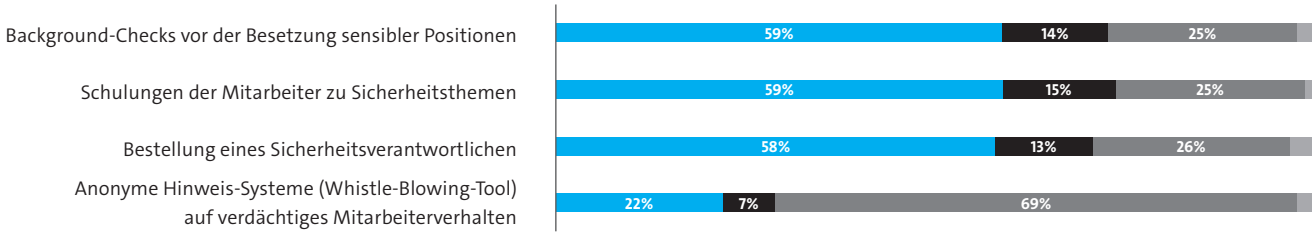
Mitarbeitern kommt sowohl bei der Ausführung als auch bei der Erkennung von Angriffen die größte Bedeutung zu. Ein entscheidender Faktor beim Thema Unternehmenssicherheit ist deshalb der richtige Umgang mit dem Personal. 59 Prozent der Befragten führen Hintergrund-Prüfungen von Personen, die auf sensible Positionen gesetzt werden sollen, durch. Hierzu gehört beispielsweise die Sichtung von Social Media Profilen. Schulungen zu Sicherheitsthemen setzen immerhin 59 Prozent der befragten Industrieunternehmen ein. Das ist ein deutlicher Anstieg zu den Ergebnissen aus der Studie im Jahr 2016. Da waren es nur rund 43 Prozent.

58 Prozent der befragten Unternehmen bestimmen einen Sicherheitsverantwortlichen im Unternehmen. Damit kommt das Thema auch in der Management-Ebene an. Die Bestimmung eines solchen Verantwortlichen ist für ein umfassendes Sicherheitsmanagement unabdingbar. Entscheidend ist, dass das Thema IT-Sicherheit zur Chefsache gemacht und es über eigene Wirtschaftsschutz-Beauftragte oder Informations-Sicherheitsbeauftragte im Unternehmen institutionalisiert wird.

Anonyme Hinweissysteme wie Whistle-Blower-Tools werden nur bei rund 22 Prozent der Unternehmen eingesetzt. Hier bekommen Mitarbeiter die Möglichkeit, Missstände und Versäumnisse extern betriebener Systeme zu melden, ohne sich selbst dabei als »vermeintliches Einfallstor« outen zu müssen.

Abbildung 22: Sicherheitsvorkehrungen im Bereich Personal 2018

Welche der folgenden Sicherheitsvorkehrungen im Bereich Personal kommen in Ihrem Unternehmen bereits zum Einsatz bzw. plant Ihr Unternehmen in Zukunft einzusetzen?
Basis: Alle befragten Industrieunternehmen (n=503)
Quelle: Bitkom Research



6 Zukünftige Bedrohungsszenarien und Eignung von IT-Sicherheitsmaßnahmen

»Ein robustes IT-Sicherheitsmanagement fängt mit gut geschulten Mitarbeitern an. Qualifiziertes Personal im Bereich IT-Sicherheit ist sehr gefragt. Investitionen in Fachkräfte lohnen sich hier besonders.«

Susanne Dehmel, Mitglied der Geschäftsleitung im Bitkom, Berlin 2018

Expertenstatement

Prof. Timo Kob
Vorstand, HiSolutions AG

Jedem Studenten der Informationssicherheit werden quasi von der ersten Vorlesung an die drei Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität eingebläut. Dennoch lag der Fokus der Schutzmechanismen zumindest in der klassischen Office-IT immer noch verstärkt auf dem Schutz der Vertraulichkeit. Erst in den letzten Jahren, befeuert durch die immer rasantere Vernetzung und Automatisierung der Produktionsanlagen, geraten die beiden anderen Sicherheitsziele Verfügbarkeit und Integrität – als Stoßrichtung von Sabotageaktivitäten – verstärkt in das Bewusstsein der Verantwortlichen.

Wie auch in der Vergangenheit spielen hier besonders empfindliche Branchen, gerade im KRITIS-Bereich die Vorreiter-Rolle. Das IT-Sicherheitsgesetz fokussiert ja etwa in erster Linie auf die Verfügbarkeit kritischer Services. Hier ist positiv zu beobachten, dass auch andere Branchen der klassischen Industrien unterdessen das Gefahrenpotenzial erkennen und diesem Thema gesteigerte Aufmerksamkeit widmen. Wichtig ist hier, dass auch das Ziel der Integrität als gleichermaßen gefährdet erkannt wird. Platt gesagt: Dass die »Maschinen laufen« ist gut, dass sie auch das richtige »ausspucken« noch wichtiger.

