Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt

Studienbericht 2020

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 | T 030 27576-203 | t.ritter@bitkom.org

Projektteam
Teresa Ritter | Véronique Stübinger (Bitkom Research GmbH)

Autoren
Michael Barth (genua GmbH) | Dr. Niklas Hellemann (SoSafe GmbH) | Prof. Timo Kob (HiSolutions) | Christoph Krösmann (Bitkom) | Ursula Morgenstern (Atos Deutschland) | Thomas Tschersich (Telekom) | Teresa Ritter (Bitkom e.V.) | Haya Shulman (Fraunhofer SIT) | Dr. Dan Trapp (Bundesamt für Verfassungsschutz) | Ralf Wintergerst (Giesecke+Devrient)

Redaktion
Linda van Rennings

Gestaltung
Anna Stolz

Bildnachweis
Titelbild: © Cherish Bryck – Stocksy United | Seite 25: © Grycaj – stock.adobe.com

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

Vorwort

Ralf Wintergerst
Group CEO von Giesecke+Devrient, Mitglied Bitkom-Präsidium

Die deutsche Wirtschaft wird zunehmend Opfer von Cyberkriminalität. 2019 waren mindestens 75 Prozent aller Unternehmen von Datendiebstahl, Industriespionage oder Sabotage betroffen, wie die vorliegende Studie des Bitkom zeigt. Mehr als die Hälfte der erfolgreichen Attacken zielte auf den Diebstahl von Identitäten: Damit erhalten Hacker beliebigen Zugang auf Netzwerke, können Infrastruktur kompromittieren und sind in der Lage, vertrauliche Finanz- oder Kundendaten zu entwenden.

Haben digitale Angriffe 2017 noch 43 Prozent aller Unternehmen in Mitleidenschaft gezogen, waren es 2019 bereits 70 Prozent. Die finanziellen Schäden, verursacht durch Produktionsausfälle oder Erpressung, aber auch durch Imageverlust, liegen laut der Studie bei über 100 Milliarden Euro pro Jahr. Es ist davon auszugehen, dass diese Zahl weiter steigen wird.

Gleichzeitig wächst auch die Digitalisierung der Wirtschaft – und mit ihr die Angriffsmöglichkeiten. So wird die Sicherheit der Informationstechnologie in Zukunft über den Erfolg von Unternehmen entscheiden. Es reicht deshalb nicht mehr, dass allein IT-Fachabteilungen vorbeugende Maßnahmen gegen Angriffe treffen. Vielmehr muss die Cyberabwehr zur Chefsache werden. Denn nur die obere Führungsebene kann die Priorität der IT-Sicherheit festschreiben, entsprechende Strukturen schaffen und notwendige Budgets freigeben. Sie muss dafür sorgen, eine Kultur der IT-Sicherheit zu fördern, und zwar über alle Abteilungen hinweg: Jeder einzelne Mitarbeiter ist ein theoretisches Opfer für Phishing-Mails und Social Engineering, wenn ihm das Bewusstsein für Cyberangriffe fehlt. Führungskräfte müssen dieses Bewusstsein schaffen und vorleben. Andererseits darf das Damokles-Schwert möglicher IT-Attacken nicht dazu führen, Mitarbeiter einzuengen. Auch für ein Klima des anspannungsfreien Arbeitens muss die Chefetage sorgen, gerade in Zeiten der zunehmenden Digitalisierung.

Unternehmen jedweder Größe, die sich nicht gründlich im Rahmen einer umfassenden IT-Sicherheitsstrategie auf Cyberangriffe vorbereiten – mit der richtigen Infrastruktur, sicherheitsorientierten Strukturen, ausreichenden Budgets, mündigen Mitarbeitern und vorbildlichen Führungskräften – laufen Gefahr, finanzielle Schäden und Imageschäden zu erleiden, und dadurch auch die Schwächung ihrer Wettbewerbsfähigkeit. Tatsächlich gibt es zahlreiche hochwertige IT-Sicherheitslösungen deutscher Anbieter, die Unternehmen maßgeschneidert auf ihre jeweiligen Bedürfnisse anpassen können.

Bei der Sensibilisierung zum Thema Informations- und Cybersicherheit spielt der Bitkom in Deutschland eine Vorreiterrolle. Gerade mittelständische Unternehmen verfügen in der Regel nicht über ausreichende Ressourcen für einen umfassenden Kompetenzaufbau rund um die Cybersicherheit. Diese Lücke hilft der Bundesverband zu schließen.

Nur im gemeinsamen Handeln aller Akteure, seien es Unternehmen, Hersteller, die Politik oder die Digitalwirtschaft, kann das Ziel erreicht werden, die Cybersicherheitslage zu verbessern und damit den Erfolg des Wirtschaftsstandorts Deutschland weiter zu fördern.

Einleitung und Methodik

Der Digitalverband Bitkom untersucht mit der vorliegenden Studie nun zum dritten Mal nach 2015 und 2017, wie es um die deutsche Wirtschaft beim Thema Wirtschaftsschutz bestellt ist. Mit der Studie hat Bitkom ein Instrument entwickelt, das umfassende Erkenntnisse über Cyberangriffe auf die deutsche Wirtschaft ermöglicht. 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 1.070 nach Branchen und Größenklassen repräsentativ ausgewählte Unternehmen 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 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 und Juni 2019 von im Vorfeld speziell geschulten Telefoninterviewern durchgeführt.

Auch die Ergebnisse der aktuellen Studie unterstreichen, dass in Zeiten der zunehmenden Vernetzung all unserer Lebensbereiche die Resilienz der deutschen Wirtschaft gegen Gefahren aus dem Cyberraum weiter ausgebaut werden muss. Es gilt einen ganzheitlichen und nachhaltigen Wirtschaftsschutz zu etablieren, der nicht allein IT-bezogene Maßnahmen, sondern insbesondere auch risikominimierende Pläne in den Bereichen Organisation und Personal umfasst. Hierbei nimmt der Faktor Mensch weiterhin eine Schlüsselrolle ein. Ein enger und vertrauensvoller Erfahrungsaustausch mit den Sicherheitsbehörden kann Unternehmen dabei unterstützen.

1 Betroffene Unternehmen

1.1 3 von 4 Unternehmen sind Opfer geworden

Beginnen wir gleich mit einem bemerkenswerten Ergebnis: 75 Prozent der Unternehmen waren in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen. Weitere 13 Prozent waren vermutlich betroffen – denn nicht immer lässt sich ein Angriff zweifelsfrei feststellen. Somit war fast die gesamte Industrie von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen oder vermutlich betroffen. Damit haben Umfang und Qualität der Angriffe auf Unternehmen dramatisch zugenommen. Zum Vergleich: In 2015 und 2017 war nur gut jedes zweite Unternehmen betroffen.

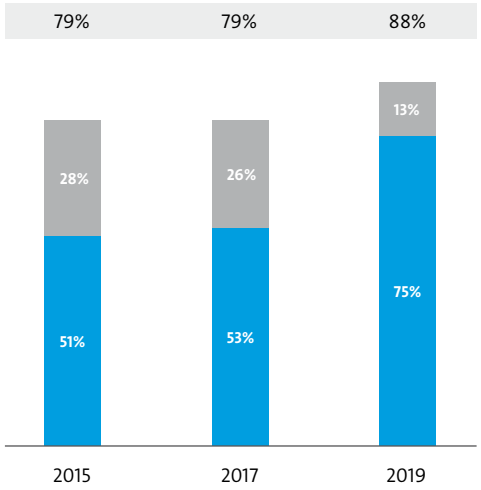


Abbildung 1: Attacken haben stark zugenommen

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

Basis: Alle befragten Unternehmen (2019: n=1.070; 2017: n=1.069; 2015: n=1.074)
Quelle: Bitkom Research

Vermutlich betroffen
Betroffen
Gesamt

1.2 Kleine Unternehmen weiterhin im Fokus der Angreifer

Im Vergleich zu den Ergebnissen aus den Jahren 2015 und 2017 steigt die Anzahl der Betroffenen oder vermutlich Betroffenen in allen Größenklassen an. Besonders die kleinen Unternehmen, mit 10 – 99 Mitarbeitern, stehen weiterhin im Fokus der Angreifer. 88 Prozent waren in den Jahren 2017 und 2018 von Spionage, Sabotage oder Datendiebstahl betroffen oder vermuten dies. Gerade kleine Unternehmen sind besonders innovativ und stark in die Lieferketten von großen Konzernen eingebunden. Der Angreifer hat es also entweder auf das Spezialwissen der KMU abgesehen oder nutzt kleine Unternehmen als Einfallstore auf Größere.

Aber auch große Unternehmen geraten zunehmend selbst unter Beschuss. So gaben 78 Prozent der Unternehmen mit mehr als 500 Mitarbeitern an, von Angriffen betroffen gewesen zu sein. Dies ist ein Anstieg von 18 Prozent im Vergleich zur Erhebung in 2017 und ein Anstieg von 24 Prozent im Vergleich zur Studie aus 2015.

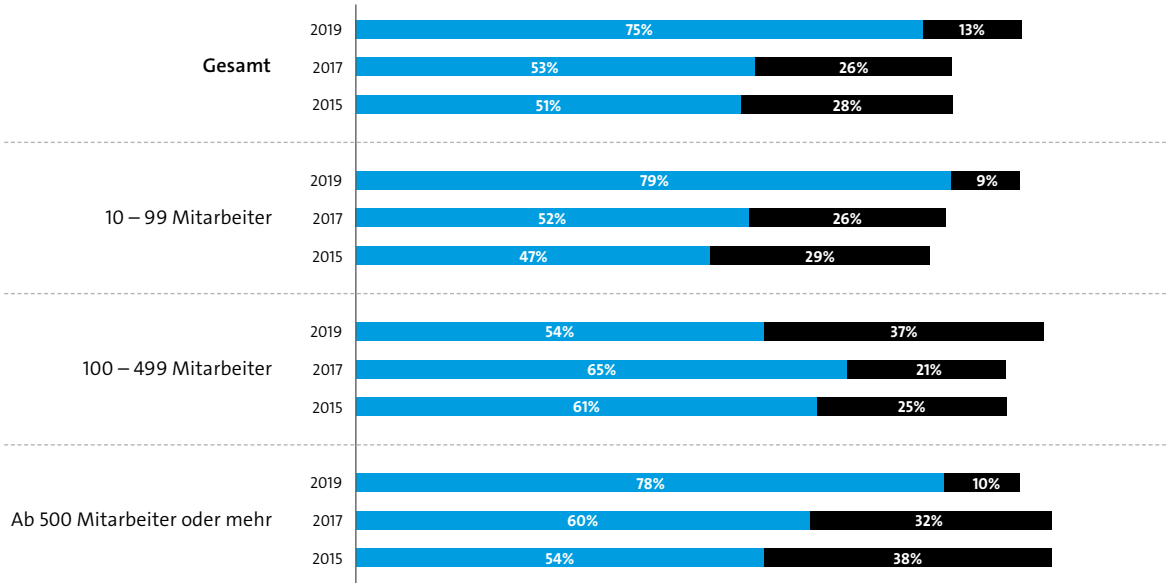


Abbildung 2: Betroffene Unternehmen nach Betriebsgrößenklasse

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

Basis: Alle befragten Unternehmen
(2019: n=1.070; 2017: n=1.069; 2015: n=1.074)
Quelle: Bitkom Research

Betroffen
Vermutlich betroffen

Experten-Statement

Thomas Tschersich
Chief Security Officer, Deutsche Telekom

Bereits heute hat jeder zweite Mensch Zugang zum Internet und schon 2020 soll die Marke von weltweit 50 Milliarden vernetzten Geräten geknackt werden. Die zunehmende Vernetzung (Internet of Things) und Digitalisierung führen automatisch auch zu mehr Schwachstellen. Genau darauf haben es Cyberkriminelle abgesehen: Angriffe erfolgen heute professioneller und automatisierter als je zuvor. Ist eine Sicherheitslücke vorhanden, wird diese auch ausgenutzt. Zuletzt hat der Emotet-Trojaner gezeigt, dass diese Angriffe deutlich aggressiver und raffinierter werden. Die Frage ist also weniger ob, sondern vielmehr wann und unter welchen Bedingungen ein Angriff stattfindet. Die Anzahl an Phishing-Mails mit Schadsoftware, Erpressungstrojanern & Co. wird in naher Zukunft weiter steigen. Und es scheint nicht so, als würde sich das bald ändern. Neben dem technologischen Fortschritt von Machine Learning und Künstlicher Intelligenz werden Cyberkriminelle auch verstärkt auf die »Schwachstelle Mensch« abzielen. Social Engineering beispielsweise, in Form von CEO-Fraud-Angriffen oder dem Enkeltrick per Stimmimitation, ist erst der Anfang einer ganzen Reihe von möglichen Missbrauchsszenarien. Manipulierte Videos, mit denen man jedem Worte in den Mund legen kann, die so nie gesagt wurden oder die Handlungen vorgaukeln, die so nie stattgefunden haben, sind alarmierende Aussichten. Wem oder was können unsere Augen und Ohren dann überhaupt noch trauen? Deep Fakes wirken heute zwar noch weitestgehend plump und durchschaubar, es wird aber nicht mehr allzu lange dauern, bis die perfekte Täuschung gelingt. Die Folgen kann sich jeder ausmalen.

Letztlich ist es ist ein nicht endenden wollendes Katz- und Mausspiel zwischen den Angreifern auf der einen Seite und dem Rest von uns auf der anderen Seite. Wobei die Angreifer einen entscheidenden Vorteil haben: Eine Schwachstelle reicht.

Mehr IT-Sicherheit ist eine gesamtheitliche Aufgabe die letztendlich nur durch eine starke Kooperation von Staat und Privatwirtschaft gemeinsam bewältigt werden kann. Wir brauchen mehr digitale Kompetenzen und müssen das Sicherheitsbewusstsein in der Gesamtbevölkerung stärken. Und auch die Medien müssen das Thema anders als bisher aufgreifen und nicht nur über Gefahren berichten, sondern dabei helfen, Lösungswege aufzuzeigen. Wir müssen uns gegenseitig warnen und voneinander lernen, nur so können wir als Unternehmen aufholen und die Komplexität von Cyber Security bewältigen.

