Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie

Studienbericht

www.bitkom.org

bitkom

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

Ansprechpartner
Cornelius Kopke | Referent Öffentliche Sicherheit & Wirtschaftsschutz | T 030 27576-203 | c.kopke@bitkom.org

Projektteam
Cornelius Kopke | Maurice Shahd | Franz Grimm (Bitkom Research GmbH)

Autoren
Cornelius Kopke | Axel Petri (Deutsche Telekom AG) | Prof. Timo Kob (HiSolutions) | Sven Malte Sopha (Cassini Consulting) | Winfried Holz (Atos Deutschland) | Dipl. Ing. Annegrit Seyerlein-Klug (Technische Hochschule Brandenburg) | Marco Schulz (marconcert GmbH) | Alexander Geschonneck (KPMG AG Wirtschaftsprüfungsgesellschaft) | Silke Kröger (Bundesamt für Verfassungsschutz) | Marius Münstermann (Rohde & Schwarz Cybersecurity GmbH)

Redaktion
Mathias Brose

Gestaltung
Katrin Krause

Bildnachweis
- Titelbild: © Cherish Bryck – Stocksy United
- Seite 5: © Liam Grant – Stocksy United | Seite 58: © mbridger68 – Fotolia.com | Seite 60: © Lumina – Stocksy United
- Grafiken unter Verwendung von © sharpnose – Fotolia.com

Inhalt

Abbildungen

Vorwort

Alter Wein in neuen Schläuchen?

Der Begriff »Wirtschaftsschutz« ist derzeit in aller Munde. Aber was ist das überhaupt? Und ist das wirklich etwas Neues, um das sich in der Vergangenheit niemand Gedanken gemacht hat?

Wirtschaftsschutz ist für uns die Summe aller Maßnahmen von Politik, Behörden und Wirtschaft zur Minimierung von Risiken bei der Unternehmenssicherheit – insbesondere im Bereich der Wirtschaftsspionage, Sabotage, Kriminalität. Die einzelnen Bestrebungen hierunter sind nicht wirklich neu. Allerdings ist es aufgrund der gestiegenen Bedrohungen in den letzten Jahren, der stetig wachsenden Digitalisierung sowie der zunehmenden hybriden Kombination von Angriffsvektoren (z. B. digital und physisch sowie gegen staatliche Stellen und Wirtschaftsunternehmen) mehr denn je erforderlich, die Kräfte von Staat und Wirtschaft zu bündeln und die Schutzmaßnahmen aufeinander abzustimmen.

Das Sicherheitsbewusstsein sowie die digitalen Kompetenzen der Anwender müssen ebenso gestärkt werden. Die Lösungen zur Absicherung sollten zudem möglichst einfach anzuwenden sein. Schließlich müssen wir bei allem, was wir tun, die Anwender »mitnehmen«, was nur über größtmögliche Transparenz auf Seiten aller Beteiligten in Staat und Wirtschaft möglich ist. All dies kann nur gelingen, wenn alle Stakeholder miteinander und nicht nur nebeneinander an diesen Zielen gemeinsam im Dialog arbeiten. Daher gilt im Wirtschaftsschutz, dass das Ganze definitiv mehr ist als die Summe seiner Teile. Und genau darum geht es bei den verstärkten Bemühungen in der jüngsten Vergangenheit wie in der Zukunft.

Die Digitalisierung zieht mehr und mehr in das tägliche Leben der Menschen ein. Alles, was digitalisiert werden kann, wird digitalisiert und alles, was vernetzt werden kann, wird vernetzt. Dieser Trend ist nicht mehr aufzuhalten und das ist auch überhaupt nicht erforderlich oder wünschenswert. Allerdings wächst mit dieser Entwicklung das Erfordernis von Vertrauen der Nutzer in die digitalen Dienste und Produkte. Dieses Vertrauen ist mit jedem einzelnen Sicherheitsvorfall gefährdet. Daher brauchen wir ein Sicherheitsniveau, das dieses Vertrauen rechtfertigt. Dies können wir nur erreichen, wenn wir alle beteiligten Kräfte im Sinne einer gemeinsamen Verantwortung bündeln und dabei jeder Stakeholder die ihm zukommende Rolle wahrnimmt.

Gleichzeitig bedeutet dies aber auch, dass wir – trotz der gewachsenen Bedrohung – alle Maßnahmen immer auch bezüglich des Erfordernisses nach hinreichenden Sicherheitsmaßnahmen sowie Datenschutz und Freiheit in der digitalen Welt sorgfältig abwägen müssen. Ein intensiver gesellschaftlicher Dialog ist weiterhin zwingend notwendig, damit das Vertrauen der Nutzer in den Schutz ihrer Daten gewährleistet werden kann. Auch das ist Aufgabe des Wirtschaftsschutzes.

In der digitalen Welt liegen weiterhin zahlreiche Herausforderungen im Wirtschaftsschutz vor uns. Aus diesem Grunde hat Bitkom 2015 den Arbeitskreis Wirtschaftsschutz gegründet. In diesem wollen wir genau die oben beschriebenen Herausforderungen angehen und ein hohes Sicherheitsniveau für die digitale Welt sicherstellen sowie die Sicherheitsmaßnahmen der digitalen Welt mit den traditionellen Sicherheitsmaßnahmen sinnvoll verknüpfen. Dafür steht der Arbeitskreis Wirtschaftsschutz und dafür stehen wir als Vorstand des Arbeitskreises. Und diesem Ziel dient auch die vorliegende Studie.

Viele Unternehmen sind sich weiterhin der Risiken eines ungewollten Know-how-Verlustes nicht bewusst oder verfügen über kein wirksames Sicherheitskonzept. Auch für die Nachsorge ist nur die Hälfte der Unternehmen gerüstet. Ein gutes Notfallmanagement könnte dafür sorgen, Schäden möglichst gering zu halten und Ausfälle zu vermeiden. Prävention und Aufklärung funktionieren nur wirksam, wenn wir Wirtschaftsschutz als Teamarbeit verstehen. Wirtschaft und Behörden sollten an einem Strang ziehen, um gemeinsam den Wirtschaftsstandort Deutschland zu schützen und unsere gute Position auf dem Weltmarkt zu verteidigen. Und überraschend hat die Studie auch ergeben, dass Unternehmen, die sich als stärker digitalisiert einschätzen, auch signifikant weniger vom Phänomen betroffen sind.

Vorstand des Bitkom Arbeitskreises Wirtschaftsschutz

Einleitung

Die Digitalisierung senkt Hürden und vereinfacht Prozesse. Das gilt für Verbraucher und Unternehmen, das gilt aber leider auch für Kriminelle. Die wichtigsten Ressourcen in der Digitalökonomie sind Daten, und mit genügend Know-how und krimineller Energie lassen sie sich abschöpfen.
Es vergeht kein Monat, in dem nicht irgendwo eine Plattform oder ein Netzwerk prominent gehackt wird. Und es ist geradezu fatal, dass die meisten Angriffe so gut gemacht oder die Angegriffenen so schlecht geschützt sind, dass noch viel häufiger Angriffe gar nicht oder viel zu spät bemerkt werden. Wertvolles, mitunter unersetzliches, Know-how rinnt durch die Finger. Wettbewerbsvorteile gehen verloren. Gerade kleine und mittlere Unternehmen sind hier begehrte Ziele.
Wirtschaft und Behörden mit Sicherheitsaufgaben stehen gleichermaßen vor derselben Herausforderung. Der Professionalisierung, Internationalisierung und Industrialisierung der Computerkriminalität und der Wirtschaftsspionage muss Einhalt geboten werden. Oft bedeutet dies, auf bestimmte Entwicklungen nur reagieren zu können. Immer bedeutet es aber einen Prozess, der nicht zu Ende geht und keinen endgültigen Sieger kennen wird. Es ist eine anspruchsvolle Aufgabe, nicht nur mit dem globalen »fairen« Wettbewerb Schritt zu halten, sondern auch das Feld des »unfairen« Wettbewerbs im Blick zu haben und sich auf die von dort kommenden und wachsenden Gefahren vorzubereiten.
Wirtschaftsschutz muss ganzheitlich verstanden werden. Er ist die Summe aller Maßnahmen von Politik, Behörden und Wirtschaft zur Minimierung von Risiken bei der Unternehmenssicherheit. Hier muss besonders Wirtschaftsspionage, Sabotage und Kriminalität als Bedrohung im Blick behalten werden.
Die Gefahr für Unternehmen, Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl zu werden, ist real. Das Know-how deutscher Unternehmen ist weltweit begehrt. Die Angreifer sind fremde Nachrichtendienste, Wettbewerber, kriminelle Organisationen oder terroristische Gruppierungen.

In einem intensiven globalen Wettbewerb um Märkte und die innovativsten Produkte richten sich Wirtschaftsspionage, Sabotage und Datendiebstahl verstärkt gegen technologieorientierte und innovative mittelständische Unternehmen. Begünstigt wird dieser Trend durch die fortschreitende Digitalisierung der gesamten Wirtschaft. Besonders in der Industrie, also in den Branchen Automobilbau, Chemie und Pharma, sind die Fallzahlen besonders hoch, wie die erste Studie aus dem letzten Jahr gezeigt hat. Deshalb hat Bitkom für die diesjährige Studie den Bereich der Industrie stärker beleuchtet und eine Spezialstudie zu der Bedrohung in diesen Branchen durchgeführt. Um ein repräsentatives Bild zu zeigen wurden deshalb die Branchen Maschinen- und Anlagenbau, Automobilbau, Chemie und Pharma, Kommunikations- und Elektrotechnik sowie sonstige Industriebereiche beleuchtet.

Viele Unternehmen sind sich der Risiken eines ungewollten Know-how-Verlustes nicht bewusst oder verfügen über kein wirksames Sicherheitskonzept. Grade die mittelständische geprägte Wirtschaft hat hier Nachholbedarf. Auch für die Nachsorge ist nur die Hälfte der Unternehmen gerüstet. Ein gutes Notfallmanagement könnte dafür sorgen, Schäden möglichst gering zu halten und Ausfälle zu vermeiden. Prävention und Aufklärung funktionieren nur wirksam, wenn wir Wirtschaftsschutz als Teamarbeit verstehen. Wirtschaft und Behörden sollten an einem Strang ziehen, um gemeinsam den Wirtschaftsstandort Deutschland schützen und unsere gute Position auf dem Weltmarkt zu verteidigen.

Aber auch ein Lichtblick hat sich abgezeichnet. Erstmals wurde untersucht, wie sich der Grad der Digitalisierung von Unternehmen auf ihre Betroffenheit im Know-how Schutz auswirkt. Ob die Digitalisierung quasi ein Beschleuniger für Betroffenheit von Wirtschaftsspionage, Sabotage und Datendiebstahl ist. Und dies hat sich nicht bewahrheitet. Je höher der Grad der Digitalisierung, desto geringer ist tendenziell sogar die Betroffenheit. Je mehr sich mit dem Thema befasst wird, desto mehr Kompetenz im Umgang ergibt sich also. Das zeigt uns, dass es insbesondere ein Thema der Aufklärung und Befähigung zum Umgang mit digitalen Technologien ist.

Mit der Spezialstudie »Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie« wollen wir dieses Thema auf einer validen Datengrundlage beleuchten. Außerdem wollen wir die Unternehmen sensibilisieren und die Diskussion über die Thematik weiter vorantreiben.

Summary

Schäden

Die Studie hat gezeigt, dass 69% der Unternehmen in den letzten zwei Jahren von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffen waren.

Dabei entstand ein Schaden von 22.4 Mrd. Euro im Jahr. Das entspricht rund 0,73% vom jährlichen BIP.

Gleichzeitig verfügen 43% der Unternehmen nicht über ein Notfallmanagement, dass es Ihnen erlaubt, Schäden einzugrenzen und im Fall der Betroffenheit möglichst schnell den Betrieb wieder aufnehmen zu können oder gar nicht erst unterbrechen zu müssen.

Es handelt sich um einen Bereich mit immensen Auswirkungen auf die deutsche Wirtschaft. Deshalb ist eine gemeinsame Anstrengung von Wirtschaft, Politik und Sicherheitsbehörden notwendig. Vor diesem Hintergrund ist es bedenklich, dass sich nur jedes fünfte Unternehmen (36%) an staatliche Stellen wendet.

Sicherheit

Von den befragten Unternehmen gaben 29% an, in den letzten zwei Jahren von Angriffen auf Ihre IT-Abteilung betroffen gewesen zu sein. Als Reaktion haben 100% technische Sicherheitsmaßnahmen ergriffen. Dazu gehören Virenscanner, Firewalls und regelmäßige Updates.

Da die Angriffe aber immer komplexer werden, sind auch zusätzliche Schutzmaßnahmen notwendig. Dazu gehören zum Beispiel Verschlüsselungstechniken insbesondere für sensible Daten, aber auch neue Technologien im Bereich Intrusion Detection, Intrusion Prevention und Data Leakage Prevention.

Hier haben viele Unternehmen noch Nachholbedarf. Dafür ist bei vielen Unternehmen auch ein Umdenken notwendig, dass sich Investitionen in Sicherheit auch langfristig auszahlen und nicht nur der monetäre Aufwand im Vordergrund stehen darf.

Organisation

Auch die Organisation kann für mehr Sicherheit sorgen. Dazu gehören unter anderem Regelungen, wer im internen Netzwerk auf welche Daten zugreifen darf und wer Zutritt zu sensiblen Bereichen eines Unternehmens bekommt. Immerhin 87% der befragten Unternehmen machen sich darüber Gedanken.

Ein Notfallmanagement gewährleistet eine schnelle Reaktion im Krisenfall. Darüber verfügt bisher nur knapp über die Hälfte (51%) der Unternehmen in Deutschland.

Eine Möglichkeit, den Aspekt der Sicherheit innerhalb der Organisation zu erhöhen, sind Sicherheitszertifizierungen. Sie zwingen das Unternehmen, sich mit dem Thema intensiv auseinanderzusetzen. In der Praxis sind sie ein geeignetes Mittel, um höhere Sicherheitsstandards im gesamten Unternehmen zu etablieren.

Faktor Mensch

Bei 60% der von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffenen Unternehmen war ein ehemaliger Mitarbeiter das Einfallstor. Die Motive sind ganz unterschiedlich. Auch kann es sich um Fälle von Naivität handeln. So ist Social Engineering, also das Manipulieren von Mitarbeitern, mit 16% eines der häufigsten Delikte.

Demgegenüber führt nur 56% der Befragten Schulungen der Mitarbeiter oder Sicherheitsüberprüfungen von Bewerbern durch. Eine angemessene Sicherheitskultur umfasst darüber hinaus die richtige Verwendung von Zugangsdaten, den korrekten Umgang mit externen Datenträgern oder Verhaltensregeln auf Reisen.

Methode

Viele deutsche Unternehmen sind aufgrund ihrer innovativen Produkte und ihrer starken Position auf den Weltmärkten ein lukratives Ziel für kriminelle Hacker und ausländische Geheimdienste. Der Diebstahl sensibler Unternehmensdaten, der Ausfall von IT-Systemen oder eine Unterbrechung der Produktion als Folge digitaler Angriffe verursachen Schäden in Milliardenhöhe. Mit der vorliegenden Studie untersucht der Digitalverband Bitkom, welche Unternehmen von entsprechenden Vorfällen betroffen sind, wer die mutmaßlichen Täter sind und ob sich die Wirtschaft ausreichend schützt. Außerdem wurde auch die Höhe der verursachten Schäden ermittelt. Ein besonderes Augenmerk wurde dabei auf die Betreiber kritischer Infrastrukturen, die für die Versorgung der Gesellschaft von besonderer Bedeutung sind, gelegt.

Dafür wurden insgesamt 1.074 nach Branchen und Größenklassen repräsentativ ausgewählte Unternehmen mit min destens zehn Mitarbeitern befragt. Es handelt sich um die bislang umfassendste empirische Untersuchung dieses Themas in Deutschland. 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, so dass die Ergebnisse ein nach Branchengruppen und Größenklassen repräsentatives Bild für alle Unternehmen ab zehn Mitarbeitern in Deutschland ergeben.

Mit der konkreten Durchführung der computergestützten telefonischen Interviews (CATI) wurde das Marktforschungsinstitut Aris Umfrageforschung mbH in Hamburg beauftragt. Die Interviews wurden von im Vorfeld speziell geschulten Telefoninterviewern im Januar und Februar 2015 realisiert. Der standardisierte Fragebogen wurde von der Bitkom Research GmbH in Zusammenarbeit mit dem Digitalverband Bitkom konzipiert.

1 Betroffene Industrieunternehmen

»Die wichtigsten Ressourcen in der Digitalökonomie sind Daten, und mit genügend Know-how und krimineller Energie lassen sich diese abschöpfen. Wir müssen es gemeinsam schaffen, der Professionalisierung, Internationalisierung und Industrialisierung von Computerkriminalität und Wirtschaftsspionage Einhalt zu gebieten. Dafür muss der Informationsaustausch zwischen Wirtschaft und Behörden weiter verbessert werden. Vor allem kleine und mittelständische Industrieunternehmen müssen noch besser über entsprechende Sicherheitskonzepte informiert werden.«

Bitkom-Präsident Thorsten Dirks am 16.03.2016 auf der Pressekonferenz zur Kooperation des Bitkom mit dem Bundesamt für Verfassungsschutz in Hannover

Der weit überwiegende Teil aller Industrieunternehmen in Deutschland ist von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen oder vermutet betroffen zu sein. Insgesamt 89 Prozent der Industrieunternehmen gabendies an. Von den kleinen Industrieunternehmen 10 bis 99 MA sind es sogar 92 Prozent. Schäden sowie andere Auswirkungen von Computerkriminalität und Wirtschaftsspionage traten bei mehr als zwei Dritteln der Industrieunternehmen auf (69 Prozent). Besonders betroffen war im vergangenen Jahr der Automobilbau sowie die Chemie- und Pharmabranche (vgl. ↗Studie »Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter«, Bitkom 2015). Daher lag der Fokus dieser Spezialstudie auf dem Industriesektor und seinen besonders befallenen Branchen. Häufigstes Delikt ist der Diebstahl von IT- oder Telekommunikationsgeräten wie Computer, Smartphones oder Tablets und der darauf gespeicherten Daten.

1.1 Spionage, Sabotage und Datenklau trifft mehr als zwei Drittel der Industrieunternehmen

Gut zwei Drittel (69 Prozent) aller Industrieunternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Weitere 20 Prozent geben an, dass ihr Industrieunternehmen vermutlich betroffen ist. Am stärksten trifft es die großen Industrieunternehmen, die 500 und mehr Mitarbeiter beschäftigen, mit 77 Prozent. Darauf folgen die kleineren Betriebe mit 10 bis 99 Beschäftigten (70 Prozent). Etwas unterdurchschnittlich sind die mittelständischen Unternehmen betroffen (64 Prozent).

Auffällig ist, dass die großen Unternehmen in Bezug auf IT-Sicherheitsvorfälle offenbar weniger im Dunkeln tappen als kleinere Unternehmen. Der Anteil vermuteter Vorfälle ist geringer (13 Prozent vs. 22 Prozent), während der Anteil aufgedeckter Fälle höher liegt als bei kleineren Betrieben (77 Prozent vs. 70 Prozent).