Die Integrität spielt im übertragenen Sinne noch eine weitere zukünftig an Bedeutung gewinnende Rolle in einer globalisierten kompetitiven Wirtschaft. Und auch hier kann man im Großen erkennen, was die Unternehmen im Kleinen erwartet:

»Cyber Spying Is Out, Cyber Lying Is In« prognostizierte das Magazin »Foreign Policy« schon 2015. Anders ausgedrückt: Warum soll ich mir die Mühe machen, durch Sabotage die Lieferfähigkeit und Produktqualität zu senken, wenn ich durch soziale Medien etc. mit einfachsten Mitteln und ohne große Gefahr der Erkennung der Urheberschaft zumindest den Anschein solcher Probleme wecken kann? Auch dies ist eine Bedrohung im Cyberraum, der sich trotz breiter Diskussion um echte oder vermeintliche Wahlmanipulation, Internet-Trolle etc. immer noch zu wenige Unternehmen stellen und die auch innerhalb der Unternehmen neuer Formen der Kooperation bei der Abwehr, z. B. mit der Unternehmenskommunikation bedarf.

Unentdeckte Sicherheitslücken als größte Bedrohung

Die Studie hat auch einen Blick in die Zukunft gewagt. Welche Gefahren beim Thema IT-Sicherheit stehen für die Industrie zukünftig im Fokus? Nahezu alle Befragten nannten die sogenannten Zero-Day-Exploits als größte Gefahr (96 Prozent). Dabei nutzen Angreifer Sicherheitslücken in Software aus, die bis dahin unbekannt waren. 93 Prozent fürchten die Infizierung mit Schadsoftware, zwei Drittel (68 Prozent) gaben den Mangel an qualifizierten IT-Sicherheitskräften als Bedrohung an. Ein Thema, das erst seit kurzem akut ist, ist das Anzapfen von Rechenleistungen von außen, um etwa Kryptowährungen zu schürfen. Im Vergleich wird dieses Thema aber seltener als Bedrohung gesehen, nur 29 Prozent der Unternehmen nehmen es als echte Gefahr wahr.

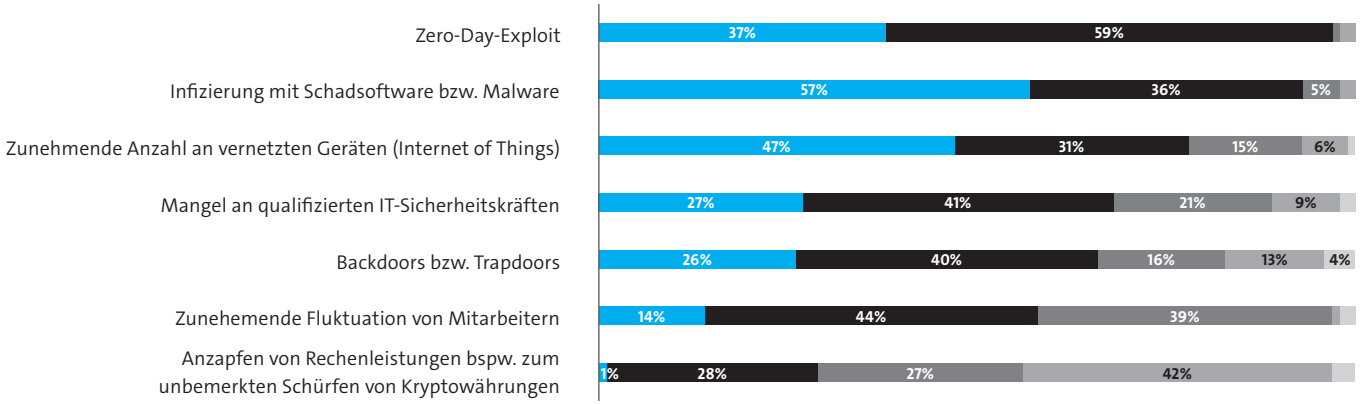


Abbildung 23: Zukünftige Bedrohungsszenarien

Inwieweit betrachten Sie die folgenden Szenarien als zukünftige Bedrohung für die IT-Sicherheit Ihres Unternehmens?