1.3 Diebstahl und Social Engineering häufige Delikte

Neben der allgemeinen Betroffenheit von Unternehmen, befasst sich die Studie auch mit den unterschiedlichen Arten von digitalen und analogen Angriffen. Demnach berichtet jedes fünfte Unternehmen (21 Prozent), dass ihm sensible digitale Daten bzw. Informationen gestohlen wurden. Fast genau so viele Unternehmen (17 Prozent) waren von der Sabotage der Informations- und Produktionssysteme oder Betriebsabläufe betroffen. Bei jedem achten Unternehmen (13 Prozent) ist die digitale Kommunikation ausgespäht worden. Es wird aber nach wie vor noch oft analog angegriffen.

Bei einem Drittel der Unternehmen (32 Prozent) wurden IT- oder Telekommunikationsgeräte entwendet. Sensible physische Dokumente, Maschinen oder Bauteile wurden bei jedem Sechsten gestohlen. Weiter auf dem Vormarsch ist das sogenannte Social Engineering. Dabei werden Mitarbeiter manipuliert, um an sensible Informationen zu kommen, mit denen dann in einem weiteren Schritt zum Beispiel Schadsoftware auf die Firmenrechner gebracht werden kann. Mehr als jedes fünfte Unternehmen (22 Prozent) war davon analog betroffen, 15 Prozent digital.

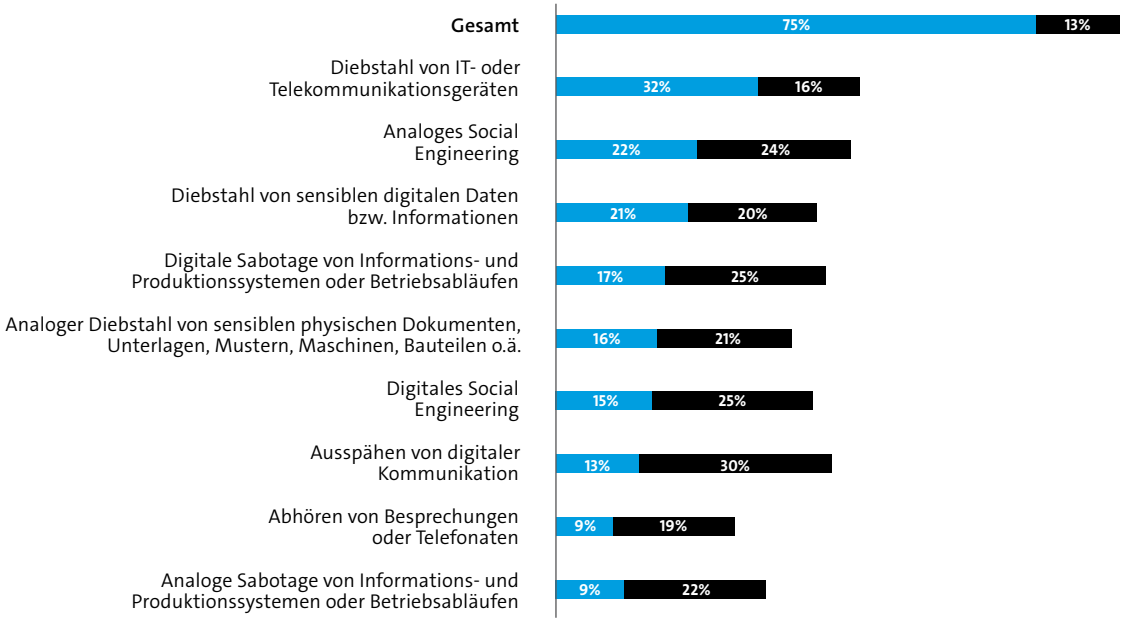


Abbildung 3:
Diebstahl und Social Engineering häufige Delikte

Von welchen der folgenden digitalen oder analogen Arten von Datendiebstahl, Industriespionage oder Sabotage war Ihr Unternehmen innerhalb der letzten zwei Jahre betroffen bzw. vermutlich betroffen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research

Betroffen
Vermutlich betroffen

1.4 Daten aller Art im Visier: Finanz-, Mitarbeiter- und Kundendaten

Datendiebstahl war eines der häufigsten Delikte, von denen die befragten Unternehmen betroffen waren. In einem weiteren Schritt fragt die Studie nach der Art der Daten, die abgeflossen sind. Angreifer haben bei ihren Attacken unterschiedlich sensible Daten erbeutet. Bei fast der Hälfte (46 Prozent) der betroffenen Unternehmen wurden Kommunikationsdaten wie E-Mails gestohlen. Bei jedem vierten Unternehmen sind durch digitale Angriffe jeweils Finanzdaten (26 Prozent), Mitarbeiterdaten (25 Prozent) und Kundendaten (23 Prozent) abgeflossen. Kritische Geschäftsinformationen wie Marktanalysen oder Preisgestaltung sind bei jedem achten Unternehmen (12 Prozent) in kriminelle Hände gefallen.

Unkritische Business-Informationen sind bei 34 Prozent abgeflossen. Das ist ein starker Rückgang im Vergleich zur Studie aus dem Jahr 2017. Hier waren es noch rund 62 Prozent. Dieses Ergebnis könnte ein Hinweis darauf sein, dass Angreifer zunehmend professioneller und gezielter ihre Angriffe zum Erfolg führen.

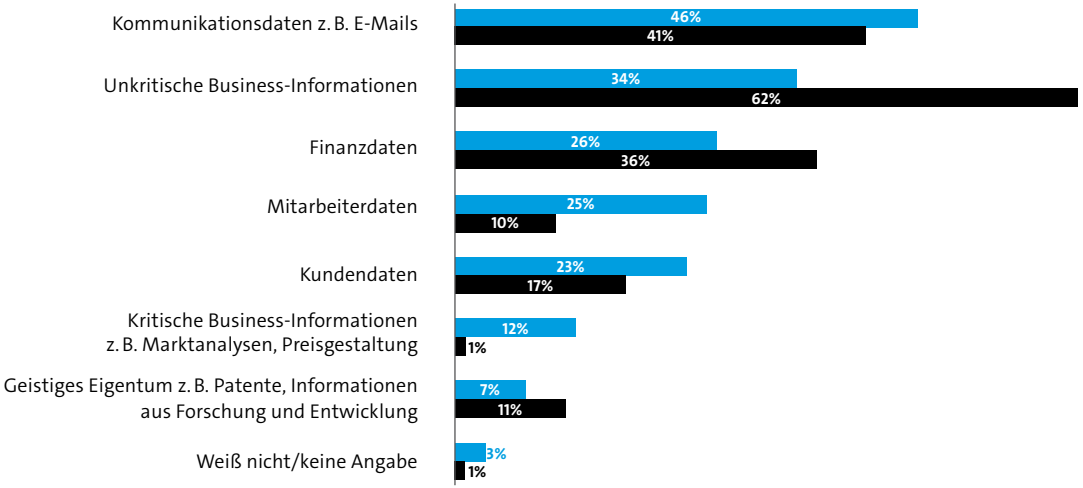


Abbildung 4:
Datendiebe interessieren Kommunikations- und Finanzdaten

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Diebstahl von sensiblen digitalen Daten betroffen waren (2019: n=229; 2017: n=178); Mehrfachnennungen in Prozent
Quelle: Bitkom Research

»Im globalen Wettbewerb kann jede Information über die Konkurrenz zum Vorteil werden – dafür greifen immer mehr Unternehmen zu kriminellen Mitteln.«

Achim Berg, Bitkom-Präsident, Berlin 2020

1.5 Marketing und Vertrieb sind attraktive Geschäftsbereiche

Die Unternehmensbereiche Marketing und Vertrieb waren am häufigsten von Sabotage, Spionage und Datendiebstahl betroffen. Drei von zehn der betroffenen Unternehmen (33 Prozent) gaben das an. Es folgen Lager und Logistik (28 Prozent), Personalwesen und Human Resources (27 Prozent) sowie die IT (27 Prozent). Aber auch die Geschäftsführung und das Management (26 Prozent), die Produktion (hinter Fertigung) und Fertigung sowie das Finanz- und Rechnungswesen (23 Prozent) sind attraktive Unternehmensbereiche für Hacker. Auf Forschungs- und Entwicklungsdaten sehen es die Angreifer in dem gleichen Maße ab, wie auf Daten des Einkaufs. Beide Bereiche waren in 15 bzw. 16 Prozent der Fälle Ziel der Angreifer.

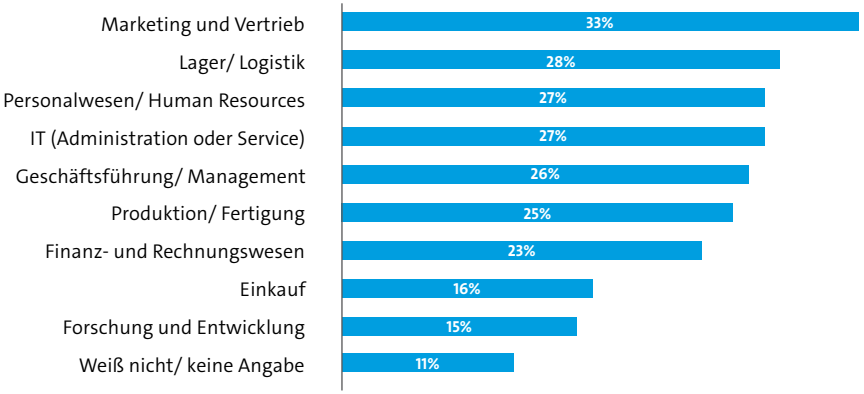


Abbildung 5:
Marketing und Vertrieb sind attraktive Geschäftsbereiche

Welche der folgenden Bereiche Ihres Unternehmens waren von Datendiebstahl, Industriespionage oder Sabotage in den letzten zwei Jahren betroffen?

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=801); Mehrfachnennungen in Prozent

Quelle: Bitkom Research

2019

1.6 Digitale Angriffe haben bei 7 von 10 Unternehmen Schäden verursacht

Gerade Cyberangriffe sind für die gesamte Wirtschaft ein Problem. 7 von 10 Unternehmen sind so in den vergangen zwei Jahren zu Schaden gekommen. Das ist ein Anstieg um 27 Prozent im Vergleich zur Studie von 2017. Ein Viertel berichtet von Angriffen auf Passwörter, ähnlich viele von der Infizierung mit Schadsoftware und durch Phishing-Angriffe. Das sogenannte Spoofing führte bei 8 Prozent zu Schäden. Hierbei handelt es sich um Methoden, mit denen sich Authentifizierungs- und Identifikationsverfahren untergraben lassen, etwa indem IP-Pakete beim Datentransfer manipuliert werden und sie dadurch falsche Absenderinformationen beinhalten.

Die Ergebnisse geben einen deutlichen Hinweis darauf, dass Hacker zunehmend mehr Zeit und Ressourcen in ihre Arbeit investieren. Die Freizeithacker von früher haben sich zu gut ausgerüsteten und technologisch oft sehr versierten Cyberbanden weiterentwickelt – zuweilen mit Staatsressourcen im Rücken.

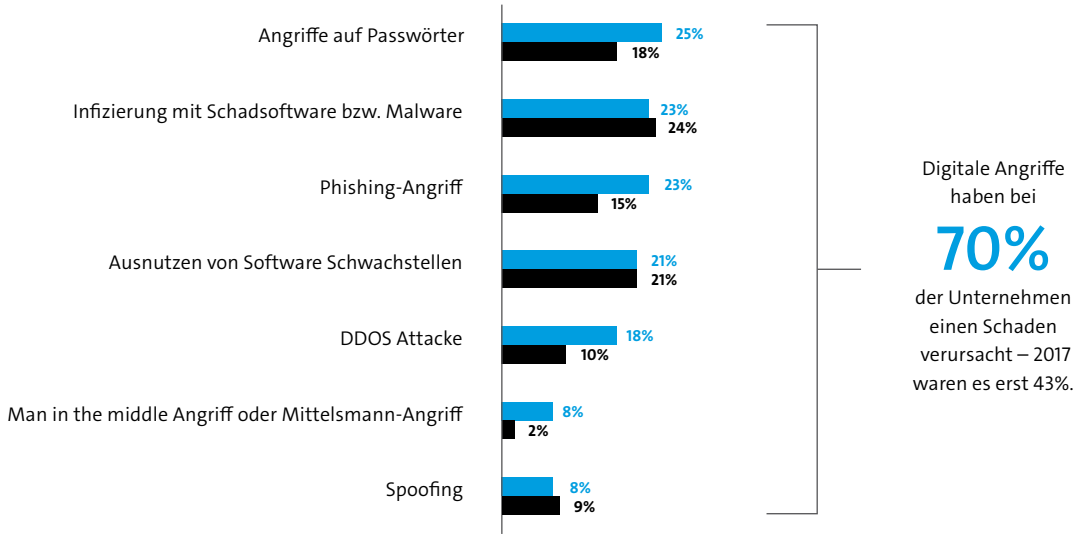


Abbildung 6: Digitale Angriffe haben bei 7 von 10 Unternehmen Schäden erzeugt

Welche der folgenden Arten von digitalen Angriffen haben innerhalb der letzten zwei Jahre in Ihrem Unternehmen einen Schaden verursacht?

Basis: Alle befragten Unternehmen (2019: n=1.070; 2017: n=1.069); Mehrfachnennungen in Prozent
Quelle: Bitkom Research

»Umfang und Qualität der Angriffe auf Unternehmen haben dramatisch zugenommen. Die Freizeithacker von früher haben sich zu gut ausgerüsteten und technologisch oft sehr versierten Cyberbanden weiterentwickelt – zuweilen mit Staatsressourcen im Rücken.«

Achim Berg, Bitkom-Präsident, Berlin 2020

1.7 Cyberattacken nehmen weiter zu

Die Unternehmen wurden auch befragt, wie sich die Anzahl der Cyberattacken in den letzten zwei Jahren entwickelt hat. 74 Prozent der befragten Unternehmen gaben an, dass die Angriffe stark bzw. eher zugenommen haben. In 23 Prozent der Fälle sind sie unverändert geblieben.