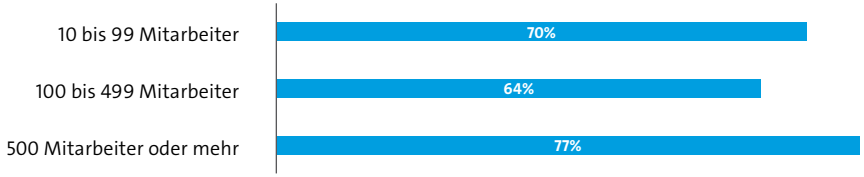


Abbildung 1: Betroffene Industrieunternehmen nach Betriebsgrößenklassen

Basis: Alle befragten Industrieunternehmen (n=504)
Quelle: Bitkom Research

Experten-Statement

Winfried Holz, CEO, Atos Deutschland

Der Cyberspace ist längst nicht mehr unschuldige Spielwiese für den kreativen wissenschaftlichen Austausch zur Förderung des Fortschritts – er gleicht eher dem wilden Westen: Das weltweite Datennetz ist durchsetzt von professionellen Hackern, die entweder als Söldner oder im eigenen Interesse Unternehmen angreifen. Deutschland, mit seiner starken und weltweit führenden Industrie, gehört zu den beliebtesten Zielen. Der größte Teil der deutschen Industrieunternehmen war in den vergangenen zwei Jahren von Sicherheitsvorfällen betroffen oder vermutet es zumindest. Mit 36 Prozent richteten sich die meisten Angriffe auf die Produktion und Fertigung. Dies sind klare Angriffe auf die Wettbewerbsfähigkeit der betroffenen Unternehmen – entweder durch Sabotage oder durch den Diebstahl geschäftskritischer Daten.

Die digitale Transformation der Unternehmen im Sinne von Industrie 4.0 verschärft diese Situation noch: Indem immer mehr Daten verfügbar gemacht werden und die Grenzen der internen IT-Infrastrukturen aufweichen, entstehen immer neue Angriffsmöglichkeiten. Doch zur Digitalisierung gibt es keine Alternative. Daher müssen wir alle Anstrengungen der Wirtschaft und Politik bündeln, um ganzheitliche Sicherheitsmechanismen ›by design‹ und ›by development‹ in die Industrie-4.0-Prozesse zu implementieren. Im wilden Westen haben sich Recht und Ordnung gegen die Gesetzlosigkeit durchgesetzt. Im Cyberspace wird uns das auch gelingen.

1.2 Maschinen und Anlagenbau in der Industrie am stärksten betroffen

Betrachtet man die betroffenen Industrieunternehmen nach Branchen, zeigen sich keine erheblichen Unterschiede: Leicht überdurchschnittlich von Computerkriminalität und Wirtschaftsspionage betroffen ist der Maschinen- und Anlagenbau (70 Prozent). Direkt danach folgen die Chemie- und Pharmaindustrie mit 68 Prozent sowie die Hersteller von Kommunikations- und Elektrotechnik mit 65 Prozent.

Bemerkenswert ist die Entwicklung in der Automobilbranche. Nicht zuletzt wegen der Herausforderung der Digitalisierung und der selbstfahrenden Fahrzeugtechnologien haben die deutschen Fahrzeugbauer und ihre Zulieferer in den vergangenen Jahren signifikant in IT-Sicherheit investiert. Das zeigt offenbar Wirkung: In diesem Jahr ist der Automobilbau mit 61 Prozent betroffener Unternehmen die am wenigsten von Computerkriminalität befallene Branche. Im Vorjahr lag sie mit 68 Prozent noch an der Spitze.

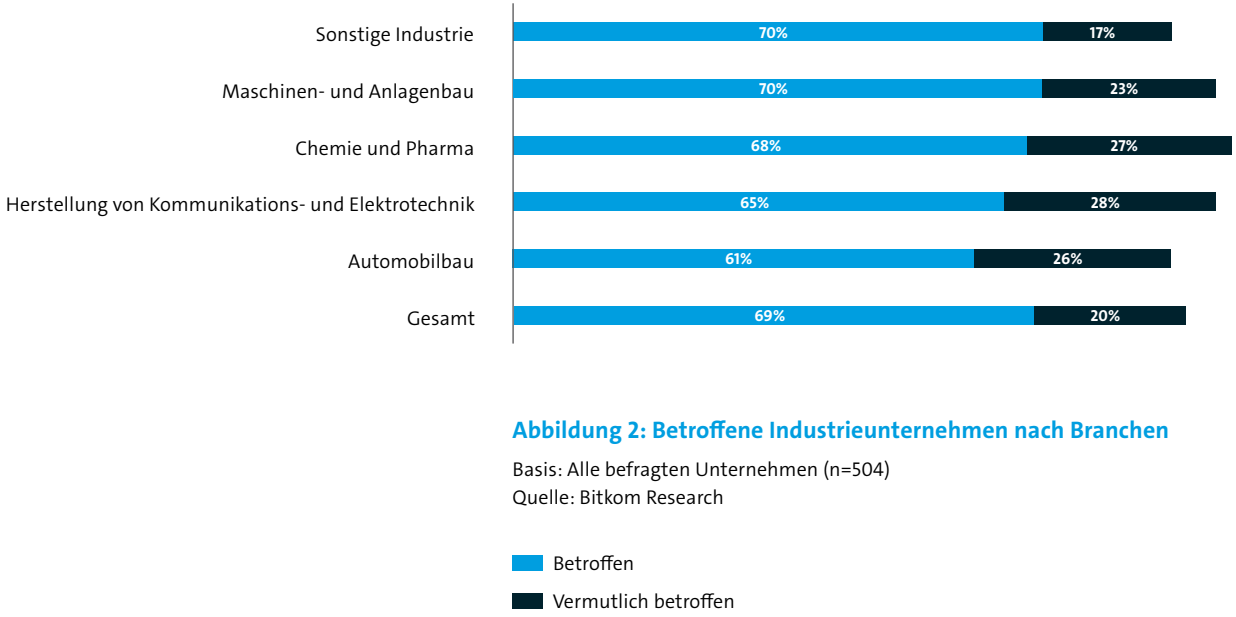


Abbildung 2: Betroffene Industrieunternehmen nach Branchen

Basis: Alle befragten Unternehmen (n=504)
Quelle: Bitkom Research

1.3 Höhere Digitalisierung führt zu geringerer Betroffenheit

Ein besonderes Augenmerk wurde bei der Befragung auf das Digitalisierungsniveau der Unternehmen gelegt. Hintergrund war, dass aus Sicht der Experten die zunehmende Vernetzung auch zu steigenden Sicherheitsrisiken führt. Stärker digitalisierte Unternehmen müssten also auch stärker von Computerkriminalität betroffen sein, so die Vermutung.
Das Gegenteil ist jedoch der Fall – zumindest laut dieser Studie: Der Anteil betroffener Industrieunternehmen, die ihren Digitalisierungsgrad als sehr oder eher hoch einschätzen, ist um 11 Prozentpunkte geringer als bei denjenigen Betrieben, die sich einen sehr oder eher niedrigen Digitalisierungsgrad zuschreiben.

Eine Erklärung könnte darin liegen, dass die Auseinandersetzung mit der Digitalisierung automatisch auch das Thema IT-Sicherheit auf den Plan ruft. Je mehr sich die Unternehmen digitalisieren, umso wichtiger werden ihnen offenbar die Sicherheitsstandards und desto effektiver wird ihr Schutz gegen IT-Angriffe.

Weitere Werte und Zahlen zu dem Grad der Digitalisierung von Industrieunternehmen befinden sich im Kapitel 2.1:Grad der Digitalisierung der Industrie.

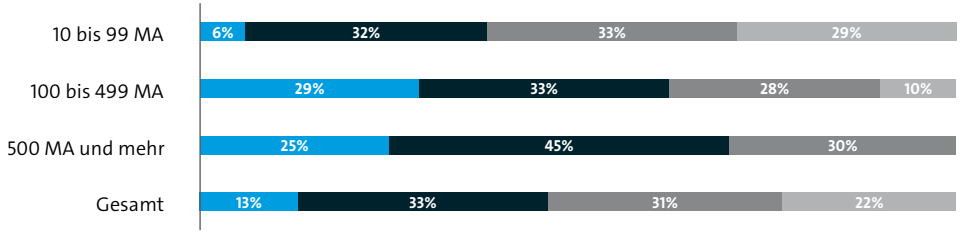


Abbildung 3: Einschätzung Digitalisierungsgrad nach Betriebsgrößenklassen

Basis: Alle befragten Unternehmen (n=504)
Quelle: Bitkom Research

1.4 Häufigster Vorfall ist der Diebstahl von Daten und Datenträgern

Das am häufigsten auftretende Delikt ist der Diebstahl von IT- und Telekommunikationsgeräten: In 32 Prozent der befragten Industrieunternehmen sind in den letzten zwei Jahren zum Beispiel Computer, Smartphones oder Tablets gestohlen worden. Allerdings geht daraus nicht hervor, ob es die Täter auf das Gerät oder die darauf befindlichen Informationen abgesehen haben. Diese Zahl hat sich gegenüber der Erhebung aus dem letzten Jahr nicht verändert.

Bei immerhin jedem fünften der befragten Industrieunternehmen (20 Prozent) sind sensible physische Dokumente, Muster, Bauteile oder sogar Maschinen gestohlen worden. Dies zeigt, dass die Verbindung von physischer Sicherheit und Cybersicherheit ein wesentliches Thema für die Unternehmenssicherheit ist.

Fast ebenso viele Befragte berichten jeweils vom Diebstahl sensibler elektronischer Dokumente bzw. Daten (19 Prozent) sowie von der Sabotage ihrer IT-Systeme oder Betriebsabläufe (18 Prozent). Der Angriff auf den französischsprachigen TV-Sender TV5 Monde war im Jahr 2015 ein typischer Fall von erfolgreicher Sabotage. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Fall dokumentiert, bei dem in Deutschland ein Hochofen nach einem IT-Angriff schwer beschädigt wurde. Solche Vorfälle werden mit der immer stärkeren Vernetzung zunehmen.

Etwa ein Sechstel (16 Prozent) der Industrieunternehmen registrierte in den vergangenen zwei Jahren Fälle von Social Engineering. Bei dieser Methode geht es darum, Mitarbeiter zu manipulieren, um an bestimmte Informationen zu gelangen. Häufig geht Social Engineering gezielten Hacking- oder Phishing-Angriffen voraus. Mithilfe von Informationen aus dem Umfeld der Mitarbeiter werden dann beispielsweise täuschend echte E-Mails von vermeintlichen Bekannten verfasst, deren Anhang vom Adressaten geöffnet wird. Auf diese Weise gelangt Schadsoftware (wie Trojaner) auf die Computer, die in der Folge Passwörter und andere Daten auslesen.

Bei 6 Prozent der Industrieunternehmen ist die elektronische Kommunikation ausgespäht worden. Der Anteil der vermuteten Angriffe ist hier am höchsten. Immerhin fast ein Viertel der Industrieunternehmen (23 Prozent) vermuten auf diese Weise ausspioniert worden zu sein. Das Abhören von Telefonaten oder Besprechungen gehört eher zu den selteneren Fällen der Wirtschaftsspionage. Nur fünf Prozent der Industrieunternehmen haben nach eigenen Angaben in den vergangenen zwei Jahren solche Angriffe festgestellt und 12 Prozent vermuten dies.

Zusammenfassend zeigt sich, dass nahezu alle Fälle von Sabotage oder Spionage im wirtschaftlichen Umfeld heute auf digitale Daten oder die Informations- und Kommunikationsinfrastruktur der Industrieunternehmen abzielen. Das ist eine direkte Folge der inzwischen weit fortgeschrittenen Digitalisierung in der deutschen Industrie.

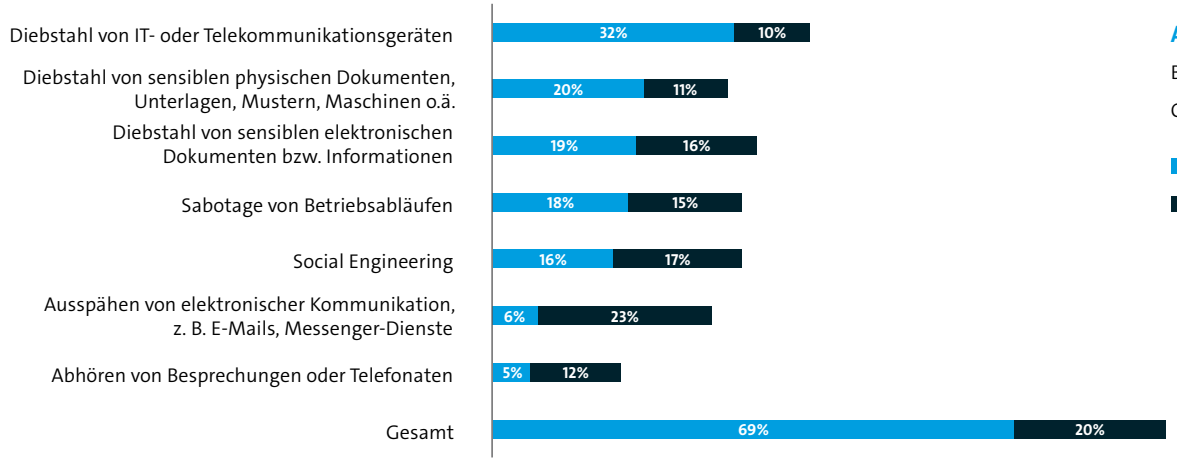


Abbildung 4: Aufgetretene Delikte

Basis: Alle befragten Industrienternehmen (n=504)

Quelle: Bitkom Research

Betroffen

Vermutlich betroffen

1.5 Kosten entstehen vor allem durch Rechtsverfolgung und Imageschäden

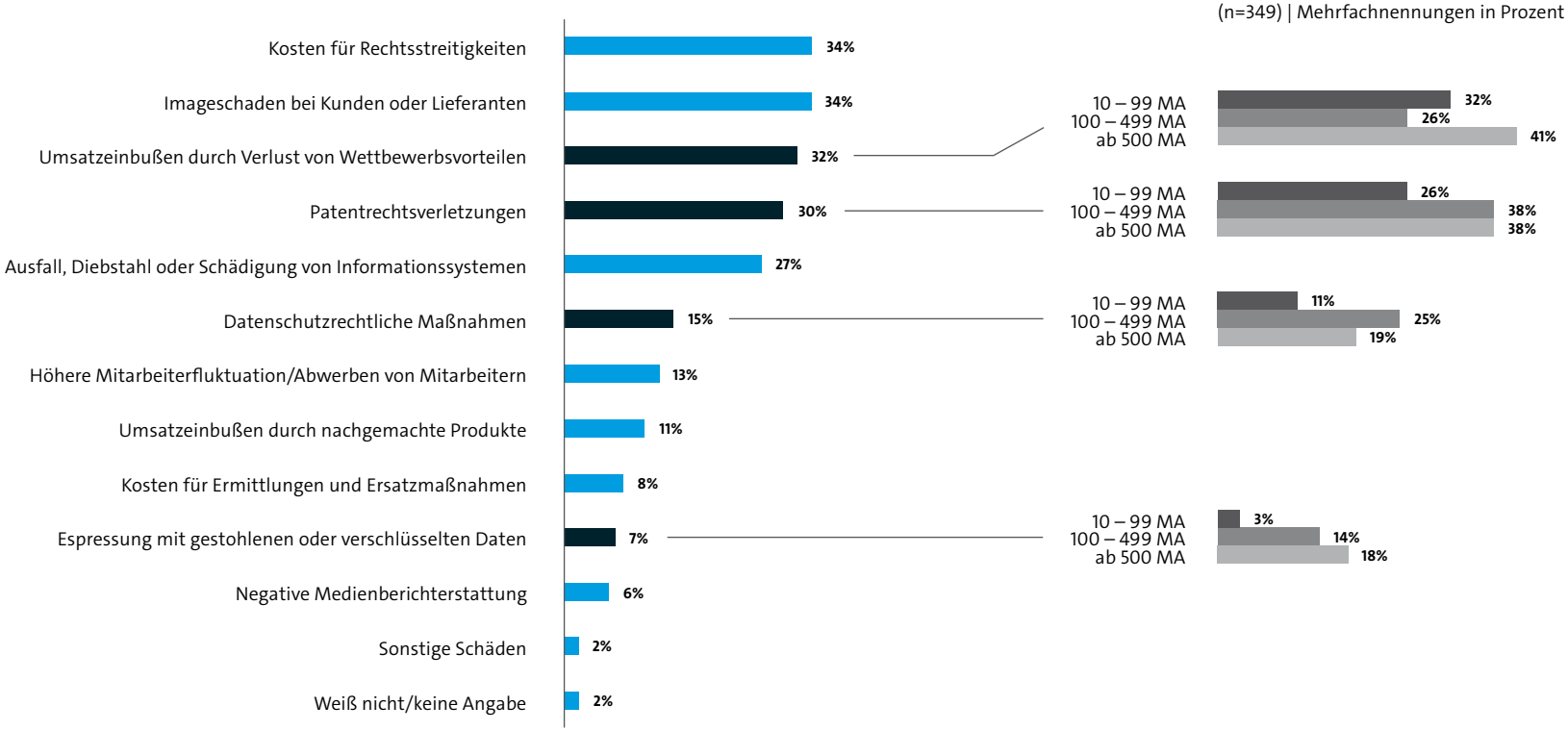
Jeweils mehr als ein Drittel der von Angriffen betroffenen Industrieunternehmen waren in der Folge mit Rechtsverfolgungskosten und mit Imageschäden konfrontiert (je 34 Prozent). Dicht darauf folgen Wettbewerbsnachteile (32 Prozent). Diese können entweder indirekt durch Angriffe entstehen, weil die Konkurrenz durch die Kenntnis neuer Fertigungsmethoden effizienter produziert. Oder sie führen direkt zu Verlusten, z. B. durch Unterbieten bei Ausschreibungsverfahren und den damit einhergehenden Auftragsverlust, wie bereits 1994 zwischen Airbus und Boeing geschehen.

An vierter Stelle nennen die Industrieunternehmen Patentrechtsverletzungen (30 Prozent). Der Ausfall, Diebstahl oder die Schädigung von Informationssystemen kommt hingegen erst an fünfter Stelle und wurde von mehr als einem Viertel der betroffenen Unternehmen berichtet (27 Prozent). Hervorzuheben ist auch, dass die Wettbewerbsnachteile besonders die großen Unternehmen mit mehr als 500 Mitarbeitern betreffen. Hier berichten sogar 41 Prozent der befragten Industrieunternehmen, dass ihnen Schäden entstanden sind.

Für mittelständische Unternehmen waren in einem Viertel aller Fälle (25 Prozent) datenschutzrechtliche Maßnahmen nach einem Vorfall ein Kostentreiber. Die Digitalisierung wird auch hier die Nähe zum Kunden immer wichtiger werden lassen, damit digitale Geschäftsmodelle funktionieren (Plattformökonomie). Kosten entstehen bei datenschutzrechtlichen Schäden vor allem durch Informationskosten der betroffenen Personen.