Basis: Alle befragten Industrieunternehmen (n=503) | Abweichungen von 100 Prozent sind rundungsbedingt
Quelle: Bitkom Research

Qualifiziertes Personal als bester Schutz vor Sabotage, Datendiebstahl oder Spionage

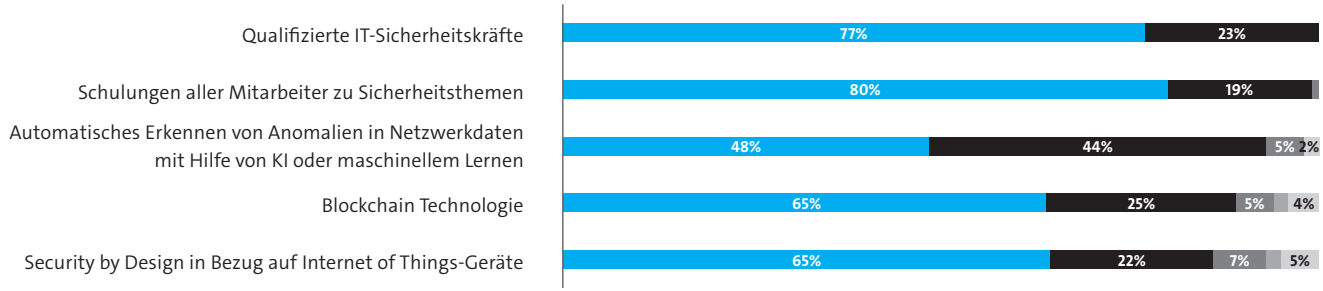
Für die deutsche Industrie sind IT-Sicherheitsexperten der beste Schutz gegen Cyberattacken. Jedes Industrieunternehmen (100 Prozent) hält qualifizierte IT-Sicherheitskräfte für eine geeignete Maßnahme, um sich gegen Datendiebstahl, Industriespionage oder Sabotage zu wappnen, 77 Prozent sehen dies als sehr geeignet. Ähnlich wichtig sind für sie Schulungen aller Mitarbeiter zu Sicherheitsthemen. 99 Prozent des produzierenden Gewerbes findet dies wichtig.

Aber nicht nur die Investition in das Personal ist der Industrie wichtig. Für die IT-Sicherheit spielen auch neue Technologien wie Blockchain oder Künstliche Intelligenz (KI) eine große Rolle. Zwei Drittel (65 Prozent) schätzen die Blockchain als sehr geeignete Technologie für die IT-Sicherheit ein, ein Viertel (25 Prozent) als eher geeignet. Zudem benennt fast die Hälfte der Befragten (48 Prozent) das automatische Erkennen von Anomalien in Netzwerkdaten mit Hilfe von KI oder maschinellem Lernen als sehr geeignete Sicherheitsmaßnahme. Weitere 44 Prozent finden dies eher geeignet. Hier lässt sich in der Tat eine große Diskrepanz zwischen der theoretischen Eignung und dem tatsächlichen Einsatz der Technologie feststellen. Wie in Kapitel 5.1 bereits beschrieben, planen nur drei Prozent der Unternehmen zeitnah KI als unterstützende Maßnahme beim Erkennen von Anomalien einzusetzen.

Bezogen auf das Internet der Dinge halten zwei Drittel der Industrieunternehmen (65 Prozent) den Ansatz »Security by Design« für besonders geeignet, weitere 22 Prozent sehen diesen Ansatz als eher geeignete Sicherheitsmaßnahme. Security by Design bedeutet, dass Geräte mit einer Internetverbindung schon bei ihrer Entwicklung auf Sicherheit ausgelegt werden.

Abbildung 24: Eignung von IT-Sicherheitsmaßnahmen

Für wie geeignet halten Sie die folgenden IT-Sicherheitsmaßnahmen, um Ihr Unternehmen zukünftig gegen Datendiebstahl, Industriespionage oder Sabotage effektiv zu schützen?
Basis: Alle befragten Industrieunternehmen (n=503) | Abweichungen von 100 Prozent sind rundungsbedingt
Quelle: Bitkom Research



7 Cyber-Versicherungen

Experten-Statement

Marco Schulz
Geschäftsführer, marconcert GmbH

Diese Studie belegt auch in diesem Jahr eindrucksvoll die Anfälligkeit deutscher Unternehmen für hohe bis existenzbedrohende Schäden durch digitale Wirtschaftsspionage, Sabotage und Datendiebstahl. Passend hierzu hat das World Economic Forum im Global Risks Report 2018 deutlicher denn je vor Cyberangriffen als Top-Risiko gewarnt. In Deutschland sind besonders Hidden Champions im Visier und bezeichnenderweise neigen ausgerechnet jene tendenziell dazu, Cyber-Risiken zu unterschätzen.