Die Studie unterscheidet auch zwischen KRITIS und Nicht-KRITIS-Sektoren. 80 Prozent der KRITIS-Sektoren haben eine Zunahme der Angriffe vernommen. Im Nicht-KRITIS-Bereich sind es nur 73 Prozent. Dieses Ergebnis kann durchaus als Warnsignal für unsere Kritischen Infrastrukturen gesehen werden: sie sind ein zunehmend attraktiver werdendes Ziel für Cyberkriminelle.

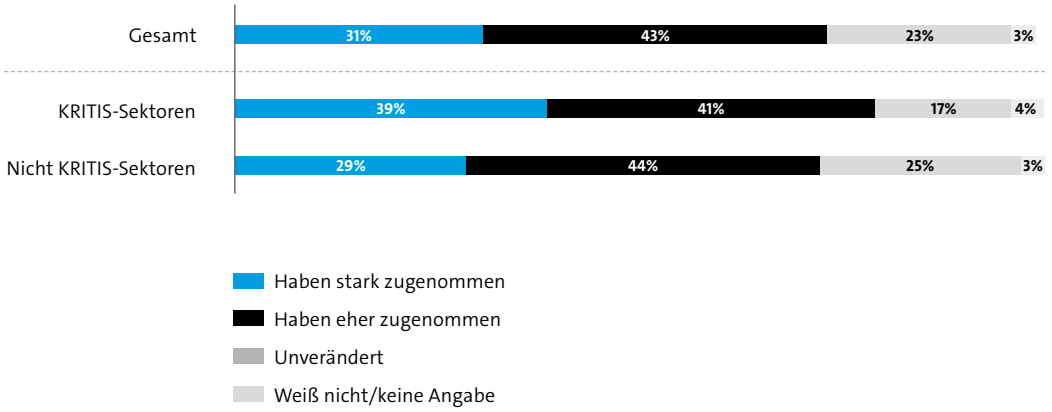


Abbildung 7:
Cyberattacken nehmen stetig zu

Wie hat sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den vergangenen zwei Jahren entwickelt?

Basis: Alle befragten Unternehmen (n=1.070); Abweichungen von 100% sind rundungsbedingt.
Quelle: Bitkom Research

1.8 Breite Mehrheit überzeugt: Künftig noch mehr Cyberattacken

Der Blick in die Zukunft sieht nicht weniger düster aus. Eine breite Mehrheit der befragten Unternehmen prognostiziert eine weitere Verschärfung der Sicherheitslage. 82 Prozent gehen davon aus, dass die Zahl der Cyberattacken auf ihr Unternehmen in den nächsten zwei Jahren zunehmen wird. Die Anzahl der Unternehmen, die glauben, dass die Angriffe abnehmen, ist verschwindend gering.

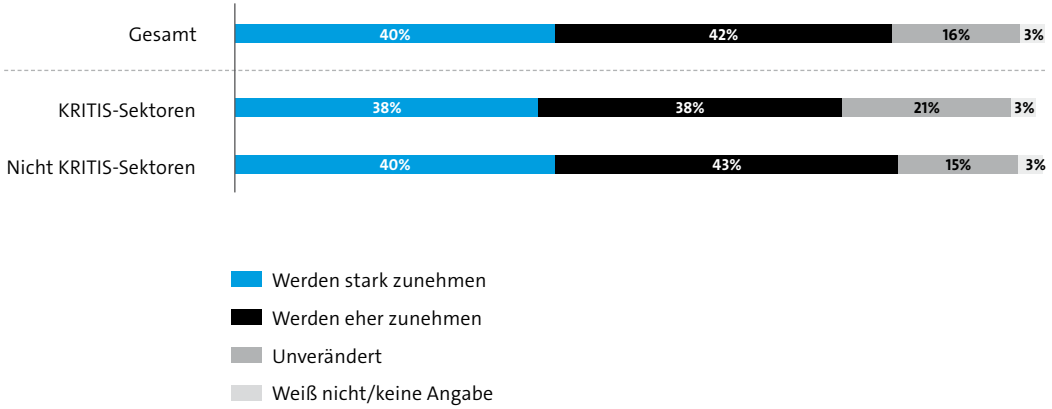


Abbildung 8: Breite Mehrheit überzeugt: Künftig noch mehr Cyberattacken

Wie wird sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den nächsten zwei Jahren im Vergleich zu den letzten zwei Jahren voraussichtlich entwickeln?

Basis: Alle befragten Unternehmen (n=1.070); Abweichungen von 100% sind rundungsbedingt.
Quelle: Bitkom Research

Experten-Statement

Dr. Haya Shulman
Abteilungsleiterin am Fraunhofer SIT

Aktuelle und zukünftige Bedrohungsszenarien: Die Resilienz und Sicherheit des Internets sind für die Stabilität moderner Gesellschaften von entscheidender Bedeutung. Angriffe im und aus dem Cyberraum bedrohen alle Aspekte unserer Online-Aktivitäten und unseres täglichen Lebens – von intelligenten vernetzten Städten und kritischen Infrastrukturen bis hin zu Finanztransaktionen und Telefonie. Das vorliegende Statement fokussiert auf Bedrohungen für zentrale Internetinfrastrukturen und Funktionen, die für die Gewährleistung der Sicherheit von Anwendungen und Diensten von entscheidender Bedeutung sind. Wir führen einige der wichtigsten Bedrohungen und Gegenmaßnahmen auf. Impersonation: Viele Cyberangriffe beginnen mit sogenannten Impersonation-Angriffen, d.h. der Angreifer gibt vor, eine legitime Domäne, eine legitime IP-Adresse oder ein legitimes Netzwerkgerät zu sein. Auf diese Weise erhält der Angreifer das nötige Vertrauen und die nötigen Rechte, um weitere Angriffe durchzuführen. Digitale Zertifikate für Internet Ressourcen können solche Angriffe verhindern, indem sie Nutzern und Diensten ermöglichen, einen sicheren Kommunikationskanal herzustellen, wie z. B. in Web PKI. Dennoch ist auch die Ausstellung der Zertifikate eine Herausforderung – es stellt sich nämlich die Frage, inwieweit der Besitzer einer Ressource (Domäne, IP oder Gerät) im Internet seine Identität zweifellos nachweisen kann. Solche Angriffe sind häufig und werden noch weiter zunehmen. Veraltete und fehlerhafte Infrastruktur: Fehlerhafte und nicht gepatchte Geräte sind eine der Hauptursachen für Ausfälle und Fehler und stellen signifikante Schwachstellen im Internet dar. Beispielsweise wurden in der jüngsten Vergangenheit Fehler bzw. Fehlkonfigurationen in SOHO-Routern vom Mirai-Botnet ausgenutzt, um großflächige Denial-of-Service-Angriffe auszulösen, und ein einzelnes Routing-Announcement führte dazu, dass fehlerhafte FRR Router ganze Netze vom Internet trennten. Die Resilienz des Internets hängt entscheidend von der Fähigkeit ab, solche Geräte zu identifizieren und zu patchen. Auch dieses Problem wird in der Zukunft stark an Bedeutung gewinnen. Verkehrsumleitungen: Viele Angriffe beginnen heutzutage mit missbräuchlicher Traffic-Übernahme. Dabei leitet der Angreifer den Datenverkehr über von ihm kontrollierte bösartige Netzwerke um. Dies ermöglicht das Abhören der Kommunikation sowie die Verbreitung von Malware und den Diebstahl sensibler und persönlicher Informationen. Um solche Angriffe zu verhindern, ist die Sicherung der wichtigsten Internet-Routing- und -Namenssysteme von entscheidender Bedeutung. Obwohl diese Systeme seit den frühen Formen des heutigen Internets existieren, sind sie immer noch sehr anfällig für Angriffe. Zunehmend werden diese Angriffe für politisch motivierte Spionage und Angriffe auf kritische Infrastrukturen und das Finanzsystem verwendet.

Infizierung mit Schadsoftware wird als größte Bedrohung wahrgenommen

Die Infizierung mit Schadsoftware wird von den befragten Unternehmen als größte Bedrohung wahrgenommen. Über 90 Prozent der befragten Unternehmen fürchten dieses Szenario. Auch die sogenannten Zero-Day-Exploits gelten weiterhin als große Gefahr (90 Prozent). Drei Viertel (76 Prozent) gaben an, dass die zunehmende Anzahl vernetzter Geräte eine Bedrohung darstellt und genauso viele nehmen das Einbauen von Backdoors als Gefahr wahr. Auch der Mangel an qualifizierten IT-Sicherheitsfachkräften sowie die zunehmende Fluktuation von Mitarbeitern bereiten 69 bzw. 68 Prozent der Befragten Sorge. Das Anzapfen von Rechenleistungen von außen, um etwa Kryptowährungen zu schürfen, nehmen nur 25 Prozent der Unternehmen als echte Gefahr wahr.

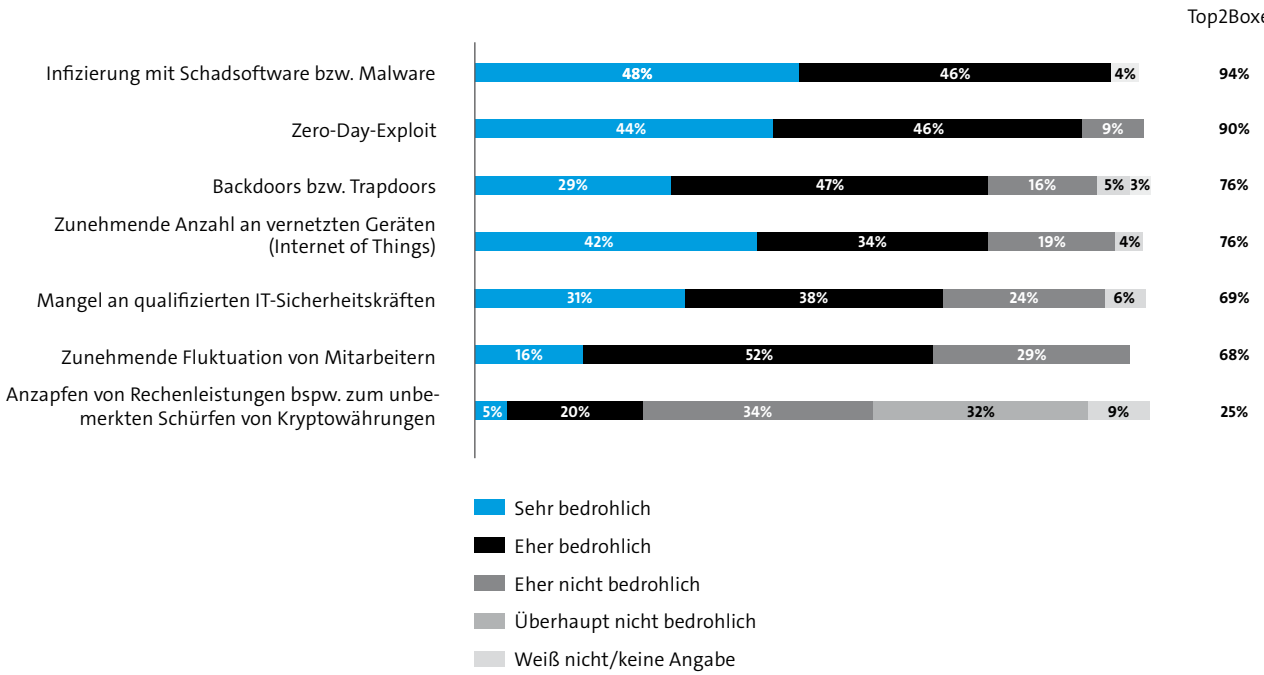


Abbildung 9: Infizierung mit Schadsoftware als größte Bedrohung

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

Basis: Alle befragten Unternehmen (n=1.070); Werte ≤2 zu übersichtlichen Darstellung ausgeblendet.
Quelle: Bitkom Research

2 Aufgetretene Schäden

Experten-Statement

Prof. Timo Kob
Vorstand HiSolutions AG

Stärkster Treiber der steigenden Schadenssummen sind immer besser erprobte Möglichkeiten zur Monetarisierung krimineller Aktivitäten u.a. durch Lösegeld – hauptsächlich zur Wiederbeschaffung verschlüsselter Daten, in steigender Zahl - und teils auch kombiniert – aber auch als Preis für Nicht-Veröffentlichung von Daten.

Häufigster Angriff ist automatisierte Ransomware kombiniert mit der Nutzung von Kryptogeld zum Lösegeldtransfer und zur (erhofften) Identitätsverschleierung. Durch die starke Öffentlichkeitswirksamkeit solcher Angriffe und bessere Vorsorgemaßnahmen sinken aber die Margen. Die besser werdende Verfolgung von Kryptogeldüberweisungen erhöht gleichzeitig den Aufwand für die Angreifer.

Aber auch die Ransomware wird besser:

- Automatische Exfiltration von E-Mails, die als Grundlage für individuell zugeschnittene Angriffs-Emails an weitere Mitarbeiter und Geschäftspartner dienen (z. B. Emotet),
- automatisierte Erstellung der passenden Angriffsmails,
- Ausspähung von Passwörtern, Bankverbindungen u. ä. (z. B. Trickbot).

Stark zunehmend seit 2018 sind gezielte, manuell unterstützte Angriffe mit hohen Lösegeldforderungen - Forderungen bis in den zweistelligen Millionenbereich sind bisher bekannt geworden. Nach automatisierten Angriffswellen werden als »lohnend« erachtete Ziele manuell ausgekundschaftet, die Kontrolle über zentrale Komponenten (z. B. Windows-Domäne) übernommen, um dann systematisch die Integrität von Backups zu zerstören und eine Ransomware koordiniert auf möglichst vielen Systemen des Unternehmens einzusetzen. Diese Angriffe werden teilweise auch mit der Drohung der Veröffentlichung von Daten kombiniert.

Bei Unternehmen mit internet-abhängigem Geschäftsmodell werden weiterhin Erpressungen mit der Drohung von Distributed-Denial-of-Service-Angriffen (DDoS) durchgeführt. Durch die Erhöhung der dem Botnetz zur Verfügung stehenden Bandbreiten haben sich gefährliche Varianten entwickelt, wie z. B. das »Carpet Bombing« - hier werden nicht mehr die IP-Adressen/Domänen des eigentlichen Opfers angegriffen, sondern schlicht alle Adressen des Internet-Service-Providers des Opfers (»upstream ISP«). Dies erschwert die klassischen Methoden zur Bekämpfung und bringt hohe Kollateralschäden mit sich.