Abbildung 5: Aufgetretene Schadensvorfälle

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=349) | Mehrfachnennungen in Prozent | Quelle: Bitkom Research



1.6 Die Produktion/Fertigung ist das zentrale Angriffsziel in der Industrie

Häufigstes Angriffsziel ist die Produktion und Fertigung, die bei mehr als einem Drittel der betroffenen Unternehmen befallen war (36 Prozent). Am zweithäufigsten wurde der Lager- und Logistikbereich (30 Prozent) angegriffen, dicht gefolgt von den IT- und Kommunikationssystemen (29 Prozent).
Sie sind das Einfallstor für digitale Spionage- und Sabotageakte. Es folgen die Bereiche Forschung und Entwicklung (23 Prozent) sowie das Marketing und der Vertrieb (21 Prozent). Weniger betroffen sind das Finanz- und Rechnungswesen, die Geschäftsleitung bzw. das Management, Einkauf sowie Personalbereiche.

Im Hinblick auf die zunehmende Vernetzung der Produktion und Fertigung im Rahmen von Industrie 4.0 ist es sehr beunruhigend, dass diese Bereiche bereits jetzt so stark befallen sind.

Dass der Bereich Forschung und Entwicklung mit 23 Prozent erst an vierter Stelle auftaucht, überrascht nur auf den ersten Blick. Die meisten kleinen Industrieunternehmen haben gar keine eigenen Forschungs- und Entwicklungsabteilungen. Dagegen geben mehr als ein Drittel (38 Prozent) der großen Industrieunternehmen ab 500 Mitarbeitern an, dass ihre F&E-Bereiche gehackt oder ausspioniert worden sind. Dies ist der Spitzenwert und bei den großen Unternehmen der am häufigsten betroffene Bereich.

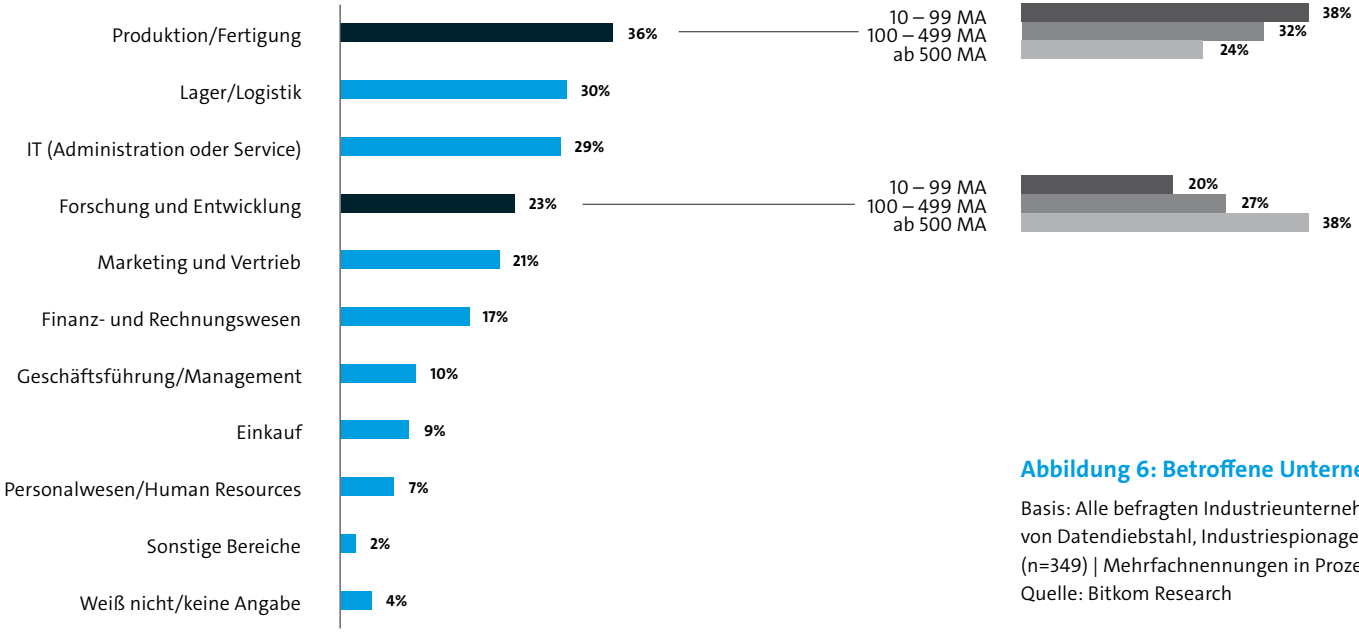


Abbildung 6: Betroffene Unternehmensbereiche

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=349) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

2 Digitalisierungsniveau

2.1 Grad der Digitalisierung der Industrie

Die Digitalisierung schreitet voran und bringt Vorteile wie enorme Effizienzgewinne und völlig neue Geschäftsmodelle mit sich. Allerdings wächst mit der Abhängigkeit von der Vernetzung auch die Verwundbarkeit der Unternehmen. Das war nicht zuletzt die Motivation für das IT-Sicherheitsgesetz. Deshalb sollte untersucht werden, inwiefern ein Zusammenhang zwischen der Gefährdung durch IT-Angriffe und dem Grad der Digitalisierung eines Unternehmens besteht. Dabei hat sich gezeigt, dass Unternehmen, die nach eigenen Angaben in einem höheren Maß digitalisiert sind, signifikant weniger von Vorfällen im Bereich Sabotage, Spionage oder Datendiebstahl betroffen sind als Unternehmen, die ihr Digitalisierungsniveau eher niedrig einschätzen. Stärker digitalisierte Industrieunternehmen sind um 11 Prozentpunkte weniger betroffen.

Offenbar führt also die Auseinandersetzung mit dem Thema Digitalisierung zu einem positiven Nebeneffekt für die Sicherheit des Unternehmens. Dies kann insbesondere an dem besseren Know-how im Unternehmen zu den Themen liegen.

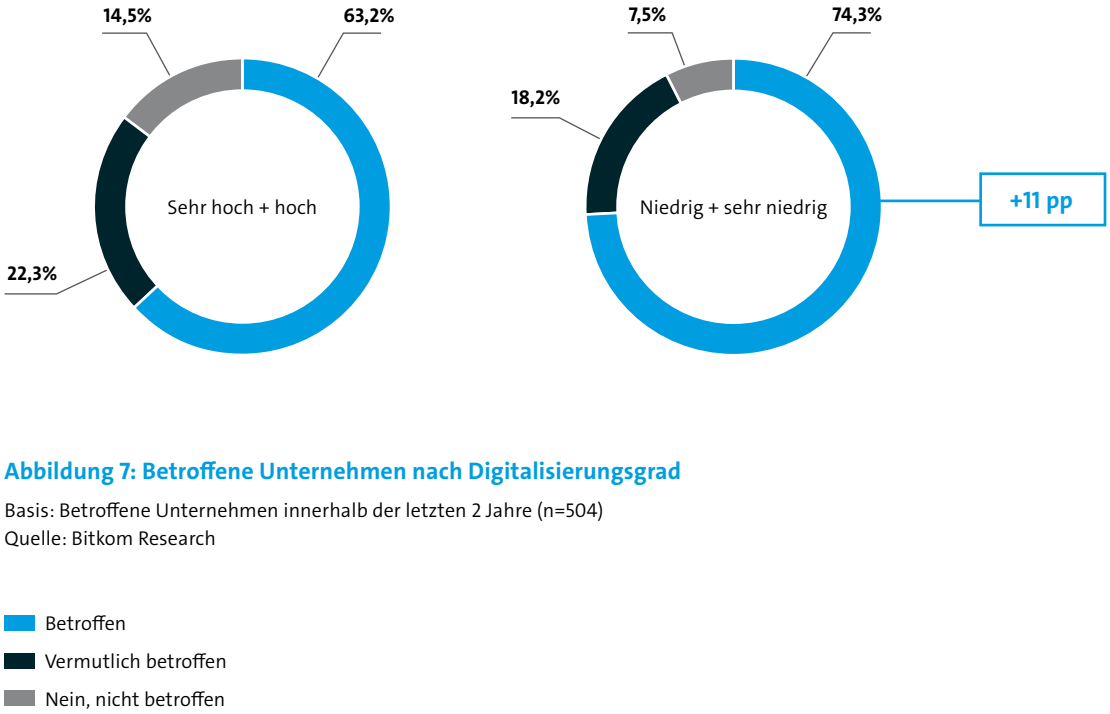


Abbildung 7: Betroffene Unternehmen nach Digitalisierungsgrad

Basis: Betroffene Unternehmen innerhalb der letzten 2 Jahre (n=504)
Quelle: Bitkom Research

2.2 Kleinere Industrieunternehmen sind weniger digital

Dabei hat ein Überblick über die Betriebsgrößenklassen ergeben, dass die kleineren Industrieunternehmen am geringsten digital arbeiten. Nur 6 Prozent der Industrieunternehmen mit 10 bis 99 Mitarbeitern stufen den Digitalisierungsgrad ihres Unternehmens als sehr hoch ein, weitere 32 Prozent schätzen ihr Unternehmen als eher hoch digitalisiert.

Bei den mittelständischen Industrieunternehmen ist der Anteil, der sich sehr hoch digital einschätzenden Unternehmen mit 29 Prozent am größten. Ein weiteres Drittel (33 Prozent) meint eher hoch digitalisiert zu sein. Bezeichnend ist auch, dass bei den größten Unternehmen keines mehr sehr niedrig digitalisiert zu funktionieren scheint. Hier stufen sich bereits 25 Prozent als sehr hoch, 45 Prozent als eher hoch und nur 30 Prozent als eher niedrig digitalisiert ein.

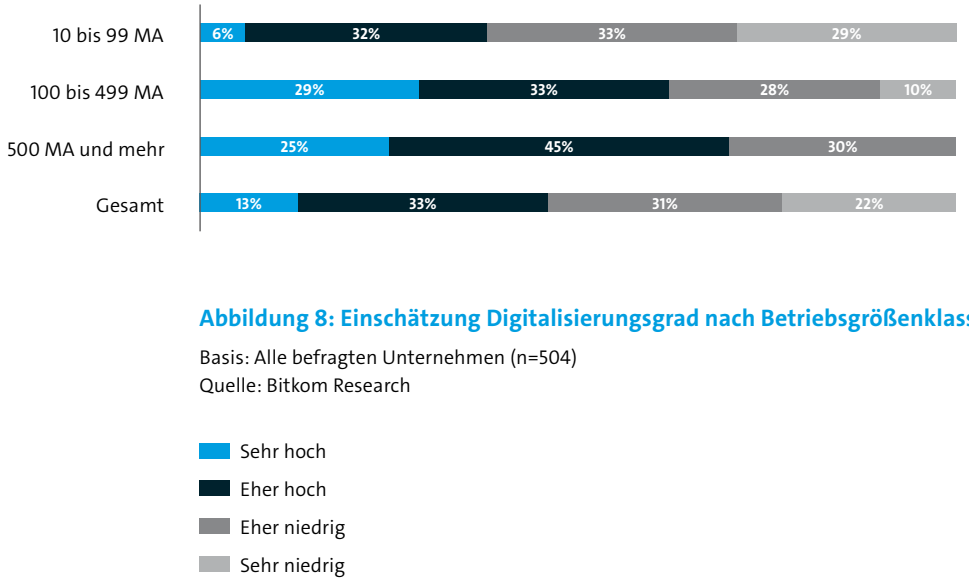


Abbildung 8: Einschätzung Digitalisierungsgrad nach Betriebsgrößenklassen

Basis: Alle befragten Unternehmen (n=504)
Quelle: Bitkom Research

2.3 Grad der Digitalisierung der Industrie nach Branchen

Der Branchenvergleich ergibt einen sehr homogenes Bild: Die Differenzen zwischen den einzelnen Industriezweigen betragen weniger als 7 Prozentpunkte. Dies zeigt, dass die Digitalisierung sämtliche Industriebereiche gleichermaßen erfasst und es nicht etwa ein Phänomen einzelner Industriebranchen ist. Am stärksten digitalisiert schätzen sich die Hersteller der Automobilbranche ein. 16 Prozent geben an, »sehr hoch« digitalisiert zu sein. Darauf folgt die sonstige Industrie (14 Prozent) sowie die Chemie- und Pharmabranche (13 Prozent), der Maschinen- und Anlagenbau (11 Prozent) und schließlich die Hersteller von Kommunikations- und Elektrotechnik (10 Prozent).

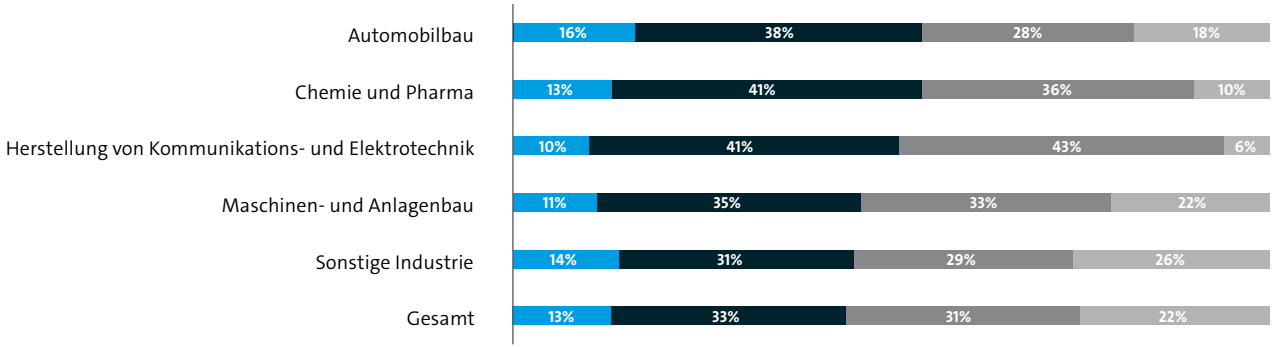


Abbildung 9: Einschätzung Digitalisierungsgrad nach Branchen

Basis: Alle befragten Industrieunternehmen (n=504)
Quelle: Bitkom Research

2.4 Digitalisierungsstrategien der Industrieunternehmen

Zum Abschluss wurden die Industrieunternehmen befragt, ob sie sich auf die Veränderungen des digitalen Wandels vorbereiten und eine Strategie dazu entwickelt haben oder dies in Zukunft tun. Hier haben die größeren Industrieunternehmen sich erkennbar mehr auf die Herausforderungen vorbereitet als die kleineren Industrieunternehmen. Denn 66 Prozent und damit zwei Drittel der Industrieunternehmen mit mehr als 500 Mitarbeitern haben bereits eine zentrale Strategie für die Digitalisierung. Bei den mittelständischen Industrieunternehmen sind es 60 Prozent und damit nur unwesentlich weniger.

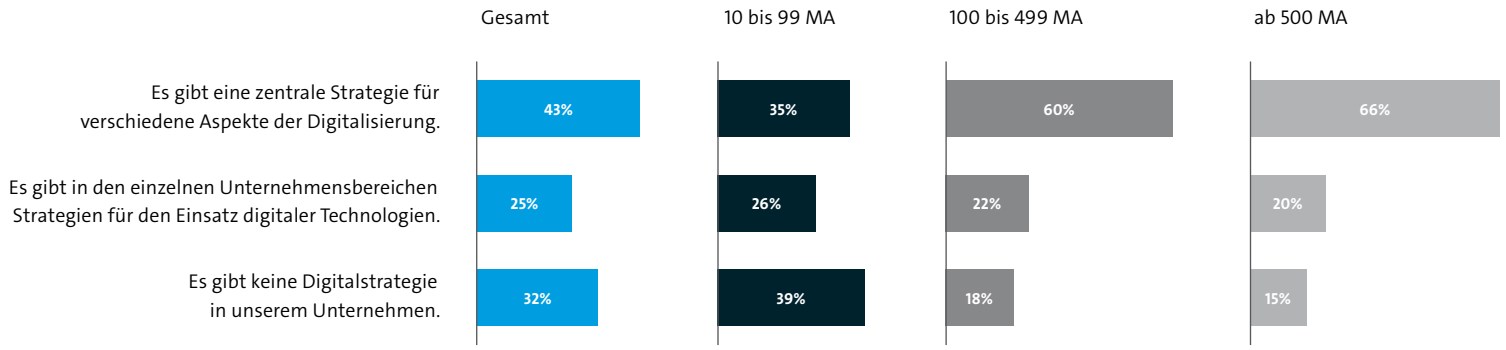
Allerdings sind die kleineren Industrieunternehmen von 10 bis 99 Mitarbeitern nur zu gut einem Drittel auf die Digitalisierung vorbereitet. Trotz einer langen Diskussion um Industrie 4.0, Plattformökonomie und disruptive Geschäftsmodelle haben sich nur 35 Prozent der kleinen Industrieunternehmen darauf eingestellt und 39 Prozent dieser kleinen Industrieunternehmen geben an, in keinem Bereich des Unternehmens über eine Digitalisierungsstrategie zu verfügen. Hier können die Kleinen von den Großen lernen. Von den großen Industrieunternehmen behaupten nur 15 Prozent überhaupt keine Digitalisierungsstrategie zu haben, dagegen stehen 18 Prozent der mittelständischen Unternehmen.

Bemerkenswert ist auch, dass der Anteil der Industrieunternehmen, die in Teilbereichen eine Digitalisierungsstrategie besitzen, deutlich niedriger ist als der Anteil an Industrieunternehmen, die für das gesamte Unternehmen eine Digitalisierungsstrategie festgeschrieben haben. Bei den größeren Industrieunternehmen ab 500 Mitarbeitern sind es nur 20 Prozent, die nur Teilbereiche des Unternehmens in eine Digitalisierungsstrategie eingebettet haben, während 66 Prozent eine Gesamtstrategie aufgesetzt haben. Damit wird der Trend zu einer Digitalisierung in allen Unternehmensbereichen gestützt.