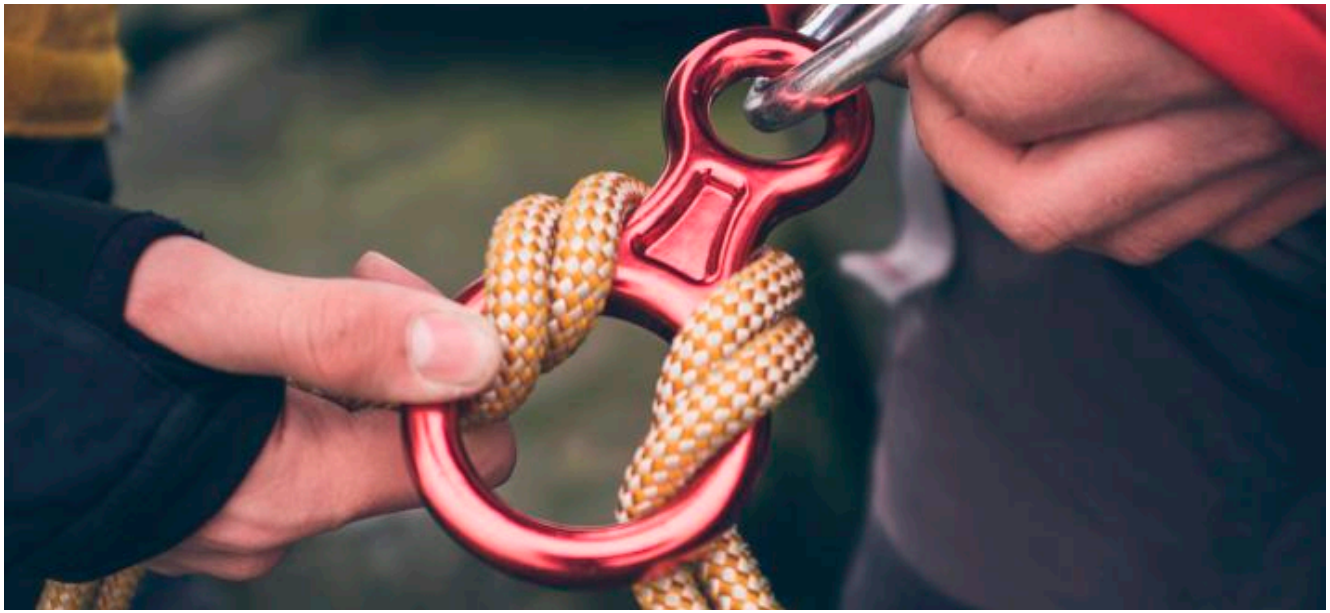
Wer sich die Mühe macht, Cyber-Risiken wahrzunehmen, diese analysiert, bewertet und nach Kräften reduziert, ist im klassischen Risikomanagement angekommen. Dabei ist es unerheblich, ob dies durch eine Gesetzgebung ausgelöst wurde, von einem Großkunden gefordert wird oder der Lernprozess mit einem schmerzlichen Vorfall im eigenen Haus beginnt.

Bei der Behandlung von Cyber-Risiken stellt sich zunehmend die Frage, ob ein immer noch hohes Restrisiko nicht mit einer Versicherung, also einem Risikotransfer, wirtschaftlich gedeckt werden kann. Während Unternehmen noch vor einigen Jahren mangels deutscher Versicherungsprodukte zwangsläufig bei angelsächsischen Versicherern landeten, wächst nun auch der deutsche Cyber-Versicherungsmarkt, wenngleich langsam und zögerlich.

Der Abschluss einer Cyber-Versicherung kann nach meiner Erfahrung durchaus nützlich sein, natürlich bei der Regulierung von Schäden, in Form von Beistand bei akuten Angriffen und sie stimuliert oft die Stärkung der eigenen Abwehrkräfte, denn die Versicherungsbedingungen sind durchaus anspruchsvoll. Die recht hohen Einstiegshürden hemmen derweil den Versicherungsmarkt, so gelten etwa Unternehmen ohne Managementsysteme für Informationssicherheit als nicht versicherbar. Angesichts des bisher bescheidenen Marktvolumens bleibt festzustellen, dass bisher nur ein Bruchteil der insgesamt immensen Risiken aus Industriespionage, Sabotage von IT und Produktionsanlagen und Cyber-Kriminalität über Versicherer umverteilt werden.

Diese Studie belegt, dass sich deutsche Unternehmen zunehmend mit Cyber-Versicherungen beschäftigen. Ich nehme dies als deutliches Indiz dafür, dass das Thema Wirtschaftsschutz immer mehr dort ankommt, wo es der Bedeutung nach hingehört: bei den Unternehmenslenkern in der Chefetage.

Versicherungen gegen Schäden aus Cyber-Angriffen sind zunehmend gefragt. Die neueren Entwicklungen zeigen, dass Versicherungsgesellschaften vermehrt auch Teile dieses Risikos abdecken und versichern. Heute gibt es bereits rund 20 Angebote von Cyber-Versicherungen – Tendenz steigend. Dabei spielt der Grad der Gefährdung durch eigene Sicherheitsmaßnahmen eine wesentliche Rolle. Unternehmen sollten ihr IT-Sicherheitsmanagement nicht vernachlässigen, nur weil sie vermeintlich gegen Schäden aus Cyberattacken abgesichert sind. Eine Versicherung sollte immer nur eine Ergänzung sein. Denn nur wer ausreichend geschützt ist, sodass die Risiken nicht ausufern, kommt als Versicherungsnehmer in Frage. Das Maß der Sicherheits-maßnahmen im Unternehmen ist außerdem entscheidend für die Prämien.