In der Statistik u. U. unterrepräsentiert sind Fälle von Industriespionage und dem Wirken staatlicher oder staatsnaher Organisationen, da hier aktiv daran gearbeitet wird, eine Entdeckung zu vermeiden. Während Industriespionage noch durch seine Auswirkungen auffallen kann, sind die Aktivitäten staatlicher Akteure oft ausschließlich auf Aktionsfähigkeit in der Zukunft ausgelegt, auf die Sammlung von Informationen und die Aufrechterhaltung von Zugriffsmöglichkeiten. Ziele sind nicht nur staatliche Organisationen, sondern auch kritische Infrastrukturen in allen Sektoren und behördennahe Dienstleister. Die weltweit steigenden Bemühungen in diesem Bereich zeichnen sich auch in einem erhöhten individuellen Risiko ab.

2.1 Schadenrechnungsmodell

Das zentrale Ziel dieser Studie ist die Bestimmung des Gesamtschadens, der durch Wirtschaftsspionage, Sabotage oder Datendiebstahl in der deutschen Wirtschaft in den zurückliegenden zwei Jahren entstanden ist. Um die Ergebnisse mit den vorherigen Untersuchungen vergleichen zu können, wurden das Studiendesign und die Methodik im Wesentlichen beibehalten.

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 Gesamtwirtschaft hochgerechnet. Bei der Berechnung der Durchschnittswerte bzw. Mittelwerte wurde die Stichprobe um Ausreißer bereinigt. Folglich kann man wie bereits bei den vorangegangen Untersuchungen von einer eher konservativen Berechnung der Schadenssummen sprechen. Die Hochrechnung erfolgte auf der Grundlage der Umsatzsteuerstatistik des Statistischen Bundesamtes.

2.2 Insgesamt über 100 Mrd. Euro Schaden pro Jahr

Bei der Berechnung der Schadenssumme werden analoge wie digitale Angriffe betrachtet. Der hierfür errechnete Gesamtschaden innerhalb der letzten zwei Jahre beträgt 205,7 Milliarden Euro, also über 100 Milliarden Euro Schaden pro Jahr. Damit wurde nahezu eine Verdopplung im Vergleich zur Schadenssumme in 2017 (55 Milliarden Euro p. a.) erreicht.

Am höchsten sind die Kosten für Ermittlungen und Ersatzmaßnahmen (36,5 Milliarden Euro), gefolgt von Kosten für Rechtsstreitigkeiten (31,2 Milliarden Euro) und Patentrechtsverletzungen (28,6 Milliarden Euro). Aber auch Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen forderte Kosten in Höhe von 27 Milliarden Euro, gefolgt von den entstandenen Kosten für Umsatzeinbußen durch nachgemachte Produkte (Plagiate) sowie durch Verlust von Wettbewerbsvorteilen in Höhe von jeweils 22, 2 Milliarden Euro. Die Erpressung mit gestohlenen oder verschlüsselten Daten verursachte einen Schaden von 10,5 Milliarden Euro und die Kosten für datenschutzrechtliche Maßnahmen (z. B. Information von Kunden), die nach einem Angriff ergriffen werden mussten, lagen bei 8,8 Milliarden Euro.

Die Gründe für den gewaltigen Anstieg der Schadenssumme sind vielfältig. Es sind deutlich mehr Unternehmen von Spionage, Sabotage und Datendiebstahl betroffen gewesen, als in der Studie von 2017. Die Angreifer werden zunehmend professioneller, investieren viel Zeit und auch finanzielle Ressourcen in ihre Arbeit. Dies hat z. B. zur Folge, dass immer mehr Schadsoftware im Umlauf ist und Angriffe deutlich erfolgreicher sind. Die Ransomware wie WannaCry (seit Mitte 2017) und der derzeitige Virus Emotet sind Beispiele, die für Angriffe auf eine große Anzahl an Unternehmen verantwortlich sind.

Delikttyp	Schadenssummen in Mrd. Euro (2019)
Kosten für Ermittlungen und Ersatzmaßnahmen	36,5
Kosten für Rechtsstreitigkeiten	31,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	28,6
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	27,0
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	22,2
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	22,2
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	18,6
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,5
Datenschutzrechtliche Maßnahmen (z. B. Information von Kunden)	8,8
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-
Sonstige Schäden	<0,1
Gesamtschaden innerhalb der letzten 2 Jahre	**205,7**

Tabelle 1: Insgesamt 102,9 Mrd. Euro Schaden pro Jahr

Schäden in Deutschland nach Delikttyp in Mrd. Euro (Basis: Selbsteinschätzung)

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=801)
Quelle: Bitkom Research

Chemie- und Pharmaindustrie weiterhin im Fokus
Die höchste durchschnittliche Schadenssummen je Unternehmen wurde in der aktuellen Studie in folgenden Branchen verursacht: Chemie & Pharma, Maschinenbau und Automobil (in dieser Reihenfolge). Unter den TOP5 waren außerdem die Energie- und Ernährungsbranche.

Die stärkste Zunahme (absolut betrachtet) der durchschnittlichen Schadenssumme je Unternehmen im Vergleich zur Studie 2017 wurde im Maschinenbau, dem Energiesektor und der Ernährungswirtschaft verzeichnet.

»Spionage und Sabotage gefährden den Wirtschaftsstandort Deutschland. Die Aufklärung solcher Verdachtsfälle ist eine der Kernkompetenzen des Verfassungsschutzes.«

Michael Niemeier, Vizepräsident des Bundesamtes für Verfassungsschutz (BfV)

3.1 Ehemalige Mitarbeiter als Gefahrenquelle

Wer sind die Täter? Vor allem ehemalige Mitarbeiter verursachen Schäden. Ein Drittel der Betroffenen (33 Prozent) sagt, dass sie von früheren Mitarbeitern vorsätzlich geschädigt wurden. Ein knappes Viertel (23 Prozent) sieht vormals Beschäftigte in der Verantwortung, ohne ihnen ein absichtliches Fehlverhalten zu unterstellen. Vier von zehn Betroffenen (38 Prozent) führen Angriffe auf Einzeltäter bzw. sogenannte Hobby-Hacker zurück. Bei einem Fünftel geht die Spur jeweils zur organisierten Kriminalität (21 Prozent) oder zu konkurriereden Unternehmen (20 Prozent). Gerade das unternehmerische Umfeld sollte nicht vernachlässigt werden. In 16 Prozent der Fälle konnten die Angriffe auf Lieferanten zurückgeführt werden. Bei 12 Prozent stammen Attacken von ausländischen Nachrichtendiensten.

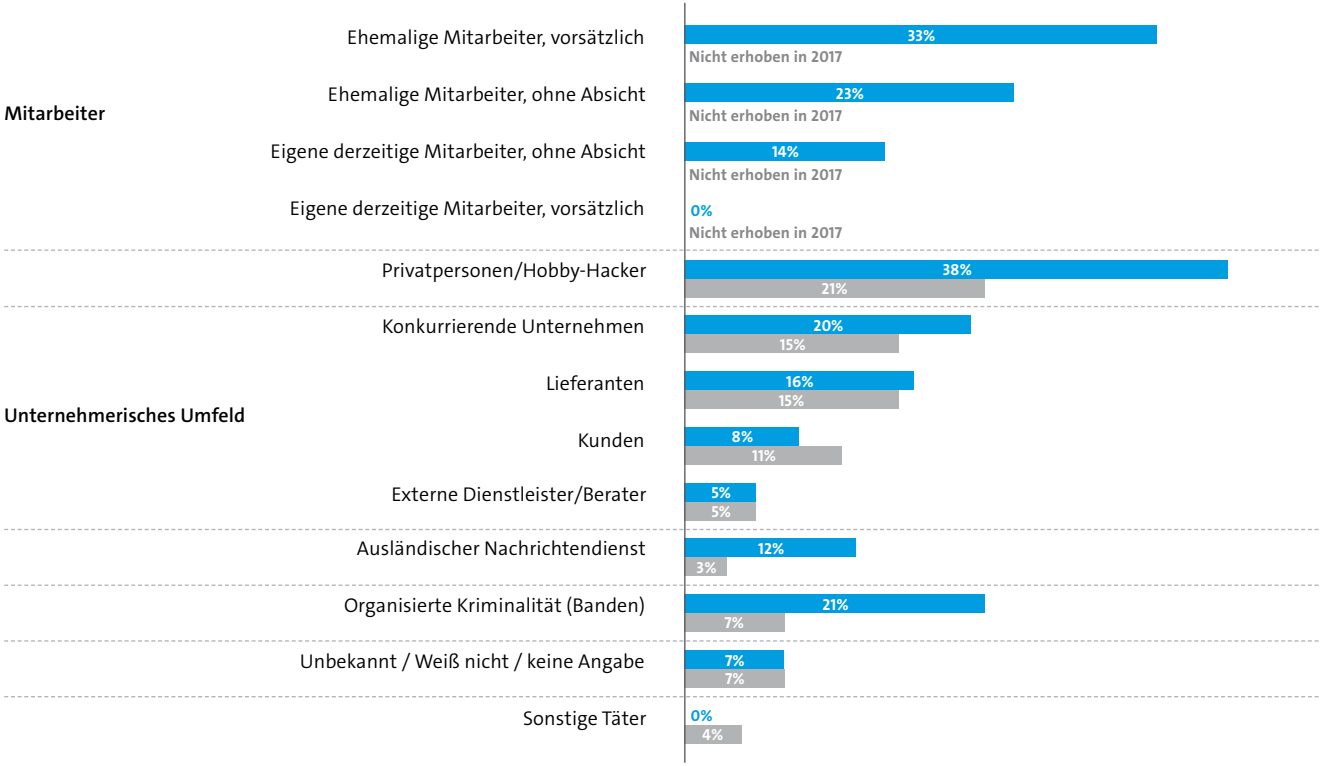


Abbildung 10: Viele Täter sind ehemalige Mitarbeiter

Von welchem Täterkreis gingen diese Handlungen in den letzten zwei Jahren aus?

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2019: n=801; 2017: n=571); Mehrfachnennungen in Prozent
Quelle: Bitkom Research

Experten-Statement

Dr. Dan Bastian Trapp
Leiter Wirtschaftsschutz beim Bundesamt für Verfassungsschutz

Die vorliegende Studie zeigt eine weiter steigende Betroffenheit deutscher Unternehmen von Datendiebstahl, Industriespionage und Sabotage. Das Bundesamt für Verfassungsschutz bearbeitet nur einen speziellen Teil dieser Fälle: Wir sind ansprechbar, wo nicht ausgeschlossen werden kann, dass hinter einem entsprechenden Angriff ein fremder Staat die Fäden zieht. Oft stehen hinter diesen staatlichen Angriffen Ressourcen, die über die Möglichkeiten gewöhnlicher Krimineller weit hinausgehen. So dürften die IT-Strukturen der meisten Unternehmen einem APT-Angriff nicht gewachsen sein. Zum Teil sind die Angriffsmethoden aber auch gezielt verschlungener. Fremde Nachrichtendienste verwenden banale kriminelle Methoden, wo höherer Aufwand nicht erforderlich ist, oder eindeutige Hinweise auf staatliche Hintergründe hinterlassen würde.

Unser gesetzlicher Auftrag ist es, Wirtschaftsspionage und -sabotage durch fremde Staaten aufzuklären. Diesen Auftrag erfüllen wir im staatlichen Interesse, aber mit einem Mehrwert für die Wirtschaft: Im Rahmen des präventiven Wirtschaftsschutzes informieren wir Unternehmen und Forschungseinrichtungen über eigene Erkenntnisse und Analysen, die dazu beitragen, dass Unternehmen sich effektiv gegen Ausforschung und Sabotage schützen können. Wir informieren einerseits über erkannte Vorgehensweisen ausländischer Wirtschaftsspionage. Andererseits entspricht unser Aufklärungsinteresse vielfach dem Interesse auch der potenziell betroffenen Unternehmen, nämlich herauszufinden, welche Strategie der Angreifer verfolgt. Warum wurde gerade dieses Unternehmen angegriffen? Auf welche Weise ist der Angreifer vorgegangen? Dabei ist für uns nicht entscheidend, ob am Schluss ein Täter strafrechtlich belangt werden kann. Wir möchten es dem Angreifer zukünftig schwerer machen und Angriffswege möglichst verschließen.

Eine positive Nachricht der Studie, die sich auch in der nachrichtendienstlichen Praxis bestätigt: Hinweise auf Angriffe kommen häufig über Mitarbeiterinnen und Mitarbeiter. Gut geschultes und sensibilisiertes Personal kann zum wesentlichen Faktor einer erfolgreichen Detektion werden.

Das Wirtschaftsschutzreferat des Bundesamtes für Verfassungsschutz – aber auch die Landesbehörden im Verfassungsschutzverbund – stehen als vertrauensvolle Ansprechpartner gerne zur Verfügung. Sprechen Sie uns an.

3.2 Angriffsursprung: Der Blick geht nach Osten

Auch wenn die regionale Herkunft nicht immer eindeutig ist, verorten fast drei von zehn Betroffenen (28 Prozent) den Ursprung der Angriffe in Osteuropa (ohne Russland). Bei ähnlich vielen (27 Prozent) stammen die Attacken aus China, 19 Prozent sehen Russland als Ursprung, dicht gefolgt von den USA (17 Prozent). Für vier von zehn Betroffenen (39 Prozent) gingen kriminelle Handlungen aus Deutschland aus, für ein Viertel (24 Prozent) war die Herkunft unklar.

