wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Aktuelle Lage der IT-Sicherheit in KMU

Annette Hillebrand
Antonia Niederprüm
Saskja Schäfer
Sonja Thiele
Dr. Iris Henseler-Unger

WIK Wissenschaftliches Institut für Infrastruktur
und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef

Bad Honnef, Dezember 2017

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Das Projekt wurde im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ von WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste erstellt.

Förderkennzeichen: BMWi-VID3-090168623-02/2016

Initiative „IT-Sicherheit in der Wirtschaft“

Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Aufgaben sind unter:
www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Impressum

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info(at)wik.org
www.wik.org

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführer und Direktor	Dr. Iris Henseler-Unger
Direktor Abteilungsleiter Post und Logistik	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzender des Aufsichtsrates	Winfried Ulmen
Handelsregister	Amtsgericht Siegburg, HRB 7225
Steuer-Nr.	222/5751/0722
Umsatzsteueridentifikations-Nr.	DE 123 383 795

Vorwort

IT-Sicherheit in KMU: Der richtige Zeitpunkt ist spätestens jetzt

Mit der Digitalisierung und Vernetzung wird IT-Sicherheit immer wichtiger, denken wir an das Internet of Things, Industrie 4.0, Smart Cars oder Smart Home. Kleine und mittlere Unternehmen (KMU) werden auch in der vernetzten Welt einen beachtlichen Teil der deutschen Wirtschaft ausmachen. So innovativ sie oft sind, verfügen sie im Gegensatz zu großen Unternehmen meist über nur eingeschränkte Ressourcen für IT-Sicherheit.

Die Studie des WIK für das Bundesministerium für Wirtschaft und Energie im Rahmen der Initiative IT-Sicherheit in der Wirtschaft setzt auf unsere Analyse von 2011/12 auf. Sie will aktuelle Erkenntnisse über das Sicherheitsniveau gewinnen und Empfehlungen ableiten, wie die IT-Sicherheit in KMU erhöht werden kann.

Die Untersuchung zeigt: Trotz zunehmender Digitalisierung mangelt es immer noch am Bewusstsein für IT-Sicherheit. Selbst da, wo das eigene Risiko als hoch gilt, wird unzureichend für Schutz gesorgt. So geben zwei Drittel der kleinen KMU an, dass IT-Sicherheit für sie eine hohe Bedeutung hat, aber nur etwa 20 Prozent von ihnen hat eine IT-Sicherheitsanalyse durchgeführt.

Zwar sind viele Angebote zur Information und Weiterbildung verfügbar, allerdings scheinen die Masse der Möglichkeiten und die Kleinteiligkeit der Angebote zu Resignation zu führen. Hier könnte ein regionaler Ansatz mit Ansprechpartnern vor Ort und einem transparenten, für KMU verständlichen Angebot weiterhelfen. Bereits gestartete Programme sollten weiter mit Blick auf die Nachhaltigkeit der Aktivitäten optimiert werden. Ideal zur Verbesserung der IT-Sicherheitslage wäre die stärkere Verbreitung von Security by Design. IT-Sicherheit sollte nicht als isoliertes Thema am Ende einer Prozesskette stehen, sondern von Beginn an mitgedacht werden.

Im Vergleich zu vor fünf Jahren hat sich die Lage der IT-Sicherheit in KMU noch nicht entscheidend verbessert. Mit Blick auf die erheblich gestiegenen Anforderungen stellt sich daher die Herausforderung umso eindrücklicher, die KMU zu unterstützen, die bestehenden Defizite der Umsetzung endlich mit Nachdruck anzugehen.

Dr. Iris Henseler-Unger
Geschäftsführerin

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Inhaltsverzeichnis

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildungsverzeichnis

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Tabellenverzeichnis

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

1 Über diese Studie: Zielsetzung, Inhalte und Methodik

Unbestritten ist, dass angesichts der zunehmenden Digitalisierung und Vernetzung der Wirtschaft IT-Sicherheit weiter an Bedeutung gewinnen wird. Dies gilt insbesondere für die kleinen und mittleren Unternehmen (KMU), die einen wichtigen Teil der deutschen Wirtschaft ausmachen und von denen viele durch ihre Innovationskraft eine hohe Bedeutung erlangt haben. Für sie dürfte es zentral sein, IT Sicherheitslösungen zu implementieren und zu nutzen, die ihre Marktstärke auch in Zukunft sichern und auszubauen.

Bereits in 2011/2012 hatte WIK im Auftrag des BMWi eine Repräsentativbefragung zur Ermittlung des IT-Sicherheitsniveaus in kleinen und mittleren Unternehmen (KMU) durchgeführt.[1] Die damalige Studie war von hoher Relevanz für die IT-Sicherheitsdiskussion der folgenden Jahre, da solide empirisch begründete Analysen der IT-Sicherheitslage in KMU in ihren vielen Facetten und Details mit einer Fülle neuer Informationen zur Verfügung standen. Angesichts der zunehmenden Bedeutung der Digitalisierung liegt es nahe, die heutige IT-Sicherheitslage der KMU nochmals vertieft und detailliert zu betrachten und zu untersuchen, ob signifikante Veränderungen zu der Situation vor 5 Jahren festzustellen sind.

Die vorliegende Studie aktualisiert daher die Ergebnisse der ersten Untersuchung, und zieht ein Fazit zur Veränderung der IT-Sicherheitslage.[2] Der Fokus liegt dabei, anders als in anderen Studien, auf den kleinen und mittleren Unternehmen. KMU sind zum Teil hoch innovativ, verfügen aber im Gegensatz zu großen Unternehmen über nur sehr eingeschränkte Ressourcen im Bereich IT-Sicherheit.

Öffentliche Institutionen sowie Verbände und Vereine bieten Schulungs- und Beratungsangebote zum Thema IT-Sicherheit an. Es existieren regionale, niedrigschwellige Angebote, die die Sprache der KMU sprechen. Diese vorhandenen Angebote benötigen eine solide Datengrundlage, um ihre Vorhaben auf die Bedarfe der KMU abstimmen zu können und an die aktuelle Lage anzupassen.

Diese Studie verfolgt zwei Hauptziele. Erstens sollen aktuelle Erkenntnisse über die Bedeutung von und den Umgang mit IT-Sicherheit in kleinen und mittleren Unternehmen gewonnen werden. Zweitens soll die Studie aus der empirischen Analyse zur Lage der IT-Sicherheit in KMU Empfehlungen ableiten, wie die IT-Sicherheit in KMU in Deutschland erhöht werden kann. Diese Empfehlungen richten sich an das BMWi sowie

1 Büllingen, F.; Hillebrand, A. (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie, September 2012 (mit zwei Repräsentativbefragungen 2011 und 2012).

2 Eine Kurzfassung der Studie ist unter www.wik.org abrufbar.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

an weitere politische und gesellschaftliche Akteure wie Verbände und Institutionen, die sich mit IT-Sicherheit beschäftigen.

Die Ergebnisse des Projekts sind an die Gesamtheit der KMU in Deutschland gerichtet und an alle Akteure, die im Bereich der Verbesserung der IT-Sicherheit tätig sind. Da die Erhebung die Gesamtheit der KMU in Deutschland abbildet und darüber hinaus branchenspezifische Auswertungen zulässt, können Schlussfolgerungen sowohl für alle KMU als auch für spezifische herauszufilternde Gruppen getroffen werden. Daran anschließend können auf valider empirischer Basis Handlungsempfehlungen für weitere Maßnahmen zur Erhöhung der Wissensdiffusion, des Wissensaustausches und des –transfers gegeben werden.

Die vorliegende Studie ist Teil der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie. Die Initiative will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Aufgaben sind unter: www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Die Studie baut auf drei methodischen Vorgehensweisen auf. In einem ersten Schritt wurden vorhandene relevante Literatur und existierende Studien zum Thema ausgewertet.[3]

Zentral für die Ergebnisse der Studie zur aktuellen Lage der IT-Sicherheit in KMU ist die Repräsentativbefragung zwischen März und Mai 2017 in Deutschland. 1.508 KMU wurden zu ihrer Einschätzung der Bedeutung von IT-Sicherheit sowie dem Umgang damit befragt. Grundgesamtheit für die Untersuchung waren kleine und mittlere Unternehmen aller relevanten Branchen[4] mit mindestens einem und maximal 499 Beschäftigten, gemäß der vom BMWi verwendeten KMU-Definition. Um neben Gesamtaussagen auch repräsentative Aussagen nach Betriebsgrößenklassen zu gewinnen, wurden zu je ei-

3 Dabei wurden aktuelle Forschungsergebnisse gesichtet und bewertet, sowie aktuelle Publikationen und Webinformationen berücksichtigt. Zu diesem ersten Analyseschritt gehörte auch der Besuch von Konferenzen und Workshops.

4 Die Branchenzuordnung wurde auf der Grundlage der nationalen Klassifikation der Wirtschaftszweige, Ausgabe 2008 (WZ 2008, Statistisches Bundesamt) vorgenommen. Die Befragung bezog Unternehmen aller Branchen ein, mit Ausnahme der für KMU kaum relevanten Branchen, "O Öffentliche Verwaltung, Verteidigung, Sozialversicherung", "P Erziehung und Unterricht", "T Private Haushalte mit Hauspersonal, Herstellung von Waren und Erbringung von Dienstleistungen durch private Haushalte für den Eigenbedarf ohne ausgeprägten Schwerpunkt" sowie „U Exterritoriale Organisationen und Körperschaften".

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

nem Drittel Kleinunternehmen (1 bis unter 50 Beschäftigte), mittlere KMU (50 bis unter 100 Beschäftigte) sowie größere Unternehmen (100 bis unter 500 Beschäftigte) befragt. Die Befragung erfolgte computergestützt telefonisch, kombiniert mit der Möglichkeit, den Fragebogen online auszufüllen, falls dies von den kontaktieren Befragungsteilnehmern präferiert wurde. Dies trifft nur auf einen geringen Teil der Antworten zu. Die überwiegende Mehrheit der Interviews wurde computergestützt telefonisch (CATI) durchgeführt.[5]

Die Repräsentativbefragung wurde drittens von 30 vertiefenden Experteninterviews ergänzt und validiert. Die befragten Experten waren Vertreter von Verbänden, Personen aus Förder- und Forschungsprojekten der Bundesministerien, Vertreter von Gremien und Behörden sowie Ansprechpartner aus Unternehmen, die das Spektrum an KMU bzw. IT und IT-Sicherheit repräsentieren. Die Expertengespräche dienten der Bewertung von Trends und Einschätzungen aus der Repräsentativbefragung sowie der Diskussion von Handlungsempfehlungen.

Verwendete KMU-Definition

WIK legt die Definition des Institut für Mittelstandsforschung in Bonn (fortan IfM) zugrunde, die das BMWi auch im Rahmen des Zentralen Innovationsprogramms Mittelstand (ZIM) verwendet.[6]

Als KMU gelten in der vorliegenden Studie somit

- ⇨ kleine und mittlere Unternehmen (KMU) in Deutschland mit
- ⇨ < 500 Mitarbeitern und
- ⇨ < 50 Mio. EUR Umsatz/Jahr in ausgewählten Branchen.

Die vom IfM verwendete KMU Definition ist weiter gefasst als die der EU-Kommission, welche zu den KMU diejenigen Unternehmen zählt, die weniger als 250 Mitarbeiter beschäftigen und einen Jahresumsatz von höchstens 50 Mio. Euro aufweisen bzw. eine Jahresbilanzsummer von maximal 43 Mio. Euro verzeichnen. Das IfM begründet diese erweiterte Abgrenzung mit der Tatsache, dass deutsche KMU im Durchschnitt größer sind als KMU in der gesamten EU.[7]

5 Die technische Durchführung der Befragung oblag Info GmbH, Berlin. Gemeinsam mit dem Dienstleister wurde ein Pretest durchgeführt und ausgewertet.

6 O.V. (2015): Häufig gestellte Fragen – ZIM-Kooperationsprojekte. URL: https://www.zim-bmwi.de/kooperationsprojekte/faqs-zim-kooperationsprojekte-ab-2015.pdf.

7 Günterberg, Brigitte und Frank Maaß (o.J.): Mittelstand im Einzelnen. Institut für Mittelstandsforschung Bonn, URL: http://www.ifm-bonn.org/statistiken/mittelstand-im-einzelnen/#accordion=0&tab=8.

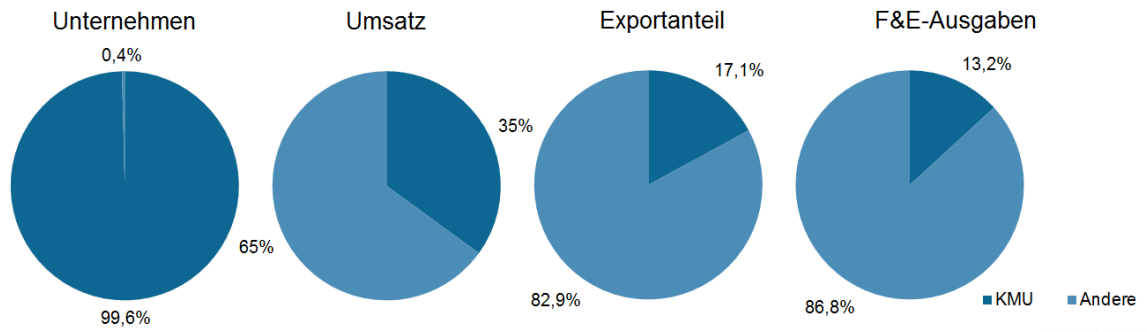
2 IT-Sicherheit in Deutschland – Hintergrund

2.1 Wirtschaftsstrukturelle Rahmenbedingungen für KMU heute

Besonders schützenswert: KMU als Rückgrat der Wirtschaft

Für das Jahr 2015 weist das Institut für Mittelstandsforschung 99,6 Prozent aller Unternehmen in Deutschland als KMU aus. Diese Unternehmen erwirtschafteten 2015 gut ein Drittel des gesamten Umsatzes deutscher Unternehmen (s. Abbildung 1). Am Export haben sie einen Anteil von 17,1 Prozent. Auch in der Forschung nehmen KMU einen bedeutenden Stellenwert ein. Ihr Anteil an den gesamten FuE-Ausgaben des Wirtschaftssektors deutscher Unternehmen lag 2015 bei 13,2 Prozent.[8]

Abbildung 1: Anteile der KMU an der Gesamtheit der Unternehmen in Deutschland im Jahr 2015[9] nach Anzahl der Unternehmen, Umsätzen, Exportanteil und F&E-Ausgaben



Quelle: Institut für Mittelstandsforschung (IfM), Bonn

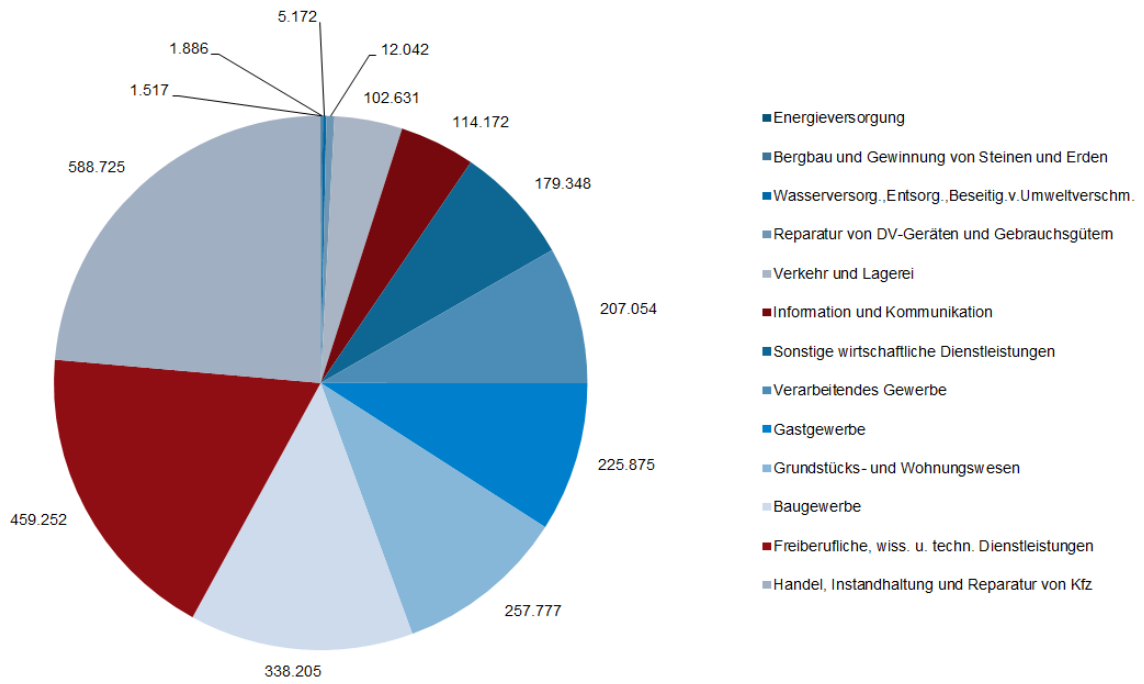
Die meisten Unternehmen sind im Wirtschaftszweig Handel, Instandhaltung und Reparatur von Kfz (WZ08-G) angesiedelt. Nach Angaben des Statistischen Bundesamtes waren das im Jahr 2014 588.725 Unternehmen. Es folgen die Branchen Freiberufliche, wiss. u. techn. Dienstleistungen (WZ08-M), Baugewerbe (WZ08-F), Grundstücks- und Wohnungswesen (WZ08-L), Gastgewerbe und Verarbeitendes Gewerbe (WZ08-C) (s. Abbildung 2).