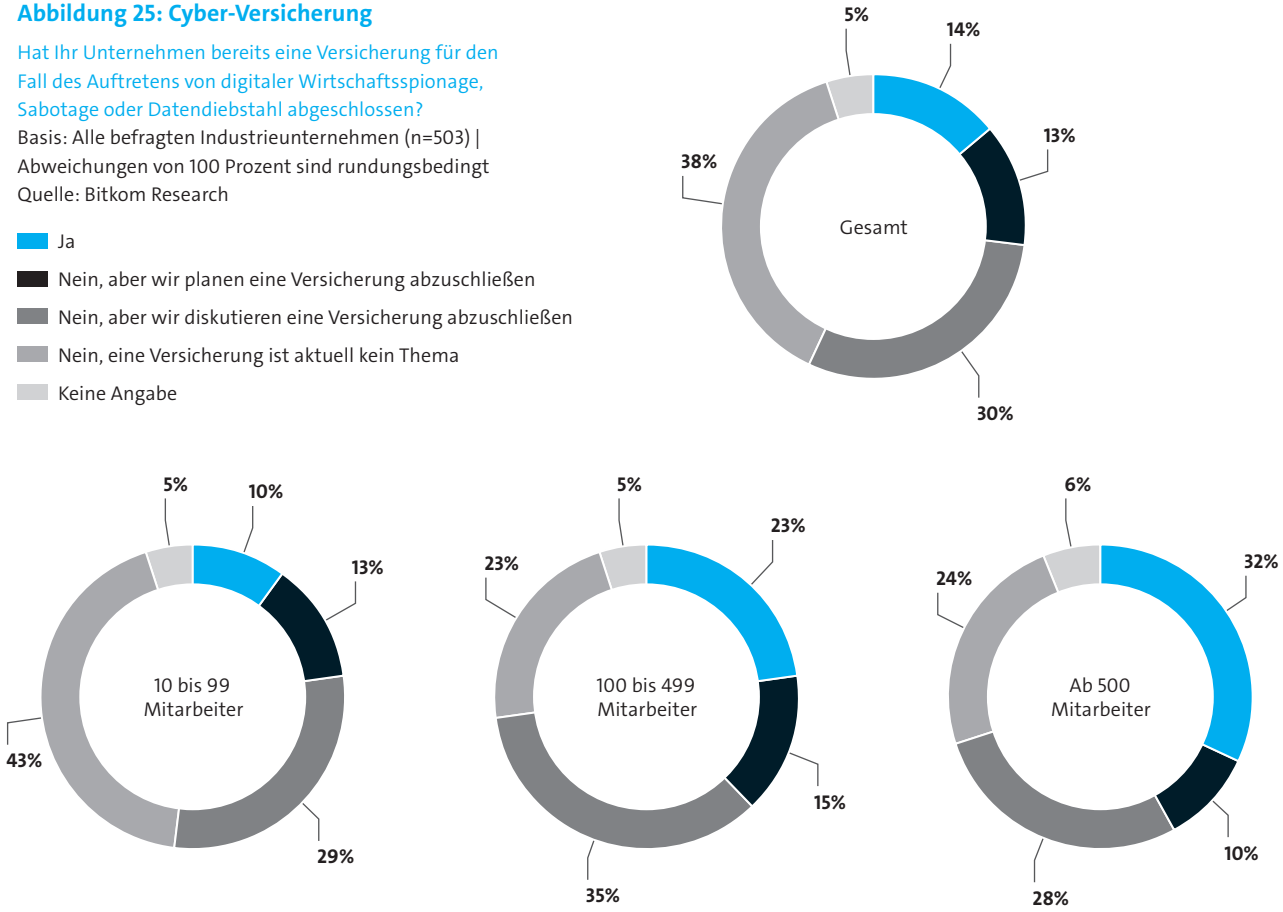


Cyber-Versicherungen sind zunehmend gefragt

Ein überraschendes Ergebnis ist, dass die Anzahl der Unternehmen insgesamt, die eine Versicherung für derartige Risiken abgeschlossen haben, schon bei 14 Prozent liegt. Auch hier lässt sich ein deutlicher Unterschied zwischen kleinen und größeren Unternehmen erkennen. Unternehmen mit mehr als 500 Mitarbeitern haben bereits in genau 32 Prozent der Fälle eine Versicherung abgeschlossen. Bei Unternehmen mit 10 bis 99 Mitarbeitern sind es gerade einmal 10 Prozent. Möglicherweise haben kleine Unternehmen nicht den richtigen Zugang zum Markt oder erfüllen in vielen Fällen nicht die hohen Anforderungen der Versicherungsgeber. Auch muss abgewogen werden, ob sich die Kosten für eine Versicherung tatsächlich lohnen. Ein Nachteil ist sicher, dass nur schwer auszumachen ist, wann tatsächlich ein Haftungsfall eintritt und wann nicht.