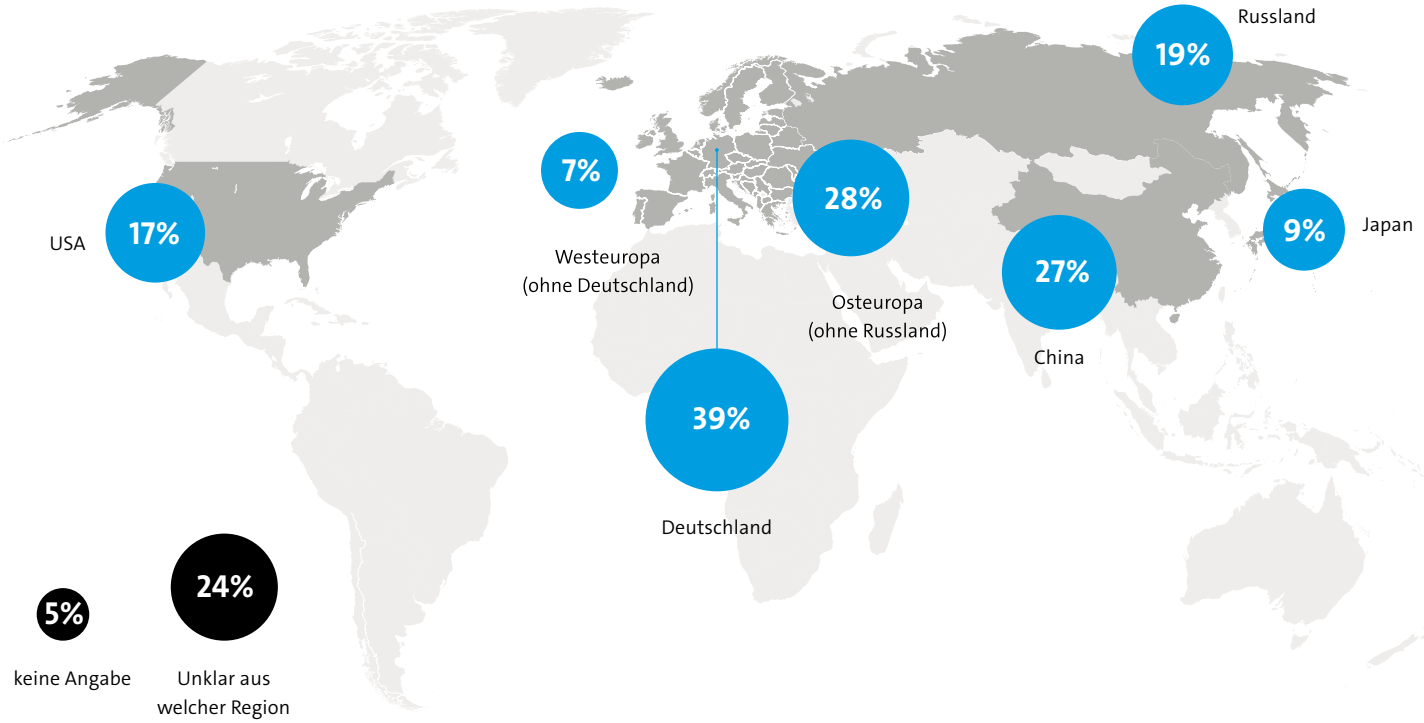


Abbildung 11: Angriffsursprung: Der Blick geht nach Osten

Konnten Sie feststellen, von wo aus diese Handlungen vorgenommen wurden?

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=801); Mehrfachnennungen in Prozent
Quelle: Bitkom Research

3.3 Hinweise durch Strafverfolgungsbehörden nehmen zu

Aufmerksame Mitarbeiter sind der beste Schutz

Wie werden Unternehmen auf die Angriffe aufmerksam? Häufig sind es gerade auch Mitarbeiter, die auf der anderen Seite dafür sorgen, dass kriminelle Handlungen aufgedeckt werden. Sechs von zehn betroffenen Unternehmen (62 Prozent) sind so erstmals auf Angriffe aufmerksam geworden. Mehr als die Hälfte (54 Prozent) erhielt Hinweise auf Angriffe durch eigene Sicherheitssysteme, bei fast drei von zehn (28 Prozent) war es hingegen reiner Zufall. Die Anzahl der Fälle, in denen ein anonymer Hinweis Klarheit schaffte, stieg von 9 Prozent im Jahr 2017 auf immerhin 29 Prozent in der aktuellen Studie. Strafverfolgungsbehörden haben nur in 13 Prozent der Fälle einen Hinweis gegeben. Das sind aber immerhin 9 Prozent mehr als in der Studie des Jahres 2017.

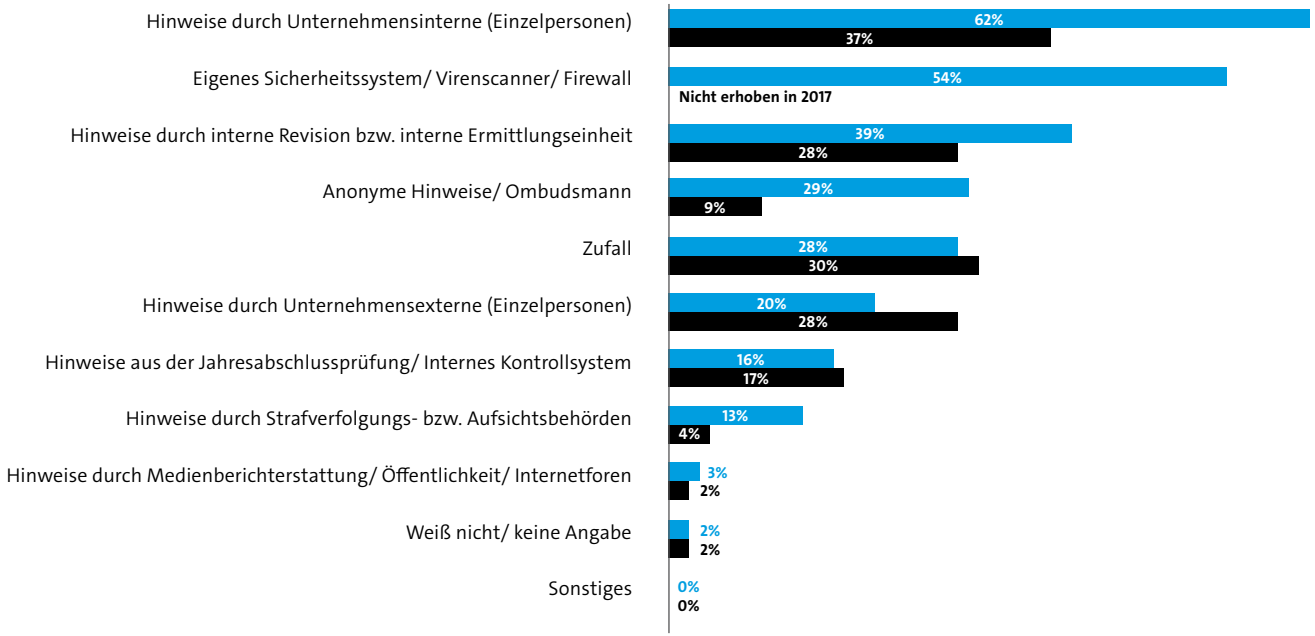


Abbildung 12:
Interne Sicherheitsmaßnahmen sind entscheidend

Wie ist Ihr Unternehmen auf diese Handlungen erstmalig aufmerksam geworden?

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2019: n=801; 2017: n=571); Mehrfachnennungen in Prozent
Quelle: Bitkom Research

»Gut geschulte Mitarbeiter sind der effektivste Schutz. So lassen sich unbeabsichtigte Schäden vorbeugen, Angriffe von außen werden besser abgewehrt und sind sie doch erfolgreich, lässt sich schnell gegensteuern.«

Achim Berg, Bitkom-Präsident, Berlin 2020

3.4 KRITIS-Betreiber häufiger gewarnt

Die Frage, ob das Unternehmen in den letzten zwei Jahren von staatlichen Stellen über einen oder mehrere sie betreffende Cybervorfälle informiert wurde, beantworteten 84 Prozent der Unternehmen aus Nicht-KRITIS-Sektoren mit nein, innerhalb der KRITIS-Sektoren sind es immerhin 31 Prozent weniger (53 Prozent). In 21 Prozent der Fälle wurden die kritischen Infrastrukturen durch das BSI informiert. Die Landesbehörden des Verfassungsschutzes (LfV) informierten in 11 Prozent der Fälle und das Bundesamt für Verfassungsschutz (BfV) in 7 Prozent. Durch die Landeskriminalämter (LKÄ) und die Polizei wurden nur 4 Prozent der KRITIS-Unternehmen gewarnt, das BKA warnte nur in einem Prozent der Fälle.

Bei allen anderen Unternehmen (nicht KRITIS) warnte das BSI in 10 Prozent der Fälle. Die Information durch die LfVs (3 Prozent), das BfV (2 Prozent) und die LKÄs (1 Prozent) waren verschwindend gering. Auf Polizei und BKA sind keine Informationen zurückzuführen.

Die Ergebnisse bestätigen eine gute Zusammenarbeit zwischen dem BSI und den Kritischen Infrastrukturen. Die KRITIS-Betreiber sind verpflichtet, in ernsten Fällen an das BSI zu melden. Der Austausch scheint auch in umgekehrter Weise zu funktionieren – kann aber deutlich ausgebaut werden.

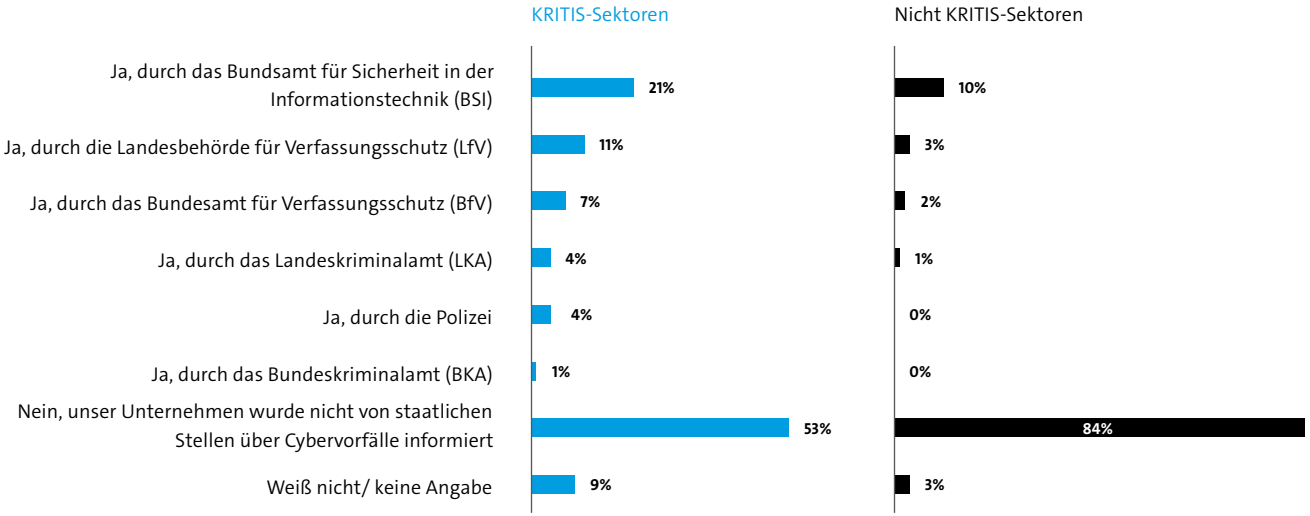


Abbildung 13: KRITIS-Sektoren häufiger gewarnt

Wurde Ihr Unternehmen im vergangenen Berichtszeitraum von staatlichen Stellen über einen oder mehrere Sie betreffende Cybervorfälle informiert?

Basis: Alle befragten Unternehmen (n=1.070);
Mehrfachnennungen in Prozent
Quelle: Bitkom Research

4 Sicherheitsvorkehrungen

Experten-Statement

Ursula Morgenstern
CEO Atos Deutschland, Mitglied Bitkom-Hauptvorstand

So vielfältig die Anforderungen an eine passgenaue IT-Umgebung sind, mindestens ebenso komplex sind die notwendigen Sicherheitsvorkehrungen. Schließlich gibt es bei Cyberattacken nicht ein definiertes Täterprofil. Neben Hobbyhackern, professionellen Dieben und ausländischen Geheimdiensten müssen besonders die Mitarbeiter bedacht werden. So sind ehemalige Kolleginnen und Kollegen verantwortlich für mehr als die Hälfte der Cybervorfälle, entweder absichtlich (33 Prozent) oder unabsichtlich (23 Prozent). Gleichzeitig sagen mehr als 60 Prozent der von Attacken betroffenen Unternehmen, dass aufmerksame Mitarbeiter wertvolle Hinweise auf die Angriffe geliefert haben.

Wir dürfen die Cybersicherheit in unseren Organisationen nicht ausschließlich auf technologische Aspekte auslegen und umsetzen: Wenn die Mitarbeiter die Sicherheitsmaßnahmen nicht verstehen oder sogar als Hindernis bei ihrer täglichen Arbeit betrachten, wird uns die beste Technologie nicht helfen.

Stattdessen müssen wir zwei Dinge tun: Erstens müssen wir in regelmäßigen Schulungen unseren Mitarbeitern klar machen, welche Bedeutung ihr Handeln auf die Sicherheit – und damit auch auf den Erfolg – unseres Unternehmens hat. Dabei muss auch klar werden, dass Sicherheitsmaßnahmen keine lästige Pflichtübung sind, sondern ein integraler Bestandteil der täglichen Arbeit. Zweitens müssen wir bei der Implementierung der Sicherheitstechnologien und -prozesse darauf achten, dass sie möglichst einfach zu nutzen sind. Die besten Instrumente sind nur so gut wie ihre Anwender.

Welche Maßnahmen lassen sich ergreifen, um Schäden durch unbeabsichtigtes Handeln oder bösartige Attacken ehemaliger Kolleginnen und Kollegen zu verhindern bzw. zu minimieren?

Indem wir die Bedeutung der Sicherheit in den Köpfen unserer Mitarbeiter verankern, können wir auch die Schäden durch ehemalige Mitarbeiter verhindern. Zugangsdaten, kritische interne oder Kundeninformationen sind auch nach dem Ausscheiden von Mitarbeitern aus dem Unternehmen gleichermaßen sensibel und müssen geschützt werden.

Konsequentes Rechtemanagement, aktuelle Sicherheitstechnologien und funktionierende Prozesse können solche Angriffe zwar nicht verhindern, aber das Risiko zumindest reduzieren.