Abbildung 10: Betroffene Industrieunternehmen nach Betriebsgrößenklassen

Basis: Alle befragten Industrieunternehmen (n=504)

Quelle: Bitkom Research



2.5 Digitalisierung schafft nebenbei auch mehr technische und organisatorische Sicherheitsmaßnahmen

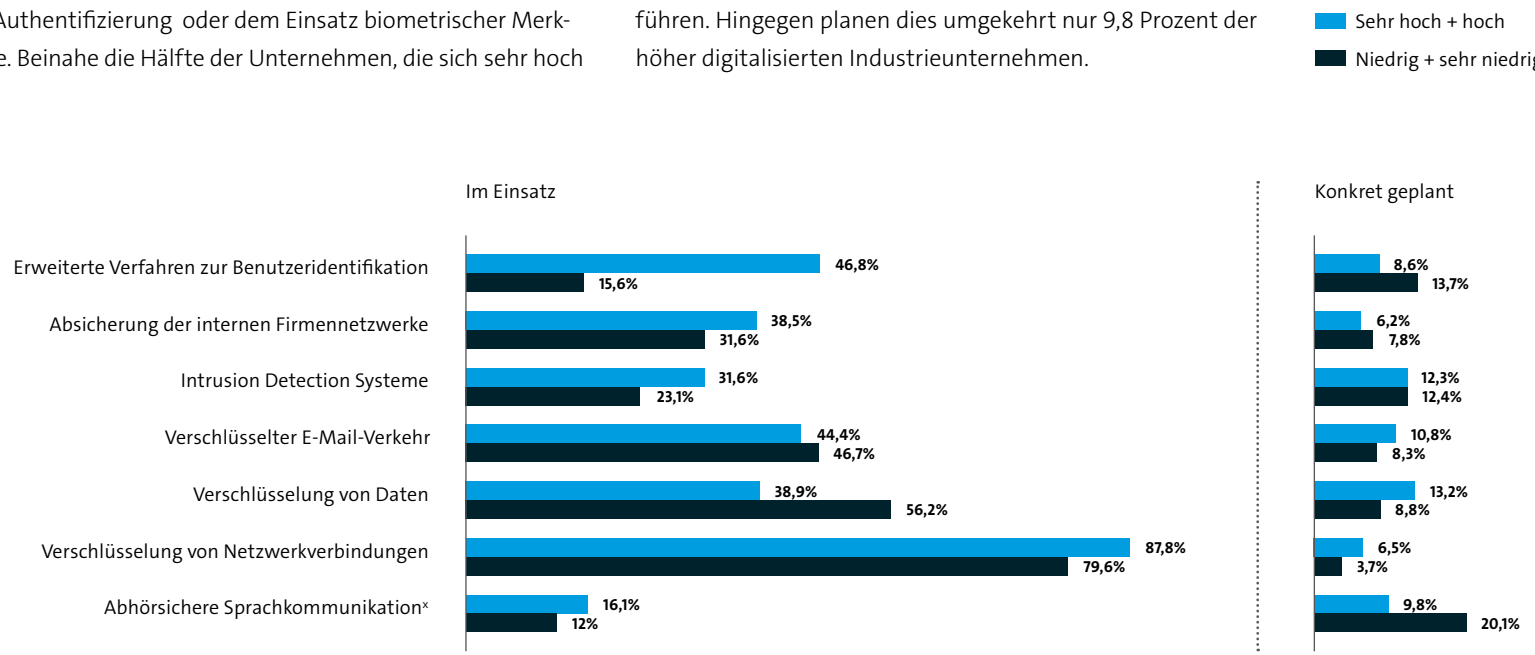
Beleuchtet man die einzelnen Sicherheitsmaßnahmen in Abhängigkeit zum Grad der Digitalisierung der Industrieunternehmen, zeigt sich, dass mit dem Mehr an Digitalisierung offenbar als Nebeneffekt auch ein Mehr an Sicherheit im Allgemeinen entsteht. Denn die Industrieunternehmen, die sich als sehr oder hoch digitalisiert einschätzen, setzen auch vermehrt technische und organisatorische Sicherheitsmaßnamen ein. Es steigt also offenbar das Bewusstsein für das Risiko und damit die Bereitschaft, diese Risiken zu verringern.

Erkennbar wird dies zum Beispiel am Einsatz von erweiterten Verfahren zur Benutzerauthentifizierung, wie der Zwei-Faktor-Authentifizierung oder dem Einsatz biometrischer Merkmale. Beinahe die Hälfte der Unternehmen, die sich sehr hoch oder hoch digitalisiert einschätzen (46,8 Prozent) nutzt solche erweiterten Verfahren, während dies bei den niedrig oder sehr niedrig digitalisierten Industrieunternehmen nur 15,6 Prozent betrifft. Diese große Diskrepanz wird in den kommenden Jahren voraussichtlich abnehmen, denn viele weniger digitalisierte Betriebe planen bereits den Einsatz weiterer technischer Sicherheitsmaßnahmen. Abhörsichere Sprachkommunikation plant zum Beispiel ein doppelt so hoher Anteil der niedrig wie der hoch digitalisierten Unternehmen (20,1 Prozent vs. 9.8 Prozent). Beispielsweise planen 20,1 Prozent der Industrieunternehmen, die sich niedrig oder sehr niedrig digitalisiert einschätzen, konkret abhörsichere Sprachkommunikation einzuführen. Hingegen planen dies umgekehrt nur 9,8 Prozent der höher digitalisierten Industrieunternehmen.

Abbildung 11: Technische Sicherheitsmaßnahmen und Digitalisierung

Basis: Alle befragten Industrieunternehmen (n=504) | [x]n=430

Quelle: Bitkom Research



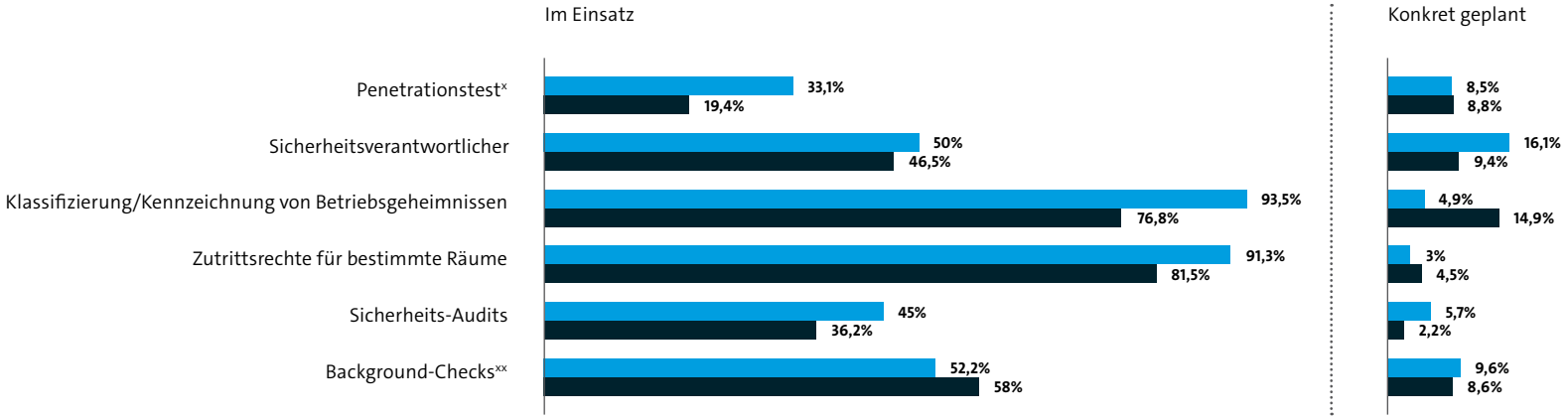
Bei den organisatorischen Sicherheitsmaßnahmen stellt es sich ähnlich dar. So haben bei den höher oder sehr hoch digitalisierten Industrieunternehmen 33,1 Prozent Penetrationstests im Einsatz, bei denen versucht wird, die Lücken im System durch Angriffssimulation zu finden. Bei den niedrig oder sehr niedrig digitalisierten Unternehmen sind es hingegen nur 19,4 Prozent. Auch haben die höher digitalisierten Industrieunternehmen rund 4 Prozentpunkte mehr Sicherheitsverantwortliche verpflichtet, kennzeichnen oder klassifizieren zu rund 17 Prozent mehr ihre Betriebsgeheimnisse, die sogenannten Kronjuwelen. Sie führen auch zu rund 9 Prozent mehr Sicherheitsaudits durch oder haben zu rund 10 Prozent mehr Zutrittsregelungen zu sensiblen Bereichen.

Dadurch zeigt sich, dass die verstärkte Befassung mit dem Thema Digitalisierung auch zu positiven Nebeneffekten wie einer besseren organisatorischen Befassung mit Sicherheitsthemen führt. Wenngleich man nicht sehen kann, was Ursachen und Wirkungen sind und ob beispielsweise diese Nebeneffekte durch die anderen, innovativen Unternehmenskulturen geprägt sind oder die professionelle Begleitung im Changemanagement auch diese Bereiche mit erfasst hat.

Abbildung 12: Organisatorische Sicherheitsmaßnahmen und Digitalisierung

Basis: Alle befragten Industrieunternehmen (n=430) | [x]n=504 | [xx]n=297

Quelle: Bitkom Research



3 Aufgetretene Schäden

»Zu den Top-Schadensfällen gehören Plagiate, bei denen Informationen durch Wirtschaftsspionage abhanden gekommen sind und die dann zum Beispiel in China schneller und kostengünstiger auf den Markt kommen.«

Marc Bachmann am 19.04.2015 bei nano in 3sat

Nach konservativen Berechnungen beläuft sich der entstandene Schaden für die gesamte deutsche Industrie auf rund 22,3 Milliarden Euro pro Jahr. Der größte Teil davon geht auf Umsatzeinbußen durch Plagiate und Patentrechtsverletzungen zurück.

3.1 Schadenberechnungsmodell

Ein zentrales Ziel dieser Studie bestand darin, den Gesamtschaden für die deutsche Industrie zu bestimmen, der durch Wirtschaftsspionage, Sabotage oder Datendiebstahl entsteht. Dementsprechend wurde der Fragebogen und die Vorgehensweise gestaltet und im Verhältnis zum Vorjahreszeitraum die Methode nicht verändert, um vergleichbare Ergebnisse zu produzieren.

Allen befragten Unternehmen wurde der Fragebogen vor dem Telefoninterview zur Verfügung gestellt. Zu Beginn des Gesprächs wurden die Unternehmen gefragt, von welchen Handlungen diese innerhalb der letzten zwei Jahre betroffen waren. Dann wurde ermittelt, welche Schäden daraus entstanden sind und in einem weiteren Schritt die Schadenssummen für die einzelnen Delikte abgefragt. Die genannten Summen wurden während des Telefoninterviews aufaddiert und dem Befragten 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 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 verbleibenden Werte berechnet. Die durchschnittlichen Schadenssummen sind somit um Ausreißer nach oben und unten bereinigt. Folglich kann man von einer 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 67 Prozent der befragten Unternehmen und entspricht rund 44.000 Unternehmen.

3.2 Pro Jahr 22 Milliarden Euro Schaden für die Industrie

Der Schaden als Folge digitaler Wirtschaftsspionage, Sabotage und Datendiebstahl liegt nach konservativen Berechnungen bei rund 22,35 Milliarden Euro pro Jahr. Mehr als ein Viertel dieser Summe und damit der größte Teil, geht auf Umsatzverluste durch Plagiate zurück. Es folgen Patentrechtsverletzungen, die ähnliche Folgen wie Plagiate haben. An dritter Stelle liegen Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen. Das kann zum Beispiel der Vorsprung bei der Einführung neuer Produkte sein, der es Industrieunternehmen erlaubt, höhere Preise zu verlangen und damit die Entwicklungskosten zu amortisieren. Hohe Kosten verursachen außerdem Rechtsstreitigkeiten, die zu den am häufigsten auftretenden Kostenpositionen im Zusammenhang mit derartigen Vorfällen zählen (s.o.). Ein weiterer großer Faktor sind Kosten infolge des Diebstahls von ITK-Geräten sowie Ausgaben, die durch den Ausfall von IT-Systemen oder die Störung von Betriebsabläufen entstehen. Ein weicher Faktor mit großem Gewicht sind Imageschäden, die nach Sicherheitsvorfällen eintreten. Gilt ein Unternehmen oder seine Produkte bei Kunden und Geschäftspartnern erst einmal als unsicher, ist das nur schwer aus der Welt zu schaffen. Ein solcher Reputationsverlust kann im schlimmsten Fall ein Unternehmen in seiner Existenz gefährden.

Delikttyp	Schadenssumme in Euro (5% getrimmtes Mittel)
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	14,2 Mrd.
Patentrechtsverletzungen (auch schon vor der Anmeldung)	9,3 Mrd.
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	5,7 Mrd.
Kosten für Rechtsstreitigkeiten	4,5 Mrd.
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	4,0 Mrd.
Imageschaden bei Kunden oder Lieferanten / Negative Medienberichterstattung	3,3 Mrd.
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	1,4 Mrd.
Kosten für Ermittlungen und Ersatzmaßnahmen	1,0 Mrd.
Höhere Mitarbeiterfluktuation / Abwerben von Mitarbeitern	0,7 Mrd.
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	0,6 Mrd.
Gesamtschaden innerhalb der letzten zwei Jahre	**44,7 Mrd.**

Abbildung 13: Aufgetretene Schäden nach Delikttyp

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=349)
Quelle: Bitkom Research

4 Täterkreis

»Oftmals sind eigene oder ehemalige Mitarbeiter das Einfallstor. Dies kann aus Unvorsichtigkeit, aber auch aus Mutwilligkeit passieren.«

Marc Bachmann am 18.04.2015 in Computer und Kommunikation, Deutschlandfunk

Ausgangspunkt für Spionage, Sabotage und Datendiebstahl ist in der Regel das enge unternehmerische Umfeld. Dazu gehören in erster Linie die eigenen Beschäftigten oder ehemalige Mitarbeiter. Insbesondere ehemalige Mitarbeiter wurden als Haupttäterfeld identifiziert. Hier zeigt sich, dass die Detektionsmaßnahmen oder die Maßnahmen, die klassisch in der Korruptionsbekämpfung eingesetzt werden, noch viel zu wenig in den Industrieunternehmen angekommen sind. Denn die Gelegenheit und die Bereitschaft zu schädigenden Handlungen werden überwiegend während der bestehenden Beschäftigung angelegt und werden erst nach dem Verlassen des Unternehmensfestgestellt. Aber auch Kunden, Lieferanten, Dienstleister und natürlich die direkten Wettbewerber, sind für Angriffe verantwortlich.

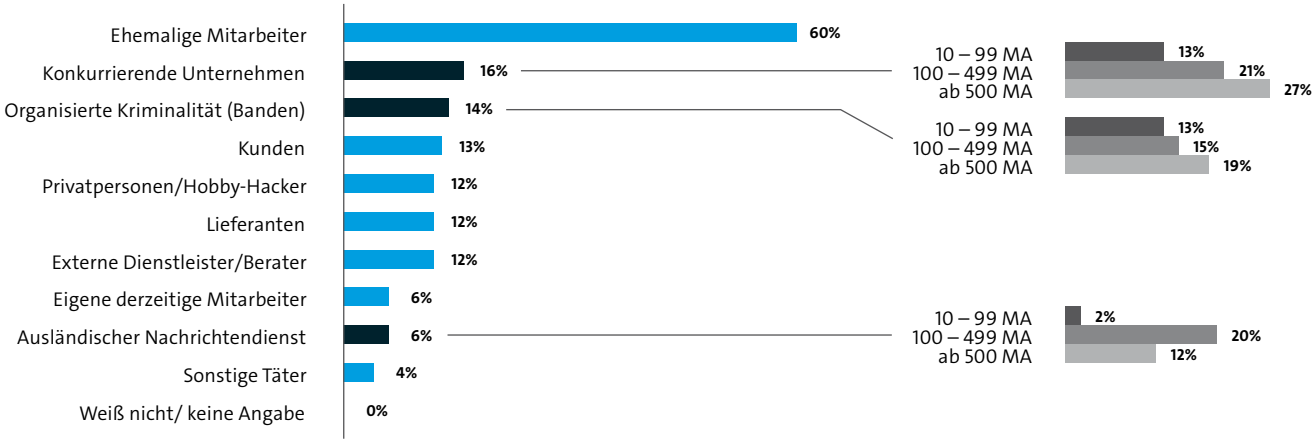


Abbildung 14: Täterkreis

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=349) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

4.1 Mitarbeiter werden zu Tätern

Der mit Abstand wichtigste Täterkreis sind ehemalige Mitarbeiter. Wobei die Gelegenheit zum Täter zu werden überwiegend während der aktiven Mitarbeit geschaffen worden sein muss. Fast zwei Drittel (60 Prozent) der betroffenen Unternehmen geben diesen Personenkreis als Täter an. Damit ist die Industrie sogar noch intensiver betroffen als die Gesamtwirtschaft im Vergleich. Dort gehörten nur insgesamt 52 Prozent der aktuellen und ehemaligen Mitarbeiter zu den Tätern. In der vorliegenden Studie trifft dies für 60 Prozent ehemalige und 6 Prozent aktuelle Mitarbeiter zu.
Nicht immer erfolgen die Taten mit böser Absicht. Vielmehr sind Unvorsichtigkeit, Unbedarftheit und Unwissen die größten Probleme. Mit diesem Wissen können Unternehmen bei den eigenen Mitarbeitern ansetzen, um die personelle Sicherheit zu erhöhen.

Die zweite große Tätergruppe mit 16 Prozent umfasst das direkte unternehmerische Umfeld, bestehend aus Wettbewerbern. Wobei die größeren Unternehmen hier offenbar mehr befürchten müssen. In der Gruppe der 100 bis 499 Mitarbeiter starken Industrieunternehmen haben bereits 21 Prozent Wettbewerber als Täter angegeben, bei Großunternehmen ab 500 Mitarbeitern sogar 27 Prozent.

14 Prozent der betroffenen Industriebetriebe nennen organisierte Bandenkriminalität (Cyber-Kriminelle) als Täter. Direkt dahinter geben Unternehmen mit 13 Prozent Kunden als Verantwortliche krimineller Handlungen an. 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.

Immerhin 12 Prozent meinen Opfer von Hobby-Hackern oder Privatpersonen geworden zu sein und 6 Prozent standen im Visier ausländischer Geheimdienste. Hier zeigt sich ebenfalls ein differenziertes Bild bei den Betriebsgrößenklassen. 20 Prozent der Industrieunternehmen mit 100 bis 499 Mitarbeiter schreiben hier die Attacke einem ausländischen Geheimdienst zu. Im Vergleich zur Gesamtwirtschaft ist dieser Wert wesentlich höher. Hier lag die Zahl im letzten Jahr bei nur 3 Prozent. Dies würde für Wirtschaftsspionage als wesentliches Problem sprechen.

Experten-Statement

Dipl. Ing. Annegrit Seyerlein-Klug, Technische Hochschule Brandenburg, Security Management

Angriffe von außen auf ihr Unternehmen:
Advanced Persistent Threats – APT

Datendiebe werden täglich raffinierter und zahlreicher. Jedes 5. Unternehmen in Deutschland wurde bereits Opfer dieser ausgefeilten Angriffe aus dem Internet. Mit über 60 Prozent sind, laut Bitkom, mittelständische Unternehmen am stärksten von IT-Spionage- oder Sabotageakten betroffen. Sehr viele Organisationen sind bereits betroffen ohne dies auch nur zu ahnen. Streuangriffe sind nicht im Mindesten so effizient wie die sog. fortgeschrittene andauernde Bedrohung (Advanced Persistent Threat, APT). Der Begriff stammt ursprünglich aus dem militärischen Umfeld. Dabei handelt es sich um gezielte und ausgearbeitete Angriffe. Nur verbirgt sich der Spion jetzt nicht hinter dem nächsten Busch, sondern im Internet. Die Angriffe werden in der Regel über einen längeren Zeitraum vorbereitet und haben das Ziel, entweder Unternehmen selbst zu berauben oder zu erpressen oder über sie Zugriffswege (Zulieferer, Partner, Familie) auf das eigentliche Ziel zu ermöglichen. Sowohl kriminelle Motive zur Erbeutung von Daten, Geld oder aber es spielen politische Motive eine Rolle, beispielsweise im Fall einer gezielten Stilllegung/Sabotage einer kritischen Infrastruktur, Produktion, Unternehmen oder Organisation, wie ein Krankenhaus. Inzwischen werden nahezu täglich weltweit sog. Cyberangriffsfälle bekannt, angefangen von Stuxnet bis hin zum kürzlich erfolgten politisch motivierten Raub der Daten der Antidoping Agentur der USA.
Im Industrieumfeld spricht man nicht gerne öffentlich über Cyberangriffe. Das heißt allerdings nicht, dass es keine Angriffe gibt. Man denke nur an den spektakulären Fall von Datenraub bei Sony im Jahr 2011, der aktuell eine für Sony schwerwiegende Neuauflage erlebt. Das Bundesamt für Sicherheit in der Informationstechnik veröffentlichte dazu regelmäßig einen Lagebericht.
Die Angreifer sind oft gut organisiert, verfügen über Zeit und Mittel, um einen komplexen Angriff auszuführen.

4.2 Wie ist der Ablauf solcher Angriffe?

Schritt 1: Informationsbeschaffung
Informationsbeschaffung über das Ziel, ein möglicherweise durchaus langwieriger Vorgang. Dabei hilft alles:

- Öffentliche, allgemeine Quellen: Was hat das Unternehmen veröffentlicht oder dessen Mitarbeiter, Partner usw.
- Berufliche und private Netzwerke um eventuelle Ansatzpunkte direkt oder indirekt zu finden, zum Beispiel den eigenen Golf- oder den Fußballverein der Kinder, die ehrenamtliche Mitarbeit oder der Freundeskreis, um Wege zur unauffälligen und vertrauensbildenden Kontaktaufnahmen zu finden.
- Telefonische Auskünfte oder Anfragen: z. B. die Frage nach dem Passwort, weil die IT etwas zurücksetzen muss...
- Besuche im Unternehmen unter einem Vorwand, z. B. um einen Artikel zu schreiben oder ein Angebot zu machen.
- Technische Scans der Infrastruktur, zum Beispiel um IP Adressen, Versionsstände, offene Ports und vieles mehr zu erkunden.

Schritt 2: Angriffsstrategie und Fuß fassen
Sind genug Informationen vorhanden, wird eine Angriffsstrategie ausgearbeitet. Dafür gibt es viele Wege immer mit dem Ziel, unbemerkt den ersten Angriffsanker zu platzieren: eine Schwachstelle, ein Passwort, einen USB-Stick oder eine angeblich vertrauenswürdige Mail mit Malware. Dazu werden die ermittelten sozialen oder Business-Kontakte genutzt, jede Art von Trick oder bekannte/unbekannte Schwachstellen der Infrastruktur genutzt.
Ziel ist es, eine Malware zu installieren, die den weiteren Kontakt zum Angreifer unbemerkt sicherstellt, indem Verbindungen aufgebaut und übernommen werden zur weiteren Kommunikation.

Schritt 3: heimliche Kommunikation
Sobald die Malware im Unternehmen etabliert werden konnte, erfolgt normalerweise eine möglichst unerkannte Kommunikation mit dem Angreifer. Dafür werden weitere unauffällige Verbindungen aus dem Netzwerk, z. B. über Schwachstellen der IT zum Rechner des Angreifers eingerichtet.

Schritt 4: Ausbreitung und Steuerung
Über die Zugriffskanäle wird weitere Malware installiert, die zum Beispiel das Netz ausspäht, Authentifikationen abgreift, Rechte erweitert, Daten exportiert oder einfach die Möglichkeit schafft, die Steuerung zentraler Funktionen übernehmen zu können.

Schritt 5: Test
Erfahrene Angreifer führen vor dem eigentlichen Angriff ein Test durch, der vom Unternehmen möglicherweise noch nicht einmal bemerkt wird oder lediglich zu einer Irritation führt, die aber keine Sorge auslöst.

Schritt 6: Angriff
Ist der Test oder die Strategie erfolgreich, wird zum geeigneten Zeitpunkt der eigentliche Angriff durchgeführt, der unter Umständen noch nicht mal bemerkt wird. Das Unternehmen registriert in der Folge vielleicht einen erfolgreichen Wettbewerber oder sogar einen Partner, der die eigenen Ideen früher oder preiswerter an den Markt bringt. Dies kann bis zur Existenzgefährdung führen.

5 Aufklärung

»Wir plädieren dafür, dass sich die Unternehmen an die Behörden wenden. Es gibt spezielle Dezernate, die sich um solche Fälle kümmern.«

Prof. Dieter Kempf am 16.04.2015 auf der Pressekonferenz zu Wirtschaftsspionage, Sabotage und Datendiebstahl in Berlin

Viele Unternehmen verlassen sich auf interne Untersuchungen, um Angriffe im Bereich Wirtschaftsspionage, Sabotage und Datendiebstahl aufzuklären. An zweiter Stelle folgen externe Spezialisten und erst an dritter Stelle staatliche Institutionen. Vor allem die Angst vor negativen Konsequenzen hält die Unternehmen davon ab, sich an die Behörden zu wenden. Sie vertrauen am ehesten der Polizei, gefolgt von Staatsanwaltschaft und BSI.

5.1 Nur jeder fünfte Betroffene wendet sich an staatliche Stellen

Mit 61 Prozent der Betroffenen hat die Mehrheit der Industrieunternehmen eine interne Untersuchung der Vorfälle durchgeführt. Rund ein Viertel (26 Prozent) hat externe Spezialisten hinzugezogen. Fast genauso viele betroffene Industrieunternehmen haben staatliche Stellen eingeschaltet (25 Prozent). Damit ist die Quote der Industrieunternehmen, die sich an staatliche Stellen wenden, höher als in der Gesamtwirtschaft aus der Studie im letzten Jahr, dort waren es nur etwa 20 Prozent.

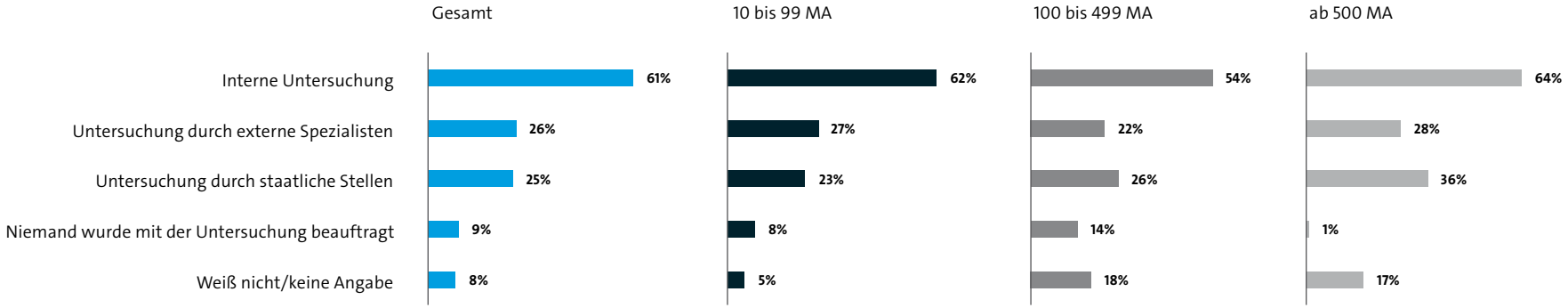
Rund jedes zehnte Unternehmen (9 Prozent) gibt an, gar nichts unternommen zu haben. Ein Grund dafür kann sein, dass der Vorfall als zu unwichtig eingestuft wurde oder keine kompetenten Ansprechpartnerbekannt waren. Es ist allerdings bemerkenswert, dass unter den kleineren mittelständischen Industrieunternehmen mit 100 bis 499 Mitarbeitern insgesamt 14 Prozent angaben, keine Konsequenzen aus den Vorfällen gezogen zu haben und 18 Prozent sich nicht explizit dazu äußern.

Die niedrige Zahl derer, die sich an staatliche Stellen wenden, ist ein Problem. Ermittlungsbehörden können nur dann erfolgreich arbeiten, wenn sie auch Kenntnis von 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 können Täter überführt und so zukünftige Delikte und weitere Opfer verhindert werden.

Abbildung 15: Untersuchung der Vorfälle

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=349) |Mehrfachnennungen in Prozent

Quelle: Bitkom Research



Experten-Statement

Marco Schulz, Geschäftsführer, marconcert GmbH

Ein professioneller Umgang mit Sicherheitsvorfällen ohne angemessen offene Kommunikation ist fahrlässig!

In den vergangenen Jahren sind Cyberangriffe auf deutsche Unternehmen erschreckend preiswert geworden. Es mag ihn noch vereinzelt geben, den klassischen Industriespion, doch auch diese Branche ist längst digitalisiert. Höchste Zeit also, die Hürde für Angriffe auf deutsche Unternehmen zu erhöhen und diese wieder kräftig zu verteuern! Das IT-Sicherheitsgesetz wie auch die Verstärkung der aufklärenden und abwehrenden Behörden sind wegweisende Maßnahmen.

Während Technologien und Prozesse zur Stärkung der IT-Sicherheit in der Summe florieren, hält die starke Abneigung der Unternehmen an, IT-Sicherheitsvorfälle zu melden. Dies gilt in vergleichbarem Maße sowohl für IT-Anbieter wie auch IT-Anwender. Die Furcht vor dem Verlust des Markenwertes und Marktanteilen mag nicht unbegründet sein, doch die Risiken der unfreiwilligen Offenlegung steigen in Zeiten der Whistleblower wie auch Wikileaks und können weitaus schädigender sein.

Diese Studie belegt, dass praktisch alle Branchen und insbesondere der Mittelstand Ziel von Cyberangriffen und Wirtschaftsspionage sind. Das Recht jedes Unternehmers an Gewährleistung der IT-Sicherheit durch Zulieferer und Dienstleister spiegelt sich in der Pflicht, diese den eigenen Kunden zu gewähren. Dies schließt die Informationspflicht ein. Unternehmen also, die Vorfälle kleinreden oder gar nicht melden, erschweren nicht nur die Aufklärung und Verfolgung, sondern behindern auch den Ausbau gemeinsamer Abwehrmaßnahmen für unsere Volkswirtschaft und Wertegemeinschaft.

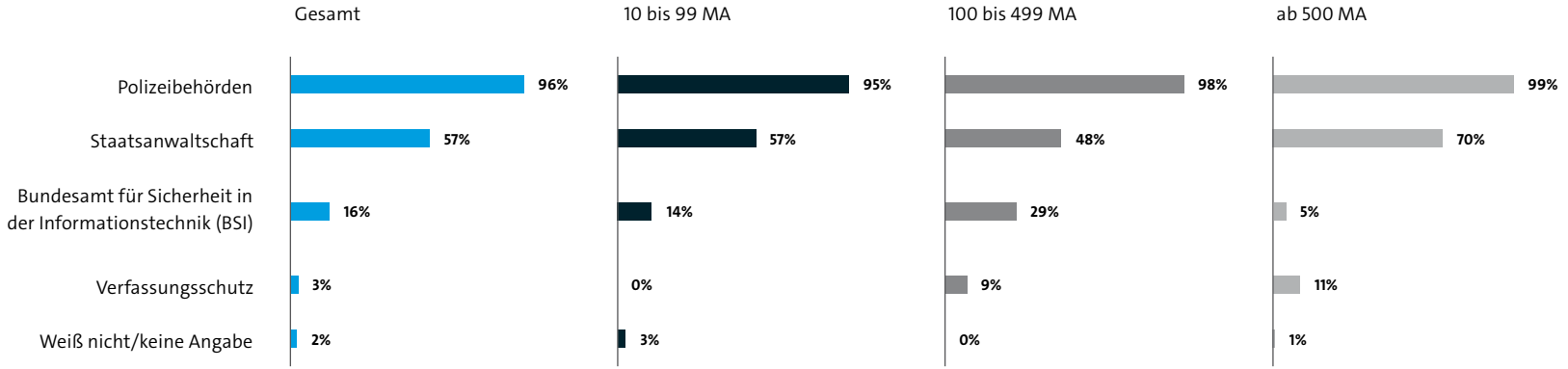
5.2 Unternehmen wenden sich am ehesten an die Polizei

Von den wenigen Unternehmen, die mit den Behörden kooperieren, wenden sich die meisten (96 Prozent) an die Polizei. Mit deutlichem Abstand folgt die Staatsanwaltschaft (57 Prozent) und das BSI (16 Prozent). Nur 3 Prozent der Unternehmen schalten den Verfassungsschutz ein. Allerdings sind es die Verfassungsschutzbehörden der Länder und des Bundes, die in Deutschland für den Wirtschaftsschutz zuständig sind. Fraglich ist, ob die Verantwortlichen in den Unternehmen diese Zuständigkeit überhaupt kennen. Hier ist im letzten Jahr mit der Initiative Wirtschaftsschutz bereits eine Plattform für mehr Information der Unternehmen geschaffen worden. Die Erhebung der Zahlen fand allerdings vor der offiziellen Bekanntgabe der Plattform statt, sodass sich dies noch nicht ausgewirkt haben dürfte.

Es ist also neben der besseren Aufklärungsarbeit der einzelnen Organisationen über das eigene Aufgabengebiet auch eine gute Abstimmung zwischen den Behörden notwendig, um effektiv gegen die Angreifer vorgehen zu können.

Abbildung 16: Eingeschaltete staatliche Stellen

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und staatliche Stellen bei der Untersuchung eingeschaltet haben (n=86)
Mehrfachnennungen in Prozent | Quelle: Bitkom Research



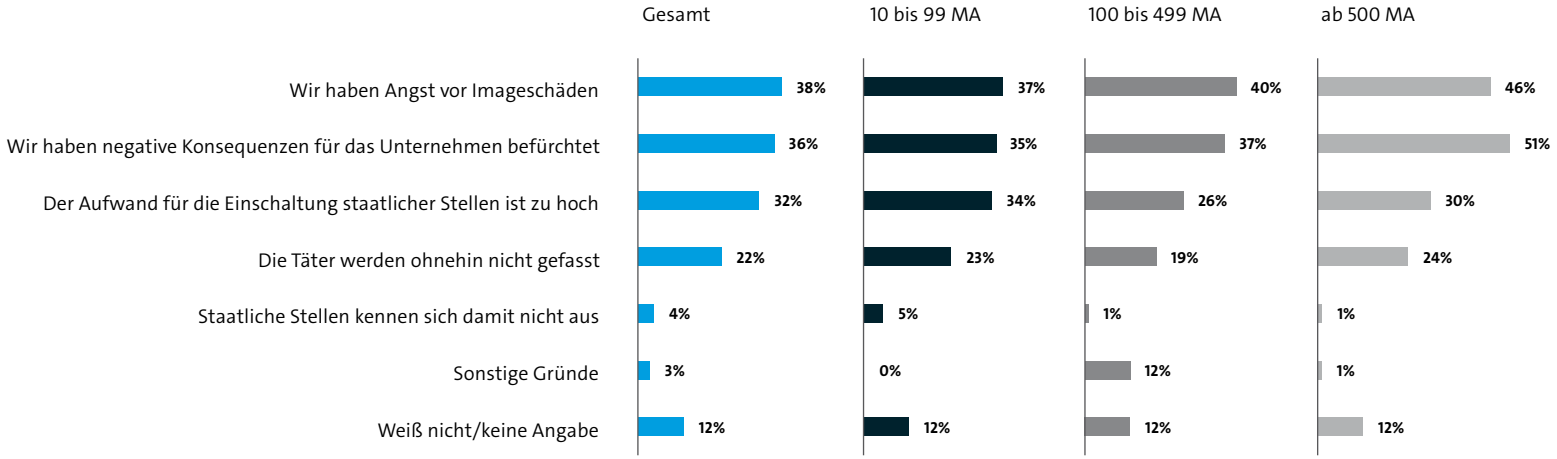
5.3 Angst vor negativen Konsequenzen

Was sind die Gründe, dass weder die Polizei, noch andere staatliche Stellen eingeschaltet werden? Mehr als ein Drittel derjenigen, die keine staatlichen Stellen informiert haben, nennt als Grund »Angst vor Imageschäden« (38 Prozent). 36 Prozent befürchten negative Konsequenzen für das Unternehmen. Das kann zum Beispiel die Sicherung von Beweismitteln wie Computern sein. Allerdings sind die speziellen Cybercrime-Abteilungen der Polizeien und die Wirtschaftsschutz-Referate der Landesämter für Verfassungsschutz sowie das Bundesamt für Verfassungschutz inzwischen gut auf derartige Situationen vorbereitet und können Beweismittel auch ohne schwerwiegende Eingriffe in den Geschäftsbetrieb sicherstellen und diskret Hilfestellung leisten.

32 Prozent nennen den hohen Aufwand als Grund, staatliche Stellen nicht einzuschalten. So müssen die betroffenen Unternehmen die Ereignisse dokumentieren und die Ermittler bei ihrer Arbeit unterstützen. Fast ein Viertel (22 Prozent) sind der Meinung, die Täter würden ohnehin nicht gefasst.

Abbildung 17: Gründe für das Nicht-Einschalten von staatlichen Stellen

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und staatliche Stellen bei der Untersuchung eingeschaltet haben (n=262)
Mehrfachnennungen in Prozent | Quelle: Bitkom Research



Experten-Statement

Alexander Geschonneck, KPMG AG Wirtschaftsprüfungsgesellschaft

Sicherheitsvorfälle, wie beispielsweise ein Datendiebstahl, erfordern in der Regel eine schnelle und angemessene Reaktion. Aus diesem Grund gehört die Reaktion auf derartige Vorfälle natürlich auch in die aktuelle Krisenplanung. Information, Klassifizierung, Eskalation, Maßnahmenplanung, interne und externe Kommunikation, Entscheidungen, Kontakt zu Behörden, Kontakt zu Stakeholdern, Nachverfolgung – diese Tasks sind im Rahmen eines IT-Sicherheitsvorfalls relevant.

Auch die Frage, welche Daten denn eigentlich gestohlen wurden, stellt viele Unternehmen häufig vor große Herausforderungen, wenn diese am Sonntagmorgen zu beantworten ist. Hier zeigen sich Mängel bei der Information Governance und bei Zugriffsrechten zum denkbar ungünstigsten Zeitpunkt.

Viele Dinge, die ich während eines IT-Sicherheitsvorfalls tun muss, lassen sich im Vorfeld hervorragend üben und führen nicht zu Überraschungen im Ernstfall. Allein sich die Frage zu stellen, was würde ich jetzt tun, wenn ich feststelle, dass ich einen Hacker im Netz habe oder meine vertraulichen Daten im Internet auftauchen oder jemand damit droht, meine Systeme in ihrer Leistungsfähigkeit einzuschränken? Wen rufe ich als erstes an? Oder wann werde ich als Führungskraft informiert, wenn jemand anderes in meinem Unternehmen diesen Anruf erhalten hat?

Ein betroffenes Unternehmen mag vielleicht den Datendiebstahl oder Spionageangriff nicht vorhersagen oder immer verhindern, was aber in der Hand des Unternehmens oder der Behörde liegt, ist der professionelle und angemessene Umgang mit dieser Situation, damit der Schaden durch Fehler in der Reaktion nicht noch größer wird.

5.4 Die Aufklärung im eigenen Haus geht vor – Wenige Industrieunternehmen wenden sich als erstes an staatliche Stellen

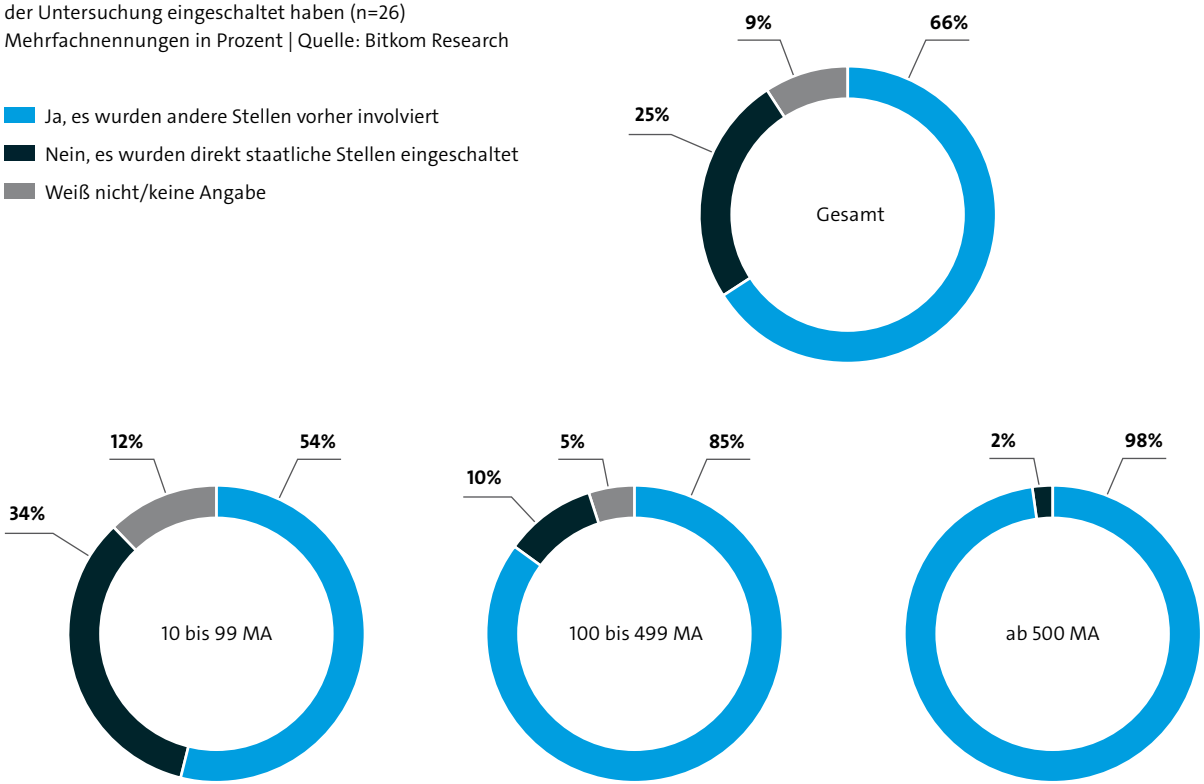
Die Studie in 2015 hat wegen der geringen Anzahl der Unternehmen die staatlichen Stellen offen gelassen, welchen Weg der Aufklärung die Unternehmen zunächst wählen. Deshalb wurde für diese Studie auch gefragt, ob vor der Einschaltung staatlicher Stellen auch andere Maßnahmen ergriffen wurden. Es hat sich gezeigt, dass insgesamt 66 Prozent der Industrieunternehmen zunächst andere Stellen mit der Untersuchung betraut hatten.

Bemerkenswert ist auch, dass es einen Zusammenhang mit der Größe der Unternehmen gibt. Je größer das Unternehmen je eher wird die Aufklärung auf anderem Wege als durch Einschaltung staatlicher Stellen gewählt. Dies kann an den besseren innerbetrieblichen Ressourcen auf diesem Gebiet liegen. Je größer die Unternehmen, desto eher können sie sich eine Unternehmenssicherheit leisten, die auch forensische Fähigkeiten besitzt, ist zu vermuten.

98 Prozent der Industrieunternehmen mit 500 und mehr Mitarbeitern haben vor der Einschaltung staatlicher Stellen andere Untersuchungsmethoden gewählt. Bei den kleinen Industrieunternehmen mit 10 bis 99 Mitarbeitern ist dieser Prozentsatz bei 54 Prozent.

Abbildung 18: Einschaltung staatlicher Stellen

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und staatliche Stellen bei der Untersuchung eingeschaltet haben (n=26)
Mehrfachnennungen in Prozent | Quelle: Bitkom Research



»Die Hacker-Angriffe aus den 90ern sind wie Steinschleudern gewesen. Heute haben wir es im Vergleich dazu mit gelenkten Mittelstreckenraketen zu tun.«

Dr. Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz, Berlin 2016

Viele Industrieunternehmen bieten wertvolles Know-how, das im internationalen Wettbewerb begehrt ist. Auch verzeichnen die staatlichen Behörden eine Zunahme von Delikten und Verschärfung der Gesamtlage. Dies sollte mit der vorliegenden Studie auch untersucht werden, daher liegt ein besonderer Fokus auf den entsprechenden Vorfällen.

Sabotage war in Zeiten vor der Digitalisierung nur durch direkten Eingriff im Unternehmen möglich. Durch die Vernetzung kann nicht mehr nur Know-how abfließen, sondern Täter können auch direkt in den Geschäftsbetrieb eingreifen, wie der Angriff auf die Hochofensteuerung bis zu dessen Zerstörung gezeigt hat. Durch Industrie 4.0 ergibt sich hier natürlich noch eine verschärfte Lage, die mehr Sensibilität für das Thema Sicherheit von Vernetzung erfordert.

Social Engineering, das Ausnutzen menschlicher Schwächen, um in Informationsnetze einzudringen, erweist sich in Zeiten von funktionierenden Firewalls und Virenscanner als immer effektiver. Die schädliche Software wird so direkt an den bestehenden Sicherheitsmaßnahmen vorbei ins Unternehmen geholt.

Ein Drittel der Industrieunternehmen (33 Prozent) hat angegeben, in den vergangenen zwei Jahren von Sabotage der Betriebsabläufe betroffen/vermutlich betroffen gewesen zu sein.

Genauso viele Unternehmen (33 Prozent) gaben an, von Social Engineering im gleichen Zeitraum betroffen oder vermutlich betroffen gewesen zu sein.

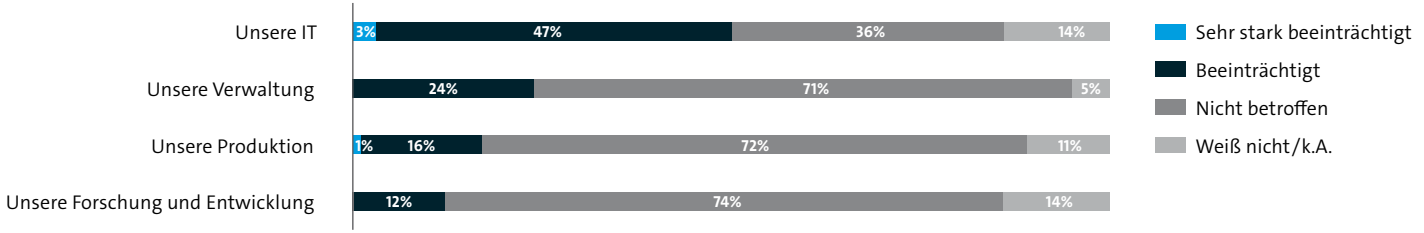
6.1 Betroffene Unternehmensbereiche durch Sabotage

Am meisten von Sabotage betroffen ist die IT der Unternehmen. So gab die Hälfte der betroffenen Industrieunternehmen an, dass ihre Informationstechnologie durch die Sabotage beeinträchtigt oder sogar sehr stark beeinträchtigt. Dies kann auf vielfältige Weise geschehen, etwa durch den Austausch betroffener Geräte und Netzwerkkomponenten, wie beim Bundestag im vergangenen Jahr oder durch DDOS Attacken, welche die Server überlasten.

Mit 24 Prozent wurde an zweiter Stelle die Verwaltung genannt und an dritter Stelle der beeinträchtigten Unternehmensbereiche mit 17 Prozent die Produktion. Sabotage der Forschungs- und Entwicklungsabteilung wurde an letzter Stelle mit nur 12 Prozent genannt. Dies lässt sich auch damit erklären, dass die Forschung und Entwicklung bislang kaum durch IT-Angriffe geschädigt werden kann. Die IT-Systeme sind da ein geeigneteres Ziel. Hier müssen sich die Industrieunternehmen demzufolge besser rüsten.

Abbildung 19: Untersuchung der Vorfälle

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Sabotage betroffen waren (n=90) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research



Experten-Statement

Silke Kröger, Bundesamt für Verfassungsschutz

Social Engineering – eine unterschätzte Angriffsmethode
Social Engineering geht meist weiterführenden Angriffen voraus. Dabei versucht der Täter das Opfer gezielt zu beeinflussen, um an Informationen zu gelangen oder es zu Handlungen zu bewegen, die seinen Zwecken dienen.
Ein geschicktes Social Engineering bleibt oft unbemerkt (nur 33 Prozent Betroffene und vermutlich Betroffene) oder wird zufällig entdeckt (35 Prozent). 69 Prozent der Unternehmen bieten keine Weiterbildung zu diesem Thema an. Dies macht deutlich, dass Social Engineering als Angriffsmethode unterschätzt wird.

Häufig wird es im Zusammenhang mit elektronischen Angriffen genutzt. Seit einiger Zeit zeigt sich jedoch auch ein erhöhtes Aufkommen an telefonischem Social Engineering. Hier wird durch geschickte Fragestellungen versucht, Organisationsdetails, Kontaktdaten etc. in Erfahrung zu bringen.

Ein einprägsames Beispiel für einen elektronischen Angriff mit besonders hochwertigem Social Engineering zeigt die E-Mail eines angeblichen Reporters aus Hong Kong.

In dieser wird den betroffenen Unternehmen eine kompromittierende Situation eines Mitarbeiters vorgetäuscht. Zur Aufklärung des Sachverhalts und um einen möglichen Imageschaden zu vermeiden, sehen sich die Verantwortlichen gezwungen, das vermeintliche Beweisvideo über den angegebenen Link aufzurufen. Über diesen installiert sich das Schadprogramm auf dem Rechner.

Der Fall wurde mit weiteren Indikatoren im Cyber-Brief 1/2015 des Bundesamtes für Verfassungsschutz veröffentlicht und ist unter ↗www.wirtschaftsschutz.info für Nutzer abrufbar.

From: Ih Ix [mailto:hk.newskey@gmail.com]
Sent: Tuesday, June 09, 2015 4:20 AM
To:
Subject: Urgent: Confirmation needed regarding a tip-off video of your company staff

Weiter Letzter

Hello, Ia am a roboter of HNN. My name is akali We've recently received an anonymous tip-off video regarding a man having sex with a prostitute in Hong Kong. The video shows that after sex, he also committed sexual abuse on the girl who we think is underage. We also got an information that the hotel room is booked by your company. We failed to reach out to your HR, but fortunately we found your email address on the Internet. So we think we may stand a better chance to reach out to you to confirm its realness. The unverified video page is as below:

http://news.hnn.hk/2015/0526/news

We hope you can identify the man or just help to forward this email to someone who might. We will appreciate it very much. Thank you!

PS: We are going to make it official release in 3 days, so please give us confirmation ASAP!

6.2 Aufklärung des Social Engineering

Von den Social Engineering Vorfällen wurden 44 Prozent durch interne Kontrollsysteme aufgedeckt. Hier zeigt sich, dass Unternehmenssicherheit ein Zusammenspiel von IT mit organisatorischen Maßnahmen benötigt.

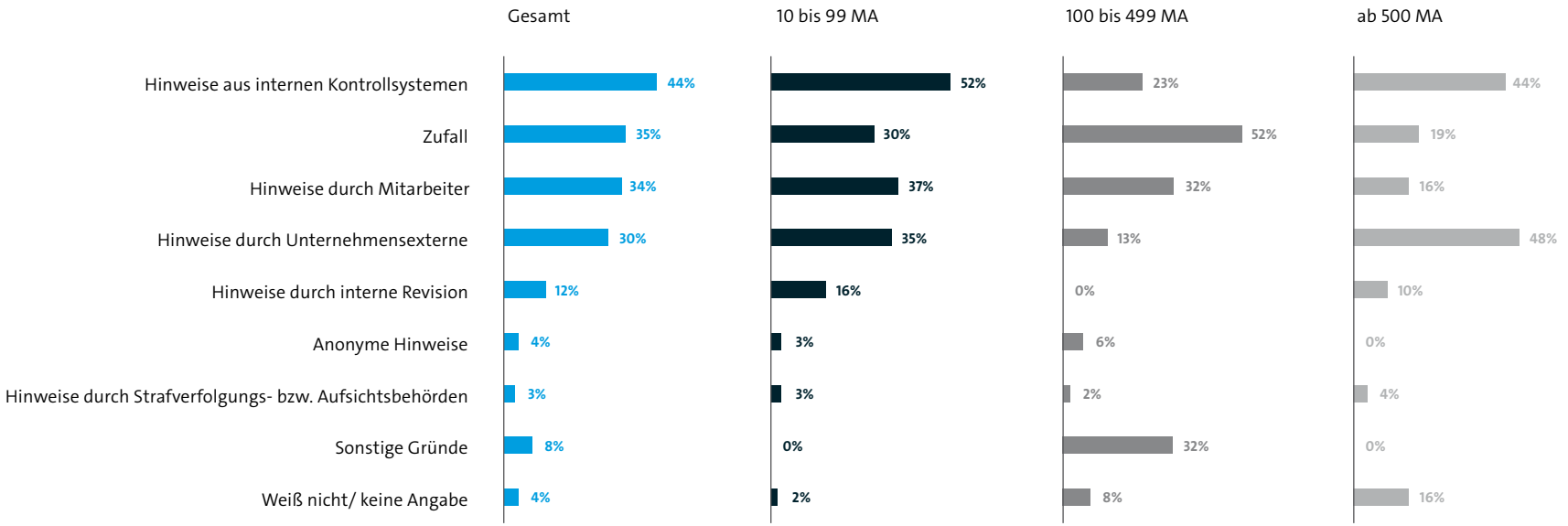
Am zweithäufigsten mit 35 Prozent der betroffenen Unternehmen wurden Social Engineering Fälle durch Zufall aufgeklärt. Knapp dahinter mit 34 Prozent kommen die Aufklärungen durch Hinweise von Mitarbeitern. Dies können sowohl die Opfer oder Beinahe-Opfer der Täuschungen sein oder aber Dritte. Ebenda wird deutlich, dass aktuelle und ehemalige Mitarbeiter nicht nur den größten Täterkreis bilden, sondern auch ein enormes Sicherheitspotenzial bieten können. In einer digitalisierten Welt sind Mitarbeiter ein besonderer Resilienzfaktor für ein Unternehmen.

Zu 30 Prozent wurden die Social Engineering Vorfälle durch Unternehmensexterne aufgeklärt und zu 12 Prozent nach einer Revision im Unternehmen. Zur Aufdeckung der Vorfälle konnten zu 4 Prozent anonyme Hinweise beitragen. Dies kann durch ein sog. Whistle-Blower-Tool geschehen, bei dem die Mitarbeiter anonym auf Missstände hinweisen können. Solche Tools sind noch nicht sehr verbreitet in Industrieunternehmen.

Abbildung 20: Eingeschaltete staatliche Stellen

Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Social Engineering betroffen waren (n=79) | Mehrfachnennungen in Prozent

Quelle: Bitkom Research



6.3 Weiterbildungsmaßnahmen zu Social Engineering

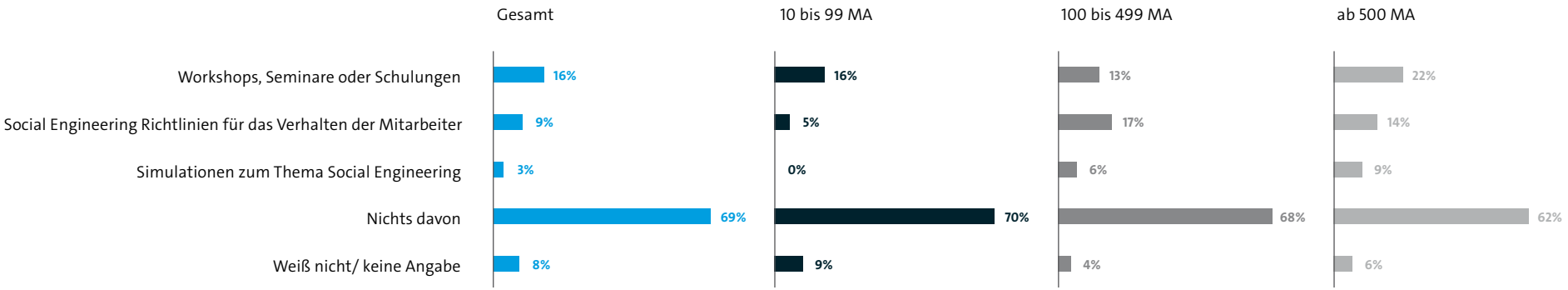
Schließlich wurde in der vorliegenden Studie untersucht, wie sich die Industrieunternehmen gegen das Phänomen Social Engineering wappnen und ihre Mitarbeiter darauf vorbereiten. Das Ergebnis ist ernüchternd. Mehr als zwei Drittel der Unternehmen (69 Prozent) führen keinerlei Maßnahmen zur Schulung, Regulierung oder zum Training gegen derartige Angriffe. Dies mag an der fehlenden Kenntnis des Phänomens liegen. Deshalb muss hier weiter kontinuierlich aufgeklärt werden.

Immerhin bieten 16 Prozent der Industrieunternehmen Workshops, Seminare oder Schulungen in diesem Bereich an. Dies ist ein wichtiger erster Schritt, um die Resilienz der Belegschaft zu erhöhen. Social Engineering Richtlinien bieten nur 9 Prozent an und Trainings oder Simulationen lediglich 3 Prozent. Allein das regelmäßige Training kann aber vor immer raffinierteren und variierenden Methoden schützen.

Abbildung 21: Gründe für das Nicht-Einschalten von staatlichen Stellen

Basis: Alle befragten Industrieunternehmen (n=504)

Quelle: Bitkom Research



7 Sicherheitsvorkehrungen

Die Industrieunternehmen haben im Bereich der Prävention in den letzten Jahren einiges getan. So sagen 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 jedes zweite Industrieunternehmen über ein Notfallmanagement.

Experten-Statement

Sven Malte Sopha, Cassini Consulting

Notfallmanagement

Obwohl die meisten Geschäftsprozesse mittlerweile sehr komplex und fast alle betrieblichen Aufgaben in hohem Maße von IT abhängig sind, hat nur jedes zweite Industrieunternehmen im Durchschnitt ein Notfallmanagement. Damit ist die Zahl im Vergleich zum Vorjahr nur unwesentlich gestiegen. Zu beobachten ist, dass sich weiterhin vermehrt die größeren Industrieunternehmen mit dem Thema auseinandersetzen. 75 Prozent der Industrieunternehmen mit mehr als 500 Beschäftigten gaben an, Regelungen für den Notfall zu haben.

Die Studienergebnisse bestätigen die eigenen Erfahrungen: Die meisten Organisationen beschäftigen sich zwar entgegen der eigenen Aussagen mit Notfallprävention, die entsprechenden Maßnahmen werden jedoch meist nicht als Notfallvorsorge bezeichnet, sondern als IT-Sicherheitsmaßnahmen eingestuft. Prozesse und Checklisten für die Bewältigung von Notfällen sowie die Durchführung von Tests und Übungen fehlen leider meist dennoch. Die Ergebnisse der Studie unterstreichen somit, dass die Sensibilität und das Wissen um die Systematik von Notfallmanagementthemen weiterhin nur teilweise gegeben sind.

Notfallmanagement sollte ganzheitlich gedacht werden. Nicht nur die Ausfallsicherheit der IT, sondern auch die Verfügbarkeit von Infrastruktur, Personal und notwendigen Dienstleistern sollte sichergestellt werden. Eine gute Orientierung zum Notfallmanagement bietet beispielweise der Standard 100-4 des Bundesamts für Sicherheit in der Informationstechnik, der kostenfrei verfügbar ist.

»Notfälle kommen unerwartet und zu den ungünstigsten Zeitpunkten. Vorbereitet zu sein, ist Gold wert.«

Der Aufbau eines Notfallmanagements kann zusammenfassend in vier Schritten dargestellt werden:

1. **Rahmenbedingungen schaffen**: Festlegung von Vorgaben, Prozessen und Zuständigkeiten
2. **Kronjuwelen finden**: Identifikation und Bewertung der kritischen Geschäftsprozesse
3. **Absicherung Kronjuwelen**: Umsetzung von präventiven Maßnahmen und Erstellung von Notfallplänen
4. **Aufrechterhaltung Schutzniveau**: Durchführung von Tests und Übungen

7.1 Nur die Hälfte hat ein Notfallmanagement

Nur rund die Hälfte (51 Prozent) aller Industrieunternehmen in Deutschland verfügt über ein Notfallmanagement bei digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl.

Größere Industrieunternehmen sind inzwischen schon wesentlich besser gerüstet als kleinere. Bei Betrieben mit 500 oder mehr Mitarbeitern besitzen 75 Prozent ein Notfallmanagement. Bei mittelständischen Industrieunternehmen mit 100 bis 499 Mitarbeitern sind es 66 Prozent und bei kleineren Betrieben mit 10 bis 99 Beschäftigten nur 43 Prozent.

Ein betriebliches Notfallmanagement umfasst schriftlich geregelte Abläufe und Sofortmaßnahmen für Situationen, in denen zum Beispiel sensible Unternehmensdaten abfließen, wichtige Webseiten wie Shops oder Online-Dienste nicht erreichbar sind oder die Produktion aufgrund digitaler Angriffe beeinträchtigt ist.

Zu den Zielen des Notfallmanagements gehört es zum Beispiel, Datenabfluss zu stoppen oder beim Ausfall wichtiger Systeme die Arbeitsfähigkeit des Unternehmens so schnell wie möglich wiederherzustellen.

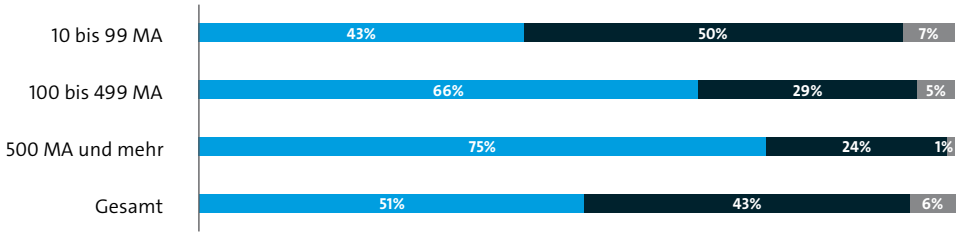


Abbildung 22: Notfallmanagement

Basis: Alle befragten Unternehmen (n=504)
Quelle: Bitkom Research

7.2 Ein bisschen Sicherheit ist immer

Über Sicherheitsmaßnahmen in der einen oder anderen Form verfügen alle befragten Industrieunternehmen. Flächendeckend setzen die Industrieunternehmen technische IT-Sicherheitsvorkehrungen ein. Dazu zählen zum Beispiel Virenscanner und Firewalls. Allerdings reichen diese in vielen Fällen nicht mehr aus (siehe Kapitel 7.3).

Knapp neun von zehn Industrieunternehmen (87 Prozent) ergreifen organisatorische Sicherheitsmaßnahmen. Dazu gehören zum Beispiel Verhaltensrichtlinien für die Nutzung von Datenträgern oder Notfallpläne für Cyberangriffe. 81 Prozent sorgen für den physischen Schutz, zum Beispiel in Form von Zutrittskontrollen oder Sicherung von Gebäuden.

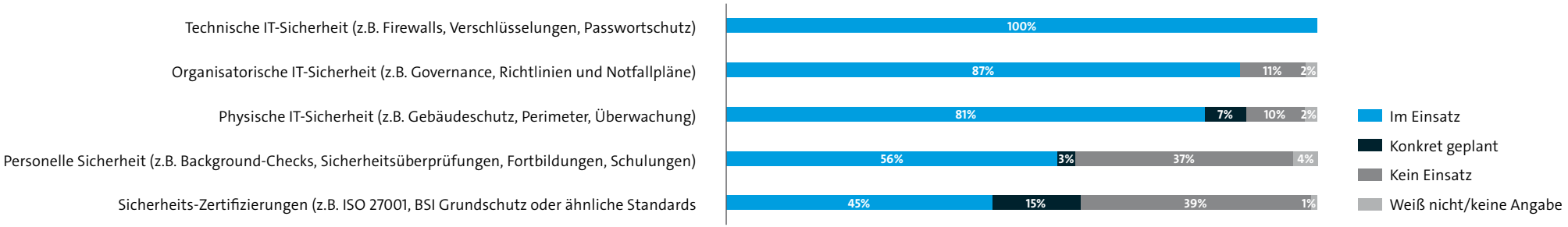
Maßnahmen der sogenannten personellen Sicherheit ergreift nur etwas mehr als die Hälfte (56 Prozent der Industrieunternehmen. Und das, obwohl die meisten Täter aktuelle oder ehemalige Mitarbeiter sind. In der Praxis zählen dazu zum Beispiel Schulungen, aber auch Sicherheitsüberprüfungen von Mitarbeitern oder Bewerbern.

Ein Sonderfall sind Sicherheitszertifizierungen, die 45 Prozent der Befragten durchführen. Im Rahmen einer Zertifizierung lassen die Industrieunternehmen ihr Sicherheitskonzept von einer externen Organisation wie dem TÜV oder dem BSI überprüfen. Bezeichnend ist, dass gerade im Industrieumfeld die Rate der konkret in Planung befindlichen Sicherheitszertifizierungen deutlich höher ist, als bei den anderen Sicherheitsmaßnahmen (15 Prozent). Dies könnte schon eine Nebenwirkung des neuen IT-Sicherheitsgesetzes sein, das Zertifizierung von den kritischen Infrastrukturbetreibern fordert.

Abbildung 23: Eingesetzte Sicherheitsmaßnahmen

Basis: Alle befragten Industrieunternehmen (n=504)

Quelle: Bitkom Research



Experten-Statement

Marius Münstermann, Rohde & Schwarz Cybersecurity GmbH

Aus dem breiten Spektrum der verfügbaren IT-Sicherheitsmaßnahmen werden heutzutage nur wenige flächendeckend genutzt. Lediglich althergebrachte Lösungen wie Firewall und Virenscanner gehören zum Standardrepertoire, obwohl diese allein keine verlässliche Sicherheit gegen Drive-by-Exploits und Ransomware bieten, wie sich an jüngsten Schadensfällen zeigt. Darüber hinaus wird in der Studie deutlich, dass es Nachholbedarf bei der Verschlüsselung von »Data in Transit« und »Data at Rest« gibt.

Aus technischer Sicht kann diese Lücke schon heute durch innovative Lösungen geschlossen werden, wie zum Beispiel ein gekapselter »Browser in the Box«, dedizierte Ethernet- und IP-Verschlüsseler als Ergänzung zu herkömmlichen Netzwerkkomponenten sowie Festplattenverschlüsselung mit 2-Faktor-Authentifizierung. Solche Lösungen integrieren sich nahtlos in eine bestehende Infrastruktur und sind bei vertrauenswürdigen Anbietern erhältlich.

Dass sie trotzdem nicht bei allen Unternehmen im Einsatz sind, liegt also offenbar weniger an der technischen Verfügbarkeit sondern vielmehr an internen Gründen, wie zum Beispiel mangelnden Ressourcen im IT-Betrieb, einem unzureichenden Budget oder einer mangelnden Sensibilisierung der Entscheider.

7.3 Technische Sicherheitsmaßnahmen

Die Industrieunternehmen in Deutschland verfügen bei der Absicherung ihrer IT-Systeme vor Cyberangriffen über einen guten Basisschutz, investieren aber noch zu selten in umfassende Sicherheitsmaßnahmen. So nutzen alle befragten Industrieunternehmen Virenscanner, Firewalls sowie einen Passwortschutz für Computer und andere Kommunikationsgeräte. Diese Funktionen sind in der Regel in den gängigen Betriebssystemen enthalten, reichen aber häufig nicht mehr aus. Die Schadsoftware wird immer komplexer und bleibt nicht selten unerkannt. Zudem kommen neue Methoden, wie das Social Engineering, hinzu, um diesen Basisschutz zu umgehen.

Immerhin vier von fünf Industrieunternehmen (83 Prozent) verschlüsseln zudem ihre Netzwerkverbindungen. Für Daten auf Festplatten oder anderen Datenträgern gilt dies nicht einmal für die Hälfte (48 Prozent). Nur 46 Prozent setzen auf eine Verschlüsselung ihres E-Mail-Verkehrs.

Lediglich 35 Prozent der befragten Industrieunternehmen verfügen über eine Absicherung gegen Datenabfluss von innen (Data Leakage Prevention) und ein gutes Viertel (27 Prozent) über spezielle Systeme zur Einbruchserkennung (Intrusion Detection). 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.

Immerhin fast ein Drittel (30 Prozent) der Industrieunternehmen setzten erweiterte Verfahren zur Benutzeridentifikation ein, zum Beispiel eine Zwei-Faktor-Authentifizierung oder biometrische Merkmale. Rund ein Viertel (26 Prozent) der Industrieunternehmen testet die eigenen Sicherheitskonzepte mit Hilfe sogenannter Penetrationstests, bei der Angriffe simuliert werden.

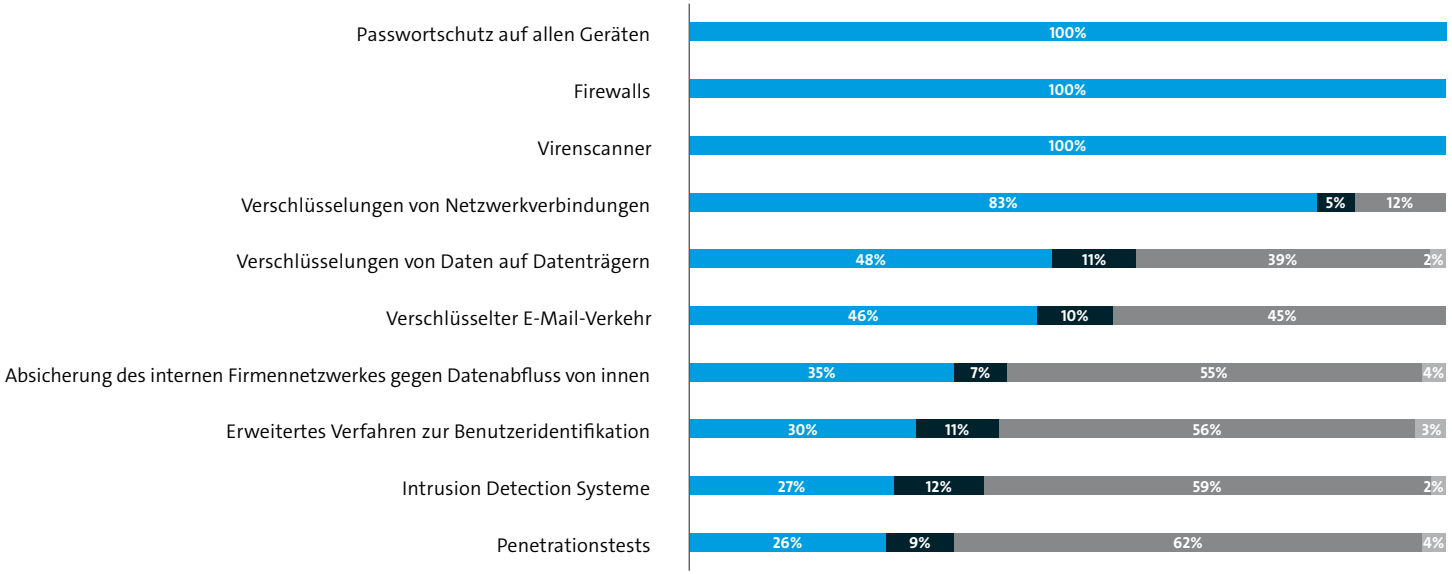


Abbildung 24: Eingesetzte technische IT-Sicherheitsmaßnahmen

Basis: Alle befragten Industrieunternehmen (n=504)

Quelle: Bitkom Research

7.4 Die Mitarbeiter als »Human-Firewall«

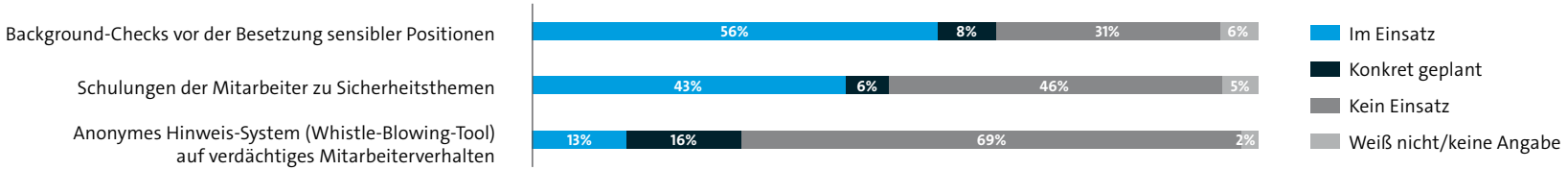
Ehemalige und aktuelle Mitarbeiter sind sowohl die größte Tätergruppe als auch entscheidend bei der Erkennung von Angriffen. Ihre Stärkung im Thema Unternehmenssicherheit, die letztlich Arbeitsplatzsicherheit bedeutet, wird damit zum entscheidenden Faktor. Wie sehen sich die Industrieunternehmen selbst gerüstet, um den Gefahren und Chancen zu begegnen? Immerhin 56 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 43 Prozent der befragten Industrieunternehmen ein.

In den Kinderschuhen stecken offenbar noch anonyme Hinweissysteme wie Whistle-Blower-Tools. Diese meist von Rechtsanwaltskanzleien extern betriebenen Systeme sollen den Mitarbeitern ermöglichen, auf Missstände und Versäumnisse hinzuweisen, ohne sie gleich öffentlich machen zu müssen.

Eine selbstkritische Analyse sollte sich in zusätzlichen Sicherheitsmaßnahmen niederschlagen. Dazu ist einerseits eine Sicherheitskultur notwendig, die alle Unternehmensteile sensibilisiert und damit viele Risiken minimiert. Aber auch Investitionen in organisatorische, personelle und technische Sicherheitsmaßnahmen sind notwendig, um den weiter bestehenden Risiken adäquat begegnen zu können.

Abbildung 25: Einschätzung zur frühzeiteigen Erkennung von Vorfällen

Basis: Alle befragten Industrieunternehmen, die Sicherheitsvorkehrungen im Bereich Personal einsetzen oder planen (n=297)
Quelle: Bitkom Research



7.5 Zu wenige Sicherheitsprofis in den Unternehmen

Die Befragung hat auch ergeben, wie viele Sicherheitsverantwortliche sich hauptberuflich mit den Themen Wirtschafts- und Know-how-Schutz sowie Informationssicherheit in den Industrieunternehmen beschäftigen. Denn zu Beginn der Befragung wurde die Verantwortlichkeit im jeweiligen Unternehmen stufenweise abgefragt. So wurde zunächst nach dem Verantwortlichen für Sicherheit und Wirtschaftsschutz gefragt und anschließend, ob der Betreffende auch für Informationssicherheit und IT-Sicherheit verantwortlich ist. Wenn aus diesem Bereich niemand gefunden wurde, sollte der Geschäftsführer die Fragen beantworten und wenn auch dieser nicht auskunftsfähig ist, der sonst im Unternehmen für Risikomanagement verantwortliche.

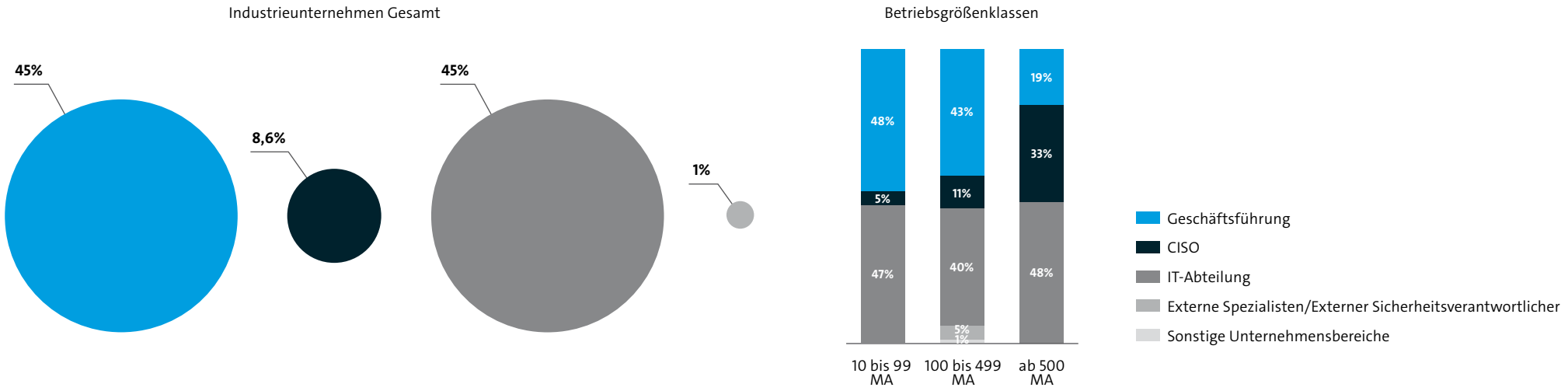
Hierbei ist Bemerkenswertes zutage gefördert worden. In der Industrie sind nur 8,6 Prozent der Industrieunternehmen mit einem Sicherheitsverantwortlichen vertreten bzw. haben einen Chief Information Security Officer (CISO). Weniger als jedes zehnte Industrieunternehmen, die natürlich von überlegenem Know-how abhängig sind, überlässt dessen Schutz jemandem, der sich damit auskennt. In 45 Prozent der Fälle ist dafür im Unternehmen der Geschäftsführer mitverantwortlich. Jedenfalls hat fast die Hälfte der befragten Industrieunternehmen ihren Geschäftsführer als Verantwortlichen beantworten lassen. Ebenso viele Unternehmen aus dem Industriesektor haben diese Aufgabe dem Verantwortlichen für IT zugeschrieben.

Schaut man in die Größenklassen der Industrieunternehmen, zeichnet sich ein differenziertes Bild ab. Die großen Industrieunternehmen ab 500 Mitarbeitern haben zu einem Drittel (33 Prozent) einen CISO. Bei den Industrieunternehmen mit 100 bis 499 Mitarbeitern sind es nur noch 11 Prozent und bei den Kleinsten ab 10 bis 99 Mitarbeitern nur noch 5 Prozent, welche die Sicherheit in professionelle Hände geben. Dies kann selbstverständlich auch ein Problem eines Fachkräftemangels sein, wobei die größeren Unternehmen mit attraktiveren Gehältern und Karrierechancen einen Marktvorteil haben können. Dennoch müssen sich alle Unternehmen darüber klar werden, dass in einer digitalisierten Informationsgesellschaft der Schutz des Rohstoffes Daten essentiell wird. Wie alle Unternehmen eine Buchhaltung, Personalmanagement und inzwischen auch Controlling unterhalten, werden sich zukünftig die Unternehmen auch um Datensicherheit und Datenschutz professionell kümmern müssen.

Abbildung 26: Sicherheitsverantwortliche in Industrieunternehmen

Basis: Alle befragten Industrieunternehmen (n=504)

Quelle: Bitkom Research



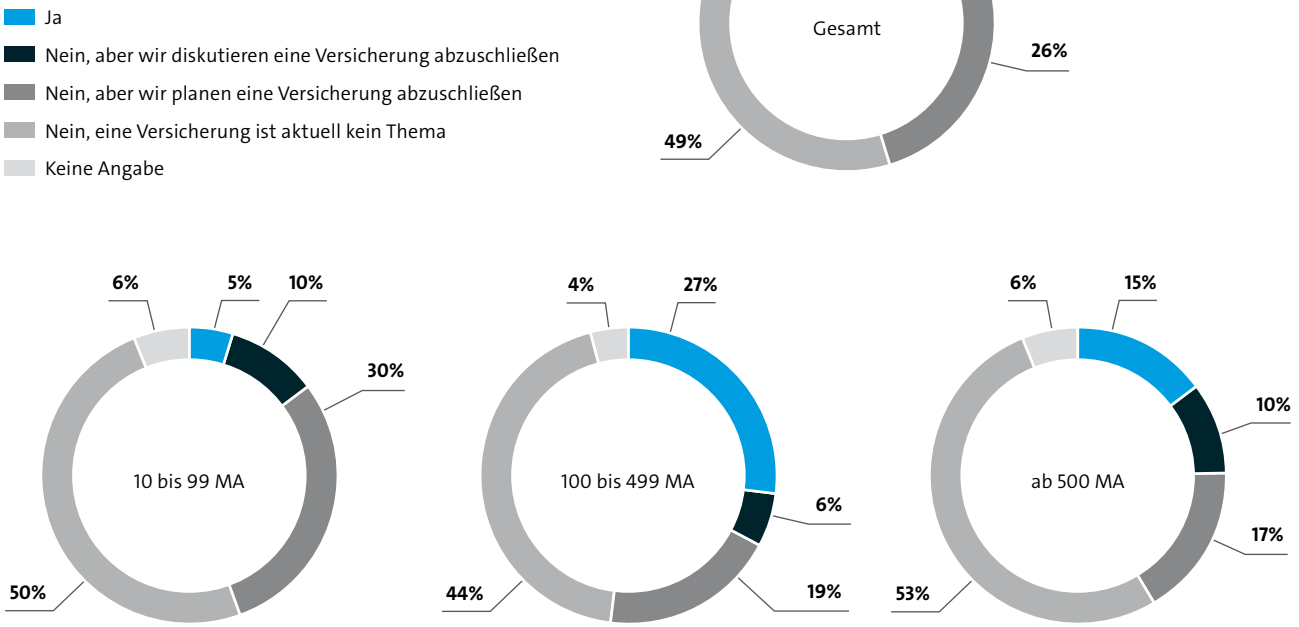
7.6 Versicherungen gegen Wirtschaftsspionage und Cyber-Crime

Ein weiterer Punkt, der so noch nicht in der letzten Studie zum Thema Wirtschaftsschutz aus dem letzten Jahr berücksichtigt wurde, ist eine Versicherung gegen Schäden aus Cyber-Angriffen oder Spionage und Sabotage. Die neueren Entwicklungen zeigen, dass Versicherungsgesellschaften vermehrt auch Teile dieses Risikos abdecken und versichern. Dabei spielt natürlich der Grad der Gefährdung durch eigene Sicherheitsmaßnahmen eine wesentliche Rolle. Nur wer ausreichend geschützt ist, sodass die Risiken nicht ausufern, kommt überhaupt in den Genuss einer Deckung. Auch das Maß der Sicherheitsmaßnahmen ist dann entscheidend für die Prämien.

Überraschend war bei den Ergebnissen, dass die Anzahl der Unternehmen insgesamt, die eine Versicherung für derartige Risiken abgeschlossen haben, schon bei 11 Prozent zu liegt, obwohl es nur eine relativ geringe Anzahl an Anbietern für dieses relativ neue Versicherungsprodukt gibt. Bei den Industrieunternehmen mit 100 bis 499 Mitarbeitern hat die Befragung sogar einen Anteil von mehr als einem Viertel (27 Prozent) ergeben.

Abbildung 27: Cyber-Versicherungen bei Industrieunternehmen

Basis: Alle befragten Industrieunternehmen (n=504)
Quelle: Bitkom Research



Experten-Statement

Axel Petri, Deutsche Telekom AG

Vertrauen

Security builds Trust. Mit der Digitalisierung unserer Gesellschaft bekommt das Vertrauen der Nutzer zusätzliche – essentielle – Bedeutung. Digitale Kriminalität und Datenlecks, aber auch die Diskussionen über den Umfang von Überwachungsmaßnahmen staatlicher Stellen weltweit haben dieses Vertrauen beschädigt. Dieses gilt es dringend wieder herzustellen.

Zum einen braucht es natürlich bessere IT-Lösungen, um Angriffe jeglicher Art zu erschweren. Der Schlüssel für Vertrauen sind allerdings Transparenz, Verhältnismäßigkeit und offener gesellschaftlicher Dialog. Den Nutzern muss Transparenz geboten werden über die Verbindungen von Staat und Wirtschaft, deren Ziele, Methoden und Grenzen. Eingriffe in die digitale Freiheit dürfen bei allem gesteigerten Sicherheitsbedürfnis die Verhältnismäßigkeit nicht aus dem Auge verlieren. Schließlich müssen wir einen breiten gesellschaftlichen Dialog führen, um Lösungen zu finden, die die Bedürfnisse aller Beteiligten berücksichtigen. Denn die Schaffung von Vertrauen ist eine gesamtgesellschaftliche Aufgabe.

8 Fazit und Empfehlungen

»Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, eine Niederlage erleiden. Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen.«

Sun Tzu, 544 v. Chr. bis 496 v. Chr., »Die Kunst des Krieges«

Die Konsequenzen aus den Ergebnissen der Studie sind ganz ähnlich wie die aus der letzten Bitkom-Studie zum Thema Wirtschaftsschutz aus dem Jahr 2015. Drei Aspekte sind nach wie vor von zentraler Bedeutung.

Erstens: Die Industrieunternehmen müssen sich als besonders begehrtes Ziel im Vergleich zu der Gesamtwirtschaft, noch stärker und schneller auf die geänderten Bedingungen einstellen. Industrie 4.0 und die zunehmende Vernetzung gerade in diesem Wirtschaftsbereich dürfen nicht unterschätzt werden. Technische Sicherheitsmaßnahmen alleine reichen nicht aus. Daneben müssen organisatorische und personelle Vorkehrungen getroffen werden. Entscheidend ist zudem, sich auf den Ernstfall vorzubereiten und Pläne zu entwickeln, wie das Ausmaß der Schäden gering gehalten werden kann. Denn einen absoluten Schutz gibt es nicht.

Zweitens: Die Vertrauensbasis zwischen staatlichen Stellen und den Unternehmen ist nur unzureichend entwickelt. Hier muss von beiden Seiten das vorhandene Engagement beibehalten und ausgebaut werden und die guten Ansätze wie die Initiative Wirtschaftsschutz genutzt werden. Nur gemeinsam sind die immer komplexeren Herausforderungen zu meistern. Wichtig ist dabei, die Vorteile für beide Seiten stärker herauszuarbeiten.

Und drittens: Beim Thema Unternehmenssicherheit müssen die Mitarbeiter mit einbezogen werden. Nur mit einem höheren Bewusstsein für Sicherheitsaspekte und gezielte Präventionsmaßnahmen kann der Schutz eines Unternehmens verbessert werden. Hier liegen nicht nur große Potenziale für die Produktivität von Industrieunternehmen, sondern auch für deren Sicherheit, die noch gehoben werden müssen.

8.1 Unternehmen müssen Sicherheitsbehörden stärker vertrauen

Das Vertrauen in die deutschen Sicherheitsbehörden ist nicht besonders stark ausgeprägt. Nur 20 Prozent der befragten Unternehmen melden Fälle von Datendiebstahl, Industriespionage oder Sabotage an staatliche Stellen. Als Gründe nennen sie unter anderem Angst vor negativen Auswirkungen, zu hoher Aufwand, geringe Chancen der Aufklärung und Inkompetenz der Sicherheitsbehörden.

Diese Sorgen sind weitgehend unbegründet. Die Sicherheitsbehörden sind fachlich gut aufgestellt und überwiegend gut ausgestattet. Auch sind sie an der Anzeige von Straftaten und einem vertrauensvollen Umgang mit den Informationen interessiert. In der Praxis sind die Behörden sogar abhängig von den Angaben der Betroffenen, um wirkungsvoll arbeiten zu können. Treten zum Beispiel bestimmte Delikte gehäuft auf, fügen sich erst die Informationen mehrerer Geschädigter zu einem Gesamtbild und tragen so zur Aufklärung der Fälle bei. Die Unternehmen helfen sich selbst am meisten, wenn sie Vorfälle zügig an staatliche Stellen weitergeben.

Auf der anderen Seite müssen sich die Sicherheitsbehörden auf Wirtschaft und Bevölkerung zubewegen. Ein positives Beispiel sind die »Zentralen Ansprechstellen Cybercrime« (ZAC) der Landeskriminalämter. Diese Kontaktstellen stehen im Fall der Fälle den betroffenen Unternehmen als helfender Partner zur Verfügung.

Generell brauchen wir mehr Kooperationsbereitschaft auf beiden Seiten. Diese Kooperationen müssen einer gemeinsamen Sache dienen: dem besseren Schutz der deutschen Wirtschaft. Für Unternehmen könnte hier nicht nur das eigene Sicherheitsbedürfnis ein Ansatz sein, sondern auch die Corporate Social Responsibility (CSR). Die Sicherheitsbehörden wiederum sollten nach Transparenz und Vertrauen streben. Bitkom arbeitet derzeit in zwei sehr erfolgreichen Kooperationen mit staatlichen Sicherheitsbehörden zusammen: mit verschiedenen Landeskriminalämtern in der »Sicherheitskooperation Cybercrime« und mit dem BSI in der »Allianz für Cybersicherheit«. Auch einzelne Unternehmen können der Allianz beitreten oder sich direkt an die Landeskriminalämter wenden.

Grundsätzlich brauchen wir weitere Kooperationen und eine intensivere Zusammenarbeit in den bestehenden Initiativen, denn nur durch die Zusammenarbeit von staatlichen Behörden und der Wirtschaft im Bereich des Wissenstransfers, der Prävention und der Steigerung des Bewusstseins lässt sich das immer komplexer werdende Feld der digitalen Sicherheit bewältigen.

8.2 Umdenken bei der IT-Sicherheit: Schadensbegrenzung ergänzt Prävention

Lange galten Firewalls und Virenscanner als das Maß der Dinge, wenn es darum ging, Unternehmen vor Hackerangriffen zu schützen. Diese Zeiten sind vorbei. Da die Bedrohungen immer vielfältiger und die IT-Infrastrukturen immer komplexer werden, reicht ein rein präventiver Ansatz zum Schutz der Unternehmensinformationen nicht mehr aus: Ein Unternehmen muss lernen, mit Sicherheitsvorfällen professionell umzugehen und den entstandenen Schaden zu minimieren. Das so genannte »Incident Management« bzw. IT-Störungsmanagement ergänzt die bisherigen Schutzkonzepte.

Der wesentliche Grund für das Umdenken ist die aktuelle Bedrohungslage. Angriffe durch kriminelle Hacker nehmen zu. Die Angriffe werden ausgefeilter, komplexer und spezifischer. Gleichzeitig nimmt die Asynchronität zwischen Angriff und Verteidigung zu: Der Angreifer muss nur ein Schlupfloch finden, die Sicherheitsverantwortlichen aber eine Vielzahl von Systemen mit noch mehr potentiellen Schwachstellen absichern. Angriffe werden arbeitsteilig und in kriminellen Strukturen organisiert und als Dienstleistung mit Support über das Internet zu günstigen Konditionen angeboten. Die Zunahme der so genannten APT-Angriffe (advanced persistent threats) zeigt, dass es für Angreifer möglich ist, sich über Jahre unerkannt in den IT-Infrastrukturen der Unternehmen zu bewegen. Das alles geschieht vor dem Hintergrund, dass die IT-Systeme immer leistungsfähiger werden und die Anzahl der potenziell gefährdeten Endgeräte im Zuge der Digitalisierung beständig zunimmt.

Der Fokus liegt deshalb zunehmend auf der Erkennung von Einbrüchen, um wie im Fall von komplexen APT-Angriffen Schadensbegrenzung betreiben zu können. Der Ausbau der Sensorik im Unternehmensnetz – im Sinne der Erkennung von Anomalien – steht also im Fokus der Sicherheitsbemühungen. In diesem Zusammenhang kommen vermehrt Angriffserkennungssysteme (intrusion detection) zum Einsatz. Diese Systeme analysieren die Datenströme in einer Organisation und melden verdächtige Aktivitäten. Sie können die Schwächen eines rein reaktiven Ansatzes mindern und sehr schnell Hinweise auf einen möglichen Sicherheitsvorfall liefern. Um die Daten der Sensorik auszuwerten, müssen Unternehmen ihre IT-Abteilungen aufstocken - finanziell, aber auch personell.

Der Ansatz zum Incident-Management darf nicht auf die Erkennung eines Angriffes beschränkt bleiben. Notwendig sind Maßnahmen zur Analyse und Beendigung des Angriffes, zur Wiederherstellung des Betriebszustandes, zur Datenwiederherstellung sowie zur Bewertung von Schäden. Dabei sollten externe Partner wie die Polizei, der Verfassungsschutz, IT-Sicherheitsdienstleister oder IT-Forensiker frühzeitig einbezogen werden. Nicht zuletzt müssen Organisationen das Verhalten im Notfall zum Beispiel in Form eines Planspiels einüben. Die Maßnahmen reichen vom Stopfen eines Datenlecks über die Information aller wichtigen Personen und der Medien bis zum Neustart des Geschäftsbetriebs.

8.3 Organisatorische, physische und personelle Sicherheit – Hinweise für Mitarbeiter

Die Sicherheit in der digitalen Welt beschränkt sich nicht auf rein technische Maßnahmen der IT-Sicherheit. Sie müssen durch organisatorische und physische Maßnahmen ergänzt werden. Dazu gehören unter anderem Regelungen, wer im internen Netzwerk auf welche Daten zugreifen darf und wer Zutritt zu sensiblen Bereichen eines Unternehmens bekommt. Letztere müssen durch entsprechende Zugangskontrollen für Mitarbeiter, Dienstleister oder Gäste gewährleistet werden. Voraussetzung dafür ist, dass das Betriebsgelände und die Gebäude geschützt werden können. Andernfalls müssen bauliche Maßnahmen ergriffen werden.

Zentraler Sicherheitsfaktor sind die Mitarbeiter. Nur etwa die Hälfte der befragten Unternehmen führt Schulungen der Beschäftigten oder Sicherheitsüberprüfungen von Bewerbern durch. Eine angemessene Sicherheitskultur umfasst darüber hinaus die richtige Verwendung von Zugangsdaten, den korrekten Umgang mit externen Datenträgern oder Verhaltensregeln auf Reisen. Der Bitkom gibt einige praktische Hinweise, wie Mitarbeiter die Sicherheit des Unternehmens gewährleisten können.

Der Mitarbeiter als wirkungsvollste »Firewall«

Jeder Mitarbeiter im Unternehmen kann wesentlich zur Sicherheit des Unternehmens beitragen. Dazu gehört die konsequente Umsetzung der Sicherheitsvorgaben, aber auch eine gewisse Aufmerksamkeit und Sensibilität für verdächtige Situationen. Befinden sich zum Beispiel nicht angemeldete Personen im Haus oder in der Abteilung, sind Türen oder Fenster defekt oder parkt neuerdings ein Kleinbus neben der WLAN-Antenne? Aber nicht nur im analogen Leben gibt es Betrugsversuche, die schnell zu einer Gefahr für die Unternehmenssicherheit werden können. Falsche Rechnungen von imaginären Lieferanten oder Buchungsbestätigungen nicht existierender Reisebüros gehören in deutschen Unternehmen zum Alltag. Unternehmen müssen ihre Mitarbeiter immer wieder zu einem kritischen Umgang mit scheinbar banalen Situationen und Informationen ermutigen. Dann liegt es an dem Anwender, hier wachsam zu sein und mögliche Gefahren zu erkennen. Jetzt braucht es nur noch den Mut, die Geschehnisse zu melden, zu prüfen und Maßnahmen daraus abzuleiten. Der Mitarbeiter ist die wirkungsvollste »Firewall« eines Unternehmens und kann nicht durch technische Geräte ersetzt werden.

Social Engineering – eine verbreitete Gefahr

Viele der Vorfälle im Bereich Wirtschaftsschutz werden von den eigenen Mitarbeitern verursacht, oftmals nicht aus krimineller Energie heraus, sondern durch Unvorsichtigkeit und Unbedarftheit. Ein beliebtes Mittel, um in abgeschlossene Netzwerke zu gelangen, sind geschenkte USB-Sticks. Nicht selten befindet sich ein Schadprogramm darauf.

Ein anderes Beispiel ist eine empfangene E-Mail, verbunden mit einem Anruf von einer externen Rufnummer, welcher sich als ein Vorgesetzter ausgibt und hektisch die Bearbeitung einer angehängten Datei verlangt. Auch hier liegt ein Schadprogramm dahinter.

In beiden Fällen heißt es, lieber einmal mehr nachgedacht oder nachgefragt. Hektik und Neugier sind hier zwei schlechte Berater, die womöglich zu einem erheblichen Schaden für die Firma führen können.

Kommunikation im öffentlichen Raum

Auf Reisen im Zug, auf dem Bahnhof oder auf dem Flughafen wird die Zeit gerne genutzt, um E-Mails zu schreiben oder wichtige Telefonate zu führen. Dabei wird oftmals vergessen, dass man sich im öffentlichen Raum bewegt und potenziell Interessierte nicht viel mehr machen müssen, als Augen und Ohren offen zu halten.

Deshalb sollten Telefonate, die sich auf keinen Fall verschieben lassen, in ruhigeren Abschnitten des Bahnhofs oder Flughafens geführt werden, und zwar mit gedämpfter Lautstärke. Das gleiche gilt für Telefonate im Zug. Zudem sollte der Laptop oder das Tablet mit einer Sichtschutzfolie ausgestattet werden. Diese verhindert ein seitliches Einsehen auf den Bildschirm und die darauf dargestellten Inhalte.

Akten und Unterlagen richtig entsorgen

Selbst beim Ausmisten der Büros sollten Mitarbeiter achtsam sein. Anstatt alles einfach in der blauen Tonne zu entsorgen, sollten Unterlagen aus dem Büroumfeld mittels Aktenvernichter zerkleinert und erst danach entsorgt werden. Unbeschädigt weggeworfene Dokumente sind für Kriminelle, aber auch die Konkurrenz ein willkommener Fundus zur Informationsgewinnung.