Abbildung 25: Cyber-Versicherung

Hat Ihr Unternehmen bereits eine Versicherung für den Fall des Auftretens von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl abgeschlossen?
Basis: Alle befragten Industrieunternehmen (n=503) | Abweichungen von 100 Prozent sind rundungsbedingt
Quelle: Bitkom Research



Cyberversicherungen lohnen sich insbesondere für kleine Unternehmen

In diesem Zusammenhang hat die Studie auch die Frage aufgeworfen, inwieweit sich der Abschluss der Cyber-Versicherung für die Unternehmen gelohnt hat. Insgesamt war der Abschluss nur bei rund 28 Prozent der Unternehmen, die in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und eine Cyber-Versicherung abgeschlossen haben, bisher lohnenswert. Interessant zu sehen ist, dass gerade kleine Unternehmen mit 10 bis 99 Mitarbeiter am meisten davon profitiert haben. Für fast jedes zweite Unternehmen in dieser Größenklasse (48 Prozent) hat sich eine Versicherung gelohnt.

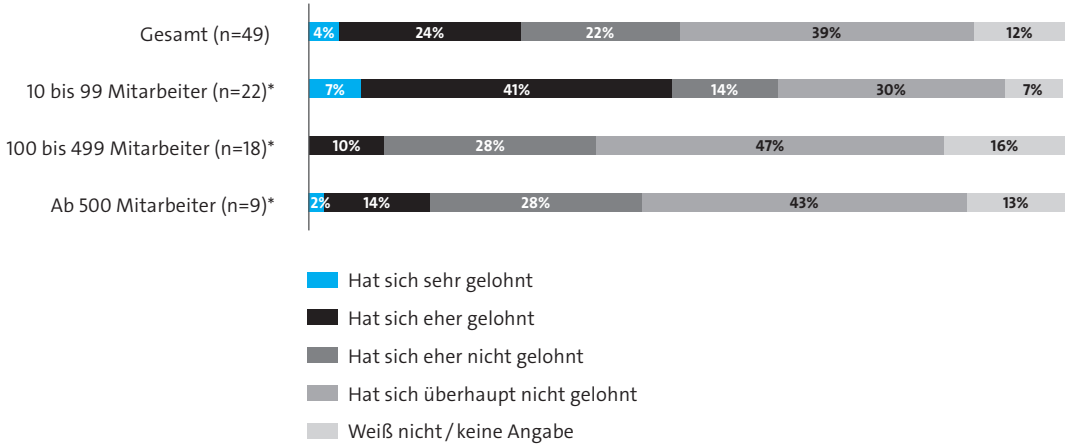


Abbildung 26: Bewertung Cyber-Versicherung 2018

Inwieweit hat sich der Abschluss der Cyber-Versicherung für Ihr Unternehmen bisher gelohnt?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und eine Cyber-Versicherung abgeschlossen haben (n=49) | Abweichungen von 100 Prozent sind rundungsbedingt
* Geringe Fallzahl (n<30)
Quelle: Bitkom Research

8 Fazit und Empfehlungen

Experten-Statement

Axel Petri
Senior Vice President Group Security Governance, Deutsche Telekom AG

»Security builds Trust.« Mit diesen Worten habe ich bereits mein Statement zur letzten BITKOM-Studie Wirtschaftsschutz begonnen. Und auch die wesentlichen Erkenntnisse aus der aktuellen Studie sind nicht grundlegend anders als vor zwei Jahren. Also alles alter Wein in neuen Schläuchen? Nein, keineswegs.