4.1 Penetrationstests bleiben Mangelware

Der erste Teil der Studie befasst sich mit den Angriffsarten, ihren Schäden und deren Aufklärung. In einem zweiten Teil widmet sich die Studie den bereits heute vorhandenen Sicherheitsmaßnahmen in den Unternehmen.

Schon seit einigen Jahren verfügen nahezu alle Unternehmen über einen technischen Basisschutz. Flächendeckend setzen Industrieunternehmen beispielsweise Passwortschutz auf allen Geräten, Firewalls und Virenscanner ein. Auch das Durchführen von regelmäßigen Backups ist bei 100 Prozent der Unternehmen im Arbeitsalltag etabliert. Derartige Funktionen sind in den meisten gängigen Betriebssystemen bereits integriert. Aufgrund der Vielzahl komplexer Schadsoftware, die täglich aus dem Boden sprießt, reicht dieser Basisschutz heute jedoch nicht mehr aus.

Eine Verschlüsselung von Netzwerkverbindungen setzen immerhin 95 Prozent der befragten Unternehmen ein. Elektronische Zugangskontrollen zu Gebäuden und Maschinen (68 Prozent), Protokollierung von Zugriffen (60 Prozent) und eine abhörsichere Sprachkommunikation (56 Prozent) werden vom mehrheitlichen Anteil der Industrieunternehmen angewandt. Auch das Thema Verschlüsselung von Datenträgern spielt bei Unternehmen zunehmend eine Rolle. Immerhin jedes zweite befragte Unternehmen setzt sie ein. Verschlüsselten E-Mail-Verkehr nutzen dagegen nur rund 39 Prozent. Ähnlich steht es um erweiterte Verfahren zur Benutzeridentifikation (38 Prozent) oder die Absicherung gegen Datenabfluss von innen (36 Prozent). Auch der Einsatz von Penetrationstest (29 Prozent) und Instrusion Detection Systemen (26 Prozent) sollte in den Unternehmen deutlich ausgeweitet werden. 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 – was leider immer häufiger der Fall ist.

Abbildung 14: Technische IT-Sicherheitsmaßnahmen (I)

Welche der folgenden technischen IT-Sicherheitsmaßnahmen kommen in Ihrem Unternehmen bereits zum Einsatz bzw. plant Ihr Unternehmen in Zukunft einzusetzen, um sich gegen Datendiebstahl, Industriespionage oder Sabotage zu schützen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research

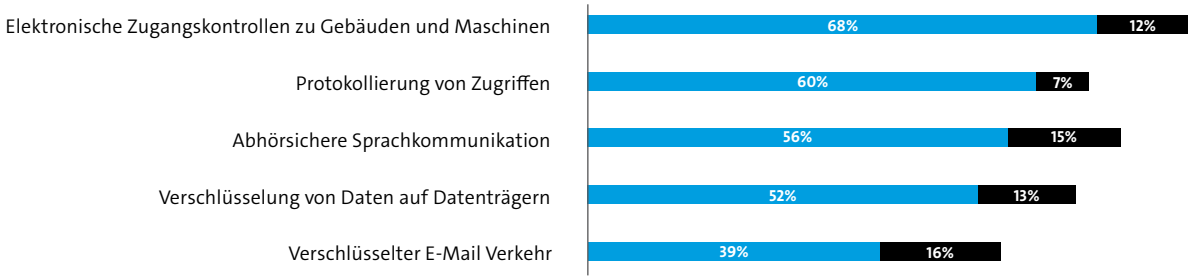


Abbildung 15: Technische IT-Sicherheitsmaßnahmen (II)

Welche der folgenden technischen IT-Sicherheitsmaßnahmen kommen in Ihrem Unternehmen bereits zum Einsatz bzw. plant Ihr Unternehmen in Zukunft einzusetzen, um sich gegen Datendiebstahl, Industriespionage oder Sabotage zu schützen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research

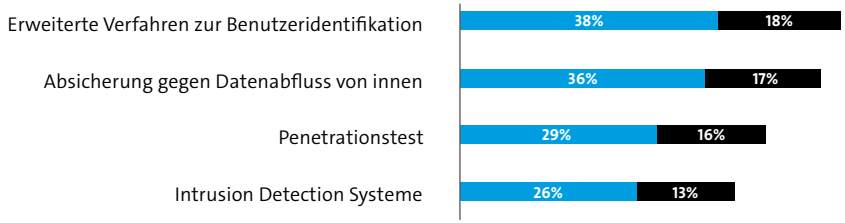


Abbildung 16: Technische IT-Sicherheitsmaßnahmen (III)

Welche der folgenden technischen IT-Sicherheitsmaßnahmen kommen in Ihrem Unternehmen bereits zum Einsatz bzw. plant Ihr Unternehmen in Zukunft einzusetzen, um sich gegen Datendiebstahl, Industriespionage oder Sabotage zu schützen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research

Einsatz künstlicher Intelligenz als IT-Sicherheitsmaßnahme?

Künstliche Intelligenz kann zum Beispiel beim Erkennen von Anomalien eingesetzt werden. Bisher sind es allerdings noch sehr wenig Unternehmen, die ihre Systeme mit dieser Technologie schützen (9 Prozent). Gerade kleine Unternehmen tun sich schwer, die etwas komplexere Methode in ihr Unternehmen zu integrieren (8 Prozent), für 57 Prozent ist es derzeit auch kein Thema. Unternehmen mit mehr als 500 Mitarbeitern setzen KI in 20 Prozent der Fälle bereits ein, weitere 16 Prozent planen den Einsatz in den nächsten 12 Monaten konkret.

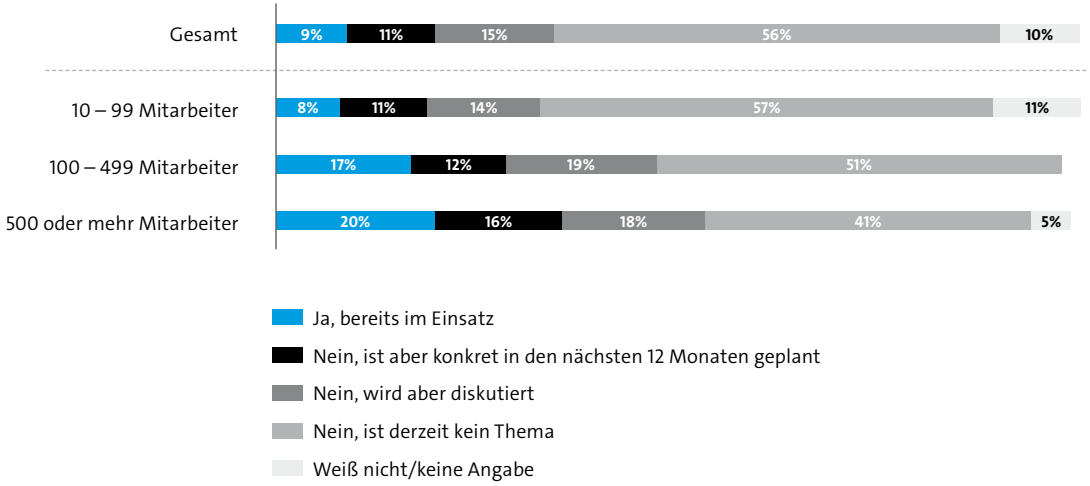


Abbildung 17: Einsatz künstlicher Intelligenz als IT-Sicherheitsmaßnahme

Kommen in Ihrem Unternehmen derzeit bereits Anwendungen mit KI zum Einsatz, um sich gegen Datendiebstahl, Industriespionage oder Sabotage zu schützen bzw. plant/diskutiert Ihr Unternehmen dies?

Basis: Alle befragten Unternehmen (n=1.070);
Werte ≤2 zur übersichtlichen Darstellung ausgeblendet.
Quelle: Bitkom Research

4.2 Clean-Desk-Policy nur in jedem zweiten Unternehmen etabliert

Genauso wichtig wie die technischen Maßnahmen sind die organisatorischen. Hierzu gehört z. B. auch die Festlegung von Zugriffsrechten auf bestimmte Informationen. Nahezu alle befragten Unternehmen haben solche Zugriffsrechte bestimmt und in ihrer Organisation etabliert (98 Prozent), 80 Prozent tun dies auch für bestimmte Räume im Unternehmen. Klare Regeln für den Umgang mit schützenswerten Informationen definieren 85 Prozent der befragten Unternehmen. Eine eindeutige Klassifizierung bzw. Kennzeichnung von Betriebsgeheimnissen haben rund 77 Prozent eingeführt. Knapp zwei Drittel der Unternehmen etablierten bestimmte Regelungen für die Mitnahme von IT- und TK-Equipment bei Geschäftsreisen.

Eine Clean-Desk-Policy wird nur von 55 Prozent der Unternehmen umgesetzt. Ein weiterer 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 der Unternehmen statt.

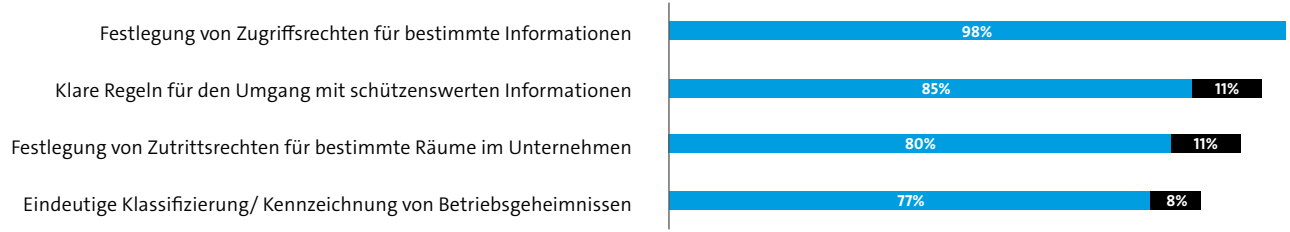
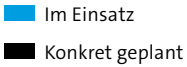


Abbildung 18: Organisatorische Sicherheitsmaßnahmen (I)

Welche der folgenden organisatorischen bzw. prozesstechnischen Sicherheitsvorkehrungen kommen in Ihrem Unternehmen bereits zum Einsatz/plant Ihr Unternehmen in Zukunft einzusetzen, um sich gegen Datendiebstahl, Industriespionage, Sabotage zu schützen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research



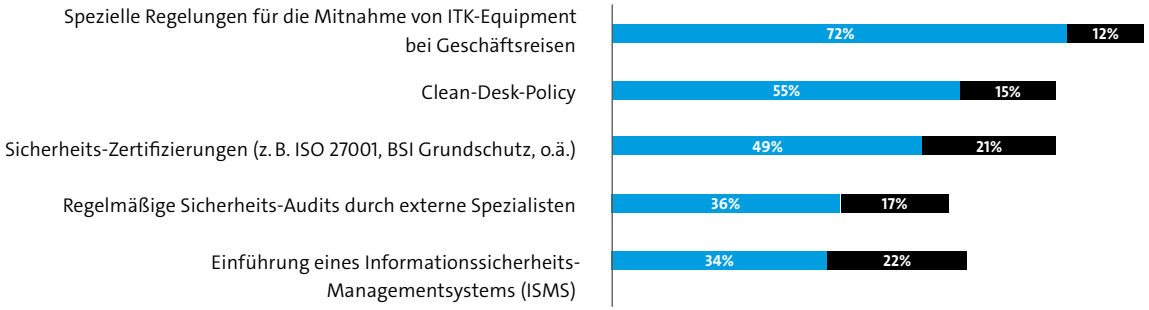
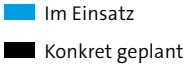


Abbildung 19: Organisatorische Sicherheitsmaßnahmen (II)

Welche der folgenden organisatorischen bzw. prozesstechnischen Sicherheitsvorkehrungen kommen in Ihrem Unternehmen bereits zum Einsatz/plant Ihr Unternehmen in Zukunft einzusetzen, um sich gegen Datendiebstahl, Industriespionage, Sabotage zu schützen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research



Notfallmanagement

Die aktuelle Studie zeigt, dass gerade mal knapp jedes zweite Unternehmen über ein Notfallmanagement[1] verfügt, das im Ernstfall zum Tragen kommt. Der Wert der kleinen und großen Unternehmen hat sich über die letzten Jahre angeglichen.

Ein größerer Unterschied herrscht zwischen Unternehmen der KRITIS und Nicht-KRITIS-Branchen. Kritische Infrastrukturen haben in 59 Prozent der Fälle ein Notfallmanagement etabliert. Alle übrigen Unternehmen in nur 46 Prozent der Fälle.

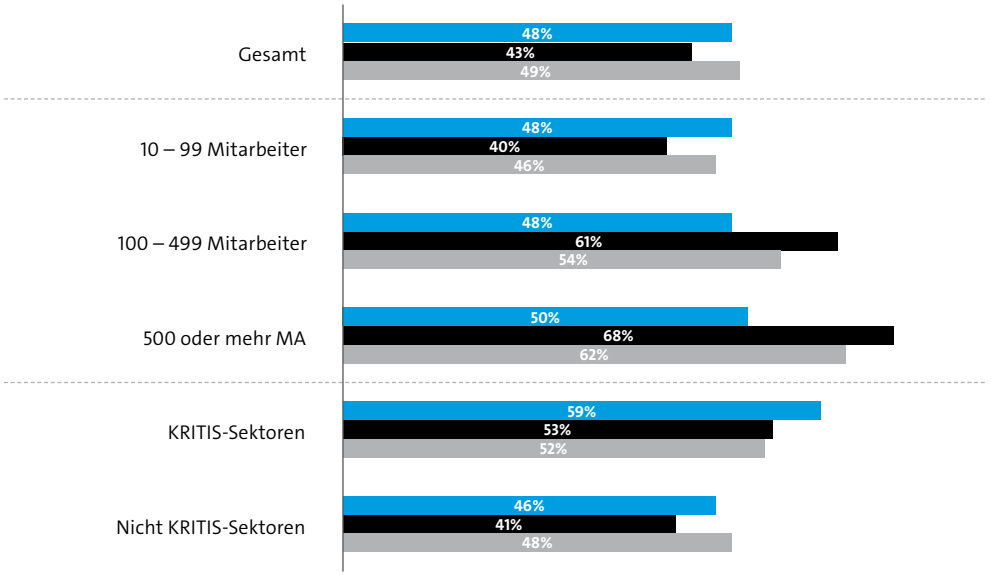


Abbildung 20: Notfallmanagement

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 Unternehmen (2019: n=1.070; 2017: n=1.069; 2015: n=1.074); *Antwortkategorie [Ja]
Quelle: Bitkom Research

1 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.

4.3 Mitarbeiter nach wie vor zu wenig im Fokus

Auch die aktuelle Studie zeigt, dass Mitarbeiter beim Thema Wirtschaftsschutz eine Schlüsselrolle einnehmen. Sie sind sowohl für eine Vielzahl der erfolgreichen Angriffe verantwortlich als auch für deren zeitnahe Aufdeckung. Ihre Stärkung im Thema Unternehmenssicherheit, die letztlich Arbeitsplatzsicherheit bedeutet, wird damit zum entscheidenden Faktor. Die Zahlen zeigen, dass das noch nicht bei jeder Unternehmensführung angekommen ist. Nur 63 Prozent der Befragten führen regelmäßige Schulungen zu Sicherheitsthemen mit ihren Mitarbeitern durch. Das ist zwar ein Anstieg von 10 Prozent zum Vergleichsjahr, aber noch lange nicht ausreichend.

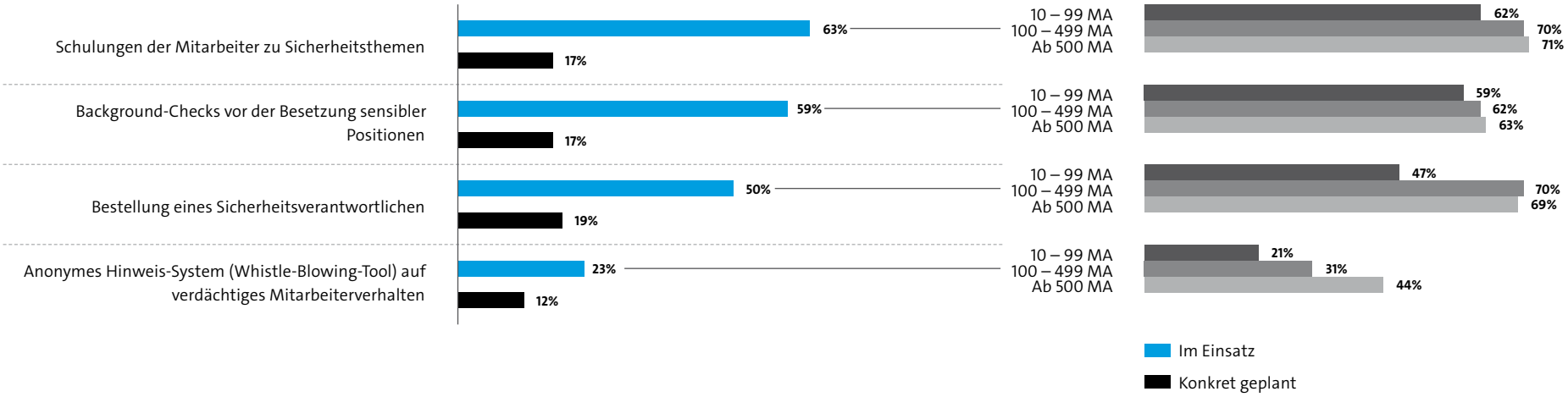
Nur jedes zweite befragte Unternehmen bestimmt einen Sicherheitsverantwortlichen im Unternehmen. Damit kommt das Thema auch in der Management-Ebene an. Die Bestimmung eines solchen Verantwortlichen ist für ein umfassendes Sicherheitsmanagement unabdingbar. Entscheidend ist, dass das Thema IT-Sicherheit zur Chefsache gemacht und es über eigene Wirtschaftsschutz-Beauftragte oder Informationssicherheitsbeauftragte im Unternehmen institutionalisiert wird.

Hintergrund-Prüfungen[2] von Personen, die auf sensible Positionen gesetzt werden sollen, finden nur in 59 Prozent der Unternehmen statt. Anonyme Hinweissysteme wie Whistle-Blower-Tools[3] werden nur bei rund 23 Prozent der Unternehmen eingesetzt.

Abbildung 21: Personelle Sicherheitsmaßnahmen

Welche der folgenden Sicherheitsvorkehrungen im Bereich Personal kommen in Ihrem Unternehmen bereits zum Einsatz bzw. plant Ihr Unternehmen in Zukunft einzusetzen, um sich gegen Datendiebstahl, Industriespionage oder Sabotage zu schützen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research



2 Hierzu gehört beispielsweise die Sichtung von Social Media Profilen.
3 Hier bekommen Mitarbeiter die Möglichkeit, Missstände und Versäumnisse in extern betriebenen Systemen zu melden, ohne sich selbst dabei als »vermeintliches Einfallstor« outen zu müssen.

Experten-Statement

Dr. Niklas Hellemann
Geschäftsführer, SoSafe Cyber Security Awareness

Ein abgedunkelter Raum. Eine Gestalt mit Kapuzenpulli vor einem Bildschirm mit Netzwerkdatenströmen. Das ist das Klischeebild des modernen Hackers.

Teils befeuert durch Darstellungen in Filmen und Serien, gehen die meisten Menschen heutzutage davon aus, dass Cyber-Angriffe ausschließlich technische Vorgänge sind. Sicherheitslücken werden identifiziert und dann »hackt« sich der Angreifer irgendwie »in das Netz«.

Dass dieses Bild heutzutage nicht unbedingt der Realität entspricht, zeigen spektakuläre Fälle wie der des Berliner Kammergerichts oder des Verlagshauses Heise, bei denen jeweils durch Verschlüsselungstrojaner die IT-Systeme komplett außer Gefecht gesetzt wurden. Mitarbeiter hatten hier zuvor auf, teils sehr gut gemachte, Phishing-Emails geklickt.

Und wie die vorliegenden Studienergebnisse auch noch einmal deutlich aufzeigen, beginnt der Großteil der Angriffe auf Unternehmen mittlerweile bei den Mitarbeitern. Nahezu alle Attacken, ob ungezielter Flächenangriff oder komplexe APT-Kampagne zeigen: Cyberangriffe besitzen heutzutage nahezu immer eine menschliche Komponente bzw. ein Element des »Social Engineerings«.

Social Engineering beschreibt die Manipulation von Menschen, um sie zu einer Handlung mit vermeintlich negativer Konsequenz zu bewegen, wie beispielsweise das Eingeben von Nutzerdaten oder das Herunterladen von Malware. Social Enigneering kann hierbei über verschiedene Kanäle erfolgen, also über Anrufe, SMS oder eben auch über Phishing-E-Mails.

Die »Social Engineers« bedienen sich hierbei der gesamten Klaviatur der modernen Psychologie. Sie sind also alles andere als eigenbrötlerische Technik-Freaks, sondern in vielen Fällen sozial sehr versiert. Und sie investieren immer mehr Zeit in die Informationssuche und Vorbereitung ihrer Angriffe: die Zahl der zielgerichteten Phishing-Angriffe nimmt dramatisch zu.

Es gelingt ihnen so immer besser, unsere »psychologischen Knöpfe« zu drücken, also Mechanismen auszunutzen, die tief in unserem Denken und Handeln verankert sind. Am erfolgreichsten sind dabei Neugier, Vertrauen und Druck, wie wir aus simulierten Phishing-Angriffen bei unseren Kunden sehen können. Eine vermeintliche E-Mail vom Scanner aus der Vorstandsetage beispielsweise wird zu einem sehr hohen Anteil angeklickt, einfach weil wir uns brennend für diese vermeintlich geheime Informationen interessieren.

Um der Bedrohung durch Social Engineering zu begegnen, muss man also das besagte Klischee des menschenscheuen Angreifers aufbrechen. Man muss Mitarbeitern und Bürgern vermitteln, dass Cyber-Angriffe nicht irgendwo aus dem Netz kommen, sondern dass sie selbst im Fadenkreuz stehen – und dass Cyberkriminelle hierbei ganz gezielt unsere menschlichen Schwächen ausnutzen.

4.4 Interne Sicherheitsmaßnahmen sind entscheidend

Wie in den Studien zuvor halten knapp 100 Prozent der befragten Unternehmen qualifizierte IT-Sicherheitskräfte für besonders (69 Prozent) bzw. eher (30 Prozent) geeignet, die Organisation effektiv gegen Datendiebstahl, Industriespionage oder Sabotage zu schützen. Die Schulung aller Mitarbeiter zu Sicherheitsthemen folgt direkt an zweiter Stelle. 76 Prozent der Unternehmen halten sie für sehr geeignet, weitere 21 Prozent für eher geeignet. Auch das automatische Erkennen von Anomalien in Netzwerkdaten mit Hilfe von KI oder maschinellem Lernen sowie Security by Design von vernetzten Geräten sehen die meisten Unternehmen als geeignete Maßnahmen zum Unternehmensschutz an. Die Blockchain-Technologie halten dagegen nur 80 Prozent der Unternehmen für sehr oder eher geeignet.

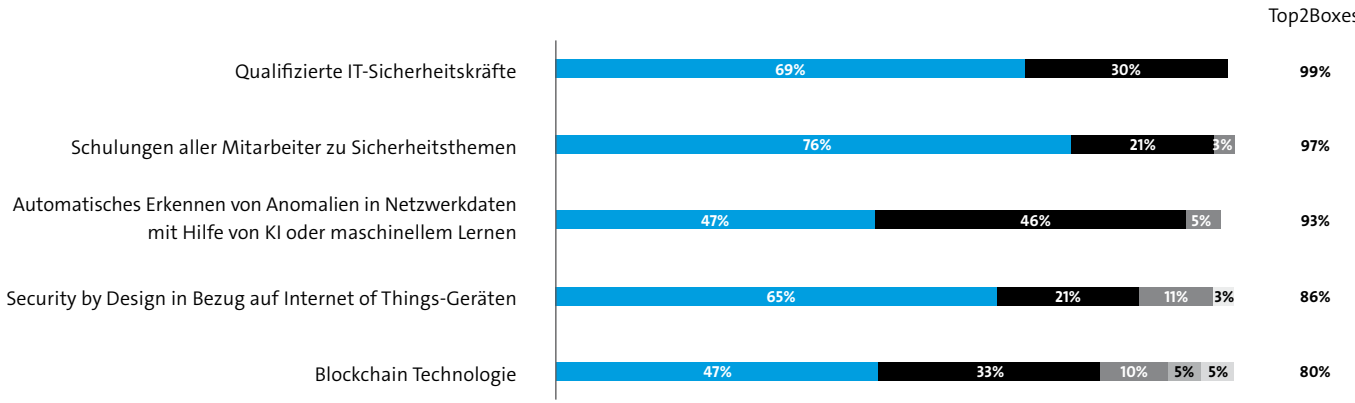


Abbildung 22:
Eignung von IT-Sicherheitsmaßnahmen

Für wie geeignet halten Sie die folgenden IT-Sicherheitsmaßnahmen, um Ihr Unternehmen zukünftig gegen Datendiebstahl, Industriespionage oder Sabotage effektiv zu schützen?

Basis: Alle befragten Unternehmen (n=1.070); Werte ≤2 zur übersichtlichen Darstellung ausgeblendet.
Quelle: Bitkom Research

4.5 Cyber-Versicherungen als Ergänzung zu internen Sicherheitsmaßnahmen

Eine Cyber-Versicherung kann eine Ergänzung zu umfassenden technischen, organisatorischen und technologischen Maßnahmen zum Schutze der Organisation sein. Teile des Risikos von Cyberangriffen werden mittlerweile vermehrt von Versicherungsgesellschaften abgedeckt und versichert. Unternehmen sollten ihr IT-Sicherheitsmanagement aber in keinem Falle vernachlässigen, nur weil sie vermeintlich gegen Schäden aus Cyberattacken abgesichert sind. Denn nur wer ausreichend geschützt ist, sodass die Risiken nicht ausufern, kommt überhaupt in den Genuss einer Deckung. Auch muss abgewogen werden, ob sich die Kosten für eine Versicherung tatsächlich lohnen. Es ist nach wie vor schwer auszumachen, wann tatsächlich ein Haftungsfall eintritt und wann nicht.

Die Anzahl der Unternehmen insgesamt, die eine Versicherung für derartige Risiken abgeschlossen haben, ist zur Vergleichsstudie aus dem Jahr 2017 um 3 Prozentpunkte auf 17 Prozent gestiegen. Der Unterschied zwischen kleinen und größeren Unternehmen bleibt weiter bestehen. Unternehmen mit mehr als 500 Mitarbeitern haben bereits in mehr als 27 Prozent der Fälle eine Versicherung abgeschlossen. Bei Unternehmen mit 10 bis 99 Mitarbeitern sind es mittlerweile immerhin 16 Prozent (Anstieg um 6 Prozent). Ebenso bei den Unternehmen mit 100 – 499 Mitarbeitern.

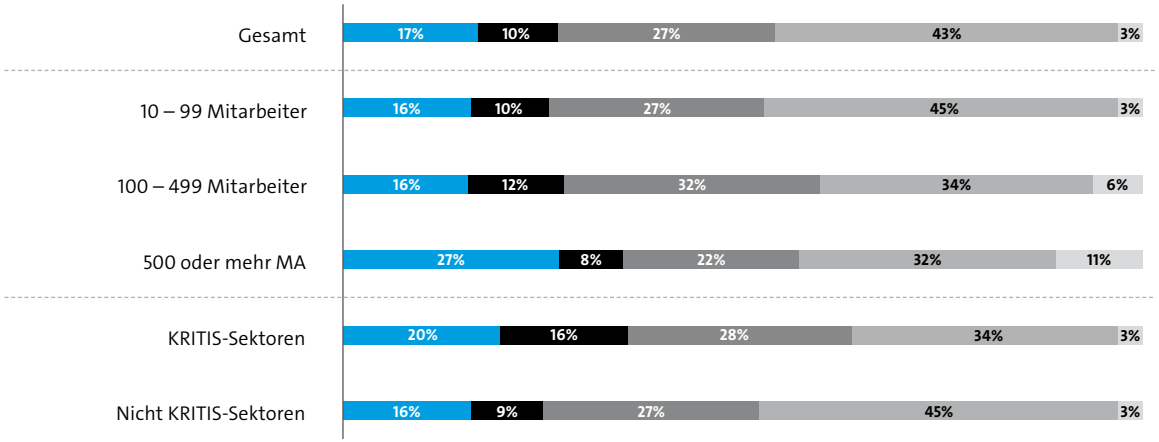


Abbildung 23: Cyber-Versicherung (I)

Hat Ihr Unternehmen eine so genannte Cyber-Versicherung für den Fall des Auftretens von digitaler Wirtschaftsspionage, Sabotage, Datendiebstahl oder Hackerangriffe abgeschlossen?