8 Institut für Mittelstandsforschung Bonn (o.J.): Volkswirtschaftliche Bedeutung der KMU. URL: http://www.ifm-bonn.org/statistiken/mittelstand-im-ueberblick/. Die Angaben für das Jahr 2015 umfassen die zurzeit aktuellsten Erhebungen des IfM.

9 Institut für Mittelstandsforschung Bonn (o.J.): Volkswirtschaftliche Bedeutung der KMU. URL: http://www.ifm-bonn.org/statistiken/mittelstand-im-ueberblick/#accordion=0&tab=0.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 2: Branchenverteilung KMU[10] nach Anzahl der Unternehmen



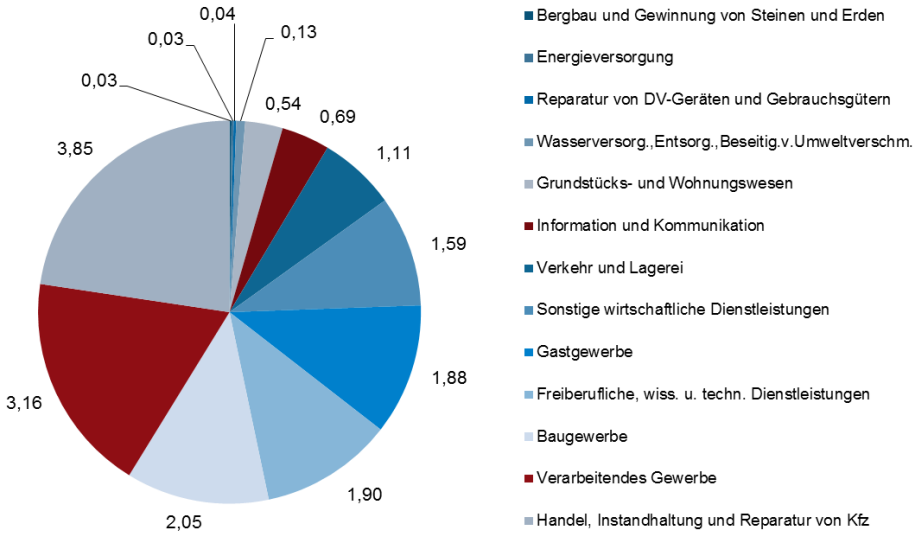
Quelle: Institut für Mittelstandsforschung (IfM), Bonn

Gemessen an der **Anzahl der tätigen Personen** sind im Jahr 2014 die meisten KMU im Wirtschaftszweig Handel, Instandhaltung und Reparatur von Kfz (WZ08-G), mit 3,85 Mio. tätigen Personen, gefolgt vom Verarbeitenden Gewerbe (WZ08-C), mit 3,16 Mio. tätigen Personen, aktiv. Es folgen die Branchen Baugewerbe (WZ08-F), Freiberufliche, wiss. u. techn. Dienstleistungen (WZ08-M), Gastgewerbe (WZ08-I), Sonstige wirtschaftliche Dienstleistungen (WZ08-N) sowie Verkehr und Lagerei (WZ08-H) mit jeweils mehr als 1 Mio. tätigen Personen (s. Abbildung 3).

10 Die Angaben beziehen sich auf KMU mit bis zu 249 Mitarbeitern und einem Umsatz von max. 50 Mio. Euro, entsprechend den Angaben des Statistischen Bundesamtes.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 3: Branchenverteilung der KMU[11] nach Anzahl der tätigen Personen (in Mio.)



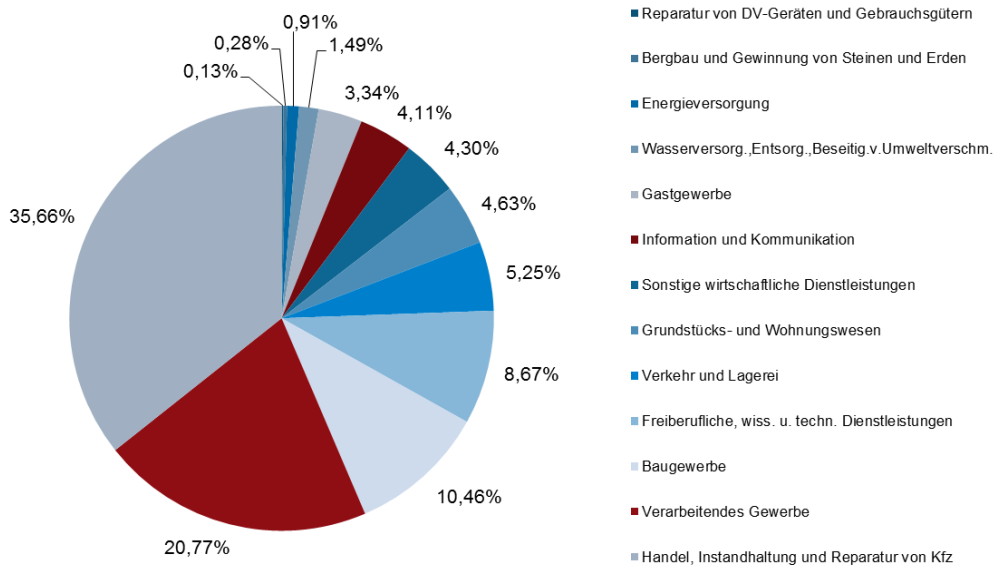
Quelle: Institut für Mittelstandsforschung (IfM), Bonn

Ein ähnliches Bild liefert auch der Branchenvergleich nach Umsätzen. Die größte Branche gemessen an den Umsätzen stellt die Branche Handel, Instandhaltung und Reparatur von Kfz (WZ08-G), mit 36 Prozent der Umsätze, dar, gefolgt vom Verarbeitenden Gewerbe (WZ08-C), welches für 21 Prozent der Umsätze von KMU im Jahr 2014 verantwortlich war. Damit sind diese beiden Branchen für mehr als die Hälfte Gesamtumsätze von KMU im Betrachtungszeitraum verantwortlich. Zur weiteren Verteilung (s. Abbildung 4).

11 Die Angaben beziehen sich auf KMU mit bis zu 249 Mitarbeitern und einem Umsatz von max. 50 Mio. Euro, entsprechend der Angaben des Statistischen Bundesamtes.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 4: Branchengrößen von KMU[12] nach Umsatz (in Prozent)



Quelle: Institut für Mittelstandsforschung (IfM), Bonn

In zwei Betrachtungsebenen, nach Umsatz und Anzahl tätiger Personen, sind die Branche Handel, Instandhaltung und Reparatur von Kfz, Verarbeitendes Gewerbe und Baugewerbe unter den ersten größten drei Branchen vertreten.

Familienunternehmen in Deutschland: Im Zeitraum von 1998 bis 2014 ist die Anzahl **familien- oder eigentümergeführter Unternehmen** von 94,8 Prozent auf 93,6 Prozent zurückgegangen.[13] Eine andere Erhebung[14] unterscheidet zwischen familien- und eigentümergeführten Unternehmen. Demnach machen familienkontrollierte Unternehmen 91 Prozent der Unternehmen in Deutschland aus. 87 Prozent sind außerdem eigentümergeführte Familienunternehmen. Hier wird deutlich, dass der größte der Teil der Unternehmen, der von einer geringen Personenanzahl kontrolliert wird, auch eine Beteiligung des Eigentümers in der Leitung aufweist.

Hidden Champions: Laut einer Erhebung des ZEW aus dem Jahr 2015 gehören in Deutschland etwa 1.600 Unternehmen zu den Hidden Champions, sind also Weltmarktführer für ihr Produkt. Die Unternehmen in dieser Gruppe sind meistens eher klein, obwohl sie als Weltmarktführer global agieren. Durchschnittlich erwirtschaften die Unter-

12 Die Angaben beziehen sich auf KMU mit bis zu 249 Mitarbeitern und einem Umsatz von max. 50 Mio. Euro, entsprechend der Angaben des Statistischen Bundesamtes.
13 Wolter, H.-J. unter Mitarbeit von Sauer, I. (2017): Die Bedeutung der eigentümer- und familiengeführten Unternehmen in Deutschland. IfM Bonn: IfM-Materialien Nr. 253, Bonn.
14 Gottschalk, Sandra et al. (2014): Die volkswirtschaftliche Bedeutung der Familienunternehmen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

nehmen aus der Gruppe der Weltmarktführer einen Jahresumsatz von weniger als 100 Millionen Euro und beschäftigen weniger als 300 Beschäftigte.[15] Hidden Champions findet man in Nischenmärkte. Sie zeichnen sich durch eine hohe Spezialisierung und somit durch schützenswertes Spezialwissen aus.

Unternehmensneugründungen: Seit 2011 ist die Zahl der Unternehmensgründungen[16] ebenso wie die der Liquidationen in Deutschland rückläufig (siehe Abbildung 5). Der Saldo ist negativ. Die Anzahl der Unternehmen geht also zurück. Im Jahr 2016 wurden 282.000 Unternehmen gegründet und 311.000 Unternehmen geschlossen. Das heißt im Vergleich zu dem Vorjahr gibt es 29.000 Unternehmen weniger.[17] Knapp jedes dritte Unternehmen wird innerhalb der ersten drei Geschäftsjahre wieder geschlossen. Es herrscht also eine stetige Dynamik innerhalb der deutschen Unternehmenslandschaft. Dies macht kontinuierliche, sich wiederholende Informationsangebote und Unterstützungsangebote für Unternehmen in Deutschland erforderlich, da immer wieder neue Akteure in den Markt eintreten.

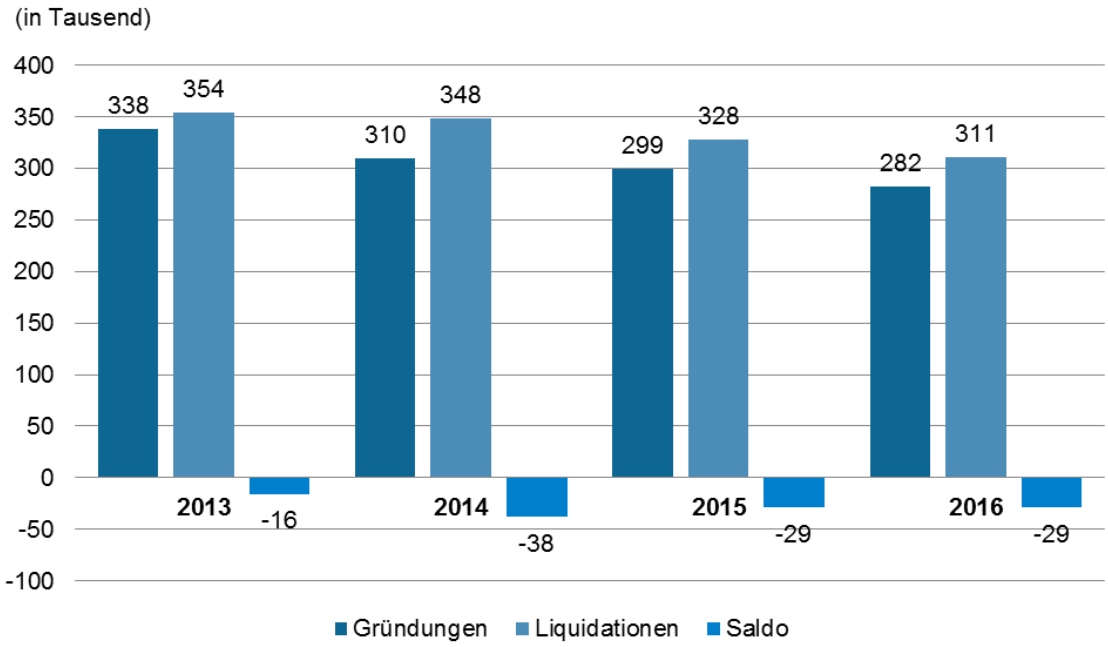
Digitale Gründer: Jeder fünfte Gründer ist im Jahr 2016 außerdem ein **„digitaler" Gründer**. Ein digitales Unternehmen zeichnet sich dadurch aus, dass Kunden das Angebot ausschließlich durch den Einsatz digitaler Technologien nutzen können. Dazu zählen zum Beispiel App-Anbieter, Webdesigner oder Softwareentwickler. Das macht deutlich, dass die Gefahr für Cyberangriffe groß ist, da alles, also die gesamte Wertschöpfung, digital stattfindet.[18]

15 Rammer, Christian und Alfred Spielkamp (2015): Hidden Champions – Driven by Innovation: Empirische Befunde auf Basis des Mannheimer Innovationspanels. ZEW-Dokumentation Nr. 15-03, Mannheim.
16 Gewerbliche Existenzgründungen ohne Nebenerwerbsgründungen und freie Berufe.
17 IfM (2016): Gründungen und Unternehmensschließungen. URL: http://www.ifm-bonn.org/statistiken/gruendungen-und-unternehmensschliessungen/#accordion=0&tab=1. Abgerufen am: 16.08.2017.
18 Metzger, Georg (2017): KfW-Gründungsmonitor 2017.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 5: Saldo aus Gründungen und Liquidationen seit 2013



Quelle: IfM Bonn; nicht erfasst: Nebenerwerbsgründungen und freie Berufe, 2017

Verschiedene Faktoren sprechen dafür, dass in Deutschland besonders schützenswerte Gruppen von Unternehmen vorhandenen sind, die aufgrund ihrer Größe und damit beschränkten finanziellen und personellen Ressourcen das Thema IT-Sicherheit oftmals nur unzureichend vollständig selbst erschließen können. Zahlreiche deutsche Hidden Champions stellen ein attraktives Ziel für Cyberangriffe dar. Vor dem Hintergrund einer dynamischen Unternehmenslandschaft scheint ein kontinuierliches, sich wiederholendes Informationsangebot außerdem hilfreich.