Denn die Digitalisierung schreitet voran. Die technische Entwicklung ist weiter rasant und scheint immer schneller zu werden. Das Vertrauen der Menschen in Digitalisierung ist Grundvoraussetzung für erfolgreiche digitale Geschäftsmodelle. Und hier liegt enormes Potenzial für die Wirtschaft, aber natürlich auch Risiken für den Wirtschaftsschutz.
Und diese sind keineswegs ausschließlich digital. Mehr denn je gilt, dass Sicherheit in den Unternehmen ganzheitlich betrachtet werden muss. Auch und gerade den Mitarbeitern muss bewusst werden, dass sie mit ihrem persönlichen Verhalten (analog oder digital) die Sicherheit des Unternehmens beeinflussen. Dabei müssen die Unternehmen ihnen praktikable Lösungen bieten.
Das schwächste Glied in der Kette bestimmt das Sicherheitsniveau. Deshalb müssen die einzelnen Player heute mehr denn je ihre Einzelinteressen zurückstellen und das große Ganze im Blick haben. Daher sind alle Stakeholder auf staatlicher, privater und gesellschaftlicher Ebene gefragt, ihren Teil zu leisten und Sicherheit dort zu gewährleisten, wo sie am effektivsten zu erzielen ist. Zum Beispiel dadurch, dass Hard- und Softwareprovider bei IT-Schwachstellen Updates bereitstellen. Nur durch Kooperation aller Beteiligten kann die Abwehrfähigkeit der Wirtschaft auf einem angemessenen Niveau gewährleistet werden. Wir müssen zusammenarbeiten.

Unabdingbar für ein erfolgreiches Zusammenspiel von Wirtschaft, Staat und Gesellschaft ist Vertrauen. Insbesondere zwischen staatlichen Stellen und Unternehmen. Der Schlüssel liegt im regelmäßigen Austausch zu generellen Herausforderungen der Sicherheit ergänzt um enge Zusammenarbeit bei der gemeinsamen Bewältigung von Sicherheitsvorfällen. So können – auch wenn natürlich kein absoluter Schutz möglich ist – die immer komplexeren Herausforderungen bewältigt werden.

Mittels Transparenz, Verhältnismäßigkeit und einem offenen gesellschaftlichen Dialog kann der gesetzliche Regelungsrahmen auf die digitalen Herausforderungen justiert werden. Dann werden wir ein Sicherheitsniveau erreichen, dass das zwingend erforderliche Vertrauen der Nutzer in die digitalen Dienste und Services schafft. Denn »Security builds Trust«.

Wirtschaft und Behörden mit Sicherheitsaufgaben stehen vor denselben Herausforderungen. Wir beobachten eine Professionalisierung, Internationalisierung und Industrialisierung von Cybercrime bei gleichzeitig enormer Vergrößerung der Angriffsfläche. Nur mit einem umfassenden Wirtschaftsschutz, der alle Maßnahmen von Politik, Behörden und Wirtschaft zur Minimierung von Cyberrisiken zusammenführt, können wir die Gefahren eindämmen. Besonders Wirtschaftsspionage, Sabotage und Datendiebstahl sind auch weiterhin eine große Bedrohung. Dies belegen die Zahlen der Spezialstudie Wirtschaftsschutz auch in diesem Jahr.

Organisatorische, technische und personelle Sicherheit
Erschreckend ist, dass viele Unternehmen das Thema Sicherheit noch heute zu sehr auf die leichte Schulter nehmen. Auch weil insbesondere kleinen Unternehmen das nötige Bewusstsein und das entsprechende Know-how fehlen. Deshalb ist der erste und wichtigste Schritt, IT-Sicherheit im Unternehmen zur Chefsache zu machen und eigene Wirtschaftsschutz-Beauftragte oder Informations-Sicherheitsbeauftragte zu bestimmen, die die Themen dann in die Breite tragen. Entsprechend müssen Unternehmen vorbeugen und ein robustes IT-Sicherheitsmanagement aufbauen, aktuell halten und engagiert betreiben. Dazu gehört die organisatorische, technische und personelle Sicherheit im Betrieb.

Die organisatorische Sicherheit
Unternehmen kommen nicht mehr umhin ein präventives und permanentes Risikomanagement zu etablieren. Ein umfassendes Risikomanagement kann dabei helfen externe Gefahren zu identifizieren, interne Schwachstellen aufzudecken und rechtzeitig zu beheben. Dazu gehört auch die Etablierung eines Notallplans, der im Ernstfall zum Tragen kommt. Im Krisenfall kommt es auf eine schnelle Reaktion an, was klare Zuständigkeiten und Abläufe voraussetzt.

Zugriffsrechte auf Daten, physische Zugangsrechte für sensible Bereiche sowie eine »Clean-Desk-Policy«, die überprüft welche Daten am Arbeitsplatz nötig sind, fallen genauso unter eine umfassende organisatorische Sicherheit, wie ein Besuchermanagement, das den richtigen Umgang mit Gästen und Delegationen festlegt. Nicht selten bekommen Gäste bei Betriebsführungen Einblick in sensible Bereiche eines Unternehmens.