Basis: Alle befragten Unternehmen (n=1.070)
Quelle: Bitkom Research

Tatsächlicher Nutzen der Versicherung weiter umstritten

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 22 Prozent der Unternehmen bisher lohnenswert. Dagegen hat sich der Abschluss für 39 Prozent der Unternehmen überhaupt nicht gelohnt. Kleine und große Unternehmen profitieren am wenigsten. Deutlich lohnenswerter scheint eine Versicherung für Unternehmen mit 100 – 499 Mitarbeiter zu sein. Für immerhin 38 Prozent hat sich der Abschluss gelohnt.

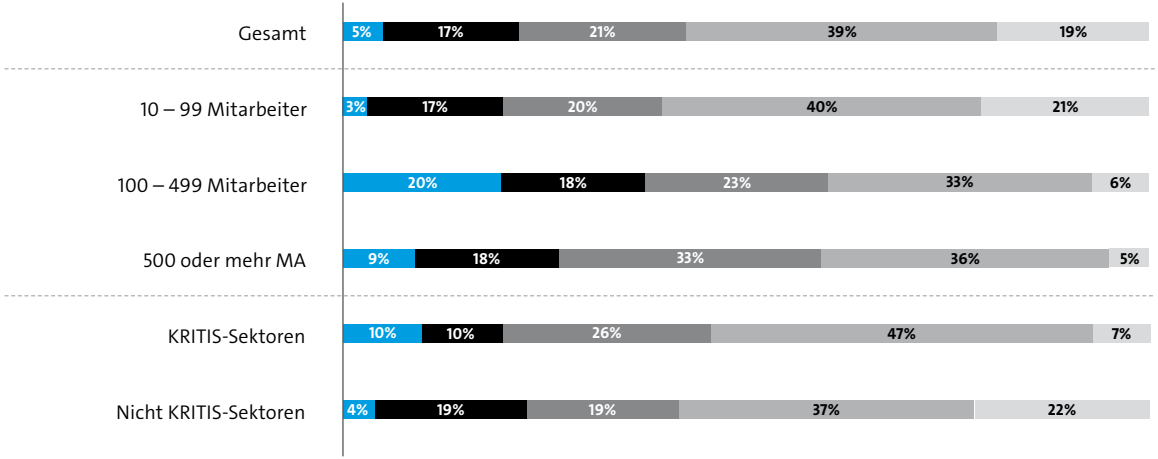


Abbildung 24: Cyber-Versicherung (II)

Inwieweit hat sich der Abschluss der Cyber-Versicherung für Ihr Unternehmen bzw. Ihre Organisation bisher gelohnt?

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und die eine Cyber-Versicherung abgeschlossen haben (n=137)
Quelle: Bitkom Research

5 Die goldenen Regeln für den Wirtschaftsschutz

5.1 Die goldenen Regeln für den Wirtschaftsschutz

Organisatorische, technische und personelle Sicherheit
Wenn es um konkrete Maßnahmen zum Schutz der Unternehmen geht, konnten in fast allen Kategorien (leichte) Verbesserungen festgestellt werden. Dennoch: noch lange nicht ist das Thema digitaler Wirtschaftsschutz flächendeckend in den Unternehmen etabliert. Das liegt unter anderem daran, dass viele Unternehmen sich der Gefahr noch immer nicht bewusst sind. Aufgrund ihrer Größe können sie sich oftmals nicht vorstellen, attraktives Ziel für Angreifer zu sein. Zum anderen handelt es sich bei Cyberangriffen um eine Gefahr, die im täglichen Geschäft erstmal nicht auftaucht. Was sichtbar wird sind allerdings die Kosten, die ein adäquater Schutz nun einmal mit sich bringt. Auch weiterhin fehlen gerade bei kleineren Unternehmen finanzielle Ressourcen sowie entsprechendes Know-how, um Maßnahmen im Bereich der organisatorischen, technischen und personellen Sicherheit umzusetzen.

Bitkom hat die »Goldenen Regeln für den Wirtschaftsschutz« entwickelt, die dabei unterstützen sollen, ihr Unternehmen bestmöglich vor den Gefahren im Cyberraum zu schützen:

1. **Sicherheit gehört in die Chefetage**
   Sicherheitsbewusste Mitarbeiter sind der beste Schutz. Die Chefetage sollte hier mit gutem Beispiel voran gehen. Zuvorderst braucht es eine Kultur im Unternehmen, die den bewussten Umgang mit Informationen und Daten fördert. Aber auch ein Grundverständnis von aktuellen Sicherheitsbedrohungen sowohl für Führungskräfte als auch für ihre Mitarbeiter ist essentiell, um die Gefahren im Unternehmen richtig einschätzen zu können. Hier kann es helfen, eigene Wirtschaftsschutz-Beauftragte oder Informations-Sicherheitsbeauftragte zu bestimmen, die die Themen dann in die Breite tragen. Wichtig ist, dass ein Austausch über alle Abteilungen gegeben ist. IT-Sicherheit ist ein Querschnittsthema und kann nicht isoliert betrachtet werden.

2. **Prioritäten setzen**
   Nicht alle Informationen und Werte eines Unternehmens können in gleichem Maße geschützt werden. Unternehmen sollten Prioritäten setzen und sich auf ihre »Kronjuwelen« konzentrieren. Hierzu gehört, dass Kerngeschäftsprozesse und notwendige Unterstützungsprozesse identifiziert werden, kritische Infrastrukturen bekannt sind und sensible und unternehmenskritische Daten und Informationen festgelegt werden. Entsprechende Sicherheitsmaßnahmen sind dann festzulegen, zu priorisieren und umzusetzen.

3. **Lassen Sie sich helfen**
   Der Markt an Sicherheitsdienstleistern ist groß und bietet für jede Art von Unternehmen passende Services und Produkte an. Gerade für kleine Unternehmen können diese eine sinnvolle Unterstützung sein. Um anforderungsgerechte Dienstleistungen entsprechend beschaffen zu können, müssen zuerst Unterstützungsbedarfe identifiziert werden. Wichtig ist, dass Dienstleistungen nur eine Ergänzung sind. Wer seine eigenen Kerngeschäftsprozesse und Kronjuwelen nicht kennt und nicht über ein grundlegendes Verständnis von aktuellen Sicherheitsbedrohungen verfügt, wird sein Unternehmen nie ausreichend schützen können.

4. **Schweigen ist nicht immer Gold**
   Schweigen ist meist eine schlechte Alternative. Im Ernstfall helfen neben IT-Sicherheitsdienstleistern auch die Sicherheitsbehörden. Eine enge und präventive Zusammenarbeit mit Sicherheitsbehörden ist deshalb schon im Vorfeld eines Angriffs sinnvoll. Um einen Angriff umfassend aufarbeiten zu können, sollten Sicherheitsbehörden bei Sicherheitsvorfällen frühzeitig eingebunden werden.

5. **Sicherheit als Routine**
   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[4]. Aber Maßnahmen einmal zu etablieren reicht nicht aus: Sicherheit ist ein kontinuierlicher Prozess. Bewerten Sie Ihre Gefährdungen und Maßnahmen regelmäßig. Zuständigkeiten und Verantwortlichkeiten sind festzulegen. Prozesse und Methoden beim Umgang mit Sicherheitsvorfällen sollten definiert, ein angemessenes Intervall sowie der Umfang zur Überprüfung von Gefährdungen und Maßnahmen sollte festgelegt werden. Bei Bedarf ist rechtzeitig Unterstützung zu holen (intern/extern).

4 Die einzelnen Maßnahmen werden auf den Folgeseiten aufgeführt.

5.2 Sicherheitsmaßnahmen im Detail

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 einen umfassenden organisatorischen Schutz, 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. Umso anspruchsvoller die Maßnahme aber, desto weniger Unternehmen nutzen sie. Täglich neue Schadsoftware wird zunehmend komplexer und bleibt somit in vielen Fällen unerkannt. Deshalb reichen Virenscanner und Firewall nicht mehr aus. Hinzu kommen die stetig wachsende Angriffsfläche und raffinierte Hackermethoden, wie beispielsweise das Social Engineering. Der Basisschutz sollte deshalb unbedingt um die Verschlüsselung von Datenträgern und E-Mailverkehr sowie um spezielle Angriffserkennung ergänzt werden. Die Überwachung vernetzter Geräte und die Erkennung von Anomalien durch beispielsweise 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 in 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 Mitarbeitern auf sensiblen Positionen einen Hintergrundcheck durchlaufen müssen oder die Möglichkeit besteht, als Mitarbeiter Missstände und Versäumnisse anonym melden zu können.

6 Wirtschaft fordert mehr Zusammenarbeit

»Der Bitkom ist für das BfV ein wichtiger Partner im Wirtschaftsschutz. Das BfV hat daher bereits im Jahr 2016 mit dem Bitkom ein 'gemeinsames Handeln für digitale Sorgfalt und zum Schutz von Know-how in Deutschland' vereinbart.«

Michael Niemeier, Vizepräsident des Bundesamtes für Verfassungsschutz (BfV)

6 Wirtschaft fordert mehr Zusammenarbeit

In weiten Teilen liegt es an den Unternehmen selbst, wie breit sie sich im Kampf gegen digitale Angriffe aufstellen. Die Studie hat im vorherigen Kapitel aufgezeigt mit welchen Maßnahmen Unternehmen sich selbst schützen können. Besonders wichtig bei der Bekämpfung von Cybercrime ist aber auch der Austausch von Informationen und Erfahrungen. Dies sollten Unternehmen zum einen untereinander tun, zum anderen 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.

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.

Abbildung 25: Wirtschaft wünscht sich mehr Zusammenarbeit

Inwieweit stimmen Sie den folgenden allgemeinen Aussagen zu aktuellen politischen Debatten im Bereich Wirtschaftsschutz zu?

Basis: Alle befragten Unternehmen (n=1.070); *Antwortkategorien [Stimme voll und ganz zu] & [Stimme eher zu]
Quelle: Bitkom Research

Schlusswort

Michael Barth
Head of Department Corporate Affairs genua, Vorsitzender AK Sicherheitspolitik Bitkom

Die Ergebnisse der Studie Wirtschaftsschutz zeigen deutlich, dass die Wirtschaft sich in den entscheidenden Fragen der Cybersicherheit mehr Unterstützung wünscht. Es geht den Unternehmen nicht nur um einen besseren Informationsfluss zwischen Staat und Unternehmen, sondern auch um die konkrete Hilfestellung bei IT-Sicherheitsfragen. In den letzten Jahren wurden bereits gute Fortschritte erzielt: Beispiele sind das aus meiner Sicht sehr begrüßenswerte Wachstum der Allianz für Cybersicherheit auf mehr als 4000 Unternehmen und Institutionen oder der weitere Ausbau der ↗ Sicherheitskooperation Cybercrime zwischen Bitkom und mittlerweile sechs Polizeibehörden. Diese Initiativen haben ein Klima geschaffen, das eine Zusammenarbeit von Staat und Wirtschaft – fördert.

In den Institutionen ist im Moment viel Bewegung. So haben die Landeskriminalämter mit den ZACs (Zentrale Ansprechstelle Cybercrime) mittlerweile feste Ansprechstellen geschaffen. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich als nationale Cybersicherheitsbehörde mit dem Anspruch positioniert, die IT-Sicherheit in der Digitalisierung zu gestalten. Ich beobachte umfangreiche Maßnahmen, möglichst viele Unternehmen mit ihren Empfehlungen sowie zahlreichen technischen Hilfestellungen zu erreichen. Hier leistet insbesondere die ↗ Allianz für Cybersicherheit[5] erfolgreiche Arbeit. Woran liegt es also, dass sich die Wirtschaft wie in der Studie Wirtschaftsschutz zu sehen, dennoch mehr Unterstützung durch den Staat wünscht, und wie sollte diese aussehen?

Der Blick auf die Vielzahl an Organisationen, die sich mit dem Thema Cybersicherheit beschäftigen, macht es den Unternehmen nicht nur schwer, den für sie passenden Ansprechpartner zu finden. Fast noch schwieriger ist es sich an der Vielzahl von Initiativen aktiv zu beteiligen und so von ihnen zu profitieren. Durch die überwältigende Anzahl an Publikationen und Empfehlungen wird eine regelrechte Informationsflut erzeugt. Wer sich nicht dezidiert damit beschäftigt, kann die Informationsflut kaum bewältigen. Für die Wirtschaft ist Information aus einer Hand wichtig, je konkreter desto besser. Insofern gilt es von staatlicher Seite, einige wenige zentrale Stellen zu stärken und die konsolidierten Informationen, die zum Beispiel im weiterentwickelten nationalen Cyberabwehrzentrum zwischen verschiedenen Behörden zusammenlaufen, in geeigneter Form auch der Wirtschaft verfügbar zu machen. Eine reine Cybersicherheitslage für den Staat adressiert nur einen Teil des Gemeinwesens.

Aber auch die Wirtschaft muss sich öffnen, sowohl in der gemeinschaftlichen Zusammenarbeit als auch in Richtung Staat. Es liegt an Politik und Wirtschaft, einen gemeinsamen, umsetzbaren Weg der Zusammenarbeit zu finden, denn in der Fläche wird es der Staat alleine nicht richten können. Dazu braucht es einen offenen Informationsaustausch und die Bereitschaft von beiden Seiten, sich auf Wesentliches zu konzentrieren.

5 Mit der 2012 durch Bitkom mitgegründeten Allianz für Cyber-Sicherheit verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 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 500 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