2.2 Bedrohungsszenarien im Bereich IT-Sicherheit - Medienpräsenz des Themas Informationssicherheit

Mediale Berichterstattung treibt Suchanfragen zu Sicherheitsthemen

Eine erhöhte Anzahl von Suchanfragen lässt sich meist einem bestimmten medialen Ereignis zuordnen. In den vergangenen zwei Jahren gab es beispielsweise laut Google Trends zwei Peaks für die Suchbegriffe „Bundesamt für Sicherheit in der Informationstechnik“ und „Informationssicherheit“. Eine Recherche in den online Archiven von Tageszeitungen lässt eine Zuordnung zu zwei Ereignissen zu. Der Anstieg im Februar 2014 ist vermutlich auf den Diebstahl von Onlinezugangsdaten zu E-Mailkonten im

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Februar 2014 zurückzuführen über den das BSI berichtete. Der Peak im April 2014 passt zum Bekanntwerden der Nutzung des Heartbleed-Fehlers durch die NSA (Siehe dazu Objektive Einschätzung der Bedrohungslage

Die tatsächliche Bedrohungslage, im Gegensatz zur Einschätzung der Bedrohungslage durch Unternehmen selbst, ist schwer zu ermitteln. Die verfügbaren Statistiken des Bundeskriminalamtes basieren auf den angezeigten Straftaten. Allerdings wird nicht angegeben, welche Straftaten bei Unternehmen und welche bei Privatpersonen gemessen wurden.

Bundeslagebild Cybercrime 2016: Straftaten im Vergleich zum Vorjahr um 80,5 Prozent gestiegen

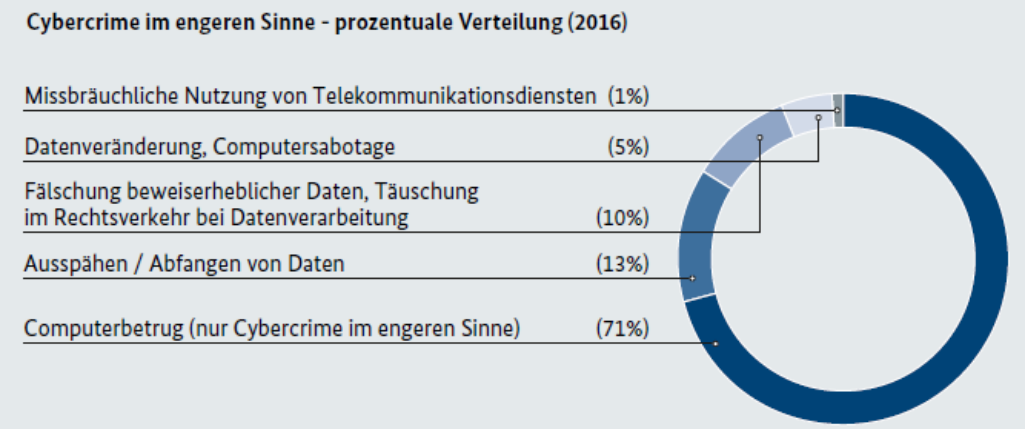
Auf Basis der Daten der polizeilichen Kriminalstatistik (fortan PKS) veröffentlicht das Bundeskriminalamt (fortan BKA) jährlich ein Bundeslagebild Cybercrime. Die Autoren verweisen darauf, dass mit einem großen Dunkelfeld zu rechnen ist. Das heißt, man geht davon aus, dass eine große Anzahl von Cybercrime-Straftaten nicht zur Anzeige gebracht wird.

Im Jahr 2016 wurden in der PKS im Bereich **Cybercrime** 82.649 Straftaten erfasst. Damit ist die Anzahl erfasster **Straftaten** im Vergleich zum Vorjahr um 80,5 Prozent gestiegen[19]. Von den im Jahr 2016 erfassten Straftaten konnten knapp 39 Prozent aufgeklärt werden. Das bedeutet einen leichten Anstieg von 6 Prozentpunkten im Vergleich zum Vorjahr.

Die meisten Straftaten (71 Prozent) fallen in die Kategorie Computerbetrug. Darunter fällt zum Beispiel der Sachverhalt, dass eine Person mithilfe einer falschen Bankkarte Geld abhebt. Weitere Straftaten sind das Abfangen von Daten (13 Prozent der erhobenen Straftaten), die Fälschung beweiserheblicher Daten (10 Prozent) sowie Datenveränderung (5 Prozent) (siehe Abbildung 6).

19 Der starke Anstieg ist neben einer tatsächlichen Zunahme der Straftaten auch auf eine veränderte Zuordnung von Straftaten zurückzuführen. So bestand im Vergleich zu den Vorjahren die Möglichkeit, Fallzahlen aus dem Bereich (allgemeiner) Betrug, als Computerbetrug zu erfassen. (Vgl. BKA 2017, S. 5)

Abbildung 6: Prozentuale Verteilung von Straftaten im Bereich Cybercrime



Quelle: BKA, 2017, S. 6

Die polizeiliche Statistik ermittelt **entstandene Schäden** ausschließlich für Computerbetrug und der missbräuchlichen Nutzung von Telekommunikationsdiensten. Dabei macht der Schaden durch Computerbetrag 50,9 Mio. Euro im Jahr 2016 aus und entspricht nahezu der Gesamtschadenssumme von 51,63 Mio. Euro. Diese Zahlen liefern allerdings kein umfassendes Bild des tatsächlichen Schadens durch Cybercrime. Zum einen umfasst die Schadenssumme nur Schäden für die Fälle Computerbetrug und missbräuchliche Nutzung von Telekommunikationsdiensten. Die Schäden, die durch Computersabotage, Fälschung beweiserheblicher Daten oder durch Ausspähen entstehen, werden nicht berücksichtigt. Oftmals sind diese Schäden auch nicht zu beziffern. Darüber hinaus ist die finanzielle Auswirkung eines Reputationsverlustes oder Imageschadens nicht darstellbar. Hinzu kommen Schäden durch nicht angezeigte Straftaten im Bereich Cybercrime.

Weiterhin erhebt das BKA Straftaten, bei denen **das Internet als Tatmittel** genutzt worden ist. Im Jahr 2016 wurde das Internet bei 253.290 Straftaten als Tatmittel genutzt. Somit ist die Anzahl der Straftaten mit dem Tatmittel Internet im Vergleich zum Vorjahr um 3,6 Prozent gestiegen. Betrugsdelikte, vor allem Warenbetrug, machten dabei den Großteil der Straftaten aus.

Eine der häufigsten Formen des Identitätsdiebstahls im digitalen Bereich bildet „Phishing im Zusammenhang mit Onlinebanking“. Allerdings hat sich die Zahl der Fälle

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

im Jahr 2016 auf einen fünf Jahres Tiefstand reduziert und im Vergleich zum Vorjahr um mehr als 50 Prozent abgenommen.[20]

Die Lage der IT-Sicherheit in Deutschland 2016, BSI

Der Bericht des BSI geht auf aktuelle Entwicklungen im Bereich IT-Sicherheit ein. Das umfasst:

- Gefährdungslage (Cloud, Softwareschwachstellen, Hardwareschwachstellen, Kryptografie, Mobilkommunikation, Standardsetzung, Internet-Infrastruktur
- Bewertung der Schwachstellen in IT-Systemen
- Illustration von Angriffsmitteln- und Methoden (Schadprogramme, Ransomware, Social Engineering, Advanced Persistent Threats, Spam-Verlauf, Botnetze, DDoS, Drive-by-Exploits, Identitätsdiebstahl, Seitenkanalangriffe)

Dabei handelt es sich um eine Zusammenfassung der aktuellen Lage zumeist ohne konkrete Zahlenangaben. Im Wesentlich zeigt der Bericht, dass eine Professionalisierung der Angreifer zu beobachten ist. Ebenso werden mehr und mehr Varianten von Schadprogrammen bekannt. Zudem verlieren Abwehrmaßnahmen an Wirksamkeit und die Bedrohung durch Ransomware hat sich seit Ende 2015 deutlich verschärft.

Beispiele für IT-Sicherheitsskandale und Angriffe der letzten Jahre

NSA-Skandal. Massive Überwachung der Kommunikation durch Nachrichtendienste

Das allgemeine Interesse der Unternehmen an Sicherheitsthemen dürfte spätestens seit dem sogenannten NSA-Skandal im Jahr 2013 gestiegen sein. Die auch unter dem Titel „Snowden-Affäre“ oder „NSA-Enthüllungen“ bekanntgewordenen globale Überwachungs- und Spionageaffäre bezeichnet die im Juni 2013 geschehenen Enthüllungen des ehemaligen Mitarbeiters eines externen Dienstleisters des Nachrichtendienstes Edward Snowden. Veröffentlicht wurden die Informationen von der Washington Post und dem britischen Guardian. Snowden machte damit die verdachtsunabhängige Überwachung der Telekommunikation und des Internets durch die Vereinigten Staaten von Amerika und anderen Nachrichtendiensten öffentlich. Konkret belegt wurde dieser Sachverhalt auf Basis von als vertraulich gekennzeichneten Unterlagen des Nachrichtendienstes National Security Agency (NSA). Die NSA verwendete zur Spionage u.a. das Programm Prism, was als Abkürzung für "Planning tool for Resource Integration, Synchronization, and Management" steht. Durch die Enthüllungen von Edward Snowden wurde der massive Umfang bekannt, im dem Nachrichtendienste weltweit die kabelgebundene und drahtlose Kommunikation überwachen und systematisch auswerten.[21]

20 BKA (2017): Cybercrime Bundeslagebild 2016.
21 Vgl. Bendrath, Ralf (2014): Überwachungstechnologien. In: Aus Politik und Zeitgeschichte, APuZ 18–19/2014. / Muscat, Sabine (2013): Prism-Leak - Ein Held, ein Staatsfeind, ein Mann voller Rätsel. In:

Ausschnitte aus dem medialen Echo verdeutlichen die Risiken für Unternehmen in Deutschland:

„Wanzen installiert: NSA soll EU-Einrichtungen ausgespäht haben“, 29.06.2013, Handelsblatt[22]

„NSA-System XKeyscore Die Infrastruktur der totalen Überwachung“, 31.07.2013, Spiegel online[23]

„Wirtschaftsspionage durch amerikanische Geheimdienste: Ausgespäht und ausgenommen“, 12.07.2013, Süddeutsche Zeitung[24]

„Neue Snowden-Enthüllungen: NSA entwickelt Super-Computer zum Ausspähen“, 03.01.2014, Handelsblatt[25]

Stuxnet: Kritische Infrastruktur als Angriffsziel

2010 kam es mit Hilfe des Computerwurms Stuxnet zur Sabotage von Industrieanlagen. Experten vermuten, dass diese aufwendige Malware eine der teuerste der bisher Erlebten war. Als vermutetes Ziel gelten ein Atomkraftwerk sowie eine Urananreicherungsanlage im Iran. Ende November 2010 gab der iranische Präsident bekannt, dass Zentrifugen der Urananreicherungsanlage sabotiert worden waren.[26] Der Angriff zielte somit auf kritische Infrastrukturen ab.[27]

“Iran says nuclear programme was hit by sabotage”[28]*, 19.11.2010, BBC*

“Stuxnet: Der Wurm, der aus dem Nichts kam“[29]*, 24.12.2010, Spiegel*

Zeit online, 11.06.2013. / Bundeszentrale für politische Bildung (2014): Ein Jahr NSA-Skandal - der Netzdebatte Rückblick. URL: https://www.bpb.de/dialog/netzdebatte/192953/ein-jahr-nsa-skandal-der-netzdebatte-rueckblick.

22 O.V. (2013): NSA soll EU-Einrichtungen ausgespäht haben. In: Handelsblatt.com, 29.06.2013, URL: http://www.handelsblatt.com/politik/international/wanzen-installiert-nsa-soll-eu-einrichtungen-ausgespaeht-haben/8425146.html.

23 Lischka, Konrad und Christian Stöcker (2013): Die Infrastruktur der totalen Überwachung. In: Spiegel.de, 31.07.2013, URL: http://www.spiegel.de/netzwelt/netzpolitik/xkeyscore-wie-die-nsa-ueberwachung-funktioniert-a-914187.html.

24 Obermaier, Frederik und Tanjev Schultz (2013): Wirtschaftsspionage durch amerikanische Geheimdienste - Ausgespäht und ausgenommen. In: Süddeutsche Zeitung.de, 12.07.2013, URL: http://www.sueddeutsche.de/politik/wirtschaftsspionage-durch-amerikanische-geheimdienste-ausgespaeht-und-ausgenommen-1.1719795.

25 O.V. (2014): Neue Snowden-Enthüllungen - NSA entwickelt Super-Computer zum Ausspähen. In: Handelsblatt.com, 03.01.2014, URL: http://www.handelsblatt.com/politik/international/neue-snowden-enthuellungen-nsa-entwickelt-super-computer-zum-ausspaehen/9282678.html.

26 BBC (2010): Iran says nuclear programme was hit by sabotage. In: BBC online, 29.11.2010. URL: http://www.bbc.com/news/world-middle-east-11868596.

27 Ernst, Nico (2010): Stuxnet kam über russischen Zulieferer. In: Zeit online am 29.09.2010. URL: http://www.zeit.de/digital/internet/2010-09/stuxnet-langner-iran.

28 BBC (2010): Iran says nuclear programme was hit by sabotage. In: BBC online, 29.11.2010. URL: http://www.bbc.com/news/world-middle-east-11868596.

29 Kremp, Matthias (2010): Stuxnet Der Wurm, der aus dem Nichts kam. In: Spiegel online, am 24.12.2010. URL: http://www.spiegel.de/netzwelt/web/stuxnet-der-wurm-der-aus-dem-nichts-kam-a-735970.html.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

„Stuxnet kam über russischen Zulieferer“[30], 29.09.2010, Zeit

„Trojanerangriff: Hackerprogramm Stuxnet attackiert Irans Atomanlage“[31], 26.10.2010, Zeit

WannaCry und Petya: Verschlüsselung von Unternehmensdaten

Im Mai 2017 erregte die Ransomware WannaCry große Aufmerksamkeit durch die Verschlüsselung von Dateien bei zahlreichen Unternehmen. Das Schadprogramm forderte von den Anwendern eine Zahlung in der Kryptowährung Bitcoin, um einen Datenverlust zu verhindern. Bei dem Angriff, kam es zu Vorfällen in mehr als 100 Ländern[32]. Zu den bekanntesten Opfer zählen die Deutsche Bahn, FedEx, das russische Innenministerium, die Produktion von Renault und Krankenhäuser in Großbritannien. Bei der Deutschen Bahn waren durch das Schadprogramm Anzeigetafeln nicht mehr verfügbar, in Großbritannien konnten die Krankenhäuser nicht mehr auf digitale Patientenakten zugreifen.[33] Sicherheitssoftwareanbieter wie Kaspersky oder Avast erfassten innerhalb weniger Stunden Angriffe im mittlere fünfstelligen Bereich auf Nutzer ihrer Schutzlösung.[34]

Da die Ransomware nur veraltete und nicht gepatchte Systeme angreifen konnte, machte sie deutlich, wie viele Unternehmen bekannte Sicherheitsupdates nicht einspielen. Die Windowsschwachstelle, die dabei genutzt wurde, wurde zuvor schon von der NSA entdeckt und sollte für eigene Angriffe genutzt werden. Deshalb wurde Microsoft nicht über die Schwachstelle informiert. Im März 2017 stellte Microsoft einen Patch für den Exploit für aktuell unterstützte Systeme zur Verfügung. Für ältere Systeme wie Windows XP wurde kein kostenloser Patch zur Verfügung gestellt. Eine Hackergruppe veröffentlichte die Schwachstelle im April 2017.