Die technische Sicherheit
Die Studie zeigt auf, dass ein technischer Basisschutz nahezu in allen Organisationen eingesetzt wird. Da Schadsoftware aber immer komplexer wird und in vielen Fällen unerkannt bleibt, reichen diese Methoden nicht mehr aus. Hinzu kommen die stetig wachsende Angriffsfläche und raffinierte Hackermethoden, wie beispielsweise das Social Engineering. Der Basisschutz sollte deshalb unbedingt um Verschlüsselung und eine spezielle Angriffserkennung ergänzt werden.
Die Überwachung vernetzter Geräte und Erkennung von Anomalien beispieslweise durch ein Security Information Event Management ist ebenso empfehlenswert, wie die Beachtung von Security by Design bei allen Schnittstellen und vernetzten Geräten.

Die personelle Sicherheit
Dass Social Engineering so erfolgreich ist, weist auf Lücken innerhalb der personellen Sicherheit im Unternehmen hin. Dabei sollte der Fokus eines umfassenden Sicherheitsmanagements immer auch auf den eigenen Mitarbeitern liegen. Arbeitsplatzspezifische Schulungen und die Sensibilisierung zu Themen wie Spionage, Sabotage und Datendiebstahl sollten regelmäßig stattfinden. Zur personellen Sicherheit gehört aber auch, dass Mitarbeiter auf sensiblen Positionen einen Hintergrundcheck durchlaufen müssen oder die Möglichkeit besteht, als Mitarbeiter Missstände und Versäumnisse anonym melden zu können.

Nur wenn IT-Sicherheit in der Unternehmenskultur verankert ist, kommt sie auch bei den Mitarbeitern an. Hierfür ist gerade in kleinen und mittleren Unternehmen ein Umdenken nötig. Sich darüber im Klaren zu sein, dass man schon morgen Opfer einer Attacke sein kann, ist der erste Schritt hin zu einem notwendigen Bewusstsein für die Gefahren von Cybercrime.

Sicherheitszertifizierungen
Die Ergebnisse der Studie zeigen, dass Sicherheitszertifizierungen immer noch ein Sonderfall sind. Die Überprüfung des eigenen Sicherheitskonzepts durch eine externe Organisation wie den TÜV oder das BSI ist aber durchaus sinnvoll.

Zusammenarbeit und Vertrauen zwischen Unternehmen und Sicherheitsbehörden stärken

Unternehmen können selbst sehr viel tun, um sich zu schützen. Besonders wichtig bei der Bekämpfung von Cybercrime ist aber auch der Austausch von Informationen und Erfahrungen. Dies sollten Unternehmen zum einen untereinander tun, aber auch mit den staatlichen Behörden. Bestehende Kooperationen, wie beispielsweise die Sicherheitskooperation Cybercrime zwischen Bitkom und sieben Landeskriminalämtern oder die Allianz für Cybersicherheit, sind Plattformen, auf denen der Austausch funktioniert. Solche Organe sollten fortgeführt und ausgebaut werden.

Die Befürchtung, dass durch das Einschalten von Sicherheitsbehörden eine Veröffentlichung des Angriffs folgt und damit ein großer Imageverlust einhergeht, haben immer noch zu viele Unternehmen. Kooperationen zwischen Wirtschaft und Industrie können solche Zweifel aus dem Weg räumen. Unternehmen trauen Behörden oft nicht zu, den Herausforderungen technisch und mit ausreichend Know-how gewachsen zu sein. Die Zentralen Anlaufstellen Cybercrime (ZAC) der Landeskriminalämter sind auf Cyber-Angriffe spezialisiert und bringen die richtige Kompetenz und Erfahrung mit, um diese gewinnbringend mit Unternehmen, insbesondere KMU, zu teilen.

Letztlich kann nur ein umfangreiches Lagebild erstellt werden, wenn alle Vorfälle flächendeckend bei den Sicherheitsbehörden gemeldet werden. Hier spielt dann aber auch der Austausch unter den Behörden eine Rolle. Wichtige Informationen sollten automatisch mit anderen zuständigen Stellen geteilt werden. So können neue Angriffswege erkannt und andere Unternehmen rechtzeitig gewarnt und geschützt werden.

Ganzheitlicher und nachhaltiger Wirtschaftsschutz

Mit der Wirtschaftsschutzstudie hat der Bitkom ein Instrument entwickelt, das umfassende Erkenntnisse über Cyberangriffe auf die deutsche Wirtschaft ermöglicht. Die Ergebnisse der Studie unterstreichen, dass in Zeiten der wachsenden globalen Bedeutung des Cyberraums ein besonderes Augenmerk auf die Abwehr von Cyberangriffen auf die deutsche Wirtschaft gerichtet werden muss. Ziel muss ein ganzheitlicher und nachhaltiger Wirtschaftsschutz sein, der nicht allein IT-bezogene Maßnahmen, sondern insbesondere auch risikominimierende Pläne in den Bereichen Organisation, Personal und Sensibilisierung umfasst. Insbesondere KMU sind künftig gefordert in einen ausreichenden Schutz zu investieren. Hierbei steht der Faktor Mensch zentral im Fokus.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 400 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom