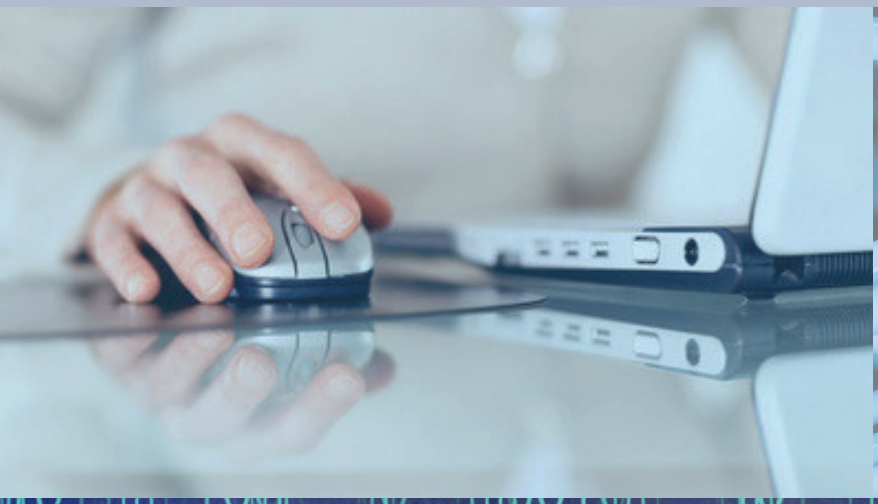
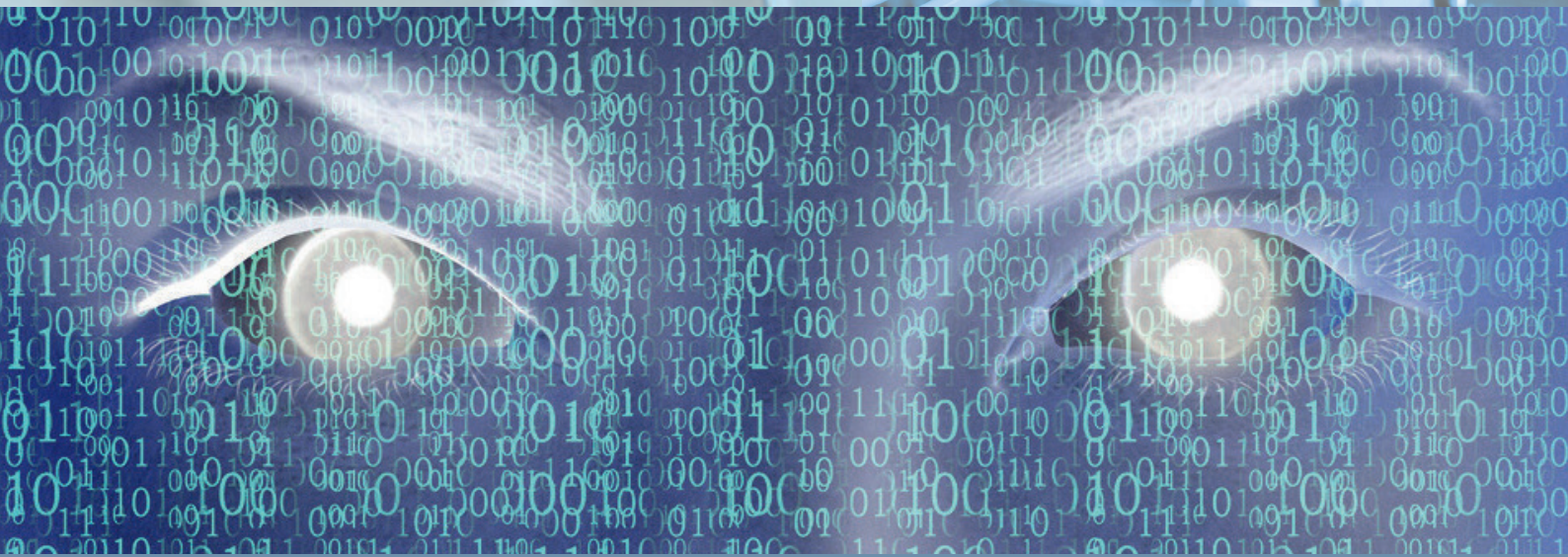
Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

SiFo-Studie 2018/19

Gefährdungen in baden-württembergischen Unternehmen durch Ausspähungen, Know-how-Abflüsse und Datenmanipulationen





Genderhinweis: Aus Gründen der besseren Lesbarkeit wird im Text auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht. Dies impliziert keine Benachteiligung des weiblichen Geschlechts, sondern ist im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen.

Dies impliziert keine Benachteiligung des weiblichen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

Vorwort

Baden-Württemberg hat – wie kein anderes Land – einen starken Mittelstand mit hoher industrieller Kompetenz und einer großen Bandbreite innovativer Produkte und Dienstleistungen. Das Wissen, das hier vorhanden ist, ist deshalb auch für fremde Geheimdienste und Konkurrenten von großem Interesse. Wir müssen feststellen: Jahr für Jahr entstehen gravierende Schäden, weil durch Cyberangriffe illegal Informationen abgegriffen werden. Und wir müssen davon ausgehen, dass Cyberangriffe künftig weiter zunehmen. Für die betroffenen Unternehmen wird es immer schwieriger, Cyberangriffe rechtzeitig zu erkennen – oft genug ist es schon schwierig, sie überhaupt zu erkennen. Die Bedeutung der IT-Sicherheit ist deshalb schon heute hoch und wird noch weiter wachsen. Sie spielt auch eine entscheidende Rolle in der Digitalisierungsarbeit unserer Landesregierung.

Vor diesem Hintergrund veröffentlicht das Sicherheitsforum Baden-Württemberg nun diese Studie zu den Gefährdungen in baden-württembergischen Unternehmen durch Ausspähungen, Know-how-Abflüsse und Datenmanipulationen. Das Sicherheitsforum – ein Zusammenschluss aus Unternehmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden des Landes Baden-Württemberg – hat bereits in der Vergangenheit zwei viel beachtete Studien zum Thema Know-how-Schutz in Auftrag gegeben. Die vorliegende Studie bietet eine aktuelle Bestandsaufnahme zur IT-Sicherheit in baden-württembergischen Unternehmen. Sie zeigt auf, dass Cyberangriffe der häufigste Gefährdungsfaktor für den ungewollten Informationsabfluss sind. Jedes sechste Unternehmen verzeichnete in den letzten vier Jahren unbefugte Zugriffe auf schutzwürdige Daten. Solche Zugriffe und Ausspähungen können gravierende Folgen für ein Unternehmen haben: Zehn Prozent der Unternehmen geben das unmittelbare Schadensausmaß durch die Wiederherstellung bzw. den Ersatz der betroffenen Systeme als „gravierend", weitere 12 Prozent als „hoch" an. Die Dunkelziffer in diesem Bereich ist hoch, da die Unternehmen vielfach aufgrund fehlender Detektions- und Monitoring-Systeme nicht in der Lage sind zu beziffern, wie oft sie Opfer eines Cyberangriffs waren. Die Studie macht die Defizite beim Schutz vor Wirtschaftsspionage anschaulich. Das schafft die Voraussetzungen dafür, den Unternehmen gezielt Handlungsempfehlungen in Form eines IT-Sicherheitskonzeptes geben zu können. Das auf der Studie basierende IT-Sicherheitskonzept soll gerade auch kleine und mittelständische Unternehmen dabei unterstützen, ihre Wettbewerbsvorteile und ihr Know-how wirksam gegen Cyberangriffe abzusichern und bestehende Sicherheitslücken zu schließen.

Dem Sicherheitsforum wünschen wir bei seiner Arbeit viel Erfolg!

Thomas Strobl
Stellvertretender Ministerpräsident
Minister für Inneres, Digitalisierung und Migration des Landes Baden-Württemberg

Dr. Nicole Hoffmeister-Kraut MdL
Ministerin für Wirtschaft, Arbeit und Wohnungsbau des Landes Baden-Württemberg

Inhaltsverzeichnis

1 Einführung

1.1 Auftrag und Fragestellung

Das Sicherheitsforum Baden-Württemberg (SiFo) unterstützt Unternehmen und Organisationen darin, ihr Wissen und ihre Innovationen zu schützen. Die Sensibilisierung kleiner und mittlerer Unternehmen stellt dabei einen besonderen Tätigkeitsschwerpunkt des Sicherheitsforums dar. Das Sicherheitsforum hat in der Vergangenheit bereits Studien herausgegeben, welche die Auswirkungen von Informationsverlusten durch Wirtschaftsspionage und Konkurrenzausspähung in Baden-Württemberg analysiert haben. Seit der Erstellung der letzten SiFo-Studie 2009/2010 hat sich jedoch die spezifische Gefährdungslage stark verändert.

IT-Systeme sind hochentwickelteren Cyberangriffen (wie etwa Manipulation portabler USB-Geräte oder Advanced Persistent Threats) ausgesetzt, die etablierte Schutzmechanismen zunehmend ins Leere laufen lassen. Zudem ist durch die fortschreitende Digitale Transformation die Erreichung eines wirksamen Basisschutzes aufgrund der Vielzahl an internetfähigen Geräten und der Vielfalt unterschiedlicher IT-Systeme im Unternehmensalltag weitaus schwieriger zu erreichen, als dies noch vor wenigen Jahren der Fall war. Insbesondere die zunehmende Vernetzung von Industriesteuerungssystemen mit heterogenen externen Anwendungen („Industrie 4.0“) und Fernsensorik („Internet der Dinge“) stellt neuartige Herausforderungen an die Absicherung von Unternehmensnetzen.

Das Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg hat deshalb in Kooperation mit dem Sicherheitsforum Baden-Württemberg im Frühjahr 2018 die Erstellung einer Studie zu den Gefährdungen, insbesondere für die IT-Sicherheit, in baden-württembergischen Unternehmen ausgeschrieben. Kernbestandteil der Studie stellt eine Online-Umfrage unter baden-württembergischen Unternehmen dar, mit deren Hilfe eine empirische Fall- und Schadensanalyse durchgeführt und die ergriffenen Präventions- und Sicherheitsmaßnahmen im Bereich IT-Sicherheit zur Abwehr von Ausspähungen, Know-how-Abflüssen und Datenmanipulationen erhoben werden sollen.

Die Ergebnisse der Studie sollen zudem in ein zielgruppengerechtes IT-Schutzkonzept für kleine und mittlere baden-württembergische Unternehmen münden. Dieses IT-Schutzkonzept soll Handlungsempfehlungen für präventive Sicherheitsmaßnahmen enthalten und als Handreichung für Geschäftsführung und für IT-Verantwortliche aufbereitet werden. Zusätzlich zu klaren Handlungsanweisungen sollen Checklisten zur Selbstüberprüfung sowie Verweise auf weiterführende Informationen und Dokumente integriert werden.

Mit der Studiendurchführung wurde das Konsortium aus der Goldmedia GmbH Strategy Consulting, Berlin (Goldmedia) und dem Institut für Internet-Sicherheit des Fachbereichs Informatik und Kommunikation der Westfälischen Hochschule, Gelsenkirchen (if(is)) beauftragt. Der Auftrag zur Studiendurchführung wurde am 27.06.2018 durch das Logistikzentrum Baden-Württemberg erteilt.

1.2 Studienmethodik

Die Erhebung der Studie erfolgte als anonyme teilnehmeroffene Online-Befragung. Ziel der Unternehmensbefragung war es, eine Stichprobe von mindestens 200 Unternehmen zu erreichen.

Auf Grundlage der letzten SiFo-Studie hat das Konsortium aus Goldmedia und if(is) den zugrundeliegenden Fragebogen im Sommer 2018 umfassend überarbeitet und aktualisiert. Dabei wurde die Erhebungsmethodik dahingehend weiterentwickelt, dass auch neuartige Bedrohungsszenarien für die IT-Sicherheit, die durch die Digitale Transformation entstehen, angemessen berücksichtigt werden. Die final mit dem Auftraggeber abgestimmte Fassung der Befragung wurde im Oktober 2018 auf den Goldmedia-Umfrageserver aufgespielt, der von der Hetzner Online GmbH, Gunzenhausen, gehostet wird.

Teilnehmergewinnung

Die Teilnehmer der Unternehmensbefragung wurden durch einen gemeinschaftlichen, koordinierten Teilnahme-Aufruf vieler baden-württembergischer Kammern, Verbände und Initiativen als Multiplikatoren für die Befragung rekrutiert.

Tab. 1: Multiplikatoren der Erhebung (Auswahl)

Beteiligte Multiplikatoren aus Baden-Württemberg (Auswahl)	
Allianz für Sicherheit in der Wirtschaft Baden-Württemberg	Landesverband der Baden-Württembergischen Industrie
Allianz Industrie 4.0 Baden-Württemberg	Landkreistag Baden-Württemberg
Baden-Württembergischer Handwerkstag	Mittelstand 4.0-Agentur Handel
Baden-Württembergischer Industrie- und Handelskammertag	Mittelstand 4.0-Kompetenzzentrum Stuttgart
Beratungs- und Wirtschaftsförderungsgesellschaft für Handwerk und Mittelstand GmbH	Portal "Wirtschaft digital" des Landes Baden-Württemberg
ClusterAgentur Baden-Württemberg	Smart Home and Living Baden-Württemberg
DEHOGA Beratung GmbH	Südwestmetall
Digitalisierungshomepage des Landes Baden-Württemberg	UAV DACH e.V. – Verband für unbemannte Luftfahrt
fokus.energie	Unternehmerverband Metall
Handwerk International Baden-Württemberg/Enterprise Europe Network	Verband für Energie- und Wasserwirtschaft Baden-Württemberg
Koordinierungsstelle KRITIS-Unternehmen	Verein Deutscher Ingenieure – VDI Landesverband Baden-Württemberg
Landesamt für Verfassungsschutz Baden-Württemberg	VKU – Landesgruppe Baden-Württemberg
Landeskriminalamt Baden-Württemberg	

Die Unterstützungsleistung der Multiplikatoren umfasste vor allem die Kommunikationsmaßnahmen über qualifizierte E-Mail-Verteiler, Newsletter/Verbandszeitschriften, Webseiten und weitere Kommunikationswege (z. B. Social-Media-Aktivitäten). Insbesondere die baden-württembergischen Industrie- und Handelskammern und die baden-württembergischen Handwerkskammern haben ihre Mitglieder mehrfach über ihre Webseiten und

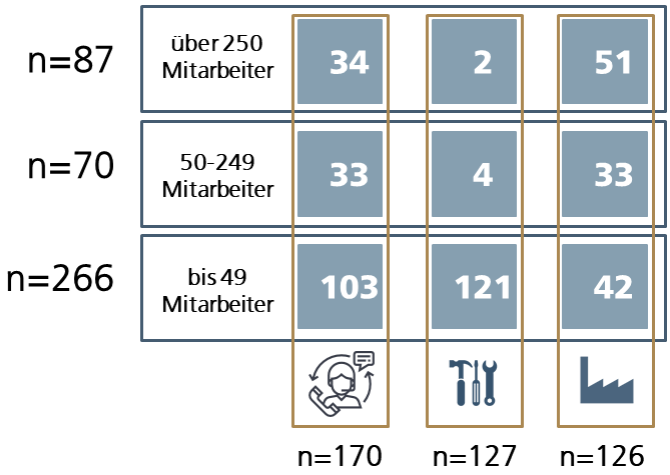
E-Mail-Verteiler bezüglich der Befragung informiert und um Teilnahme gebeten. Über 25 baden-württembergische Kammern, Verbände und Initiativen haben sich von Oktober bis Dezember 2018 als Multiplikatoren der Befragung beteiligt. Eine Auswahl der an der Teilnehmerrekrutierung beteiligten Unternehmen und Institutionen gewährt Tab. 1.

Die Auftragnehmer Goldmedia/if(is) haben keine Unternehmen kontaktiert, die Erstansprache zur Teilnahme geschah ausschließlich durch baden-württembergische Multiplikatoren auf Basis von Kommunikationselementen, die vom Auftragnehmer zur Verfügung gestellt wurden. Die Kommunikationselemente enthielten jeweils einen URL Link zu einer Startseite der Befragung auf der Webseite des Sicherheitsforums (sicherheitsforum-bw.de). Die Befragung wurde auf dem Goldmedia-Umfrageserver durchgeführt, die Teilnehmer erreichten den Umfrageserver über einen eingebetteten Link auf der Webseite des Sicherheitsforums.

Durchführung der Unternehmensbefragung und gezogene Stichprobe

Start der Online-Befragung war der 7. November 2018. Die Feldzeit der Online-Befragung endete am 4. Januar 2019. Während der Feldzeit wurden insgesamt 423 vollständige Fragebögen durch baden-württembergische Unternehmen ausgefüllt.

Tab. 2: Zusammensetzung der gezogenen Unternehmensstichprobe



Großunternehmen (ab 250 Mitarbeitern) sind mit n=87 in der Stichprobe vertreten, in vergleichbarem Umfang auch die mittelgroßen Unternehmen mit n=70. Die kleinen Unternehmen (mit maximal 49 Mitarbeitern) bilden mit n=266 die größte Unterstichprobe (vgl. Tab. 2).

Die Unternehmen der Stichprobe lassen sich drei verschiedenen Tätigkeitssektoren zuordnen: Handwerksunternehmen, Industrie- bzw. Produktionsunternehmen und Dienstleistungsunternehmen (inkl. des Gesundheitssektors). 170 Dienstleistungsunternehmen (inkl. des Gesundheitssektors) haben an der Befragung teilgenommen. Handwerksunternehmen sind mit n=127 in der Stichprobe gleich stark vertreten wie Industrie- bzw. Produktionsunternehmen (n=126). Der Maschinen- und Anlagenbau bildet mit n=45 die größte Branche innerhalb des Industrie- bzw. Produktionssektors.

In den folgenden Kapiteln wird in der Regel die gesamte Unternehmensstichprobe der baden-württembergischen Unternehmen (n=423) herangezogen.

Bei spezifischen Fragestellungen an Unterstichproben wird jedoch hiervon abgewichen und die jeweilige Unterstichprobe kenntlich gemacht. So wurden industrielle Präventions- und Sicherheitsmaßnahmen bspw. nur für Industrie- bzw. Produktionsunternehmen ausgewertet (vgl. Kapitel 2.4). Die Fragen zur Fall- und Schadensanalyse (ab Kapitel 4.2 ff.) wurden nur solchen Unternehmen gestellt, die auch von einem Sicherheitsvorfall betroffen waren und unter Umständen hieraus einen Schaden erlitten haben.

2 Präventions- und Sicherheitsmaßnahmen

In diesem Kapitel werden die bereits ergriffenen Präventions- und Sicherheitsmaßnahmen der befragten baden-württembergischen Unternehmen dargestellt. Zunächst wird im Abschnitt 2.1 allgemein betrachtet, wie sich die Investitionen in Präventions- und Sicherheitsmaßnahmen bei den befragten Unternehmen in den vergangenen vier Jahren entwickelt haben. In den darauffolgenden Abschnitten wird detailliert aufgeschlüsselt, welche Maßnahmen im Einzelnen von den Unternehmen ergriffen werden. Die zahlreichen Maßnahmen, die in der Studie abgefragt wurden, gliedern sich in die Bereiche Personal und Geschäftsablauf, Datensicherheit und Verschlüsselung sowie in den Bereich IT-Sicherheit in der Produktion/Industrie. Letztgenannter Fragenbereich wurde nur den Unternehmen aus Industriebranchen mit mehr als 50 Mitarbeitern gestellt.

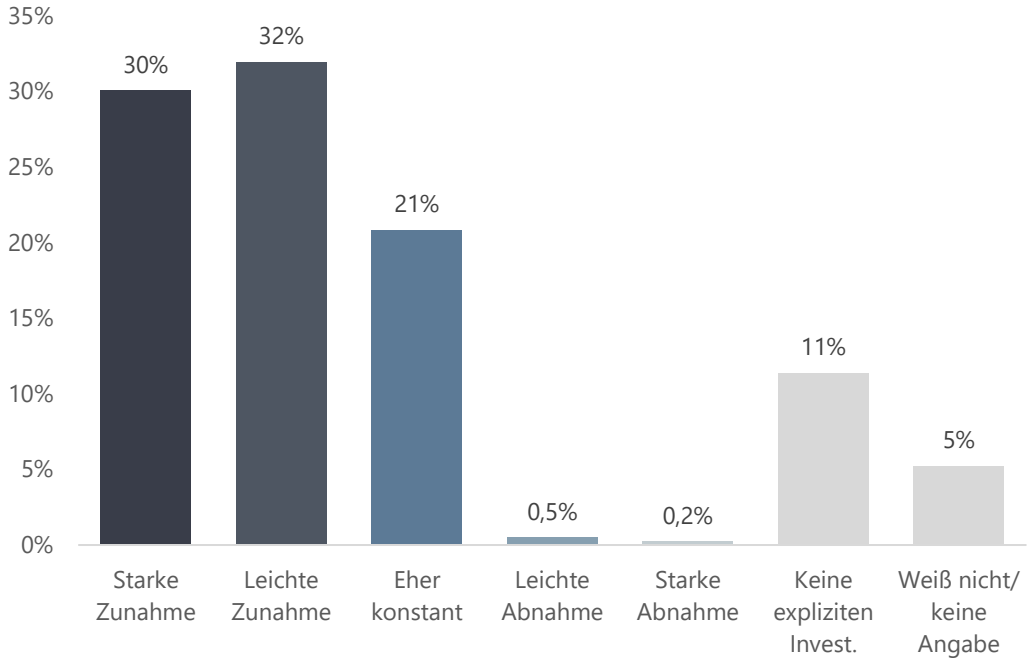
2.1 Investitionen in Präventions- und Sicherheitsmaßnahmen

Zunächst wurde im Rahmen der Befragung erhoben, wie sich die Investitionen in Präventions- und Sicherheitsmaßnahmen der baden-württembergischen Unternehmen entwickelt haben. Die Investitionstätigkeit ist hierbei ein robuster Indikator für den Stellenwert einer Ausgabe innerhalb des Unternehmens, da Investitionsentscheidungen in der Regel ein längerer, teils überjähriger Planungs- und Entscheidungsprozess vorausgeht. Aus diesem Grund wurde die Investitionstätigkeit auch nicht ausschließlich für das vergangene Jahr (2018), sondern für den Zeitraum der letzten vier Jahre (2015 – 2018) erhoben.

Im Ergebnis haben sich die Investitionen von Unternehmen in Baden-Württemberg in Präventions- und Sicherheitsmaßnahmen in den Jahren 2015 bis 2018 positiv entwickelt: 30 Prozent der befragten Unternehmen (n=423) geben eine starke Zunahme an Investitionen an, während rund 32 Prozent der befragten Unternehmen eine leichte Zunahme verzeichnen (vgl. Abb. 1).

Der Anteil der Unternehmen, die eine Abnahme an Investitionen in Präventions- und Sicherheitsmaßnahmen angeben, liegt bei unter einem Prozent. Lediglich 0,5 Prozent der befragten Unternehmen stellen eine leichte Abnahme an Investitionen fest, während weitere 0,2 Prozent der Unternehmen eine starke Abnahme an Investitionen verzeichnen.

Abb. 1: Investitionen in Präventions- und Sicherheitsmaßnahmen in den letzten vier Jahren, in Prozent, 2015 – 2018



Stichprobe: n=423 Unternehmen. Frage: „Wie haben sich Ihre Investitionen in Präventions- und Sicherheitsmaßnahmen in den letzten vier Jahren entwickelt?"

Der strategische Stellenwert, den Unternehmen den Präventions- und Sicherheitsmaßnahmen beimessen, erkennbar an den getätigten Investitionen, ist in den letzten vier Jahren deutlich gestiegen: Über 60 Prozent der Unternehmen geben an, dass ihre Investitionen in Präventions- und Sicherheitsmaßnahmen leicht bzw. stark zugenommen haben.

2.2 Maßnahmen im Bereich Personal und Geschäftsablauf

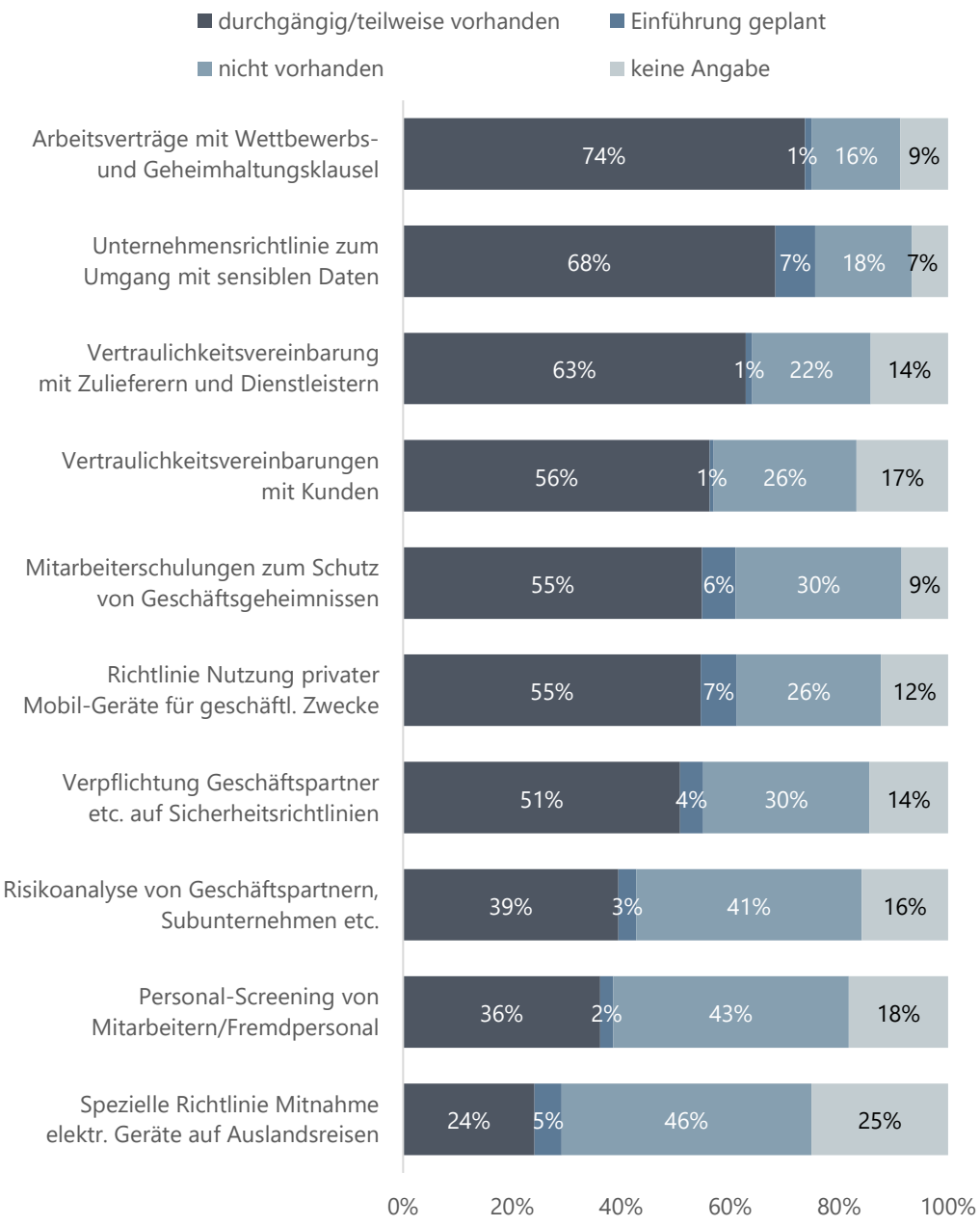
Die Aufnahme von Wettbewerbs- und Geheimhaltungsklauseln in Arbeitsverträgen ist die am meisten verbreitete Maßnahme im Bereich Personal und Geschäftsablauf. Für das Jahr 2018 geben rund 74 Prozent der befragten Unternehmen an, dass sie bereits durchgängig oder teilweise mit Wettbewerbs- und Geheimhaltungsklauseln in Arbeitsverträgen arbeiten (vgl. Abb. 2).

Unternehmensrichtlinien zum Umgang mit sensiblen Daten sind im vergleichbaren Umfang vorhanden, rund 68 Prozent der befragten Unternehmen haben durchgängig oder zumindest teilweise eine solche Unternehmensrichtlinie verabschiedet. In etwas geringerem Umfang finden Vertraulichkeitsvereinbarungen für Zulieferer und Dienstleister Anwendung: Rund 63 Prozent der befragten Unternehmen verpflichten Zulieferer bzw. Dienstleister zumindest teilweise zur Vertraulichkeit. Im Kundenverhältnis liegt der entsprechende Wert nur geringfügig niedriger, bei rund 56 Prozent der Unternehmen.

Spezifische Richtlinien zur Nutzung privater Mobilgeräte für geschäftliche Zwecke sind bei gut der Hälfte der befragten Unternehmen (rund 55 Prozent) durchgängig oder teilweise vorhanden. In gleichem Umfang (rund 51 Prozent) ist es zumindest teilweise üblich, Geschäftspartner zur Einhaltung der eigenen Sicherheitsrichtlinien zu verpflichten.

Vergleichsweise selten werden Richtlinien für die Mitnahme von elektrischen Geräten auf Auslandsreisen erlassen. Diese existieren nur etwa bei rund einem Viertel der befragten Unternehmen. Allerdings sind Auslandsreisen bei vielen Unternehmen mit vorwiegend regionalem Tätigkeitsschwerpunkt kein relevantes Szenario, und die Zahl der Unternehmen „ohne Angaben" war mit rund 25 Prozent vergleichsweise hoch. Dies kann u.a. darauf hindeuten, dass ggf. Richtlinien zur Anwendung kommen, diese jedoch innerhalb des Unternehmens nicht allgemein bekannt sind.

Abb. 2: Präventions- und Sicherheitsmaßnahmen im Bereich Personal und Geschäftsablauf, in Prozent, 2018



Stichprobe: n=423 Unternehmen. Frage: „Gibt es in Ihrem Unternehmen die folgenden Präventions- und Sicherheitsmaßnahmen?"

Präventions- und Sicherheitsmaßnahmen, die über rein vertragliche Regelungen hinausgehen, sind erwartungsgemäß weniger verbreitet, da sie wiederkehrend Aufwand und Kosten verursachen.

Am häufigsten wurden von solchen Maßnahmen Mitarbeiterschulungen angeführt. Diese werden noch von mehr als der Hälfte der Unternehmen (rund 55 Prozent) als Präventionsmaßnahme eingesetzt. Allerdings fallen hierunter auch einmalige Schulungen von Mitarbeitern, etwa bei Beginn der Betriebszugehörigkeit. Die Zahl der Unternehmen, die ihre Mitarbeiter wiederkehrend schult, dürfte geringer als die Hälfte der befragten Unternehmen sein.

Rund 40 Prozent der Unternehmen geben an, dass Risikoanalysen von Geschäftspartnern, Subunternehmen, etc. durchgeführt werden. Ein Personal-Screening von eigenen Mitarbeitern bzw. von Fremdpersonal wird von rund 36 Prozent der befragten Unternehmen zumindest teilweise durchgeführt. Obwohl diese Maßnahmen nicht besonders weit unter den baden-württembergischen Unternehmen verbreitet sind, erwägen kaum zusätzliche Unternehmen deren Einführung. Nur rund 2 bzw. 3 Prozent der Unternehmen planen die Einführung von Risikoanalysen von Geschäftspartnern und Personal-Screenings.

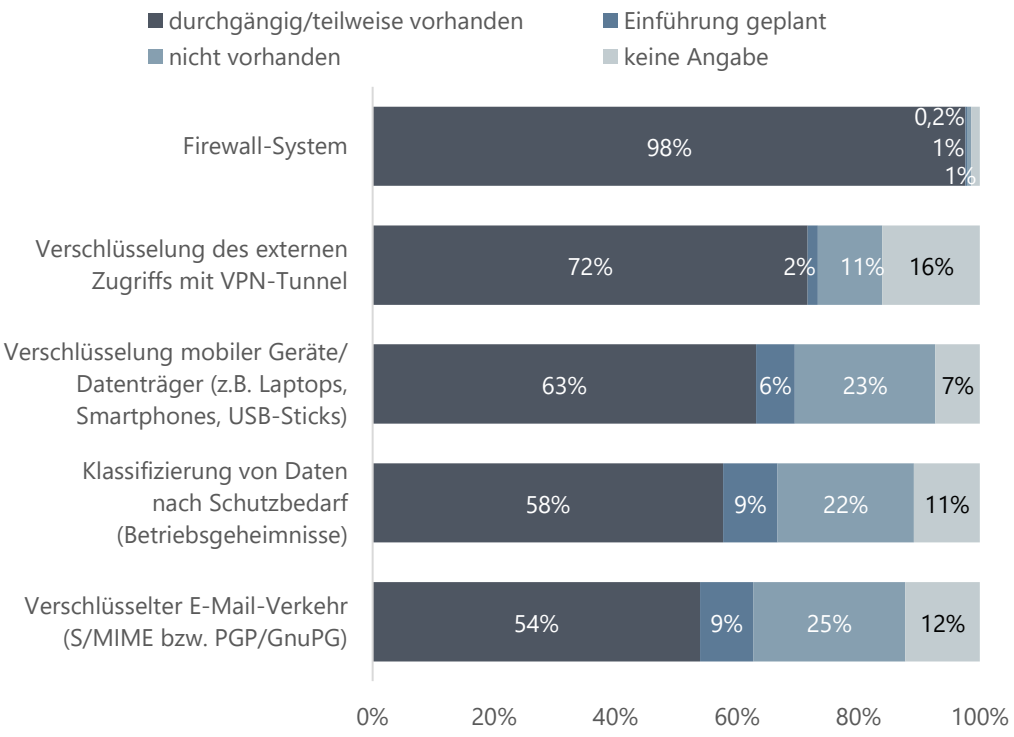
Im Hinblick auf Maßnahmen im Bereich Personal und Geschäftsablauf lässt sich aufgrund der Ergebnisse der Befragung daher folgendes Fazit ziehen:

Erfreulicherweise sind vertragliche Regelungen vergleichsweise weit verbreitet. Unternehmensrichtlinien zum Umgang mit sensiblen Daten werden in rund zwei Dritteln der befragten Unternehmen eingesetzt, Arbeitsverträge mit Wettbewerbs- und Geheimhaltungsklauseln sogar in knapp drei Vierteln der Unternehmen. Von aufwendigeren (und kostenintensiveren) Maßnahmen, wie etwa Risikoanalysen und Personal-Screenings, macht nur ein gutes Drittel der Unternehmen Gebrauch. Mitarbeiterschulungen zur Prävention von Ausspähungen, Know-how-Abflüssen und Datenmanipulationen werden von etwa der Hälfte der Unternehmen durchgeführt. Dieser Wert ist zwar nicht unerfreulich, mit Hinblick auf künftige Herausforderungen der Digitalen Transformation (z. B. Industrie 4.0) allerdings langfristig nicht befriedigend.

2.3 Maßnahmen im Bereich Datensicherheit und Verschlüsselung

Gängige technische Lösungen zur Datensicherheit und Verschlüsselung sind in den befragten Unternehmen bereits weit verbreitet. Mit rund 98 Prozent geben nahezu alle befragten Unternehmen an, dass im Bereich Datensicherheit und Verschlüsselung durchgängig oder teilweise ein Firewall-System vorhanden ist (vgl. Abb. 3). Die Verschlüsselung des externen Zugriffs über VPN-Tunnel wird von rund 72 Prozent der befragten Unternehmen durchgängig oder teilweise genutzt. Zudem ist davon auszugehen, dass auch der Großteil der Unternehmen, die hier nicht auskunftsfähig waren (rund 16 Prozent) ebenfalls über einen verschlüsselten VPN-Zugriff verfügen. Mobile Geräte sind zumindest bei 63 Prozent der Unternehmen durchgehend oder teilweise verschlüsselt im Einsatz.

Abb. 3: Präventions- und Sicherheitsmaßnahmen im Bereich Datensicherheit und Verschlüsselung, in Prozent, 2018



Stichprobe: n=423 Unternehmen. Frage: „Gibt es in Ihrem Unternehmen die folgenden Präventions- und Sicherheitsmaßnahmen?"

Technische Lösungen, die nur mit größerem Aufwand in der IT-Infrastruktur implementiert werden können, sind weniger weit verbreitet. Die durchgängige Klassifikation schutzbedürftiger Daten erfolgt bei 58 Prozent der befragten Unternehmen zumindest teilweise. Die verschlüsselte E-Mail-Kommunikation mittels S/MIME bzw. GnuPG/PGP-Zertifikaten erfolgt nur in gut der Hälfte der Unternehmen (rund 54 Prozent).

In Anbetracht der geringen Verbreitung von E-Mail-Verschlüsselung unter privaten Nutzern sind 54 Prozent zunächst zwar ein hoher Wert. Allerdings erklärt ein Wert um 50 Prozent in Unternehmen auch, warum die verschlüsselte E-Mail-Kommunikation nicht schneller an Verbreitung gewinnt. Auch in Unternehmen ist E-Mail-Verschlüsselung, anders als etwa der Einsatz einer Firewall, noch lange kein Mindeststandard für vertrauliche digitale Kommunikation.

2.4 Maßnahmen im Bereich IT-Sicherheit in der Produktion/Industrie

Bei der befragten Unterstichprobe der Produktions- bzw. Industrieunternehmen ab 50 Mitarbeitern (n=95) wurden zahlreiche weitere Merkmale erhoben, die ausschließlich im Rahmen der industriellen Produktion relevant sind. Hierbei handelt es sich vor allem um technische Sicherheitslösungen und fortgeschrittene IT-Systeme, die in der Regel eine arbeitsteilige IT-Abteilung vor Ort voraussetzen (vgl. Abb. 4).

Im Ergebnis der Befragung stellte sich heraus, dass vor allem physische (IT-)Sicherheit stark verbreitet ist: Bei rund 85 Prozent der befragten Industrieunternehmen finden Zugangskontrollen zu den sensiblen Bereichen statt, in der Regel als Ergänzung zur Absicherung des Firmenareals mit Zugangskontrollen. Mit 94 Prozent ist bei nahezu allen Unternehmen der Serverbereich besonders physisch abgesichert (vgl. Abb. 4).

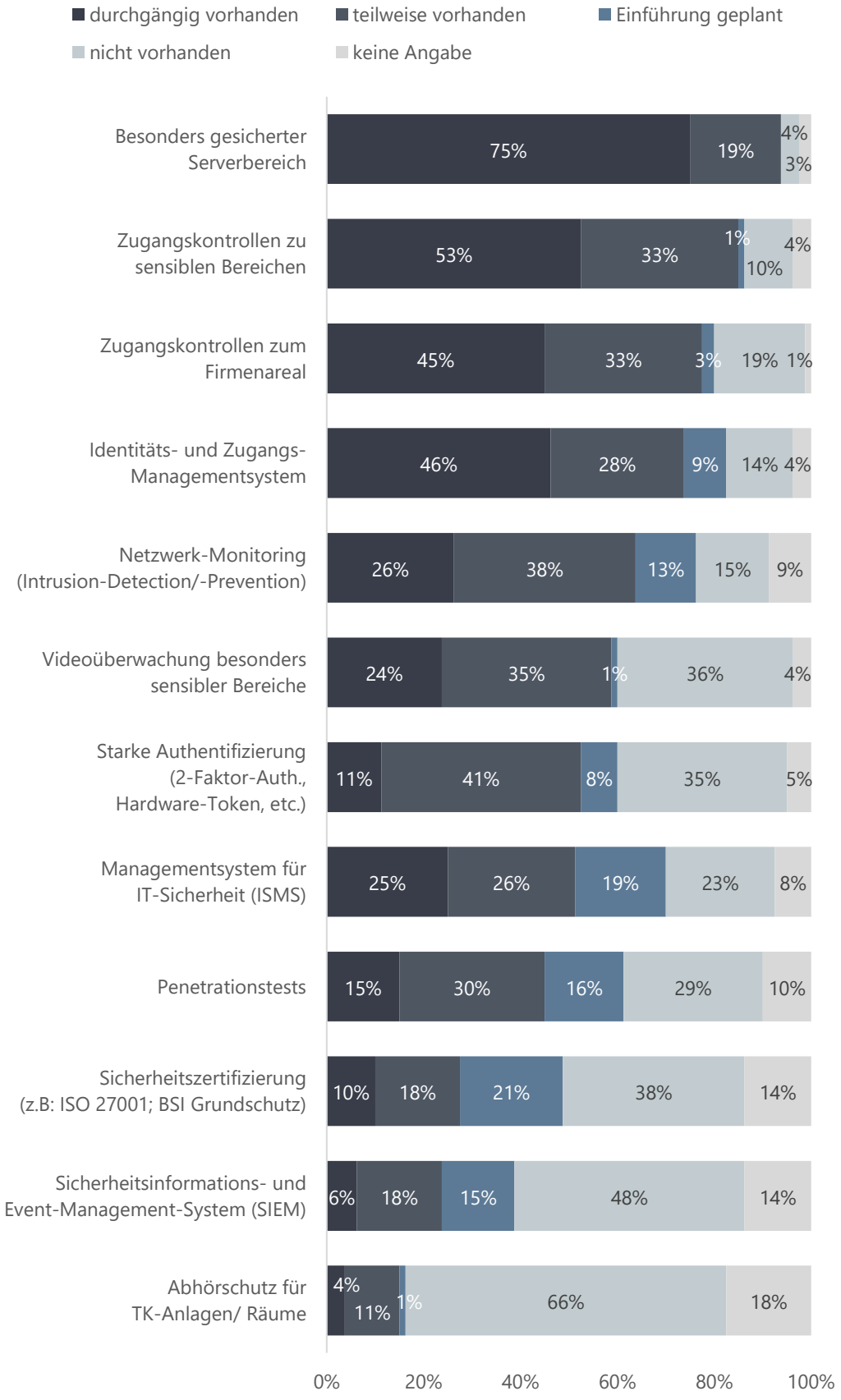
Im Vergleich hierzu ist die digitale Absicherung überraschend abgeschlagen: Etwa zwei Drittel der Unternehmen besitzen zwar eine Form des Netzwerk-Monitorings, aber nur rund ein Viertel der befragten Unternehmen verfügt über ein durchgehendes Netzwerk-Monitoring mit Intrusion-Detection bzw. -Prevention-Systemen. Im Kontext der Abwehr von Cyber-Angriffen kommt der Netzwerküberwachung eine zentrale Bedeutung zu, leider ist gerade hier festzustellen, dass es in den befragten Unternehmen noch gravierende Defizite in der zugrundeliegenden Netzwerk-Infrastruktur gibt.

Für andere, besonders aufwendige Sicherheitsmaßnahmen sind vorwiegende Nennungen in der Kategorie „nur teilweise vorhanden" weniger problematisch, da besonders aufwendige Maßnahmen, wie z. B. Sicherheitszertifizierungen, in der Regel nur bestimmte Systemumgebungen betreffen.

Insofern ist die (mindestens teilweise) Verbreitung von Sicherheitsinformations- und Ereignismanagement-Systemen (SIEM) mit rund 24 Prozent, bzw. von Sicherheitszertifizierungen (rund 28 Prozent) durchaus ein positives Ergebnis der Befragung. Gleichzeitig wird deutlich, dass dieser wünschenswerte „Goldstandard" der Informationssicherheit erst von einem knappen Drittel der befragten Industrieunternehmen erreicht wurde.

Vergleichsweise häufig werden hingegen Managementsysteme für die Informationssicherheit (ISMS) eingesetzt: Diese finden sich bereits in rund der Hälfte (rund 52 Prozent) der befragten baden-württembergischen Industrieunternehmen. In ähnlicher Größenordnung (45 Prozent) ist der Anteil der Unternehmen, die Penetrationstests durchführen, um Schwachstellen der eigenen System- und Anlagenkonfiguration zu ermitteln.

Abb. 4: Präventions- und Sicherheitsmaßnahmen im Bereich IT-Sicherheit in der Produktion, in Prozent, 2018



Stichprobe: n= 95 Industrieunternehmen ab 50 Mitarbeitern. Frage: „Gibt es in Ihrem Unternehmen die folgenden Präventions- und Sicherheitsmaßnahmen?"

3 Risiken und Herausforderungen der Digitalen Transformation

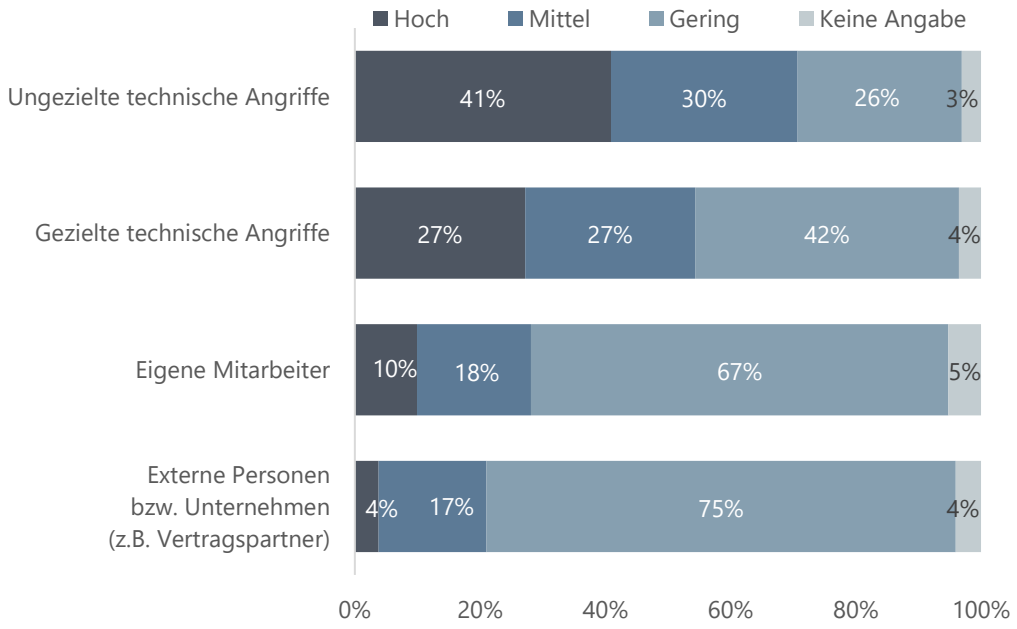
Neben den bereits ergriffenen Präventions- und Sicherheitsmaßnahmen bilden die Risiken und Herausforderungen der Digitalen Transformation einen weiteren Schwerpunkt der Erhebung. Zunächst wird hierbei in diesem Kapitel auf die konkreten Risiken für Geschäfts- und Betriebsgeheimnisse eingegangen, im darauffolgenden Abschnitt stehen die längerfristigen Herausforderungen der Digitalen Transformation im Vordergrund. Im dritten Abschnitt des Kapitels wird dargestellt, wie die befragten Unternehmen den Einsatz von unterschiedlichen Unterstützungsinstrumenten beurteilen.

3.1 Angriffsrisiko auf Geschäfts- und Betriebsgeheimnisse

Die befragten baden-württembergischen Unternehmen sehen vor allem in ungezielten technischen Angriffen ein hohes Risiko für die eigenen Geschäfts- und Betriebsgeheimnisse. Ungezielte technische Angriffe werden von rund 41 Prozent der befragten Unternehmen als hohes Risiko bewertet. Gezielte technische Angriffe werden von rund 27 Prozent mit einem hohen Risiko beurteilt (vgl. Abb. 5).

Im Gegensatz dazu wird das Angriffsrisiko durch eigene Mitarbeiter oder externe Vertragspartner als gering eingeschätzt. Mindestens zwei Drittel der befragten Unternehmen sehen sowohl durch eigene Mitarbeiter als auch durch externe Personen bzw. Unternehmen lediglich eine geringe Gefahr.

Abb. 5: Unternehmenseinschätzung zum Angriffsrisiko auf Geschäfts- und Betriebsgeheimnisse in den nächsten vier Jahren, in Prozent, 2018



Stichprobe: n=423 Unternehmen. Frage: „Wie hoch schätzen Sie das Risiko von Angriffen auf die Geschäfts- und Betriebsgeheimnisse Ihres Unternehmens in den nächsten vier Jahren ein?"

Das klassische Risikoszenario der Wirtschaftsspionage und Konkurrenzausspähung, in dem die eigenen Mitarbeiter Geschäfts- oder Betriebsgeheimnisse entwenden, wird somit viermal geringer eingeschätzt als das Risiko, Opfer eines ungezielten Angriffes zu werden.

Die Ergebnisse der Risikoeinschätzung liefern ein bemerkenswertes Ergebnis. Den Unternehmen ist die abstrakte Gefährdung durch Cyber-Angriffe deutlich stärker bewusst als das klassische Risiko des Know-how-Abflusses durch das Verhalten der eigenen Mitarbeiter. Statt einer Awareness für die Gefährdungslage mangelt es somit eher an einer Awareness für geeignete Präventions- und Sicherheitsmaßnahmen, um ein befriedigendes Schutzniveau sicherzustellen.

3.2 Herausforderungen der Digitalen Transformation für Industrieunternehmen

Die zunehmende Vernetzung der deutschen Wirtschaft, insbesondere durch die fortschreitende Digitale Transformation, sorgt dafür, dass immer mehr Daten digital zugänglich und damit auch angreifbar werden. Daher wurden die baden-württembergischen Industrieunternehmen mit mehr als zehn Mitarbeitern (n=137), neben der Einschätzung des zukünftigen Angriffsrisikos auf Geschäfts- und Betriebsgeheimnisse, zusätzlich nach den spezifischen Herausforderungen der Digitalen Transformation in Industrieunternehmen befragt.

Die künftigen strategischen Herausforderungen der Digitalen Transformation werden von Industrieunternehmen insbesondere im Bereich der internen und externen Vernetzung der Produktionsanlagen als hoch eingeschätzt: Rund 52 Prozent der befragten Unternehmen schätzen diese als hoch ein (vgl. Abb. 6).

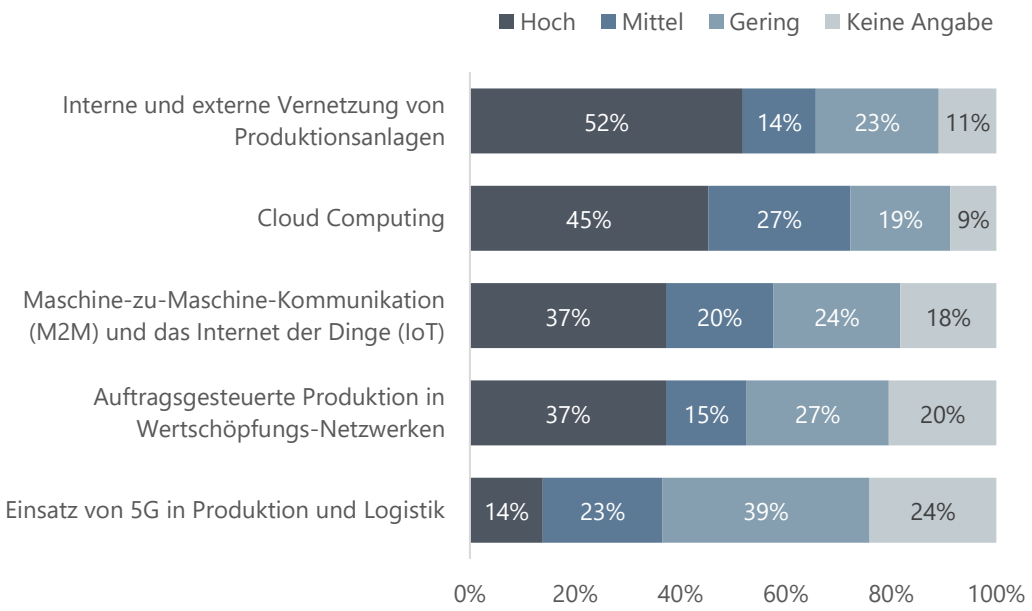
Auch das Cloud Computing wird von rund 45 Prozent der Unternehmen als große Herausforderung gesehen, nur 19 Prozent der befragten Unternehmen sehen im Cloud Computing lediglich geringe Herausforderungen auf sich zukommen.

Die Maschine-zu-Maschine-Kommunikation im Kontext des Internets der Dinge und die auftragsgesteuerte Produktion in Wertschöpfungs-Netzwerken stellen ein gutes Drittel der befragten Unternehmen vor große Herausforderungen.

Durch den Einsatz des neuen Mobilfunkstandards 5G in der Produktion und Logistik entstehen neue Herausforderungen für Industrieunternehmen. Diese können zwar durch vernetzte Produktionsabläufe einen höheren Automatisierungsgrad erreichen und 5G u.a. zur digitalisierten Lagerverwaltung einsetzen. Allerdings erfordert die höhere Vernetzung zugleich eine Zunahme an IT-Sicherheitsmaßnahmen, da die Angriffsfläche für Spionage und Sabotage deutlich erhöht wird.

Diese Herausforderungen durch 5G werden jedoch von den meisten Unternehmen eher als nachrangig betrachtet. Rund 40 Prozent der befragten Unternehmen beurteilen diese als gering. Nur rund 14 Prozent beurteilen die spezifischen Herausforderungen durch den 5G-Einsatz als hoch.

Abb. 6: Unternehmenseinschätzung zu den Herausforderungen der digitalen Transformation, in Prozent, 2018



Stichprobe: n=137 Industrieunternehmen mit mind. zehn Mitarbeitern. Frage: „Wie hoch schätzen Sie die folgenden Herausforderungen im Kontext der digitalen Transformation für Ihr Unternehmen ein?"

Im Ergebnis lässt sich feststellen, dass die zunehmende interne und externe Vernetzung von Produktionsanlagen von den befragten Unternehmen als die größte Herausforderung der digitalen Transformation angesehen wird. Wenig überraschend wird das, mit der externen Vernetzung eng verwandte, Cloud Computing von den befragten Unternehmen als ähnlich herausfordernd eingeschätzt.

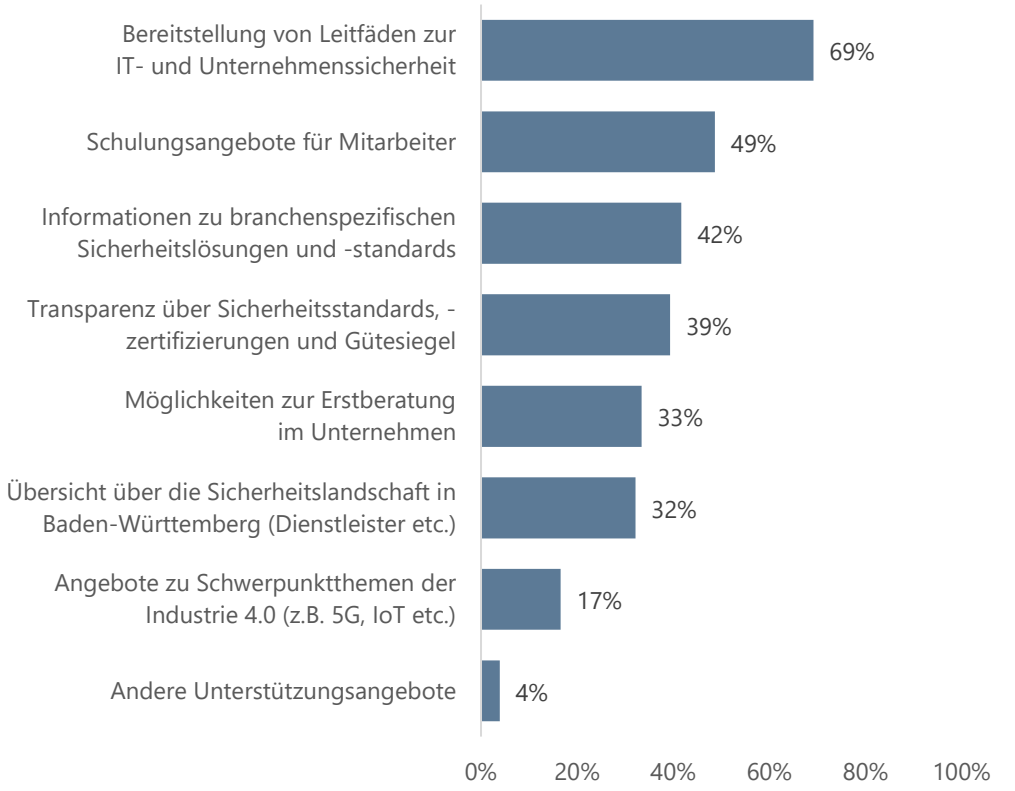
3.3 Unterstützungsbedarfe der baden-württembergischen Unternehmen

Im Kontext der künftigen Risiken und Herausforderungen wurde ebenfalls erhoben, welche spezifischen Angebote und Fördermaßnahmen von den Unternehmen als sinnvoll angesehen werden, um sie beim Prozess der Digitalen Transformation zielgerichtet zu unterstützen (vgl. Abb. 7).

Mit rund 69 Prozent formuliert der überwiegende Teil der baden-württembergischen Unternehmen den Wunsch nach Leitfäden zur IT- und Unternehmenssicherheit (vgl. Abb. 7). Für rund 42 Prozent der Unternehmen wären darüber hinaus auch Informationen zu branchenspezifischen Sicherheitslösungen und -standards interessant.

In Schulungsangeboten sieht rund die Hälfte der befragten Unternehmen eine sinnvolle Unterstützung für ihr Unternehmen.

Abb. 7: Gewünschte Unterstützungsangebote der Unternehmen, in Prozent, 2018



Stichprobe: n=423 Unternehmen. Frage: „In welchen Bereichen würden Sie sich verstärkt Unterstützungsangebote wünschen?“ (Mehrfachnennungen möglich)

Möglichkeiten zur Erstberatung im Unternehmen werden, ebenso wie Übersichten zu baden-württembergischen Anbietern und Dienstleistern von Sicherheitslösungen, noch von rund einem Drittel der befragten Unternehmen als sinnvolle Unterstützungsangebote angesehen. Spezielle Themenangebote zur Industrie 4.0, z. B. zum Mobilfunkstandard 5G oder zum Internet der Dinge (IoT), werden nur noch von rund 17 Prozent der befragten Unternehmen als Unterstützungsbedarf artikuliert.

Der überwiegende Wunsch nach Leitfäden zur IT- und Unternehmenssicherheit zeigt, dass die befragten Unternehmen an strukturierten, allgemein gültigen Informationen zu IT- und Unternehmenssicherheit (Best Practices, Stand der Technik, usw.) interessiert sind. Zudem zeigen die Befragungsergebnisse, dass die Unternehmen in der Aufklärung und Schulung ihrer Mitarbeiter ein sinnvolles Unterstützungspotenzial sehen.

Informationsangebote in Baden-Württemberg

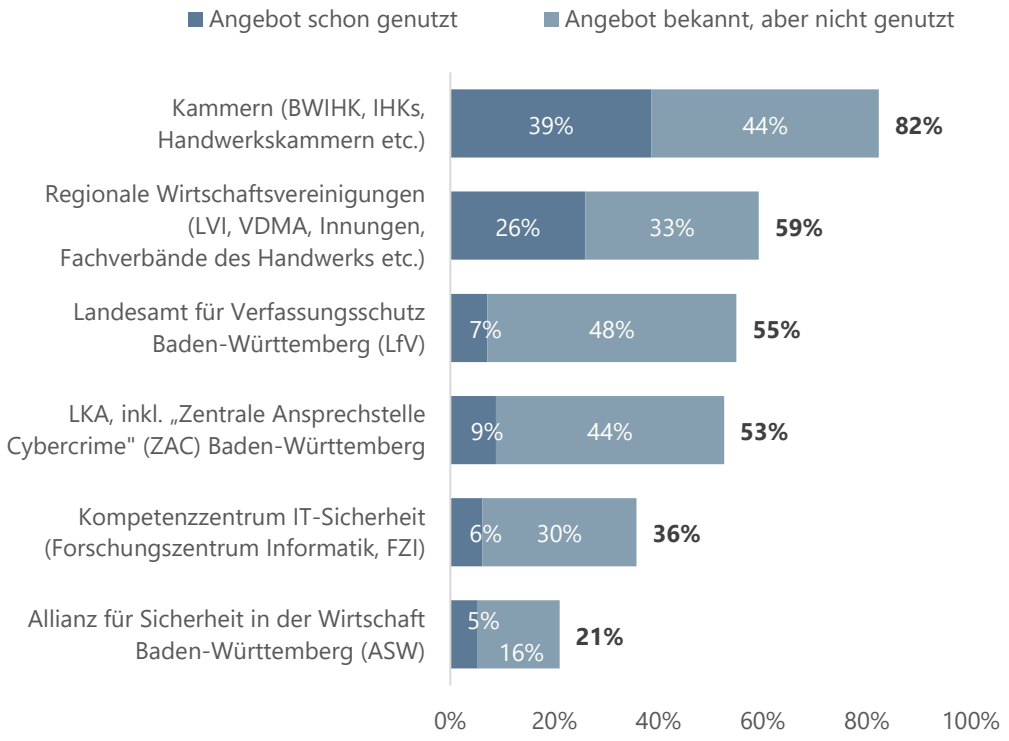
Zahlreiche Institutionen und Organisationen in Baden-Württemberg informieren umfangreich und regelmäßig zu den Themenkomplexen IT- und Unternehmenssicherheit. Jedoch unterscheidet sich der Bekanntheits- und Nutzungsgrad der Informationsangebote (vgl. Abb. 8).

Die Angebote der Kammern haben dabei die mit deutlichem Abstand höchste Relevanz für die befragten Unternehmen: 82 Prozent der befragten Unternehmen kennen die Angebote bzw. haben diese schon genutzt.

Für viele Unternehmen sind zudem die Angebote der regionalen Wirtschaftsvereinigungen, des Landesamtes für Verfassungsschutz und des Landeskriminalamts mit seiner zentralen Ansprechstelle Cybercrime (ZAC) relevant: Diese Angebote kennen bzw. nutzen rund 53 bis 59 Prozent der befragten baden-württembergischen Unternehmen.

In der Nutzung führen sowohl die Angebote der Kammern (rund 39 Prozent) als auch die Angebote der regionalen Wirtschaftsvereinigungen (26 Prozent) die Liste an. Andere Informationsangebote wurden von weniger als 10 Prozent der befragten Unternehmen bereits genutzt. Die Angebote des Verfassungsschutzes und des Landeskriminalamtes sind mit 48 bzw. 43 Prozent jedoch vielen der befragten Unternehmen bekannt.

Abb. 8: Nutzung der Informationsangebote von baden-württembergischen Organisationen, in Prozent, 2018



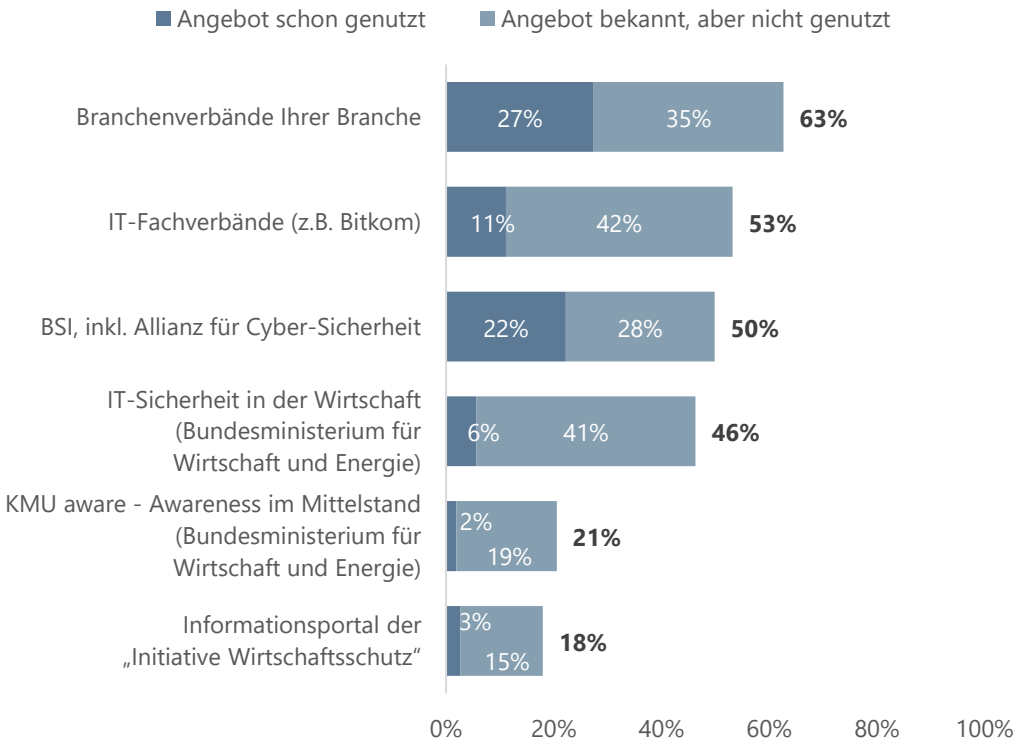
Stichprobe: n=423 Unternehmen. Frage: „Kennen oder nutzen Sie die Informationsangebote folgender Einrichtungen?"

Überregionale Informationsangebote

Die Angebote der jeweiligen Branchenverbände sind rund 63 Prozent der befragten Unternehmen bekannt und wurden von rund 27 Prozent bereits genutzt. Die Informationsangebote des BSI (inkl. „Allianz für Cyber-Sicherheit") haben einen ähnlich hohen Nutzungsgrad von rund 22 Prozent der befragten Unternehmen (vgl. Abb. 9).

Angebote der IT-Fachverbände sind rund 53 Prozent der Unternehmen bekannt, werden allerdings nur durch weitere rund 11 Prozent genutzt. Das vor rund drei Jahren gestartete Informationsportal der „Initiative Wirtschaftsschutz" ist bereits rund 18 Prozent der Unternehmen bekannt, wurde allerdings erst von rund 3 Prozent der Unternehmen aktiv genutzt.

Abb. 9: Nutzung der Informationsangebote überregionaler Organisationen, in Prozent, 2018



Stichprobe: n=423 Unternehmen. Frage: „Kennen oder nutzen Sie die Informationsangebote folgender Einrichtungen?"

4 Fall- und Schadensanalyse

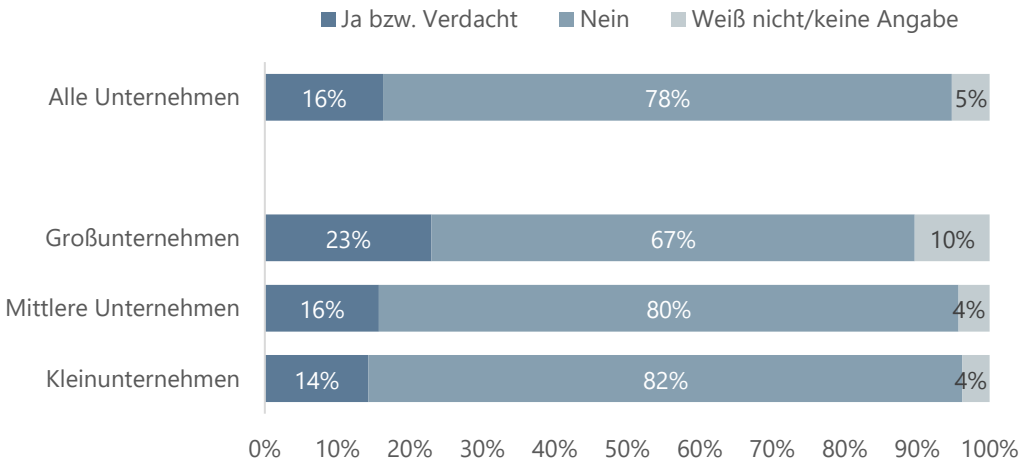
In diesem Kapitel werden die Fälle von Datenabzügen und Datenmanipulationen analysiert, von denen die baden-württembergischen Unternehmen in den letzten vier Jahren betroffen waren.

4.1 Unbefugte Zugriffe auf schutzwürdige Daten

Rund 16 Prozent aller befragten Unternehmen in Baden-Württemberg geben an, dass sie in den letzten vier Jahren unbefugte Zugriffe auf schutzwürdige Daten des Unternehmens verzeichnet haben oder unbefugte Zugriffe vermuten (vgl. Abb. 10).

Die befragten Großunternehmen (über 249 Mitarbeiter) sind am stärksten von unbefugten Zugriffen betroffen. In den vergangenen vier Jahren verzeichneten Großunternehmen mit rund 23 Prozent signifikant höhere Zugriffs- und Verdachtsfälle als mittlere Unternehmen (rund 16 Prozent) und Kleinunternehmen (rund 14 Prozent).

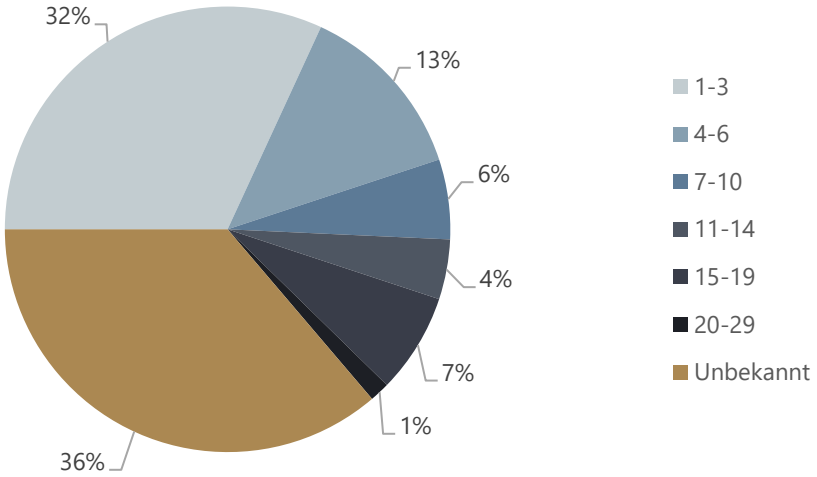
Abb. 10: Unbefugter Zugriff* auf schutzwürdige Daten des Unternehmens in den letzten vier Jahren, in Prozent, 2015-2018



** „Zugriff" umfasst sowohl Datenabzüge als auch Datenmanipulationen*
Stichprobe: n=423 Unternehmen. Frage: „Haben Unbefugte in den letzten vier Jahren Zugriff auf schutzwürdige Daten Ihres Unternehmens erlangt?"

Die Häufigkeit von unbefugten Zugriffen auf schutzwürdige Daten über einen Vier-Jahres-Zeitraum wird von 32 Prozent der von unbefugten Zugriffen betroffenen Unternehmen (n=69) mit ein bis drei Vor- und Verdachtsfällen beziffert (vgl. Abb. 11). 13 Prozent der betroffenen Unternehmen schätzen die Häufigkeit unbefugter Zugriffe auf vier bis sechs Fälle, 6 Prozent der Unternehmen gehen von sieben bis zehn Vor- und Verdachtsfällen in den letzten vier Jahren aus. Weitere 13 Prozent der betroffenen Unternehmen schätzen, dass sie mehr als 10 Ereignisse mit unbefugtem Zugriff in den vergangen vier Jahren erlitten haben.

Abb. 11: Anzahl unbefugter Zugriffe auf schutzwürdige Daten in den letzten vier Jahren bei den betroffenen Unternehmen, in Prozent, 2018



Stichprobe: n=69 Unternehmen mit Vorfällen oder Verdachtsfällen in den letzten vier Jahren.
Frage: „Wie viele Vor- und Verdachtsfälle (unbefugter Zugriff) gab es in Ihrem Unternehmen in den letzten vier Jahren? Bitte schätzen Sie die ungefähre Anzahl der Vor- und Verdachtsfälle in Ihrem Unternehmen in den letzten vier Jahren."

Ein großes Problem für die Quantifizierung von unbefugten Zugriffen ist deren Detektion. 36 Prozent der befragten Unternehmen, die innerhalb der letzten vier Jahre unbefugte Zugriffe verzeichneten, können die Anzahl der Vor- und Verdachtsfälle nicht näher beziffern.

Hierin zeigen sich die gravierenden Folgen durch Defizite bei Netzwerküberwachungsmaßnahmen, welche die Befragung bei der Ausstattung mit Netzwerküberwachungstechnik ergeben hat: Nur 26 Prozent aller Unternehmen verfügen über eine durchgehende Netzwerkprotokollierung (vgl. Kapitel 2.4). In Folge sieht sich über ein Drittel der von unbefugten Zugriffen betroffenen Unternehmen außer Stande, die Häufigkeit unbefugter Zugriffe überhaupt zu quantifizieren.

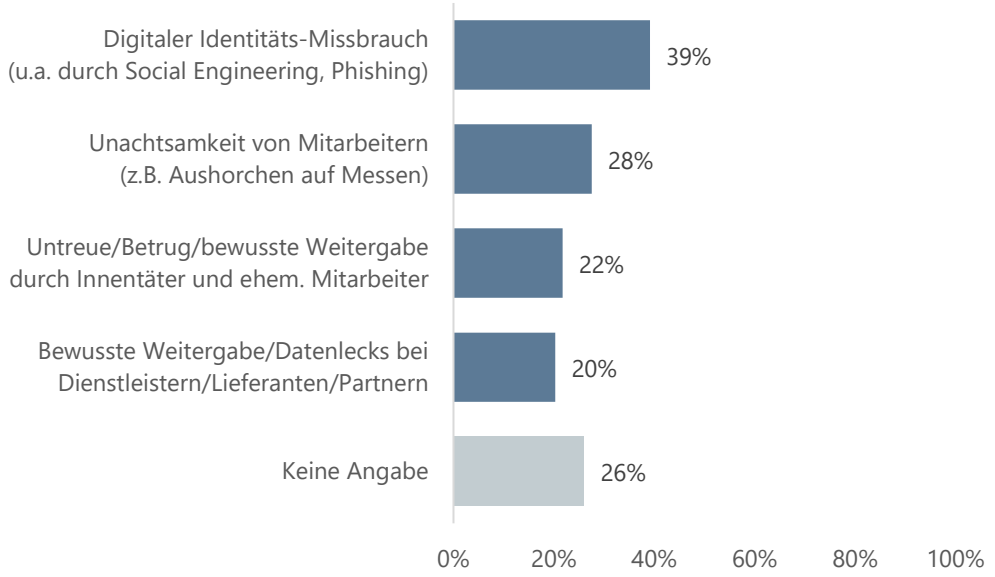
4.2 Gefährdungsfaktoren im Unternehmen

Bei den Zugriffswegen ins Unternehmen können menschliche und technische Gefährdungsfaktoren unterschieden werden.

Menschliche Gefährdungsfaktoren

Der digitale Identitätsmissbrauch, bei dem Mitarbeiter vertrauliche Informationen irrtümlich preisgeben, z. B. durch Social Engineering oder Phishing, wird mit rund 39 Prozent am häufigsten von den betroffenen Unternehmen genannt (vgl. Abb. 12). An zweiter Stelle steht die Unachtsamkeit von Mitarbeitern, die von rund 28 Prozent der betroffenen Unternehmen angegeben wird. Untreue bzw. Betrug von (ehemaligen) Mitarbeitern sowie die bewusste und versehentliche Datenweitergabe bei Dienstleistern und Geschäftspartnern werden von rund einem Fünftel der betroffenen Unternehmen als Zugriffswege ins Unternehmen genannt.

Abb. 12: Menschliche Gefährdungsfaktoren im Unternehmen, in Prozent, 2018



Stichprobe: n=69 Unternehmen mit Vorfällen oder Verdachtsfällen in den letzten vier Jahren. Frage: „Auf welchen Wegen haben Unbefugte Zugriff erhalten?" (Mehrfachnennungen möglich)

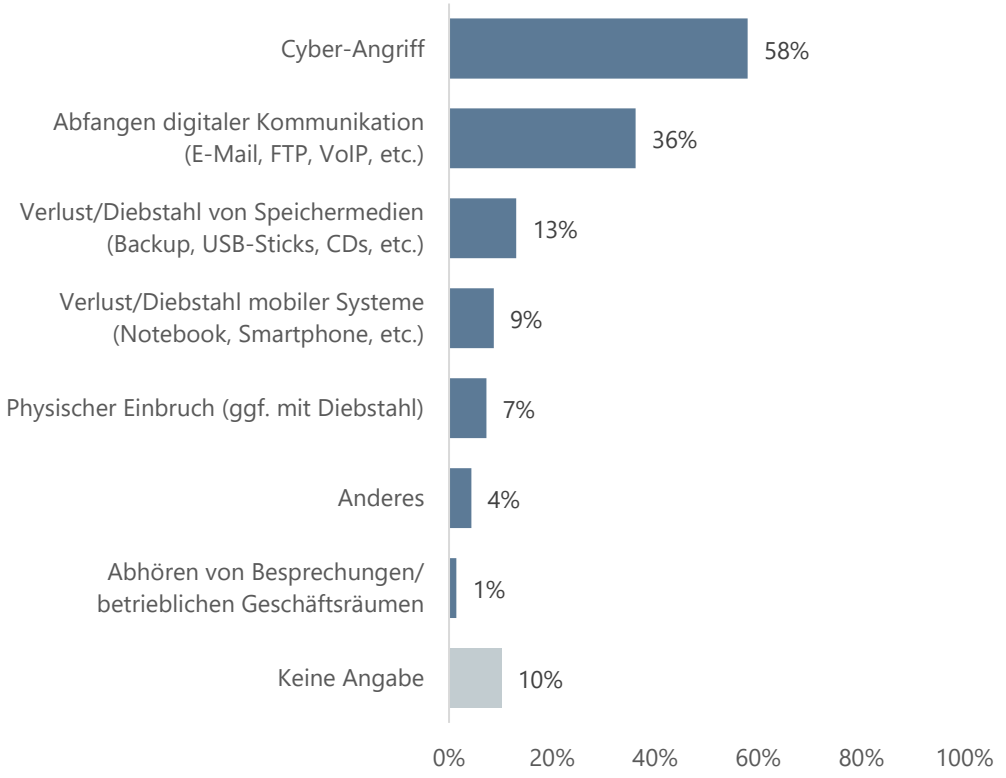
Formen des digitalen Identitätsmissbrauchs (infolge von Social Engineering und Phishing-Attacken) haben klassische Arten der Ausspähung vom Spitzenplatz verdrängt: Während der Innentäter – ein klassischer Gefährdungsfaktor im Unternehmen für Industriespionage – von 22 Prozent der betroffenen Unternehmen genannt wird, werden Formen des digitalen Identitätsmissbrauchs von nahezu doppelt so vielen betroffenen Unternehmen als Gefahrenfaktor benannt (rund 39 Prozent).

Technische Gefährdungsfaktoren

Der mit Abstand häufigste technische Gefährdungsfaktor von Unternehmen sind Cyber-Angriffe: Bei 58 Prozent der betroffenen Unternehmen erfolgte der unbefugte Zugriff auf diesem Weg (vgl. Abb. 13). Das Abfangen digitaler Kommunikation wie Email, FTP, VoIP etc. war bei rund 36 Prozent der befragten Unternehmen die Ursache für einen unbefugten Zugriff. Weiterhin wurde der Verlust und Diebstahl von Speichermedien von 13 Prozent der betroffenen Unternehmen als technischer Zugriffsweg genannt.

Ein Einbruch als Ursache von unbefugten Zugriffen (rund 7 Prozent) oder das Abhören von Besprechungen bzw. betrieblichen Geschäftsräumen (rund 1 Prozent) wurde hingegen nur von wenigen betroffenen Unternehmen als Zugriffsweg genannt.

Abb. 13: Technische Gefährdungsfaktoren im Unternehmen, in Prozent, 2018



Stichprobe: n=69 Unternehmen mit Vorfällen oder Verdachtsfällen in den letzten vier Jahren. Frage: „Auf welchen Wegen haben Unbefugte Zugriff erhalten?" (Mehrfachnennungen möglich)

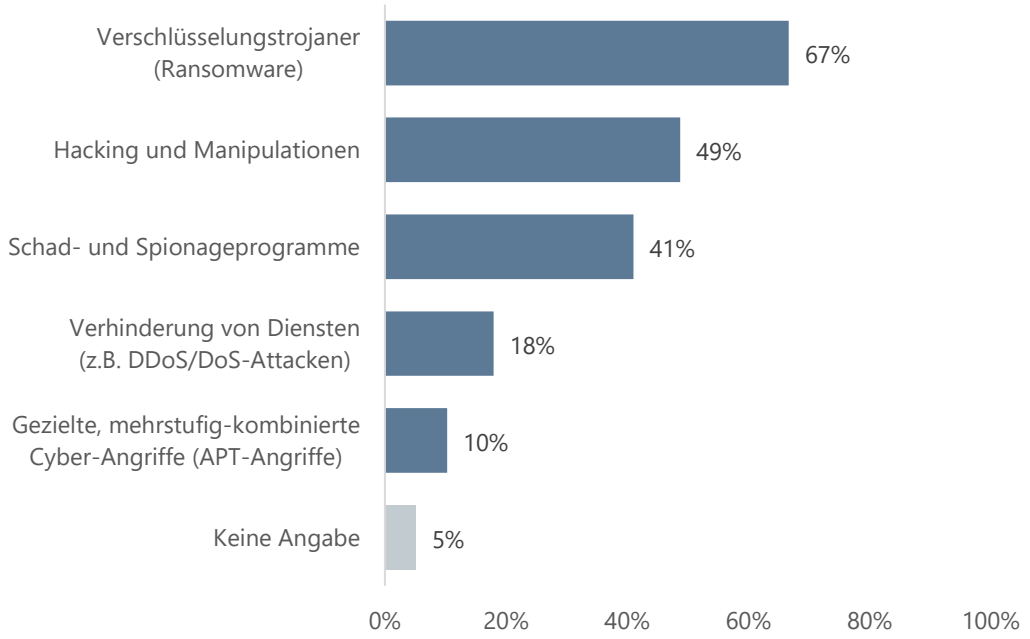
4.3 Cyberangriffe

Zwei Drittel der in den letzten vier Jahren von Cyberangriffen betroffenen Unternehmen (n=40) machen als Ursache vor allem Verschlüsselungstrojaner aus: So geben rund 67 Prozent der betroffenen Unternehmen an, von sogenannter „Ransomware" angegriffen worden zu sein (vgl. Abb. 14). Bei rund 49 Prozent der Unternehmen wurden Angriffe darüber hinaus durch Hacking und Manipulationen durchgeführt. 41 Prozent der von Cyberangriffen betroffenen Unternehmen geben an, dass über Schad- und Spionageprogramme unbefugter Zugang zu Daten erzielt wurde.

Deutlich weniger Unternehmen, rund 18 Prozent, waren von der Verhinderung von Diensten (z. B. DDoS- oder DoS-Attacken) betroffen.

Auch die hoch entwickelten „mehrstufig-kombinierten Cyber-Angriffe" (APT) stellen mittlerweile mehr als nur eine theoretische Gefahr dar: Rund 10 Prozent der von Cyberangriffen betroffenen Unternehmen gaben an, dass sie Ziel von mehrstufig-kombinierten Cyber-Angriffen wurden. Dabei werden APT-Angriffe auch verstärkt durch ausländische Nachrichtendienste vorgenommen. Diese erreichen ein anhaltend hohes qualitatives Niveau und sind aktuell wie künftig eine hohe Gefährdung für die Informationssicherheit. Die Komplexität des Angriffsszenarios wird hierbei ständig verfeinert. Für Betroffene ist es daher immer schwerer, insbesondere staatlich gesteuerte Cyberangriffe rechtzeitig – bzw. überhaupt – zu erkennen.

Abb. 14: Arten von Cyber-Angriffen auf baden-württembergische Unternehmen in den letzten vier Jahren, in Prozent, 2015-2018

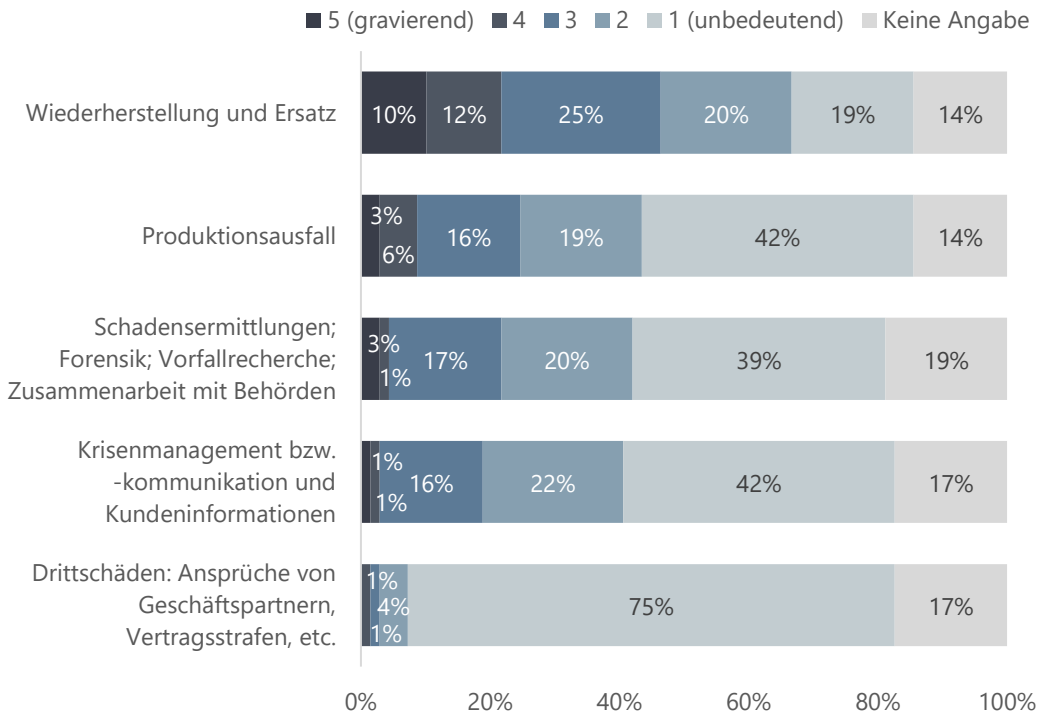


Stichprobe: n=40 Unternehmen, die von Cyber-Angriffen betroffen waren. Frage: „Bitte erläutern Sie, welchen Cyber-Angriffen Sie ausgesetzt waren." (Mehrfachnennungen möglich)

4.4 Schadensausmaß durch unberechtigte Zugriffe

Unberechtigte Zugriffe können zum Teil gravierende Folgen für ein Unternehmen haben: 10 Prozent der Unternehmen mit Vor- und Verdachtsfällen in den letzten vier Jahren (n=69) geben das unmittelbare Schadensausmaß durch die Wiederherstellung bzw. den Ersatz betroffener Systeme als gravierend an, weitere 12 Prozent geben die dadurch unmittelbar entstandenen Wiederherstellungs- bzw. Ersatzkosten als hoch an (vgl. Abb. 15). Die Schäden für Produktionsausfall, Schadensermittlungen, Krisenmanagement und Drittschäden wurden hingegen nur von weniger als 10 Prozent der betroffenen Unternehmen als hoch bzw. gravierend eingestuft. Rund zwei Drittel der Unternehmen klassifizieren das Schadensausmaß in diesen Kategorien als niedrig bzw. als unbedeutend (vgl. Abb. 15).

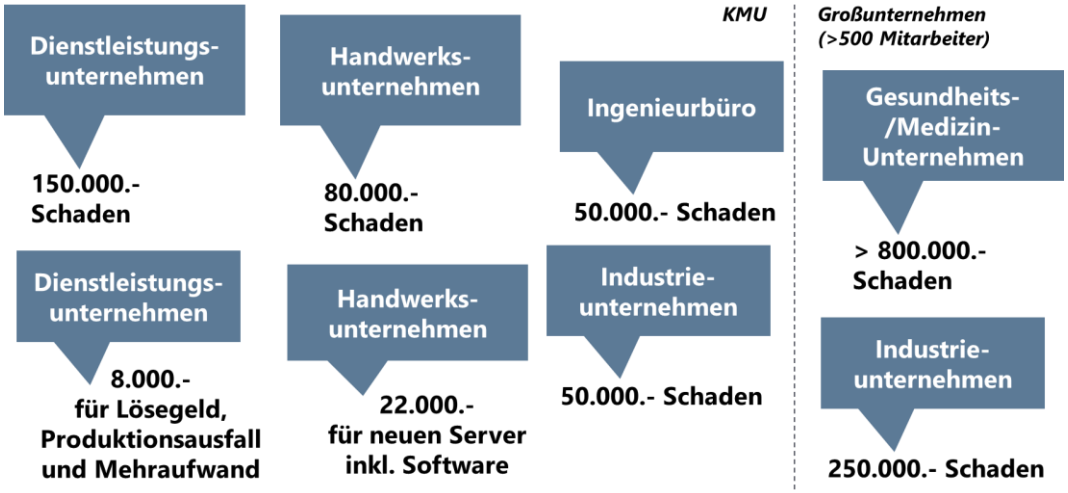
Abb. 15: Ausmaß (Kosten) der unmittelbaren Schäden durch unerlaubte Datenzugriffe, in Prozent, 2018



Stichprobe: n=69 Unternehmen mit Vor- und Verdachtsfällen in den letzten vier Jahren, Skala: 1 (unbedeutend) bis 5 (gravierend). Frage: „Wie bedeutsam waren die unmittelbaren Schäden für Ihr Unternehmen infolge von Know-how-Abflüssen und Ausspähungen in den letzten vier Jahren?"

Zusätzlich zum Schadensausmaß wurden auch absolute Schadenshöhen der Vorfälle mit unerlaubten Datenzugriffen abgefragt. Hierbei zeigte sich, dass sämtliche Branchen von Vorfällen betroffen sind und deren unmittelbare Schäden schnell fünfstellige Summen erreichen können.

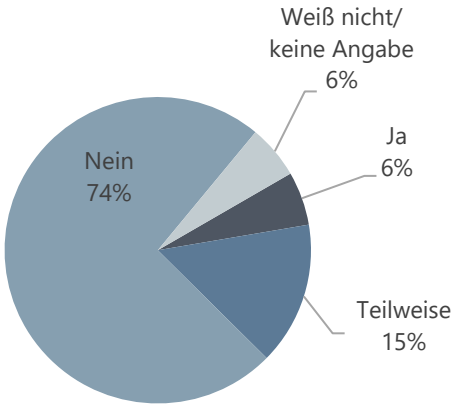
Abb. 16: Individuelle Schadenssummen durch Vorfälle in den letzten vier Jahren (Beispiele betroffener Unternehmen), 2018



Stichprobe: n=31 Unternehmen mit signifikanten, bezifferbaren Schäden aus Vor- und Verdachtsfällen in den letzten vier Jahren. Frage: „Wie hoch schätzen Sie die Summe der unmittelbaren Schäden, die Ihrem Unternehmen aufgrund der eben genannten Vorfälle in den letzten vier Jahren entstanden ist?"

Im mittleren Schadensbereich lagen die gemeldeten Schadenssummen oft zwischen 20.000 und 50.000 Euro – unabhängig von der Größe der betroffenen Unternehmen. Für kleine Unternehmen können daher schon begrenzte Schadensereignisse mit Schadenssummen zwischen 20.000 und 50.000 Euro erhebliche wirtschaftliche Auswirkungen mit sich bringen. Bei Großunternehmen liegen die erhobenen Schadenssummen deutlich höher, so wurde von Schadensereignissen mit 250.000 Euro, bzw. von mehr als 800.000 Euro Schadenssumme berichtet.

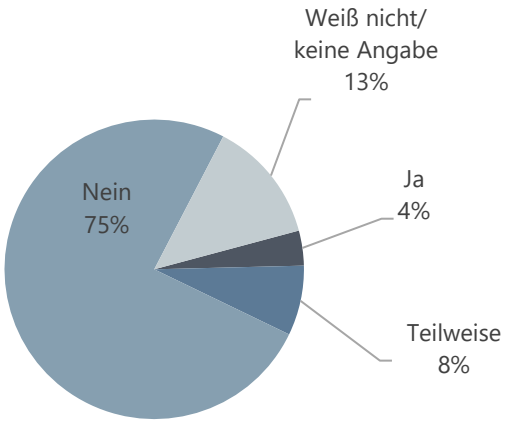
Abb. 17: Durchführung eines internen Schadenscontrolling bei den betroffenen Unternehmen, in Prozent, 2018



Stichprobe: n=53 Unternehmen mit Vor- und Verdachtsfällen in den letzten vier Jahren und bedeutenden unmittelbaren Schäden (=mind. Angabe „3" bei Skala: 1-unbedeutend bis 5-gravierend). Frage: „Wurde ein internes Schadenscontrolling durchgeführt, indem die entstandenen finanziellen Schäden exakt bestimmt wurden?"

Die Bezifferung der Schadenshöhe ist aufgrund eines fehlenden Schadenscontrolling für kaum ein Unternehmen exakt möglich: So führen nur rund 6 Prozent der betroffenen Unternehmen, die unerlaubte Zugriffe auf Daten und bedeutende unmittelbare Schäden verzeichneten (n=53), ein internes Schadenscontrolling durch. Rund 15 Prozent führen teilweise ein internes Schadenscontrolling durch, während mit rund 74 Prozent der Großteil der betroffenen Unternehmen kein internes Schadenscontrolling durchführt.

Abb. 18: Getätigte Schadensmeldung an eine Versicherung bei den betroffenen Unternehmen, in Prozent, 2018



Stichprobe: n=53 Unternehmen mit Vor- und Verdachtsfällen in den letzten vier Jahren und bedeutenden unmittelbaren Schäden (=mind. Angabe „3" bei Skala: 1-unbedeutend bis 5-gravierend). Frage: „Wurden entstandene Schäden der Versicherung gemeldet?"

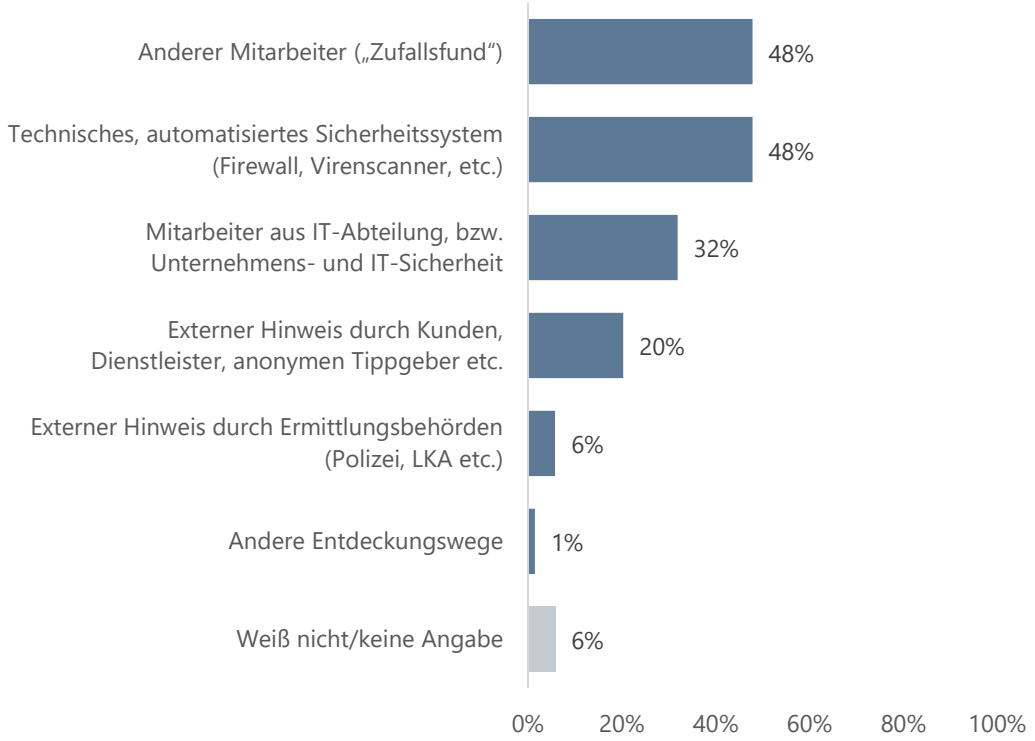
Auch werden Schäden nur in wenigen Fällen zur Regulierung an eine Versicherung gemeldet (vgl. Abb. 18). Rund vier Prozent der betroffenen Unternehmen (n=53) gaben an, dass sie ihre entstandenen Schäden ihrer Versicherung gemeldet haben, weitere rund acht Prozent der Unternehmen gaben an, dass sie Schäden zumindest teilweise an ihre Versicherung meldeten. Rund 76 Prozent der betroffenen Unternehmen gaben an, dass sie keine Schadensmeldung an ihre Versicherung abgegeben haben. Allerdings muss bei diesen Ergebnissen berücksichtigt werden, das Cyber-Versicherungen eine noch verhältnismäßig junge Versicherungssparte darstellen und nicht alle Unternehmen über entsprechende Policen verfügen.

4.5 Deliktverfolgung und Täterattribution

Die befragten Unternehmen mit Vor- oder Verdachtsfällen (n=69) gaben an, dass unberechtigte Zugriffe auf schutzwürdige Daten in rund 48 Prozent der Fälle eher zufällig durch Mitarbeiter entdeckt werden (vgl. Abb. 19). In gleichem Umfang gaben die befragten Unternehmen mit Vor- oder Verdachtsfällen an, dass Zugriffe über technische, automatisierte Sicherheitssysteme wie Firewalls oder Virenscanner erkannt wurden (48 Prozent).

Mitarbeiter aus der IT-Abteilung bzw. der Unternehmens- und IT-Sicherheit werden von rund 32 Prozent der betroffenen Unternehmen als Entdecker von unberechtigten Zugriffen angegeben, während externe Hinweise durch Kunden, Dienstleister oder anonyme Tippgeber nur bei rund 20 Prozent der Unternehmen zur Entdeckung des Angriffs beitrugen. Externe Hinweise durch Ermittlungsbehörden führten bei sechs Prozent der befragten Unternehmen zur Aufdeckung eines Angriffs, die anderenfalls unentdeckt geblieben wären.

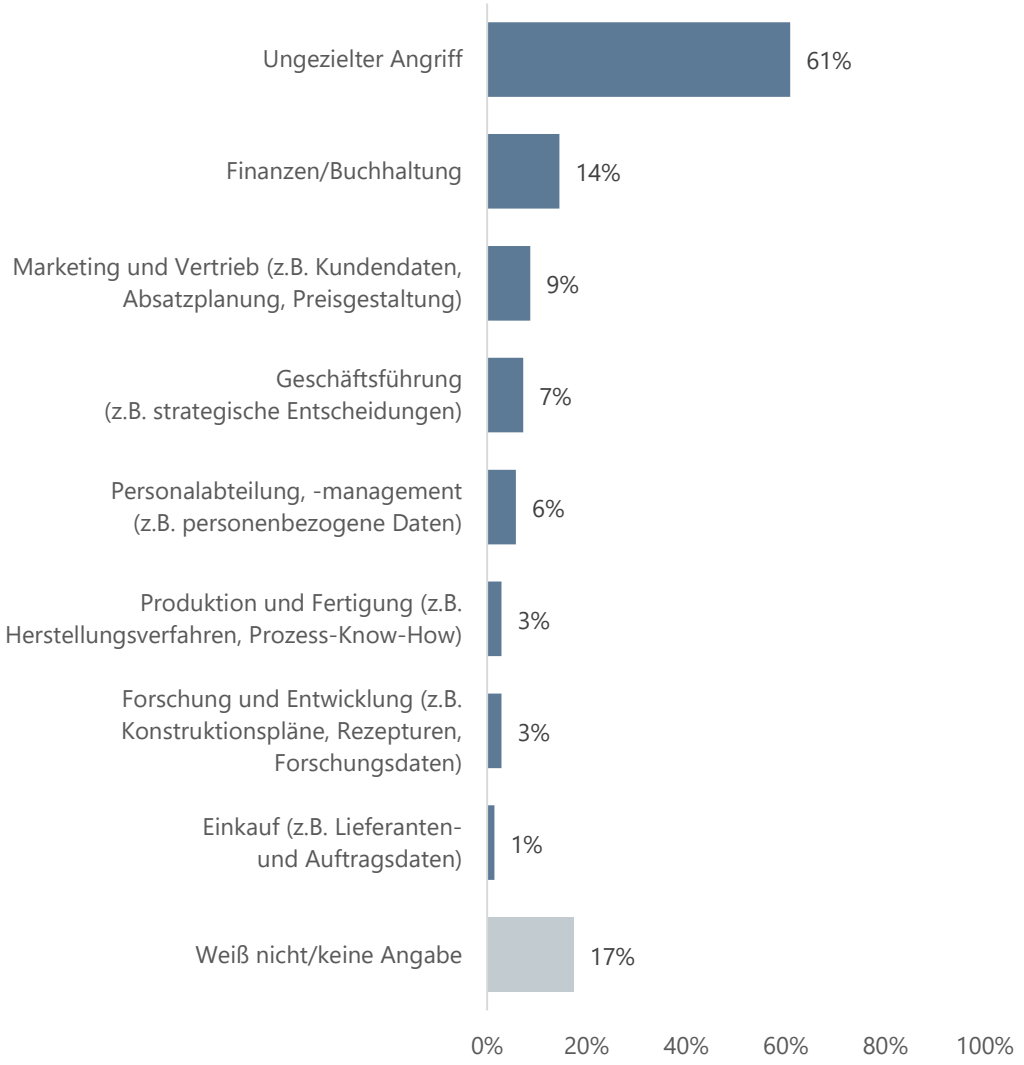
Abb. 19: Entdeckung des Angriffs, in Prozent, 2018



Stichprobe: n=69 Unternehmen mit Vorfällen oder Verdachtsfällen in den letzten vier Jahren. Frage: „Wie bzw. durch wen wurden die Angriffe zunächst entdeckt?" (Mehrfachnennungen möglich)

Am häufigsten mit rund 61 Prozent wird von den betroffenen Unternehmen angegeben, dass Angriffe keinem bestimmten Bereich galten, sondern es sich um ungezielte Angriffe auf das Unternehmen handelte (vgl. Abb. 20). Bei gezielten Angriffen wurde am häufigsten der Bereich Finanzen/Buchhaltung mit rund 15 Prozent angegeben. Weitere aufgeführte Bereiche wie Marketing und Vertrieb oder die Geschäftsführung wurden jeweils nur von unter 10 Prozent der betroffenen Unternehmen genannt.

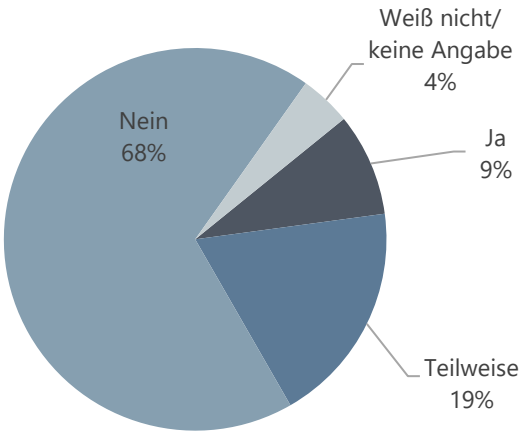
Abb. 20: Angegriffener Bereich im Unternehmen, in Prozent, 2018



Stichprobe: n=69 Unternehmen mit Vorfällen oder Verdachtsfällen in den letzten vier Jahren. Frage: „Wurde ein bestimmter Bereich innerhalb des Unternehmens angegriffen?" (Mehrfachnennungen möglich)

Die Täter bzw. Verursacher der Vorfälle sind rund 68 Prozent der betroffenen Unternehmen unbekannt. In rund 19 Prozent sind die Täter den betroffenen Unternehmen teilweise bekannt. Lediglich bei rund neun Prozent der Unternehmen sind die Täter bzw. Verursacher der Vorfälle bekannt oder es gibt konkrete Vermutungen zu den Tätern.

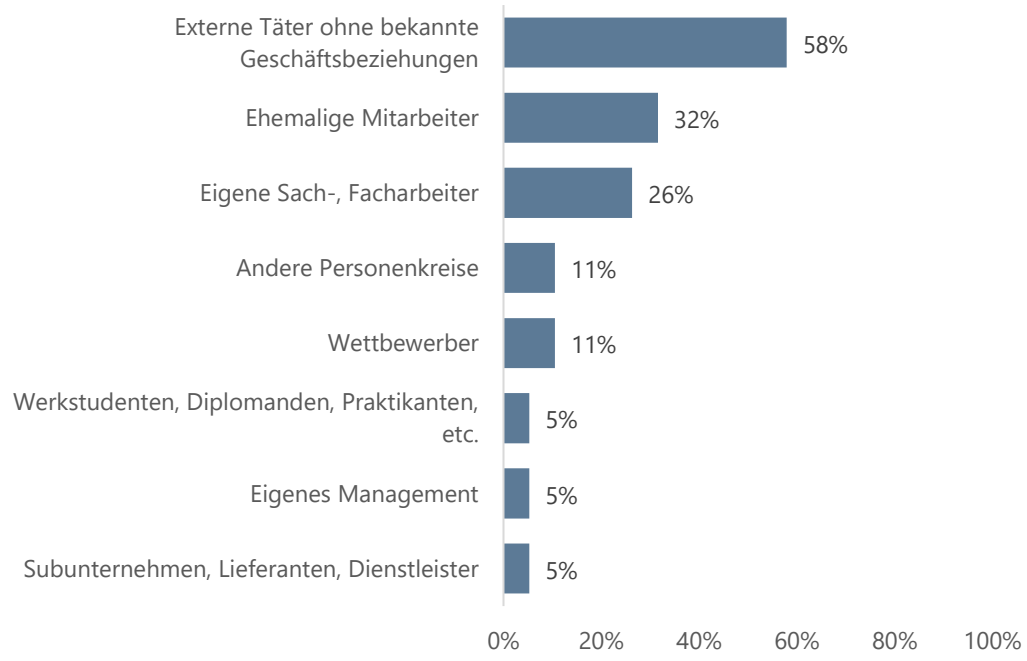
Abb. 21: Bekanntheit der Täter bzw. Verursacher der Vorfälle, in Prozent, 2018



Stichprobe: n=69 Unternehmen mit Vorfällen oder Verdachtsfällen in den letzten vier Jahren. Frage: „Sind die Täter bzw. Verursacher bekannt oder gab es konkrete Vermutungen?"

Bei den Tätern, deren Identität ermittelt werden konnte, handelt es sich mit 58 Prozent häufig um externe Täter ohne eine bekannte Geschäftsbeziehung (vgl. Abb. 22). Die Täter mit (ehemaliger) Geschäftsbeziehung kommen in Summe auf 74 Prozent der Nennungen: Ehemalige Mitarbeiter werden von rund 32 Prozent und eigene Sach- und Facharbeiter von rund 26 Prozent der Unternehmen (n=20) als Täter aufgeführt. Das eigene Management wird von rund fünf Prozent der befragten Unternehmen als Personenkreis der Täter genannt. Werkstudenten, Diplomanden oder Praktikanten sowie Subunternehmen, Lieferungen und Dienstleiter fallen mit je fünf Prozent ebenfalls unter den bekannten Personenkreis der Täter.

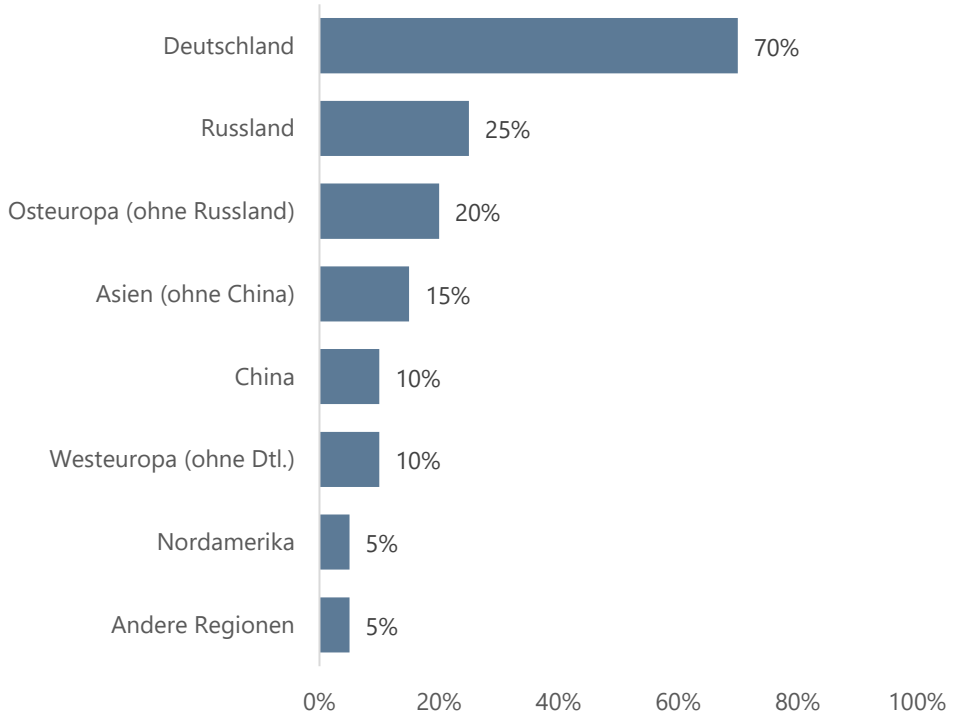
Abb. 22: Personenkreis der Täter, in Prozent, 2018



Stichprobe: n=20 Unternehmen, denen die Täter bzw. Verursacher (teilweise) bekannt sind. Frage: „Aus welchen Personenkreisen stammen die bekannten Täter bzw. Verursacher?" (Mehrfachnennungen möglich)

Zu den externen Tätern mit bekannten Geschäftsbeziehungen zählen mit rund elf Prozent Wettbewerber des Unternehmens sowie mit rund fünf Prozent Subunternehmen, Lieferanten und Dienstleister.

Abb. 23: Herkunft der Täter, in Prozent, 2018



Stichprobe: n=20 Unternehmen, denen die Täter bzw. Verursacher (teilweise) bekannt sind. Frage: „Aus welchen Regionen kamen die Ihnen bekannten Täter bzw. Verursacher?" (Mehrfachnennungen möglich)

Von den Unternehmen, denen die Täter bzw. Verursacher der Vorfälle bekannt sind (n=20), nennen 70 Prozent Deutschland als das Herkunftsland der Täter bzw. des unbefugten Datenzugriffs (vgl. Abb. 23). Russland und Osteuropa werden mit 25 bzw. 20 Prozent als häufigster ausländischer Herkunftsort genannt. China und die westeuropäischen Länder sind nach Angaben der betroffenen Unternehmen jeweils in zehn Prozent der Fälle das Herkunftsland. Nordamerika und andere Regionen sind mit jeweils fünf Prozent eher selten für Angriffe verantwortlich.

5 Handlungsempfehlungen

Die Befragungsergebnisse haben eine Reihe von Präventions- und Sicherheitsmaßnahmen aufgezeigt, bei denen noch Optimierungspotenziale bestehen, um baden-württembergische Unternehmen im Hinblick auf alte und neue Herausforderungen durch Ausspähungen, Know-how-Abflüsse und Datenmanipulationen besser zu schützen.

Zudem konnten Unternehmen ihre eigenen Wünsche und Unterstützungsbedarfe innerhalb der Befragung artikulieren, so dass in der Zusammenschau der verschiedenen Teile der Befragung eine Reihe von Handlungsempfehlungen entstanden sind, um insbesondere kleine und mittlere Unternehmen künftig zielgenauer vor den Gefahren für die IT-Sicherheit zu informieren. Die folgende Abbildung (vgl. Abb. 24) gewährt eine Übersicht über die aus der Befragung resultierenden Handlungsempfehlungen, die anschließend näher ausgeführt werden.

Abb. 24: Übersicht über die Handlungsempfehlungen

Ergebnis aus SiFo-Befragung 2018/19	Handlungsempfehlung
• Meist gewünschtes Unterstützungsangebot: Leitfäden zur IT- und Unternehmenssicherheit	➢ Bereitstellung von Leitfäden über Kammern, Verbände und regional verankerten Initiativen
• Mangelnde Awareness für Gefährdungsfaktoren, insbesondere Phishing und Social Engineering	➢ Erstellung von Schulungskonzepten, Durchführung von Schulungen zur Mitarbeiter-Awareness
• Unterschätztes Risiko: Abfangen digitaler Kommunikation	➢ Gezielte Beratung zur verschlüsselten Kommunikation (z.B. E-Mail)
• Bislang kaum systematische Überwachung des Netzwerkverkehrs in Unternehmen vorhanden	➢ Sensibilisierung „Netzwerk-Monitoring" v.a. über Branchenverbände und Allianz 4.0

Praxisorientierte Leitfäden

Am häufigsten wurde der Wunsch nach **Leitfäden zur IT- und Unternehmenssicherheit** geäußert (vgl. Abb. 7). Obwohl es bereits eine Reihe von allgemein verständlichen Sicherheitsratgebern von Organisationen und Sicherheitsinitiativen gibt (etwa vom Bundesamt für Sicherheit in der Informationstechnik oder der Allianz für Sicherheit in der Wirtschaft), scheinen diese die Informationsbedürfnisse der Unternehmen noch nicht hinreichend zu befriedigen.

Die Ergebnisse der Befragung legen nahe, dass die Existenz dieser Ratgeber in der Praxis nicht genügend bekannt ist, da vor allem Informationen zu IT-Sicherheitsthemen über Kammern und Branchenverbände rezipiert werden. Spezialisierte Angebote zur IT-Sicherheit richten sich tendenziell eher an größere Unternehmen mit entsprechendem Fachpersonal und werden dementsprechend nur von einem kleinen Teil der Unternehmen aktiv genutzt.

Um dem Wunsch nach allgemein verständlichen Sicherheitsratgebern nachzukommen, veröffentlicht das Sicherheitsforum Baden-Württemberg gemeinsam mit dieser Studie einen exemplarischen Leitfaden zur IT-Sicherheit, das „IT-Schutzkonzept", mit Orientierungshilfen

und Handlungsempfehlungen für kleine und mittlere Unternehmen zum Schutz vor Informationsabflüssen und Wirtschaftsspionage.

Schulungen zur Mitarbeiter-Awareness

Der Anwender ist oftmals das schwächste Glied der firmeneigenen Absicherung, insofern stellt **der Anwender oftmals das einfachste Angriffsziel** dar. Der digitale Identitätsmissbrauch ist dabei zum größten menschlichen Gefährdungsfaktor aufgestiegen, insbesondere durch ungezielte Angriffe wie etwa Phishing-Attacken (vgl. Abb. 12). Eine umfassende Betrachtung der IT-Sicherheit im Unternehmen muss daher vor allem beim Anwender ansetzen. Wie die Ergebnisse der Befragung zeigen, teilen auch viele Unternehmen diese Einschätzung (vgl. Abb. 7).

Regelmäßige Maßnahmen zur Mitarbeiter-Awareness sind jedoch weiterhin eher eine Ausnahme im Unternehmensalltag. Das Innenministerium unterstützt Unternehmen in Baden-Württemberg bereits durch die Cyberwehr BW. Über diese bekommen kleine und mittlere Unternehmen in IT-Notfallsituationen Unterstützung von zertifizierten Personen aus der Privatwirtschaft.

Zusätzlich bietet die Cyberwehr BW auch Schulungen zu Sensibilisierungsmaßnahmen an, die sich speziell an kleine und mittlere Unternehmen sowie Handwerksbetriebe in Baden-Württemberg richten. In verschiedenen Schulungen kann hier der Umgang mit den Bedrohungen erprobt werden. Diese Sensibilisierungsmaßnahmen können nach entsprechender Anleitung auch betriebsintern verstetigt werden.

Verschlüsselte Kommunikation

Ein überraschendes Ergebnis der Befragung war, wie häufig das Abfangen digitaler Kommunikation Ausgangspunkt für unbefugte Zugriffe auf Unternehmensinterna ist (vgl. Abb. 13). **Digitale Kommunikation ist in vielen Fällen unverschlüsselt und leicht einsehbar**, bestes Beispiel dafür ist die klassische E-Mail. Obwohl es zahlreiche komfortable kommerzielle Lösungen am Markt gibt, wird E-Mailverschlüsselung, oftmals zu Unrecht, als komplexe, wenig praxisgerechte Nischenanwendung wahrgenommen.

Insbesondere durch **die fortschreitende Entwicklung hin zu dynamischen Wertschöpfungsnetzwerken** nimmt die Bedeutung von verschlüsselter Kommunikation zu. IT-Sicherheit muss in der digital vernetzten Produktion nicht nur im eigenen Unternehmen, sondern innerhalb des gesamten Wertschöpfungsnetzwerkes sichergestellt werden.

Gerade kleine und mittlere Unternehmen fühlen sich mit der Problemlage oft überfordert, da IT-Sicherheit nicht durch einzelne Investitionen oder Maßnahmen, sondern nur durch ganze Maßnahmenbündel, die über die Anschaffung neuer Anlagen hinausgehen, erreicht werden kann. Für kleine und mittlere Unternehmen empfiehlt sich daher die Inanspruchnahme einer geförderten **Vor-Ort-Beratung, in der ein Sicherheitsberater im Rahmen einer geförderten Erstberatung** eine Begehung im Unternehmen vornimmt und das Ergebnis mit der Unternehmensleitung und seinem Sicherheits- bzw. IT-Dienstleister bespricht.

Eine solche Beratung ist zum Beispiel durch das Förderprogramm „go-digital" des Bundesministerium für Wirtschaft und Energie möglich. Darüber hinaus finanziert go-digital auch Maßnahmen, mit denen Unternehmen sich vor dem Verlust sensibler Daten schützen können, wie zum Beispiel der E-Mail-Verschlüsselung.

Fehlende Netzwerküberwachung

Auf eklatante Weise wurde in den Ergebnissen der Studie deutlich, wie hoch die Dunkelziffer unbefugter Zugriffe ist (vgl. Abb. 11). Je nach Unternehmensgröße konnte ein Drittel bis zu mehr als die Hälfte der von unbefugten Zugriffen betroffenen Unternehmen nicht quantifizieren, wie oft es in den vergangenen vier Jahren zu unbefugten Zugriffen durch Ausspähungen, Know-how-Abflüsse und Datenmanipulationen gekommen ist. Ein wesentlicher Grund hierfür liegt in **mangelnden IT-Systemen, die systematisch die Zugriffe und Datenverkehre innerhalb des Netzwerks überwachen**. Solche Netzwerk-Monitoring-Systeme (IDS/IPS-Systeme) sind nur in rund einem Viertel der befragten Industrieunternehmen durchgängig vorhanden. In Anbetracht der zunehmenden Vernetzung von Produktionsanlagen und der bevorstehenden Revolution durch die Industrie 4.0 ist dies ein alarmierend niedriger Wert.

Ein wesentlicher Grund, warum es Unternehmen generell schwerfällt, die Gefahrenlage durch Cyber-Angriffe realistisch einzuordnen, und Bedrohungen unterschätzt, aber teilweise auch überschätzt werden, sind vor allem **fehlende eigene Erfahrungswerte**. Professionelle IT-Sicherheitstools können einen wesentlichen Beitrag dazu leisten, dass Unternehmen ihre eigene Exposition und ihr eigenes Sicherheitsrisiko wesentlich besser einschätzen lernen.

Insofern empfehlen wir die aktive Beteiligung an **Sensibilisierungskampagnen** für Unternehmen, die gezielt auf die Bedeutung des Netzwerk-Monitorings abstellen. Da diese Maßnahmen vor allem Know-how-starke Branchen und Unternehmen betreffen, sollten vor allem die entsprechenden **Branchenverbände, landesweiten Netzwerke und regionalen Cluster-Initiativen** angesprochen werden.

Maßnahmen zur Kommunikationsverschlüsselung bzw. zur Netzwerküberwachung können über die **bereits bestehenden Förderprogramme** des Bundes und des Landes Baden-Württemberg gefördert werden. Hierzu zählt die **Digitalisierungsprämie**, mit der u.a. die Implementierung eines IT- oder Datensicherheitskonzepts in Unternehmen finanziell unterstützt werden kann.

6 Fazit

Die Befragung der gezogenen Stichprobe baden-württembergischer Unternehmen (n=423) zu Ausspähungen, Know-how-Abflüssen und Datenmanipulationen brachte folgende wesentlichen Ergebnisse hervor:

Präventions- und Sicherheitsmaßnahmen

Der strategische Stellenwert, den Unternehmen Präventions- und Sicherheitsmaßnahmen beimessen, ist in den letzten vier Jahren deutlich gestiegen: Über 60 Prozent der Unternehmen geben an, dass ihre Investitionen in Präventions- und Sicherheitsmaßnahmen leicht bzw. stark zugenommen haben.

Ein **Firewall-System** ist dabei der etablierte technische Mindeststandard. Mit rund 98 Prozent geben nahezu alle befragten Unternehmen an, dass in ihren Unternehmen durchgängig oder teilweise ein Firewall-System vorhanden ist.

Weit verbreitet sind zudem **vertragliche Regelungen zum Vertraulichkeitsschutz.** Unternehmensrichtlinien zum Umgang mit sensiblen Daten werden in rund zwei Dritteln der befragten Unternehmen eingesetzt, Arbeitsverträge mit Wettbewerbs- und Geheimhaltungsklauseln sogar in knapp drei Vierteln der Unternehmen. Von aufwendigeren (und kostenintensiveren) Maßnahmen, wie etwa Risikoanalysen und Personal-Screenings, macht hingegen nur ein gutes Drittel der Unternehmen Gebrauch.

Ein weiteres Ergebnis der Befragung ist, dass vor allem physische (IT-)Sicherheitsvorkehrungen, wie z. B. besonders gesicherte Serverbereiche, stark verbreitet sind, digitale Sicherheitsvorkehrungen dahinter jedoch deutlich zurückfallen: Nur rund ein Viertel der befragten Industrieunternehmen verfügt über **ein durchgehendes Netzwerk-Monitoring** mit Intrusion-Detection bzw. -Prevention-Systemen (26 Prozent).

Künftige Risiken und Unterstützungsbedarfe

Die baden-württembergischen Unternehmen sehen vor allem **in ungezielten technischen Angriffen ein hohes Angriffsrisiko** für die eigenen Geschäfts- und Betriebsgeheimnisse (41 Prozent). Das Angriffsrisiko durch eigene Mitarbeiter wird hingegen deutlich geringer eingeschätzt (10 Prozent).

Von den befragten Unternehmen wird die **zunehmende interne und externe Vernetzung von Produktionsanlagen als größte künftige Herausforderung** im Kontext der Digitalen Transformation benannt.

Es fehlt den Unternehmen demnach nicht an Problembewusstsein für die Gefährdungslage durch Cyber-Angriffe, stattdessen herrscht **ein Mangel an praxisbezogenen Kenntnissen** geeigneter Präventions- und Schutzmaßnahmen, um ein befriedigendes Schutzniveau für das Unternehmen zu erreichen.

Das zeigt auch das **große Interesse an praktischen Leitfäden zur IT- und Unternehmenssicherheit**: Rund 69 Prozent der Unternehmen formulieren den Wunsch nach strukturierten Informationen zur praktischen Umsetzung von IT- und Unternehmenssicherheit im Unternehmen (Best Practices, Stand der Technik, usw.).

Fall- und Schadensanalyse

Rund **16 Prozent aller befragten Unternehmen** in Baden-Württemberg geben an, dass sie in den letzten vier Jahren **unbefugte Zugriffe auf schutzwürdige Daten** des Unternehmens verzeichnet haben oder vermuten – das ist jedes sechste Unternehmen. Großunternehmen sind mit rund 23 Prozent deutlich stärker von Zugriffs- und Verdachtsfällen betroffen als kleine und mittlere Unternehmen.

Herausforderung Detektion

Ein großes Problem bei unbefugten Zugriffen ist deren Detektion. **36 Prozent** der befragten Unternehmen, die innerhalb der letzten vier Jahre unbefugte Zugriffe verzeichneten oder vermuteten (n=69), **können die Anzahl der Vor- und Verdachtsfälle nicht beziffern**. Bei Unternehmen mittlerer Größe (50-249 Mitarbeiter) stellt die Detektion von Datenabzügen und Datenmanipulationen ein besonders großes Problem dar: Mehr als die Hälfte der betroffenen Unternehmen (55 Prozent) kann keine Angaben zur Häufigkeit der geschehenen unbefugten Zugriffe machen. An dieser Stelle zeigen sich die Folgen der Defizite, welche die Befragung bei der Ausstattung mit Netzwerküberwachungstechnik zuvor offengelegt hat (vgl. Abschnitt Präventions- und Sicherheitsmaßnahmen).

Unberechtigte Zugriffe auf schutzwürdige Daten im Unternehmen werden **in rund 48 Prozent der Fälle eher zufällig durch Mitarbeiter entdeckt**. Gleich häufig (48%) geben die Unternehmen mit Vor- oder Verdachtsfällen an, dass unbefugte Zugriffe über technische, automatisierte Sicherheitssysteme wie Firewalls oder Virenscanner erkannt wurden.

Gefährdungsfaktor Mensch

Besonders häufig geschehen unbefugte Zugriffe infolge **eines digitalen Identitätsmissbrauchs**, bei dem Mitarbeiter vertrauliche Informationen irrtümlich preisgeben, z. B. durch Social Engineering oder Phishing. 39 Prozent der betroffenen Unternehmen geben an, dass ein digitaler Identitätsmissbrauch bereits Ursache eines unbefugten Zugriffes gewesen ist. Zum Vergleich: Der Innentäter wurde von 22 Prozent der betroffenen Unternehmen als Ursache eines Vor- oder Verdachtsfalles genannt.

Täter im Verborgenen

Im Allgemeinen können die Täter bzw. Verursacher unbefugter Zugriffe in **68 Prozent der betroffenen Unternehmen nicht ermittelt werden**. Selbst bei den Unternehmen, die Kenntnis über die Täter erlangen konnten, handelt es sich mehrheitlich (58%) um externe Täter ohne bekannte Geschäftsbeziehungen.

Zum Teil gravierendes Schadensausmaß

Unberechtigte Zugriffe können zum Teil gravierende Folgen für ein Unternehmen haben: **10 Prozent der Unternehmen geben das unmittelbare Schadensausmaß** durch die Wiederherstellung bzw. den Ersatz der betroffenen Systeme **als gravierend an**, weitere 12 Prozent der Unternehmen mit Vor- und Verdachtsfällen in den letzten vier Jahren geben den dadurch unmittelbar entstandenen Schaden als hoch an. Die erhobenen Schadenssummen lagen auch bei kleinen Unternehmen mit weniger als 50 Mitarbeitern oftmals im mittleren fünfstelligen Bereich, unabhängig von der Branchenzugehörigkeit. Großunternehmen berichteten von sechsstelligen Schadenssummen aus Vorfällen mit unbefugten Zugriffen.

Schäden werden nur selten systematisch erfasst

Die Bezifferung der exakten Schadenshöhe ist aufgrund eines fehlenden Schadenscontrolling leider kaum einem Unternehmen möglich: So führen nur rund 21 Prozent der betroffenen Unternehmen, die unerlaubte Zugriffe auf Daten und bedeutende unmittelbare Schäden verzeichneten (n=53), wenigstens teilweise ein Schadenscontrolling durch, während mit **rund 74 Prozent der Großteil der betroffenen Unternehmen kein Schadenscontrolling durchführt**. Nur ein Bruchteil der Unternehmen (4%), die unerlaubte Zugriffe auf Daten und bedeutende unmittelbare Schäden verzeichneten, meldete daraus entstandene Schäden ihrer Versicherung.

7 Abbildungsverzeichnis

8 Tabellenverzeichnis

9 Glossar

APT (Advanced Persistence Threats)	sind zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.
Cloud-Computing	stellt die Nutzung von nicht-lokalen Diensten oder einer IT-Infrastruktur über das Internet dar.
Cyber-Angriff	ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.
Datenabzug	ist ein unbefugter Zugriff und Diebstahl schutzwürdiger Unternehmensdaten.
Datenmanipulation	ist die Veränderung von schutzwürdigen Unternehmensdaten durch das Hinzufügen, Abwandeln oder Löschen von Elementen.
DDoS (Distributed Denial of Service) – bzw. DoS (Denial of Service)-Attacken	sind Verfahren, bei denen Server gezielt mit so vielen Anfragen überlastet werden, bis die Server die Aufgaben nicht mehr bewältigen können und im schlimmsten Fall zusammenbrechen. Bei den so genannten "verteilten DoS-Attacken" kommen anstelle von einzelnen angreifenden Systemen eine Vielzahl von unterschiedlichen Systemen in großflächig koordinierten Angriffen zum Einsatz. Durch die hohe Anzahl der gleichzeitig angreifenden Systeme sind die Angriffe besonders wirksam.
Digitale Transformation	beschreibt die fortlaufenden Veränderungsprozesse der Gesellschaft und der Wirtschaft durch den vermehrten Einsatz von digitalen Technologien.
Digitaler Identitätsmissbrauch	ist die missbräuchliche Nutzung personenbezogener Daten im Internet.
Firewall-System	ist ein Programm, das vor unberechtigten Zugriff schützt.
FTP (File Transfer Protocol)	ist ein Netzwerkprotokoll zur Übertragung von Dateien über IP-Netzwerke.
GnuPG (GNU Privacy Guard)/ PGP (Pretty Good Privacy)	ist eine Software, die verwendet werden kann, um Daten zu verschlüsseln und elektronisch zu signieren. Oft wird GnuPG/ PGP benutzt, um E-Mails zu verschlüsseln. Es wird ein asymmetrisches Public-Key-Verfahren verwendet, um die Nachrichten zu verschlüsseln bzw. wieder zu entschlüsseln.
Hardware-Token	fungieren ähnlich wie eine Schlüsseldatei zur Authentisierung. Allerdings ist ein Hardware-Token eine Hardwarekomponente, meist in Form eines USB-Sticks.
Industrie 4.0	beschreibt die Verzahnung der Produktion mit modernster Informations- und Kommunikationstechnik und ermöglicht bspw. eine stärker nach individuellen Kundenwünschen ausgerichtete Produktion.

Intrusion-Detection-Systeme	dienen der Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind (auch „Angriffserkennungssysteme“).
Intrusion-Prevention-Systeme	sind Intrusion-Detection-Systeme, die über die Generierung von Ereignissen (Events) hinaus Funktionen bereitstellen, die einen entdeckten Angriff abwehren können.
IoT (Internet of Things)	beschreibt die die Vernetzung physischer und virtueller Gegenstände über das Internet.
ISMS (Information Security Management System)	definiert Regeln und Methoden, um die Informationssicherheit in Unternehmen und Organisationen zu gewährleisten.
ISO 270001	ist eine internationale Norm, die Anforderungen für ein dokumentiertes Informationssicherheits-Managementsystem unter Berücksichtigung des Kontexts eines Unternehmens spezifiziert.
Know-how-Abflüsse	beschreiben den Verlust von schutzwürdigem Wissen und Erfahrungen eines Unternehmens.
Konkurrenzausspähung (ugs. „Industriespionage“)	beschreibt die Ausforschung eines Unternehmens durch einen Wettbewerber.
Maschine-zu-Maschine-Kommunikation (M2M)	ist der automatische Informations- und Datenaustausch zwischen Maschinen und Anlagen.
Mitarbeiter-Awareness	ist die Sensibilisierung der Mitarbeiter für Gefahren der IT-Sicherheit.
Netzwerk-Monitoring	ist ein Teilbereich des Netzwerk-Managements und überwacht die verschiedenen Komponenten, Ereignisse und Protokolle eines Netzwerks sowie seiner bereitgestellten Services.
Penetrationstest	ist ein Verfahren zur Überprüfung von Schwachstellen eines IT-Systems. Beim Penetrationstest werden die Erfolgsaussichten vorsätzlicher Angriffe durch die Überprüfung der Schnittstellen des IT-Systems nach außen eingeschätzt.
Personal-Screening	ist ein Testverfahren zur Beurteilung des Risikopotenzials von Mitarbeitern.
Phishing	ist ein Verfahren, mit dem Cyberkriminelle versuchen, Nutzer auf betrügerische Weise zu verleiten, Passwörter oder Nummern von Kreditkarten, Sozialversicherungen oder Bankkonten preiszugeben. Es werden gefälschte E-Mails versendet oder Nutzer werden auf eine gefälschte Website umgeleitet.
Präventions- und Sicherheitsmaßnahmen	sind Vorkehrungen zum Schutz vor unerwünschten Vorfällen.
Ransomware	verschlüsselt den Speicher des Gerätes und fordert Lösegeld, um diesen Zustand zurückzusetzen.
Risikoanalyse	ist eine systematische Analyse zur Identifikation und Quantifizierung von Risiken.
S/MIME (Secure/Multipurpose Internet Mail Extensions)	ist ein Standard zum Verschlüsseln und Signieren von Dateien anhand von digitalen und zentral ausgestellten Zertifikaten.
Schadenscontrolling	dient der exakten Bestimmung der finanziellen Schäden.
SIEM (Security Information and Event Management)	ist eine Kombination aus dem Security Information Management (SIM) und dem Security Event Management (SEM). Das

	SIM sammelt und speichert Daten und erstellt daraus Berichte, während das SEM neben der Sammlung und Korrelation von Daten auch nach definierten Kriterien den Nutzer alarmiert. Das SIEM vereint die genannten Funktionen innerhalb eines Produktes.
Social Engineering	beschreibt die zwischenmenschliche Beeinflussung von Personen, um diese so für die eigenen Zwecke zu instrumentalisieren.
VPN (Virtual Private Network)	sind in sich geschlossene virtuelle Kommunikationsnetzwerke, welche genutzt werden, um einen Fernzugriff auf ein Netzwerk zu ermöglichen.
VoIP (Voice-over-IP)	ist das Verfahren zur paketvermittelten Telefonie über das Internet.
Wirtschaftsspionage	ist die staatlich gelenkte oder gestützte, oft von Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.
Zwei-Faktor-Authentifizierung	beschreibt ein Authentifizierungsverfahren, das zwei unterschiedliche Faktoren zur erfolgreichen Authentifizierung benötigt. Z. B. werden ein richtiges Passwort und eine Schlüsseldatei benötigt, um erfolgreich authentisiert zu werden.

10 Sicherheitspreis Baden-Württemberg

Das Sicherheitsforum Baden-Württemberg verleiht seit 2007 im zweijährigen Turnus den Sicherheitspreis für herausragende Projekte der betrieblichen Sicherheit mit Zielsetzung Know-how-Schutz. Die Vergabe des Sicherheitspreises soll nicht nur in hohem Maße zur Sensibilisierung und Steigerung des Sicherheitsbewusstseins in den Unternehmen und Organisationen generell beitragen, sondern auch das Innovationspotenzial in Baden-Württemberg auf dem Sektor Sicherheit dokumentieren und fördern.

Auszeichnungswürdig sind mustergültige Projekte des personellen, technischen, organisatorischen oder rechtlichen Informationsschutzes. Dabei kann es sich um die Optimierung bereits vorhandener Strukturen oder um die Implementierung völlig neuer Mechanismen handeln. Teilnehmen können Unternehmen aller Branchen, die ihren Firmensitz oder eine Niederlassung in Baden-Württemberg haben, Organisationen und Institutionen sowie Hochschulen in Baden-Württemberg sowie Personen mit ständigem Wohnsitz in Baden-Württemberg.

Die öffentliche Preisverleihung findet auf der „eltefa" –Fachmesse für Elektrotechnik und Elektronik – auf der Messe Stuttgart statt. Alle Preisträger werden auf der Homepage des Sicherheitsforums präsentiert. Zudem werden die Preisträger und deren ausgezeichnete Projekte als Best-Practice-Beispiele in geeignetem Rahmen vorgestellt und veröffentlicht.

Wann der Sicherheitspreis das nächste Mal ausgeschrieben wird und viele weitere Informationen finden Sie auf der Homepage des SiFo unter www.sicherheitsforum-bw.de


Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION


Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen


Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND WOHNUNGSBAU


IHK
Die Industrie- und Handelskammern
in Baden-Württemberg


Baden-Württemberg
LANDESAMT FÜR VERFASSUNGSSCHUTZ


Landesverband der
Baden-Württembergischen
Industrie e. V.


ASW
Baden-Württemberg


KIT
Karlsruher Institut für Technologie


BOSCH
Technik fürs Leben


EnBW


DAIMLER


POLIZEI
BADEN-WÜRTTEMBERG


VDMA


Steinbeis


SAP


BWHT