Wenige Wochen nach dem WannaCry-Angriff folgten Angriffe mit dem Schädling namens Petya/NotPetya. Dieser nutze die gleiche Sicherheitslücke wie WannaCry. Die Angriffe starteten offenbar in der Ukraine und trafen dort neben Energieunternehmen auch die Post, Mobilfunkanbieter und Banken.[35]

---

30 Ernst, Nico (2010): Stuxnet kam über russischen Zulieferer. In: Zeit online am 29.09.2010. URL: http://www.zeit.de/digital/internet/2010-09/stuxnet-langner-iran.

31 O.V. (2010): Trojanerangriff: Hackerprogramm Stuxnet attackiert Irans Atomanlage. In: Zeit online, am 26.10.2010. URL: http://www.zeit.de/digital/2010-09/iran-stuxnet-trojaner.

32 Mansholt, Malte (2017): Erpressungs-Trojaner "Wannacry": Das müssen Sie über den Angriff wissen. In: Stern.de, 13.05.2017, URL: http://www.stern.de/digital/online/erpressungs-trojaner--das-muessen-sie-ueber-den-weltweiten-grossangriff-wissen-7451556.html.

33 O.V. (2017): "WannaCry"-Attacke - Fakten zum globalen Cyberangriff. In: Spiegel.de, 13.05.2017, URL: http://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html.

34 Mansholt, Malte (2017): Erpressungs-Trojaner "Wannacry": Das müssen Sie über den Angriff wissen. In: Stern.de, 13.05.2017, URL: http://www.stern.de/digital/online/erpressungs-trojaner--das-muessen-sie-ueber-den-weltweiten-grossangriff-wissen-7451556.html.

35 Gierow, Hauke (2017): Trojaner-Attacke trifft auch deutsche Firmen. In: Zeit.de, 27.06.2017, URL: http://www.zeit.de/digital/internet/2017-06/hackerangriff-ransomware-petya-maersk-rosneft.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

„WannaCry: Armutszeugnis für betroffene Unternehmen und Organisationen“[36]*,15.05.2017, ZDnet*

„Wanna Cry: Virus infiziert jetzt auch Blitzer“, 22.06.2017, Computerbild[37]

„Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm“, 27.07.2017, heise online[38]

2.3 Das Thema IT-Sicherheit in der empirischen Forschung

WIK hat Studien mit hoher relevant für das Thema IT-Sicherheit in KMU gesichtet und ausgewertet. Die wichtigsten Eckpunkte dieser Studien werden im Folgenden dargelegt. Zu diesen Eckpunkten zählen die Anzahl der Befragten, der Fokus auf KMU, die Methode der Erhebung sowie die Repräsentativität der Erhebungen. Folgende Studien werden betrachtet:

1. Cyber-Sicherheits-Umfrage 2016; durchgeführt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Kooperation mit: BDI, BITKOM, DIHK, GI, VDMA, VOICE und ZVEI; Oktober 2016.

2. Im Visier der Cybergangster - So gefährdet ist die Informationssicherheit im deutschen Mittelstand; Autoren: Philipp Engemann, Derk Fischer, Björn Gosdzik, Tobias Koller und Nial Moore; herausgegeben von der PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC); Februar 2017.

3. 1. Studienbericht zur Security Bilanz Deutschland 2016: IT- und Informationssicherheit: Technische Maßnahmen und Lösungen in Mittelstand und öffentlichen Verwaltungen; Autoren: Henrik Groß von techconsult u.v.m., unterstützt von Bitdefender, DATEV eG, Hewlett Packard Enterprise, msg systems ag, Jakobsoftware, Net at Work, Micro Focus und TeleTrust; April 2016.

4. DsiN-Sicherheitsmonitor Mittelstand 2016; Autoren: Stefan Brandl und Mara Zimmermann (DATEV) sowie Nadine Grau, Sascha Wilms und Nils Engler (DsiN), verantwortlich: Dr. Michael Littger (DsiN); Oktober 2016.

---

36 Schmerer, Kai (2017): WannaCry: Armutszeugnis für betroffene Unternehmen und Organisationen. In: ZDNET.de, 15.05.2017, URL: http://www.zdnet.de/88296345/wannacry-armutszeugnis-fuer-betroffene-unternehmen-und-organisationen/?inf_by=59955a68681db8b45b8b4892.

37 Lewalter, Udo; Schuldt, Rainer und Andy Voß (2017): Wanna Cry: Virus infiziert jetzt auch Blitzer. In: Computerbild.de, 22.06.2017, URL: http://www.computerbild.de/artikel/cb-News-Sicherheit-Cyber-Attacke-mit-Ransomware-Wanna-Cry-18083097.html.

38 Holland, Martin (2017): Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm. In: Heise.de, 27.06.2017, URL: https://www.heise.de/security/meldung/Rueckkehr-von-Petya-Kryptotrojaner-legt-weltweit-Firmen-und-Behoerden-lahm-3757047.html.

5. eco Studie IT-Sicherheit 2017; unter Leitung von Oliver Dehning, Kompetenzgruppe Sicherheit des eco Verbands; Juni 2017.

6. Digitalisierung und IT-Sicherheit in deutschen Unternehmen 2017; erstellt von der Bundesdruckerei GmbH in Zusammenarbeit mit KANTAR EMNID; Juni 2017.

7. Cybersicherheitsstrategie; PwC Strategy& (i.A. BMI), Mai 2016.

8. Wirtschaftsschutz in der digitalen Welt; Bitkom Research; Juli 2017.

Eine tabellarische Übersicht zu den Studien und ihren wichtigsten Eckpunkten siehe Anhang (Tabelle 4).

Die Auswertung der Studien bildet eine wichtige Grundlage sowohl für die Repräsentativerhebung und für die Experteninterviews. Gleichwohl weisen sie methodisch im Vergleich zur WIK-Erhebung Defizite auf. Eine empirische Untersuchung der aktuellen Lage der IT-Sicherheit in KMU aller Größenklassen und über alle Branchen hinweg erscheint somit gerechtfertigt und sinnvoll, um auch Kleinstunternehmen und weniger IT-affine Branchen mit einzubeziehen.

Zu den Bereichen, die in den ausgewerteten Studien zum Teil Lücken aufweisen zählen die folgenden Punkte:

- Geringe Fallzahlen: Die Fallzahl ist bei allen Studien geringer als in der Befragung durch WIK.

- Absicherung der Ergebnisse: Es findet keine Absicherung der Befragungsergebnisse durch Interviews oder eine zweite Befragungsrunde statt.

- KMU Fokus: Nur drei der sieben betrachteten Studien schließen auch Kleinstunternehmen mit ein.

- Repräsentativität: Keine der betrachteten Studien ist methodisch repräsentativ für die Grundgesamtheit der KMU in Deutschland. Zwei der Studien sind repräsentativ für Unternehmen ab zehn bzw. ab 20 Mitarbeitern.

- Handlungsempfehlungen: Drei von acht Studien umfassen keine Handlungsempfehlungen.

- Unterstützungsbedarfe: Nur eine der acht betrachteten Studien fragt explizit danach, welche Unterstützung sich KMU für die Zukunft wünschen, also nach z.B. Siegeln, Zertifikaten oder Technologieförderung.

- Zeitreihe: Die WIK-Studie setzt die Untersuchung von 2011/12 fort und ermöglicht somit einen zeitlichen Vergleich der Veränderung in Bezug auf Risikowahrnehmung, Ergreifen von IT-Sicherheitsmaßnahmen und Handlungserfordernissen.

2.3.1 Cyber-Sicherheits-Umfrage 2016, Allianz für Cybersicherheit[39]

Die Untersuchung der Allianz für Cybersicherheit ermittelt detailliert, mit welchen Angriffen Unternehmen konfrontiert waren, welche Schäden dadurch entstanden sind und welche Schutzmaßnahmen Unternehmen ergreifen.

Angriffe und Schäden: Zwei Drittel der Befragten waren in 2016 Ziel von Cyber-Angriffen

Unterschiede je nach Größe des Unternehmens: Es geben mehr große Unternehmen an, bereits Angriffe festgestellt zu haben, als kleine. Bei kleinen Unternehmen mit 1 bis 49 Mitarbeitern geben etwa 50 Prozent an, bereits Angriffe festgestellt zu haben. Bei den größten, mit mehr als 10.000 Mitarbeitern, sind es knapp 90 Prozent. Knapp die Hälfte (47 Prozent) der Befragten war Opfer eines erfolgreichen Angriffs. Etwas geringer ist der Anteil (44 Prozent) derer, die angeben einen Angriff abgewehrt zu haben.

Hauptsächlich berichten Befragte von Malware. Sowohl gezielte als auch ungezielte Infektionen mit sonstiger Malware haben mehr als die Hälfte der Teilnehmer festgestellt. Deutlich weniger Unternehmen, etwas weniger als ein Viertel, berichten von (D)DoS-Angriffen. Von Infektionen durch **Ransomware** innerhalb der letzten sechs Monate berichtet knapp ein Drittel. Knapp zwei Drittel geben an, innerhalb der letzten sechs Monate nicht durch Ransomware infiziert worden zu sein.

Produktions- oder Betriebsausfall ist der meistgenannte Schaden (31 Prozent) bei Unternehmen, die bereits unter Angriffen gelitten haben. **Dass Cyberrisiken ansteigen, geben 62 Prozent der Befragten an.** Die größte Bedrohung sieht die Mehrheit der Teilnehmer von der organisierten Kriminalität und der Wirtschaftskriminalität ausgehend. Dabei befürchten die mit Abstand meisten Teilnehmer vor allem Bedrohungen durch die Infektion mit Ransomware (etwa 68 Prozent).

Knapp drei Viertel der Unternehmen haben eine konkret benannte Person aus dem eigenen Personal, die für das Thema IT-Sicherheit gesamtverantwortlich ist. Nur sechs Prozent der Teilnehmer haben diese Funktion ausgelagert. 14 Prozent der Befragten verteilen diese Aufgabe auf mehrere Mitarbeiter und 4 Prozent der Teilnehmer geben an, keinen Mitarbeiter für diese Aufgabe zu haben.

39 BSI und Allianz für Cybersicherheit (2016): Cyber-Sicherheits-Umfrage 2016.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Schutzmaßnahmen: Basics wie Firewall und Virenscanner sind vorhanden

Die meisten (ca. 85 Prozent) geben an, sich vor Angriffen durch eine Absicherung der Netzübergänge z.B. durch eine Firewall zu schützen. Zentrale oder dezentrale Antivirus Scanner sind darüber hinaus beliebte Schutzmittel. Die große Mehrheit der Befragten hält die Maßnahmen, die bisher getroffen wurden, für nicht ausreichend, um sich vor Cyber-Angriffen zu schützen. Weniger als 20 Prozent der Befragten geben an, dass ihre Maßnahmen zum Schutz gegen Cyberangriffe ausreichen. Knapp 80 Prozent sind der Meinung, dass diese Maßnahmen nicht ausreichen.

2.3.2 Im Visier der Cybergangster - So gefährdet ist die Informationssicherheit im deutschen Mittelstand - PwC[40]

Die Studie von PwC berücksichtigt Unternehmen ab einer Größe von 200 Mitarbeitern und unterscheidet sich damit in der Zielgruppe deutlich im Vergleich zur von WIK erstellten Studie.

Die Studie von PwC fokussiert auf einige Sonderthemen. Die Studie hat eine Frage dazu aufgenommen, inwieweit das Unternehmen schon im Bereich **Industrie 4.0** aktiv ist. Mögliche Konsequenzen daraus mit Blick auf IT-Sicherheit oder eine Auswertung, ob Unternehmen, die hier bereits weiter sind auch mehr in IT-Sicherheit investieren, wurden nicht untersucht. Zudem wurde die Betroffenheit durch das **IT-Sicherheitsgesetz** betrachtet**.** Das IT-Sicherheitsgesetzt betrifft allerdings nur eine bestimmte Gruppe von Unternehmen. Kleinstunternehmen sind davon ausgenommen. 22 Prozent der Teilnehmer geben an, sich als Betreiber Kritischer Infrastrukturen im Sinne des Gesetzes zu verstehen.

Interessant ist die Frage danach, ob Unternehmen aufgrund der **Digitalisierung** in Informationssicherheit investieren. Drei Viertel der Befragten bejahen das. Kundenanforderungen spielen bei zwei Dritteln der Teilnehmer eine Rolle bei Investitionen in Informationssicherheit.

Im Jahr 2015 haben 38 Prozent der Befragten zwischen 10.000 und 50.000 Euro in Informationssicherheit investiert. Regulatorische Anforderungen wirken sich auf die **Investitionen** in IT-Sicherheit aus. Unternehmen, die vom IT-SiG betroffen sind, planen höhere Investitionen. Allerdings wurde uns in Expertengesprächen auch der umgekehrte Effekt beschrieben, nämlich dass eine nicht-Betroffenheit von Gesetzen den Eindruck vermittelt, auch weniger von Gefahren betroffen zu sein und dementsprechend weniger für Schutz sorgen zu müssen.

40 Engemann, Philipp et al. (2017): Im Visier der Cybergangster - So gefährdet ist die Informationssicherheit im deutschen Mittelstand. PwC (Hg.).

Überraschend und konträr zu den bisherigen Erkenntnissen ist das Ergebnis der Erhebung, dass sich die Mehrheit (72 Prozent) der Privatunternehmen trotz der zögerlichen Umsetzung des IT-SiG und des in der Vergangenheit eher geringen IT-Budgets gut gegen Cyberattacken geschützt fühlt. (PwC, 2017, S.12)

Die Studie bietet acht **Handlungsempfehlungen**. Diese richten sich an Unternehmen selbst. Allerdings sind die Handlungsempfehlungen, wenig konkret und sind von Unternehmen ohne externe Unterstützung nicht umsetzbar. Sie geben allerdings auf einer Seite einen kurzen Überblick über all das, was getan werden sollte.

2.3.3 IT und Informationssicherheit: Technische Maßnahmen und Lösungen im Mittelstand und öffentlichen Verwaltungen, techconsult[41]

Für die Erhebung wurden zum dritten Mal infolge 500 Mittelständler mit einer Größe von 20 bis zu 1.999 Mitarbeitern befragt. 44 Prozent der befragten Unternehmen sind der Mitarbeiterzahl nach KMU mit einer Größe von 20 – 199 Beschäftigen.

Begleitend zur Studie ist auch ein Online-Test verfügbar, der die Datenbasis für den Berichte liefert.

Neben einem **Sicherheitsindex**, der ermittelt, welche Maßnahmen bisher in Unternehmen umgesetzt wurden, wird auch ein **Gefährdungsindex** ermittelt. Dieser schätzt ab, wie gut Unternehmen gegen bestimmte Angriffe abgesichert sind bzw. von welche Gefährdungen von Angriffen ausgehen. Hauptergebnis: Unternehmen schätzen ihre eigene Sicherheitslage im Vergleich zum Vorjahr deutlich schlechter ein. Das erstreckt sich über alle Bereiche und gilt somit für technische Maßnahmen ebenso wie für rechtliche oder organisatorische.

Die Teilnehmer schätzen die Gefährdungslage im Vergleich zum Vorjahr schlechter ein. Der Index zur Gefährdungslage besteht aus zwei Hauptmerkmalen: der Absicherung gegen Angriffe und der Bedrohung durch Angriffe. Die Absicherung gegen Angriffe entwickelt sich aus Sicht der Teilnehmer leicht positiv. Diese Tendenz wird allerdings von der deutlicher höher eingeschätzten Bedrohung überlagert. Sodass sich die Gefährdungslage insgesamt im Indexwert verschlechtert hat.

Der Sicherheitsindex liegt im Jahr 2016 bei 50 Prozentpunkten und hat sich damit im Vergleich zum Vorjahr um 4 Prozentpunkte verschlechtert. Der Gefährdungsindex ist im selben Zeitraum von 48 auf 49 Prozentpunkte gestiegen. Somit nähern sich das ge-

41 Groß, Henrik et al. (2016): 1. Studienbericht zur Security Bilanz Deutschland 2016: IT- und Informationssicherheit: Technische Maßnahmen und Lösungen in Mittelstand und öffentlichen Verwaltungen. Techconsult (Hg.).

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

schätzte Sicherheitsniveau und die geschätzte Bedrohungslage an. Es besteht somit kein „Polster“ mehr zwischen dem Sicherheitsniveau und der Bedrohungslage, wie dies in den beiden Vorjahren der Fall war.

Besonderheiten: Im Branchenvergleich zeigt sich vor allem, dass die Branche Banken und Versicherungen mit einem Sicherheitsindexwert von 56 Punkten auf allen Ebenen (technisch, organisatorisch, rechtlich und strategisch) vor den anderen betrachteten Branchen liegt. Negativ auffällig im Branchenvergleich stellt sich der Sicherheitsindex im Bereich der Öffentlichen Verwaltung und Non-Profit sowie im Bereich Handel dar. Hier wird ein Wert von nur 46 bzw. 48 Punkten erreicht.

Die Studie fokussiert primär auf Lösungen und lässt weitere Faktoren wie bei Unternehmen festgestellte Angriffe außen vor.

Als Handlungsempfehlung ist aufbauend auf der Studie eine weitere Publikation „IT-Sicherheit – 5 Schritte für den Mittelstand“ verfügbar, wo sehr konkrete Zielvorgaben für die Ausgaben für IT-und Informationssicherheit gemacht werden. Dort heißt es, dass Aufgaben für IT-Sicherheit durchschnittlich nur 10 Prozent des IT-Budgets und daher nur etwa, 3 Prozent des Jahresumsatzes ausmachen.

Im Kontrast zu den geführten Expertengesprächen steht das Ergebnis der Befragung, dass die technischen Maßnahmen und Lösungen zur Berechnung des Sicherheitsindex stärker zurückgegangen sind als organisatorische, rechtliche und strategische Maßnahmen.

Grundsätzlich fährt die Studie, vermutlich entsprechend der Sichtweise der Ersteller, einen anderen Ansatz bei der Befragung. Anstatt die Lage im Bereich technischer Maßnahmen zu erfassen, werden Umsetzungsprobleme bei den jeweiligen Maßnahmen, wie beispielsweise bei der verschlüsselten Datenübertragung erfragt. Das setzt voraus, dass die teilnehmenden Unternehmen Verschlüsselung bei der Datenübertragung kennen und diese, wenn auch ggf. nicht korrekt, implementiert haben.

2.3.4 Sicherheitsmonitor Mittelstand, DsiN[42]

Seit 2011 erstellt der Verein Deutschland sicher im Netz (DsiN) den Sicherheitsmonitor. Die Ergebnisse basieren auf dem DsiN-Sicherheitscheck, den von Juni 2015 bis März 2016 1.320 Unternehmen durchgeführt haben. Mindestens 78 Prozent der Teilnehmer kommen aus KMU (nach Mitarbeiterzahl).

42 Brandl, Stefan et al. (2016): DsiN-Sicherheitsmonitor Mittelstand 2016. DsiN (Hg.).

Die Erhebung hat zum einen untersucht, wie stark Unternehmen **digitale Technologien** in ihrem Geschäftsalltag einsetzen, darunter Cloud Computing und Online-Banking. Außerdem geht die Studie vertieft der Frage nach, inwieweit rechtliche Anforderungen bei der geschäftlichen Nutzung von E-Mail, Internet und Cloud Computing bekannt sind. Bei der E-Mail-Nutzung geben 14 Prozent der Befragten an, Risiken und rechtliche Anforderungen nicht zu kennen. Beim Cloud Computing geben 22 Prozent[43] an, nicht über Sicherheitsanforderungen bzw. rechtliche Rahmenbedingungen informiert zu sein.

Zum anderen geht die Erhebung der Frage nach, welche Schutzmaßnahmen bereits eingesetzt werden. So zeigt sich, dass nur weniger als die Hälfte der Unternehmen Schutzmaßnahmen im Bereich der E-Mai-Sicherheit einsetzen. Damit ist E-Mail-Sicherheit im Rahmen dieser Erhebung weiterhin die größte Schwachstelle mit dem größten Handlungsbedarf, auch wenn die Tendenz leicht positiv ist. So setzen mehr Unternehmen als noch im vorherigen Jahr auf einen Passwortschutz für Dokumente und eine Verschlüsselung von E-Mail-Anhängen.

Die stagnierende Anzahl von Unternehmen, die Schutzmaßnahmen ergreift, interpretieren die Autoren als Zeichen dafür, dass die öffentlichen Diskussionen und die tägliche Berichterstattung über Sicherheitsvorfälle, keine erheblichen Veränderungen im Sicherheitsverhalten der Unternehmen bewirkt.

Die Studie gibt Handlungsempfehlungen, „Was Unternehmen tun können“. In diesem Abschnitt verweisen die Autoren auf Angebote des DsiN, wie beispielsweise den Cloud-Scout, der individuelle Hinweise zum Einsatz von Cloud Computing mit Blick auf IT-Sicherheit bietet.

2.3.5 eco Studie IT-Sicherheit 2017, eco Verband[44]

Im Rahmen der diesjährigen Erhebung wurden 590 Personen befragt. Davon sind knapp die Hälfte (49 Prozent) Anbieter von IT-Sicherheit. 47 Prozent sind Anwender. Fast die Hälfte der Befragten kommt aus der IT- oder TK-Branche. Es ist daher anzunehmen, dass ein Großteil der Befragten sich gut mit dem Feld IT-Sicherheit auskennt. Dementsprechend sind die Ergebnisse aber vermutlich nicht ohne weiteres auf die Gesamtheit der KMU übertragbar.

Bedrohungslage: Im Vergleich zu den Anwendern von IT-Sicherheit schätzen Anbieter die Bedrohungslage häufiger als „stark wachsend“ ein.

43 Von denen Unternehmen, die Cloud Computing nutzen.
44 Dehning, Oliver et al. (2017): eco Studie IT-Sicherheit 2017. eco Verband (Hg.).

Sonderthemen: 97 Prozent der Befragten stimmen der Aussage zu, dass das Bewusstsein für die Smart-Home-Sicherheit steigen muss. Gefragt nach den Erwartungen an ein Connected Car zeigt sich, dass zunehmend mehr Befragte im Vergleich zu 2016 mit weniger Sicherheit durch vernetzte Autos rechnen.

Als größten **Treiber für Veränderungen** im Bereich IT-Sicherheit sehen 60 Prozent der Befragten in 2016 das Internet of Things (IoT). Darauf folgende kritische Infrastrukturen für 51 Prozent der Befragten und Cloud Computing nennen 46 Prozent der Teilnehmer.

2.3.6 Digitalisierung und IT-Sicherheit in deutschen Unternehmen, Bundesdruckerei[45]

Die Studienergebnisse sind repräsentativ für die Grundgesamtheit der Unternehmen ab 20 Mitarbeitern in Deutschland. Für die Befragung wurden im Februar und März 2017 500 Interviews (CATI) mit Entscheidern für IT-Sicherheit in Unternehmen ab einer Größe von 20 Mitarbeitern geführt. Mindestens 35 Prozent der Teilnehmer kommen aus KMU mit einer Mitarbeiterzahl von maximal 99 Personen. Weitere 35 Prozent der Befragten repräsentieren Unternehmen mit 100 bis 499 Mitarbeitern.

Die Studie betrachtet IT-Sicherheit auch mit Blick auf die Digitalisierung, z.B. bei der Frage, inwiefern IT-Sicherheit als Basis für die Digitalisierung gilt. Für drei Viertel der Befragten ist IT-Sicherheit die Basis für eine erfolgreiche Digitalisierung.

Investitionen in IT-Sicherheit: Mehr als die Hälfte (56 Prozent) der Teilnehmer geht davon aus, dass sich die Investitionen in IT-Sicherheit im Vergleich zu 2016 in ihrem Unternehmen 2017 erhöhen werden. Knapp 40 Prozent nehmen an, dass die Investitionen gleichbleiben. Auffällig: In den Branchen Energie und Versorger sowie Produktion und Logistik gehen deutlich mehr Unternehmensvertreter (75 Prozent) von Zuwächsen im Bereich IT-Sicherheit aus.

IT-Sicherheitsmaßnahmen-Index: Im Durchschnitt erreichen die befragten Unternehmen einen Indexwert von 56,4. Es liegt also nur ein mittelmäßiges Schutzniveau vor. Dabei ist die Tendenz zu beobachten, dass größere Unternehmen auch einen höheren, also besseren Indexwert als kleine Unternehmen erreichen. Im Branchenvergleich sticht besonders die Banken- und Versicherungsbranche durch einen hohen Indexwert (79,5) aus der Gesamtheit heraus.

45 Bundesdruckerei (Hg.): 2017: 6. Digitalisierung und IT-Sicherheit in deutschen Unternehmen 2017.

Gesetzliche Regelungen: Es herrscht Überforderung mit gesetzl. Regelungen zum Thema Datenschutz und IT-Sicherheit, insbesondere bei kleinen U. Da sind es sogar mehr als die Hälfte (61 Prozent), die das angeben.

Kooperationen mit Anbietern von Sicherheitslösungen: Die Mehrheit der befragten Unternehmen bezieht IT-Lösungen von nur einem einzigen Anbieter. Das passt zu den Eindrücken aus den Expertenbefragungen. Die meisten Experten berichteten, dass KMU, wenn sie denn einen Dienstleister haben, oftmals alle von diesem beziehen auch wenn ggf. Kompetenzen in einigen Bereichen nicht vorhanden sind.

Nutzung von Cloud-Angebote: Unter denjenigen, die aktuell noch keine Cloud-Angebote nutzen, geben gut 80 Prozent als Grund dafür an, dass sie die Hoheit über ihre eigene IT haben wollen. Für mehr als die Hälfte spielt ein nicht ausreichender Datenschutz eine Rolle. Auch eine nicht ausreichende Datensicherheit nennt die Hälfte als Begründung dafür, dass noch keine Cloud-Angebote genutzt werden (60 Prozent sagen aber auch, dass sie keinen Bedarf haben).

Einsatz von Mitarbeiterausweisen: Bietet Schutz vor Social Engineering durch Fremde. Bei größeren Unternehmen weit verbreitet, 50 bzw. 70 Prozent verwenden solche Ausweise. Bei kleinen Unternehmen sind es nur 25 Prozent.

2.3.7 Cybersicherheitsstrategie, PwC[46]

Die von PwC (Strategy&) erstelle Studie wurde im Auftrag des BMI durchgeführt. 309 Datensätze aus einem online Fragebogen konnten in die Auswertung einfließen.

Sonderthemen: Mit Blick auf die **Zusammenarbeit von Staat und Wirtschaft** im Bereich IT-Sicherheit. Knapp drei Viertel der Teilnehmer sehen eine enge Zusammenarbeit von Staat und Wirtschaft als Voraussetzung für Cyber-Sicherheit. Einige Aufgaben wie beispielsweise die Identifikation von Schwachstellen oder die aktive Abwehr eines Angriffs sehen die Befragten klar bei den Unternehmen selbst. Einige Maßnahmen wie beispielsweise die vorausschauende Analyse von Bedrohungen sehen die Teilnehmer als Gemeinschaftsaufgabe von Staat und Wirtschaft. Bei Forschungsprojekten und Einführung von Standards im Bereich Cyber-Sicherheit sehen die Unternehmen eher den Staat in der Verantwortung. Weiterhin wird betrachtet, welche Maßnahmen den Unternehmen einen Mehrwert bieten würden. Für mehr als 80 Prozent der Befragten stellt der Informationsaustausch mit dem Staat einen Mehrwert dar. 60 Prozent sehen einen Mehrwert in mobilen staatlichen Teams, die im Falle einer Attacke Unterstützung leisten.

46 Strategy& PwC (2016): Cybersicherheitsstrategie. Im Auftrag des BMI.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Knapp 50 Prozent der Befragten geben an, in Deutschland genug kompetente IT-Sicherheitsdienstleister für den Fall eines Schadens zu sehen. Knapp ein Viertel der Befragten stimmen dieser These nicht zu.

Weitere Sonderaspekte, die in der Untersuchung berücksichtigt wurden, sind: Verfügbarkeit von IT-Sicherheitsdienstleistern im Schadensfall, staatliche Förderung von Schlüsseltechnologien und die Relevanz von Gütesiegeln.

Damit hebt sich diese Studie sich thematisch deutlich von den anderen betrachteten ab. Das lässt sich wahrscheinlich auf den Auftrag zur Studie durch das BMI zurückführen.

2.3.8 Wirtschaftsschutz, Bitkom[47]

Für diese mündliche Befragung (CATI) des Bitkom wurden 1.069 Unternehmen ab einer Größe von 10 Mitarbeitern befragt. Die Studie wird als repräsentativ für alle Unternehmen ab dieser Größe in Deutschland ausgewiesen.

Als eine von zwei Studien im Vergleichssample wird von Bitkom die Frage nach der Schadenshöhe aufgegriffen. Die höchste Schadsumme gaben die Unternehmen, die betroffen waren[48], für die Kosten der Ermittlung und Ersatzmaßnahmen sowie im Bereich Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen an. Die Summe für Schäden durch die Erpressung mit gestohlenen oder verschlüsselten Daten ist im Vergleich dazu sehr gering.

Täterkreis: Was sich in der Repräsentativbefragung des WIK zeigt, bestätigt sich auch in der Studie des Bitkom: Mehr als die Hälfte der Unternehmen, die in den letzten beiden Jahren von Industriespionage oder Datendiebstahl betroffen waren, gehen davon aus, dass aktuelle oder ehemalige Mitarbeiter für diese Handlungen verantwortlich sind. Ausländischen Nachrichtendiensten ordnen nur drei Prozent der befragten Unternehmen diese Handlungen zu.

Aufdeckung von Vorfällen: Auf die Frage, die Vorfälle bemerkt worden sind, antworten 37 Prozent der betroffenen Unternehmen, dass Einzelpersonen im Unternehmen darauf hingewiesen haben. 30 Prozent der Befragten geben an, durch Zufall auf schädliche Handlungen aufmerksam geworden zu sein. 28 Prozent der Teilnehmer haben Hinweis aus der internen Revision des Unternehmens erhalten.

Untersuchung der Vorfälle: Knapp die Hälfte der Unternehmen untersucht die Vorfälle selbst, bei einem Drittel (34 Prozent) geschieht dies durch externe Spezialisten. 31 Pro-

47 Kopke, Cornelius et al. (2017): Wirtschaftsschutz. Bitkom e.V.
48 Das waren 571 Unternehmen, also etwa 53 Prozent der teilnehmenden Unternehmen.

zent lassen die Schäden durch staatliche Stelle wie die Datenschutz-Aufsicht oder das BSI untersuchen. Vor allem aus Angst vor Imageschäden durch eine mögliche Veröffentlichung der Vorfälle haben sich befragte Unternehmen dazu entschieden, staatliche Stellen nicht einzuschalten.

Wie sich in Expertengesprächen des WIK bestätigt, zeigt auch diese Studie, dass es im Bereich personeller Maßnahmen im Vergleich zu technischen und organisatorischen Sicherheitsmaßnahmen die größten Defizite gibt.

2.3.9 Sonderthemen

Sechs der acht betrachteten Studien beziehen Sonderthemen mit ein, die über das, was die meisten Studien untersuchen, hinausgehen.

Zu diesen Themen zählen:

- Einsatz von Mitarbeiterausweisen
- Sicherheitsbewusstsein bei Smart Home
- Auswirkungen des Connected Car auf die Sicherheitslage
- Digitalisierung und Industrie 4.0 als Treiber für IT-Sicherheit
- Hemmnisse und Einsatz von Cloud-Computing
- Bekanntheit rechtlicher Anforderungen (Cloud, IT-SiG)
- Wünsche zu Themen und Intensität der Zusammenarbeit zwischen Staat und Wirtschaft im Bereich Cybersicherheit
- Status Quo zum Einbezug staatlicher Stellen bei Vorfällen

2.3.10 Zusammenfassung und Fazit

Fünf der acht betrachteten Studien umfassen das Thema **Cyberangriffe** bzw. erheben die aktuelle oder zukünftige **Bedrohungslage**. Hierzu wurde u.a. die Einschätzung der Lage, des Bedrohungspotentials, des Risikos für die Betriebsfähigkeit, die konkreten Arten und Mengen von Vorfälle oder Indikatoren zur Bewertung der Lage untersucht. Die große Mehrheit der Unternehmen, etwa 60 – 80 Prozent je nach Umfrage, empfindet die Bedrohungslage als steigend.

Fünf der acht betrachteten Studien geben **Handlungsempfehlungen**. Vier richten diese Empfehlungen an Unternehmen. Eine Studie fragt konkret nach den Wünschen der Zusammenarbeit mit dem Staat.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Sechs von acht Studien haben (organisatorische) Personalfragen im Bereich IT-Sicherheit thematisiert. Es standen dabei u.a. die Aspekte Kompetenzaufbau, Mitarbeiterschulung /-sensibilisierung, Verantwortlichkeiten für IT-Sicherheit und Outsourcing im Fokus. Wenige Erhebungen gehen auf die Schäden, die durch Angriffe entstanden sind ein. In nur zwei von acht Studien ist das Thema.

Fünf von acht Studien beleuchten, inwieweit Unternehmen technische Maßnahmen umgesetzt haben. Insgesamt bestätigen die Studien das Bild, was auch WIK in der repräsentativ Befragung ermittelt hat und welches die Experten in unseren Gesprächen ebenfalls zeichnen: Ein Basisschutz wie eine Firewall oder ein Virenscanner ist in der großen Mehrheit der Unternehmen vorhanden.

Die WIK-Studie fokussiert auf KMU nach der Definition des BMWi und bezieht auch Kleinstunternehmen mit ein. Die Erhebung konzentriert sich auf die Einschätzung aus Sicht der Geschäftsführer und IT-/IT-Sicherheitsverantwortlichen der KMU. Die erneute Erhebung, die an die Studie von 2011/12 anknüpft ermöglicht Vergleiche im Zeitverlauf. Somit schließt die WIK-Studie eine Erkenntnislücke im Bereich des Risikobewusstseins, des Ergreifens von Maßnahmen und der Handlungserfordernisse aus Sicht der KMU selbst. Die Unterstützung durch das BMWi führte zu einer hohen Bereitschaft zur Teilnahme an der Befragung.

3 WIK-Studie 2017: Strukturdaten der befragten KMU

Die repräsentative Stichprobe umfasste 1.508 KMU. Innerhalb der Unternehmen wurden hauptverantwortliche Entscheider für den IT-Bereich befragt, d.h. Geschäftsführer, IT- oder IT-Sicherheitsverantwortliche.

Abbildung 7: Zusammensetzung der Stichprobe

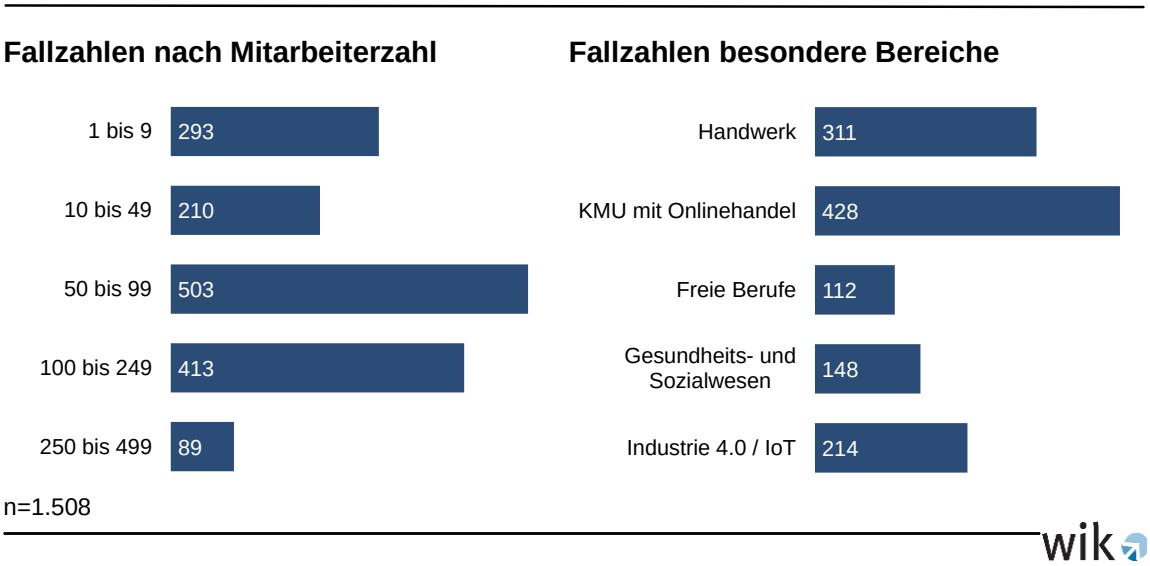


Abbildung 7 zeigt die Zusammensetzung der Stichprobe nach Mitarbeiterzahl sowie nach besonderen Bereichen, die sich nicht aus der Klassifizierung der Wirtschaftszweige ergeben. Demnach ist jedes fünfte befragte Unternehmen ein Handwerksbetrieb, und mehr als jedes vierte KMU bietet seine Waren oder Dienstleistungen über das Internet an. Etwa jedes siebte Unternehmen ist aktiv im Bereich Industrie 4.0. Diese Fallzahlen zeigen bereits die zunehmende Bedeutung von IT-Sicherheit für KMU.

Die Grundgesamtheit bildeten kleine und mittelständische Unternehmen ausgewählter Branchen in Deutschland mit mindestens einem bis maximal 499 festen Beschäftigten. Die Branchenzuordnung wurde auf der Grundlage der nationalen Klassifikation der Wirtschaftszweige, Ausgabe 2008 (WZ 2008, Statistisches Bundesamt) vorgenommen. Von der Befragung ausgeschlossen waren die Branchen, O Öffentliche Verwaltung, Verteidigung, Sozialversicherung, P Erziehung und Unterricht, T Private Haushalte mit Hauspersonal, Herstellung von Waren und Erbringung von Dienstleistungen durch private Haushalte für den Eigenbedarf ohne ausgeprägten Schwerpunkt sowie U Exterritoriale Organisationen und Körperschaften. Die Grundgesamtheit der verbleibenden Branchen umfasste N=3.671.110 Unternehmen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Die Unternehmensbefragung war als Betriebsbefragung angelegt, d.h. als Befragung von Hauptstandorten und Arbeitsstätten von Mehrbetriebsunternehmen. Zielpersonen in den Unternehmen waren die/der Geschäftsführer(in)/Inhaber(in) bzw. ein Mitglied der Geschäftsführung/-leitung, das für den Bereich IT verantwortlich zeichnet.

Die Stichprobe wurde disproportional angelegt, um neben Gesamtaussagen auch repräsentative Aussagen nach Betriebsgrößenklassen zu gewinnen. Ziel war es, jeweils zu einem Drittel Unternehmen mit 1-49 Mitarbeitern, 50-99 Mitarbeitern sowie 100-499 Mitarbeitern zu befragen. Die Gewichtungsmatrix wurde auf der Grundlage aktueller Statistiken des Statistischen Bundesamtes erarbeitet.

Von den befragten 1.508 Unternehmen erfüllten 1.505 Unternehmen das Screening-Kriterium „relevante technische Ausstattung im Unternehmen“. Es wurde eine kombinierte Befragungsmethodik eingesetzt: Die überwiegende Mehrheit der Interviews wurden computergestützt telefonisch (CATI) durchgeführt (n=1.456, d.s. 97%). Im Eingangsinterview wurde den Unternehmen (im Falle einer sich ankündigenden Interviewverweigerung) die Möglichkeit angeboten, den Fragebogen online auszufüllen. Bestand die Bereitschaft zur Online-Befragung, wurde die Mailadresse aufgenommen und ein individualisierter Online-Link versendet. Von der Möglichkeit der Online-Befragung machten 52 Unternehmen (3%) Gebrauch.

Die Befragung wurde von Info GmbH, Berlin, nach den von allen deutschen Marktforschungsverbänden anerkannten „Standards zur Qualitätssicherung in der Markt- und Sozialforschung“ in den Callcentern des Unternehmens durchgeführt. Die die Bestimmungen der 2006 veröffentlichten DIN ISO 20252 „Markt- und Sozialforschungsdienstleistungen“ wurden ebenfalls berücksichtigt.

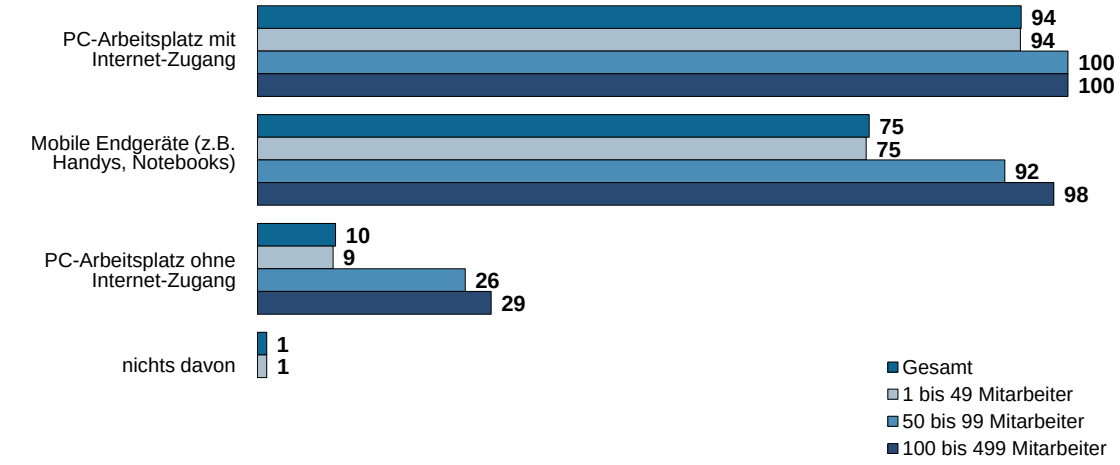
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

4 Technische Ausstattung der KMU

Von den befragten 1.508 KMU erfüllten 1.505 das Kriterium „relevante technische Ausstattung vorhanden“. PC-Arbeitsplätze mit Internetzugang sind in nahezu allen Unternehmen vorhanden (vgl. Abbildung 8), und seit 2011 weitgehend unverändert. Demgegenüber nutzt nur noch eine Minderheit der KMU PC-Arbeitsplätze ohne Internetzugang. Die Nutzung mobiler Endgeräte wie Smartphones, Notebooks und Tablets ist zwar insgesamt geringer, aber ebenfalls weit verbreitet. Der Einsatz mobiler Endgeräte ist mit der Befragung aus 2011 durch die leicht veränderte Fragestellung nur bedingt vergleichbar, der Trend geht jedoch eindeutig zu einer stärkeren Nutzung mobiler Endgeräte.

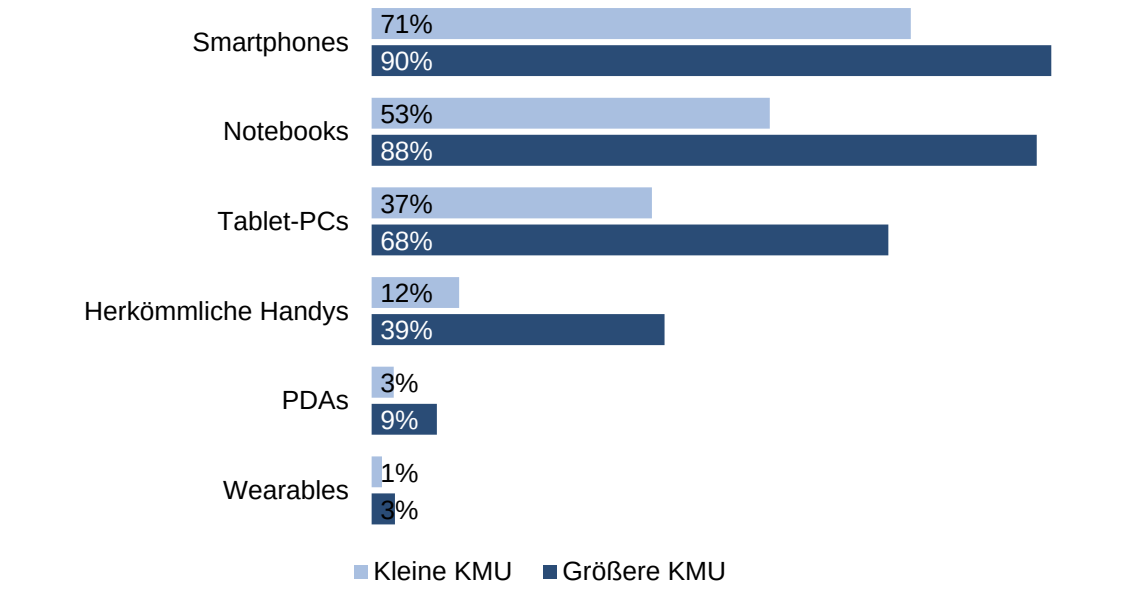
Abbildung 8: Ausstattung von KMU mit IKT



n=1.508

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 9: Nutzung mobiler Endgeräte



n=1.505

Größere KMU ab 50 Mitarbeitern nutzen mobile Endgeräte häufiger als kleine KMU bis 49 Mitarbeiter. Am weitesten verbreitet ist der Einsatz von Smartphones und Notebooks. Tablets haben stark aufgeholt im Vergleich zu 2011, sie konnten ihren Abstand zu den Notebooks auf nur 15 Prozentpunkte (gemittelt über alle KMU) verringern, im Vergleich zu 54 Prozentpunkten in 2011. PDAs ohne Telefonfunktion und Wearables (z.B. Datenbrillen) spielen keine große Rolle.

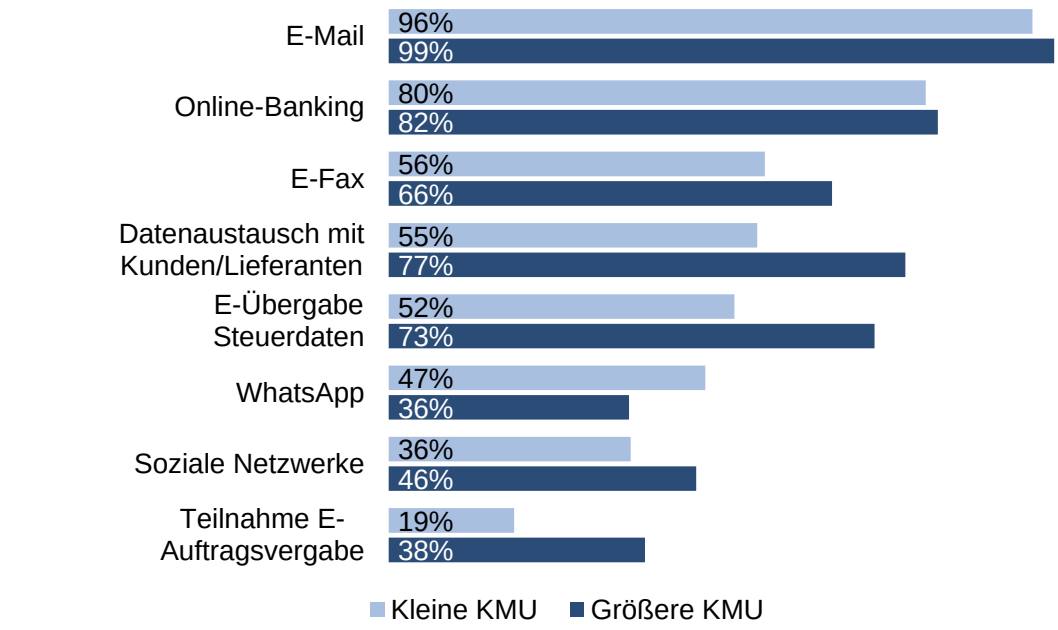
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

5 Digitalisierungsgrad: Einsatz von IT-Lösungen in KMU

Kleine und mittlere Unternehmen setzen IT-Lösungen in unterschiedlichem Ausmaß ein. E-Mail und Onlinebanking sind am weitesten verbreitet und werden von kleinen sowie größeren KMU nahezu gleichverteilt genutzt (vgl. Abbildung 10). Insbesondere kleine KMU nutzen zunehmend WhatsApp sowie soziale Netzwerke (2011: 16 Prozent nutzten soziale Netzwerke). Einerseits mag dies teilweise der beruflichen Nutzung von privaten Endgeräten geschuldet sein, andererseits zeigt es die zunehmende Bedeutung für KMU, in Onlinemedien präsent zu sein.

Abbildung 10: Nutzung elektronischer Kommunikation

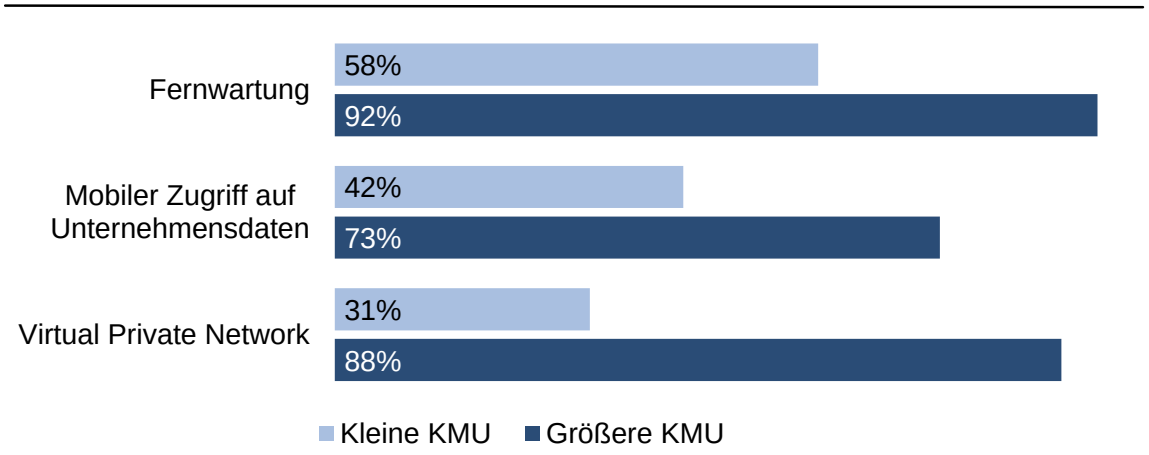


n=1.505

Komplexere IT-Anwendungen wie der Datenaustausch mit Kunden bzw. Lieferanten, die elektronische Übermittlung von Steuerdaten oder die Teilnahme an elektronischer Auftragsvergabe nutzen deutlich mehr größere KMU als kleine.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

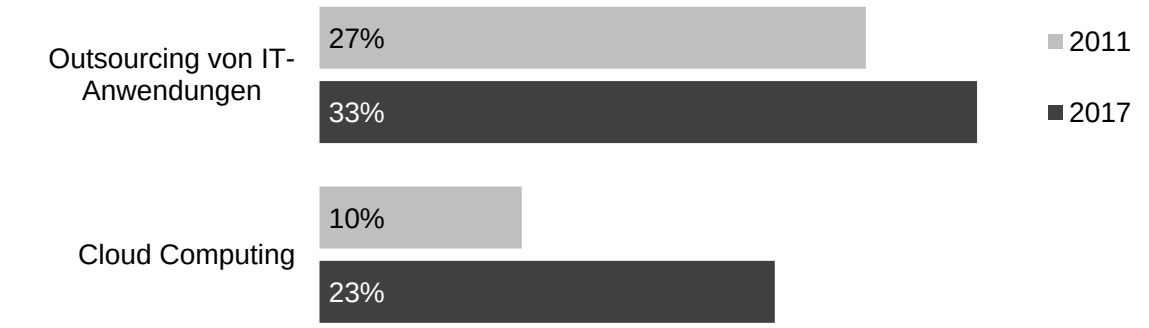
Abbildung 11: Externer IKT-Zugang in KMU



n=1.505

Starke Unterschiede existieren auch in Bezug auf den externen IKT-Zugang in KMU. Größere KMU nutzen Möglichkeiten des externen Zugangs deutlich stärker als kleine Unternehmen (vgl. Abbildung 11).

Abbildung 12: Outsourcing von IT-Anwendungen im Zeitvergleich 2011 - 2017



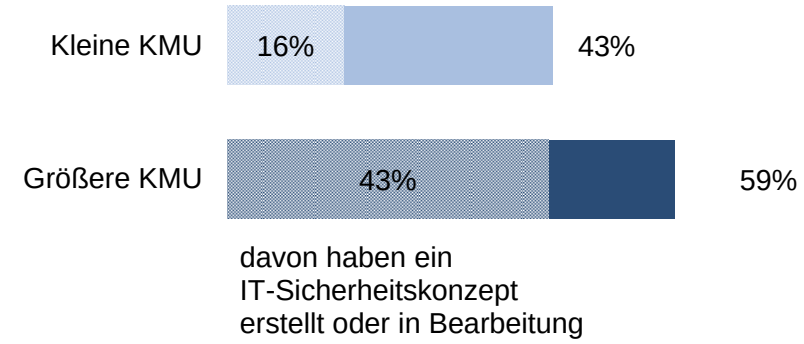
2011: n=952; 2017: n=1.505

Im Vergleich zu 2011 setzen in 2017 deutlich mehr KMU auf das Outsourcing von IT-Anwendungen (vgl. Abbildung 12). Eine starke Zunahme ist auch beim Cloud Computing zu verzeichnen, dessen Nutzung sich mehr als verdoppelte. Dabei sind kleine KMU zurückhaltender bei der Auslagerung von IT-Diensten (vgl. Abbildung 13).

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 13: Unternehmen, die IT-Anwendungen ausgelagert haben oder Cloud Computing nutzen



n=1.505

Von Unternehmen, die IT-Anwendungen ausgelagert haben oder Cloud Computing nutzen, haben nur ein Drittel der kleinen KMU und mehr als zwei Drittel der größeren ein IT-Sicherheitskonzept erstellt oder in Bearbeitung.

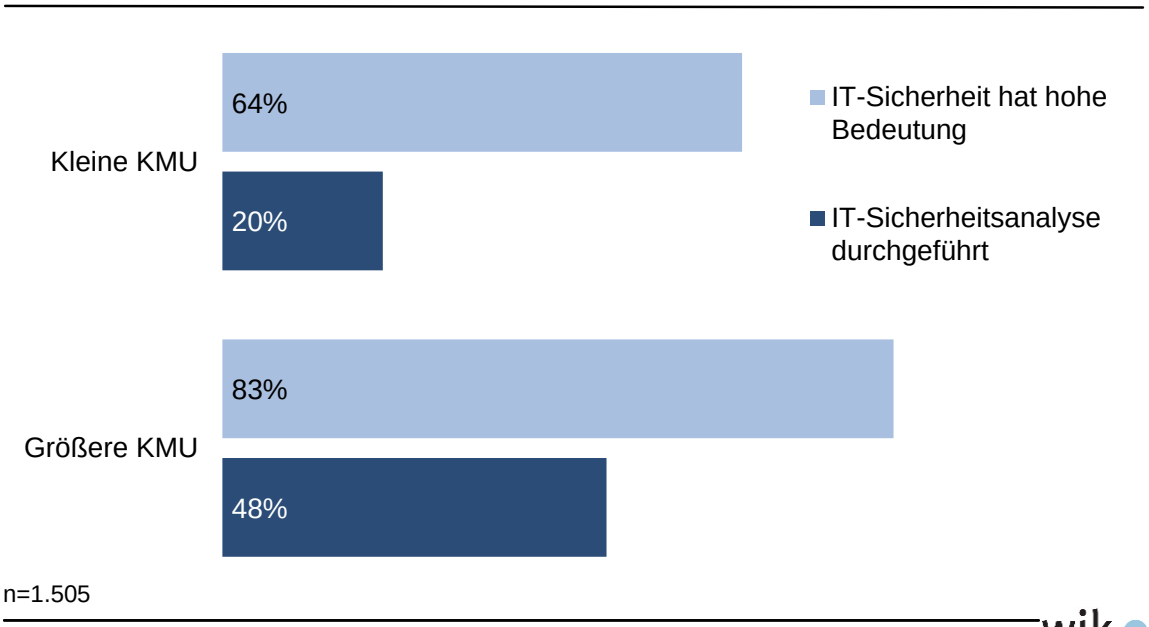
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

6 Einschätzung der Bedeutung von IT-Sicherheit

6.1 Bedeutung von IT-Sicherheit in Unternehmen

IT-Sicherheit hat im Jahr 2017 wie auch schon 2011 eine hohe Bedeutung für KMU. Wie auch vor fünf Jahren ist für insgesamt zwei Drittel der KMU die Bedeutung sehr hoch oder hoch. Dabei schätzen größere KMU IT-Sicherheit als wesentlich wichtiger ein als kleine KMU. Dies bedeutet jedoch nicht, dass die Unternehmen entsprechend handeln. Nur ein kleiner Teil dieser Unternehmen hat eine IT-Sicherheitsanalyse durchgeführt (vgl. Abbildung 14), bei größeren Unternehmen ist es aber immerhin fast die Hälfte.

Abbildung 14: Bedeutung von IT-Sicherheit



n=1.505

In dieser Diskrepanz zwischen abstrakter Bedeutung und tatsächlicher Umsetzung zeigt sich die Unsicherheit von KMU über bestehende Risiken und angemessene Lösungen. Die Vielzahl der am Markt angebotenen technischen IT-Sicherheitsmaßnahmen überfordert viele, insbesondere kleine, Unternehmen. In zahlreichen Expertengesprächen wurde deutlich, dass KMU angesichts von vorhandenen hochspezifischen Lösungen Schwierigkeiten haben, die für sie relevanten Angebote herauszufiltern.

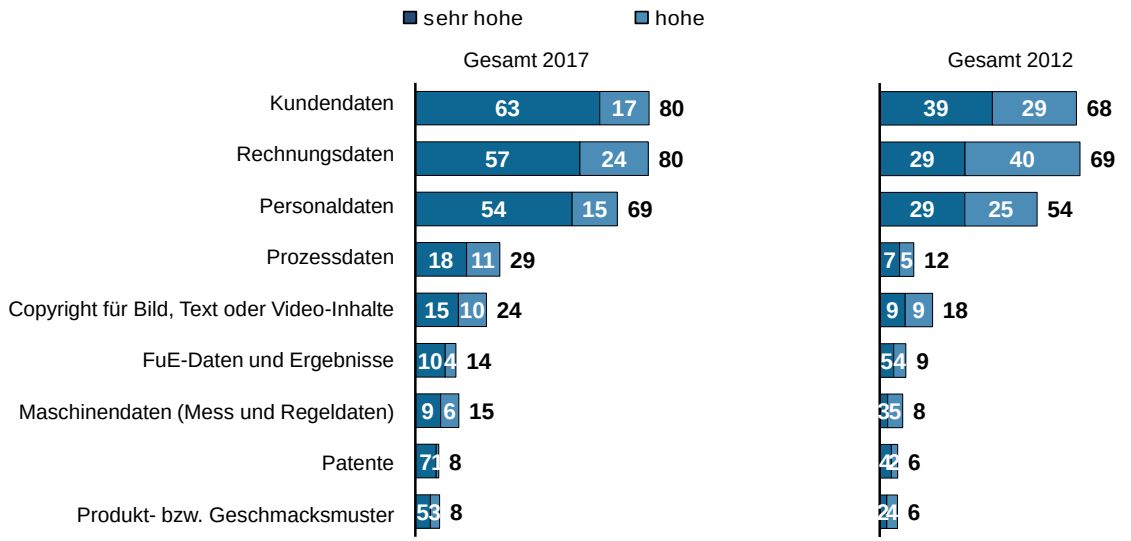
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

6.2 Einschätzung des Schutzbedarfs

Unternehmen schätzen den Schutzbedarf ihrer Datenbestände durchweg deutlich höher ein als noch in 2012. Die in den letzten Jahren prominent gewordenen Fälle von Datenleaks sowie von Schadprogrammen wie z.B. Verschlüsselungstrojanern haben zu einem gesteigerten Bewusstsein der Unternehmen geführt. Besonders ausgeprägt ist dieses Bewusstsein bei Kunden-, Rechnungs- und Personaldaten (vgl. Abbildung 15). Dennoch gibt es Unternehmen, die den Schutzbedarf ihrer Datenbestände gering oder sehr gering einschätzen.

Abbildung 15: Hohe/sehr hohe Bedeutung des Schutzbedarfs von Datenbeständen bei KMU (in Prozent)



2012: n=922; 2017: n=1.505

Frage: Welche Datenbestände oder Informationen sind in Ihrem Unternehmen besonders schützenswert? Bitte geben Sie jeweils an, ob der Schutz sehr geringe, geringe, mittlere, hohe oder sehr hohe Bedeutung hat.

Insgesamt sind besonders schützenswerte Datenbestände in den Unternehmen vor allem Kundendaten und Rechnungsdaten (jeweils 80% sehr hohe/hohe Bedeutung) sowie Personaldaten (69%). Dem Schutz der verschiedenen Datenbestände und Informationen wird auch bei der aktuellen Befragung von größeren KMU eine z.T. merklich höhere Bedeutung zuerkannt als von kleinen. Die Schutzwürdigkeit der unternehmerischen Datenbestände und Informationen wird teilweise deutlich höher eingestuft als noch 2012. Insbesondere betrifft dies Prozessdaten, Personaldaten, Kunden- und Rechnungsdaten.

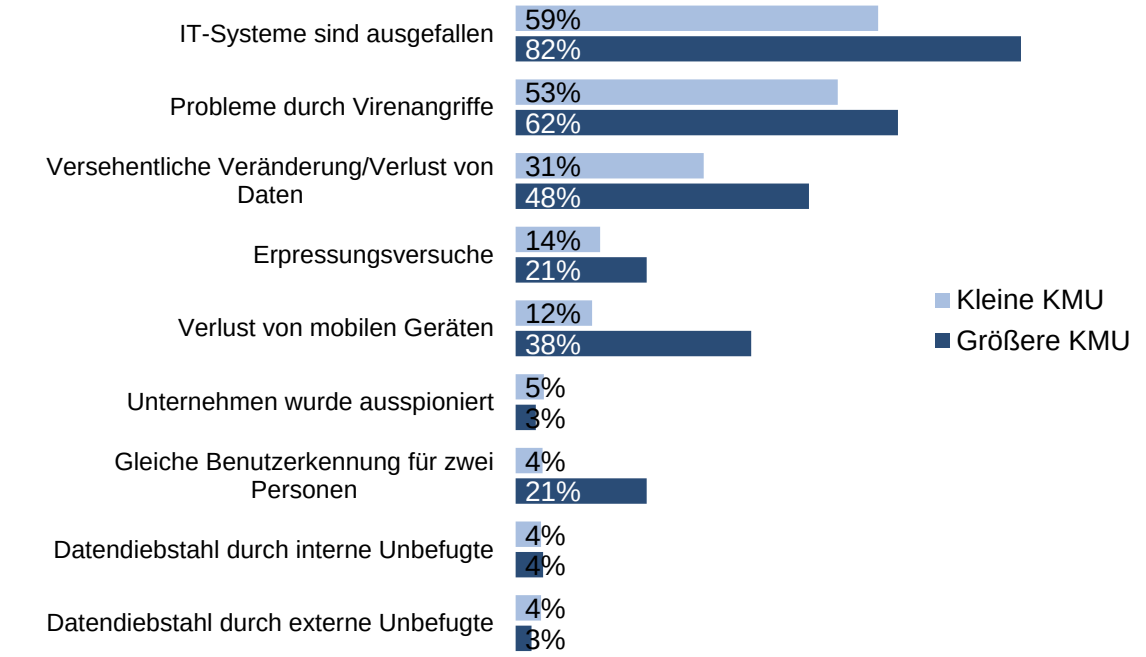
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Jedes vierte bis jedes fünfte Unternehmen schätzt die Bedeutung des Schutzbedarfs von im Unternehmen vorhandenen sensiblen Datenbeständen wie Copyrights, Forschungs- und Entwicklungsdaten, Patenten oder Produktmustern als gering oder sehr gering ein. Diese Einschätzung ist insbesondere bei kleinen Unternehmen ausgeprägt.

6.3 Hauptursachen möglicher IT-Probleme und tatsächlich aufgetretene Schadensfälle

Die überwiegende Mehrheit der KMU hat mit IT-Sicherheitsproblemen in unterschiedlicher Form zu kämpfen (vgl. Abbildung 16). Größere KMU sind durchweg häufiger betroffen als kleine Unternehmen. Große Problembereiche sind noch immer Virenangriffe und versehentlicher Datenverlust oder –veränderung, die im Vergleich zu 2011 stagnierten (vgl. Abbildung 17). IT-Systeme sind 2017 bei deutlich weniger KMU ausgefallen als 2011. Jedes fünfte Unternehmen hat keine IT-Sicherheitsprobleme bemerkt.

Abbildung 16: Konkrete Erfahrungen mit IT-Sicherheitsproblemen

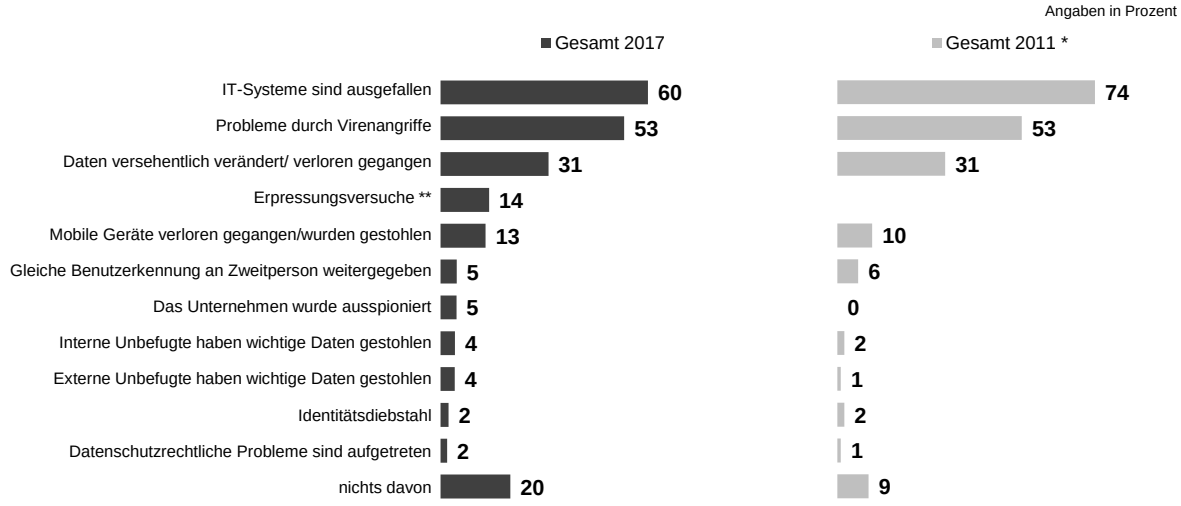


n=1.505

Frage: Haben Sie in Ihrem Unternehmen schon einmal konkrete Erfahrungen mit den folgenden IT-Sicherheitsproblemen gemacht? (Mehrfachnennungen möglich)

Der Verlust von Mobilgeräten stellt ein hohes Risiko dar, zumal dann, wenn für diese keine Schutzmaßnahmen getroffen wurden.[49] Erfahrung mit Erpressung haben 14% der KMU. Von Datendiebstählen sind KMU aller Größenklassen nur selten betroffen, vorausgesetzt, der Angriff wurde überhaupt bemerkt.

Abbildung 17: IT-Sicherheitsprobleme 2017 und 2011



2011: n=952; 2017: n=1.505

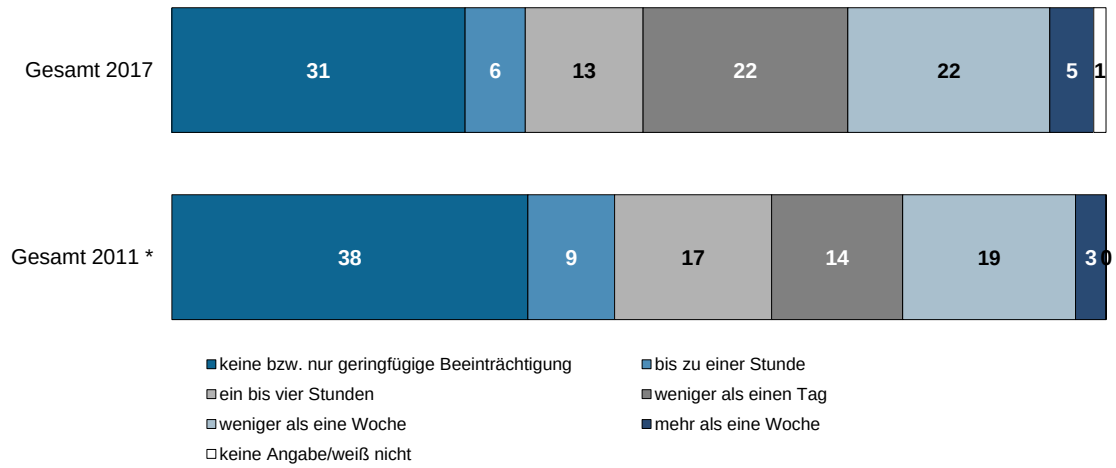
In knapp jedem dritten betroffenen Unternehmen führte das zuletzt aufgetretene IT-Sicherheitsproblem zu keinen bzw. nur geringfügigen Beeinträchtigungen (31%), bei jedem vierten Unternehmen waren die Geschäftsprozesse einen Tag und länger gestört (26%). Damit haben sich die Ausfallzeiten durch IT-Sicherheitsprobleme im Zeitverlauf nennenswert erhöht – 2011 war deutlich mehr als jedes dritte Unternehmen durch das zuletzt aufgetretene IT-Sicherheitsproblem nicht oder kaum in seinen Geschäftsprozessen gestört.

Die Geschäftsprozesse von Unternehmen, bei denen IT-Sicherheitsprobleme aufgetreten sind, waren tendenziell länger beeinträchtigt als noch 2011 (vgl. Abbildung 18). Der Anteil der Unternehmen, die keine oder nur geringfügige Beeinträchtigungen erfuhren, sank, während etwa die Hälfte der KMU mit Beeinträchtigungen zwischen mehr als vier Stunden und mehr als einer Woche zu kämpfen hatte (2011 waren dies noch 36% der KMU).

49 Einer Befragung von Deutschland sicher im Netz zufolge ist etwa jedes sechste Smartphone, Netbook oder Tablet in KMU überhaupt nicht geschützt. Vgl. DsiN (2016), DsiN SicherheitsMonitor 2016, IT-Sicherheitslage in Deutschland, S. 13.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 18: Dauer der Beeinträchtigung durch IT-Sicherheitsprobleme



n=1.505

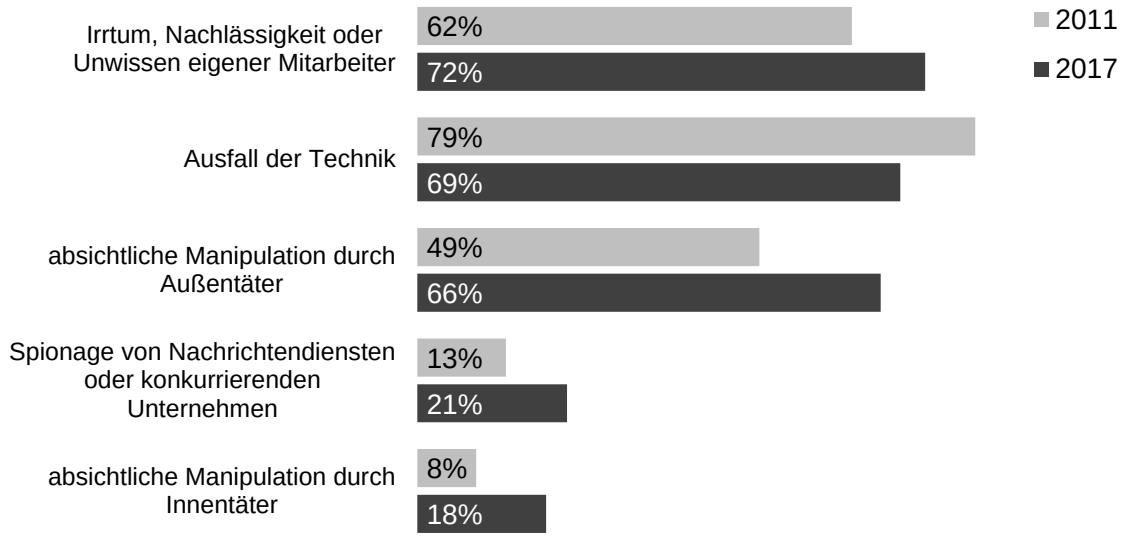
Frage: Wie lange wurden durch das letzte IT-Sicherheitsproblem in Ihrem Unternehmen Ihre Geschäftsprozesse beeinträchtigt?

Irrtum, Nachlässigkeit oder Unwissen der eigenen Mitarbeiter ist wie schon in der Befragung aus 2011 die Hauptursache für IT-Probleme und Schadensfälle in KMU (vgl. Abbildung 19) und hat weiter zugenommen. *Social Engineering* gewinnt damit weiter an Bedeutung. Im Gegensatz dazu haben technische Probleme tendenziell abgenommen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 19: Ursachen für IT-Probleme im Zeitvergleich



2011: n=952; 2017: n=1.505

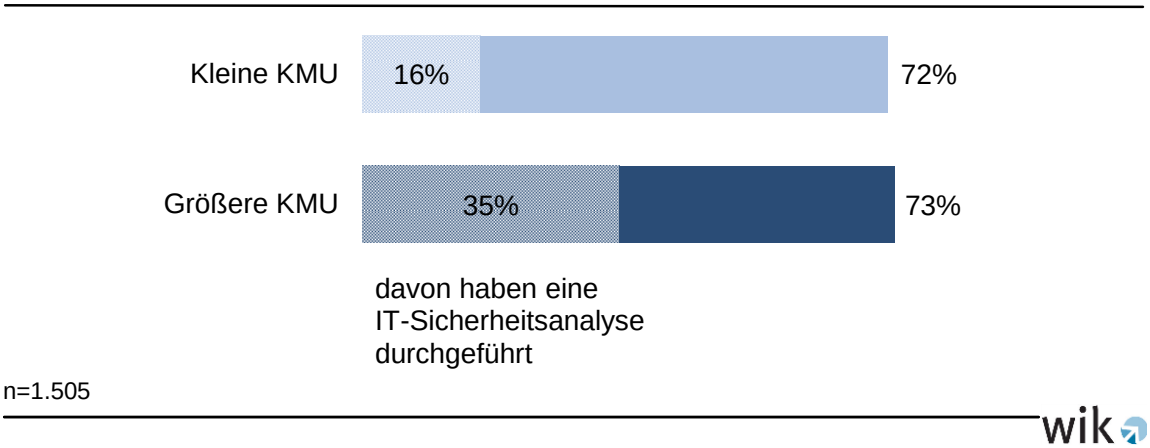
Frage: Wo sehen Sie die hauptsächlichen Ursachen für mögliche Probleme und Schadensfälle bei der IT? (Mehrfachnennungen möglich)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

6.4 Erfahrung mit Wirtschafts- und Konkurrenzspionage

Nach Einschätzung der KMU gibt es mehr Schadensfälle durch Sabotage und Spionage, sei es durch Konkurrenten oder fremde Nachrichtendienste, als noch vor fünf Jahren. Allerdings ist auch bei Unternehmen, die absichtliche Manipulation von IT oder Daten, bzw. Spionage als Ursachen für IT-Probleme und Schadensfälle ansehen, keine deutliche Zunahme bei der Durchführung von IT-Sicherheitsanalysen zu bemerken.

Abbildung 20: Unternehmen, die absichtliche Manipulation von IT oder Daten, bzw. Spionage als Ursachen für IT-Probleme und Schadensfälle ansehen



n=1.505

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

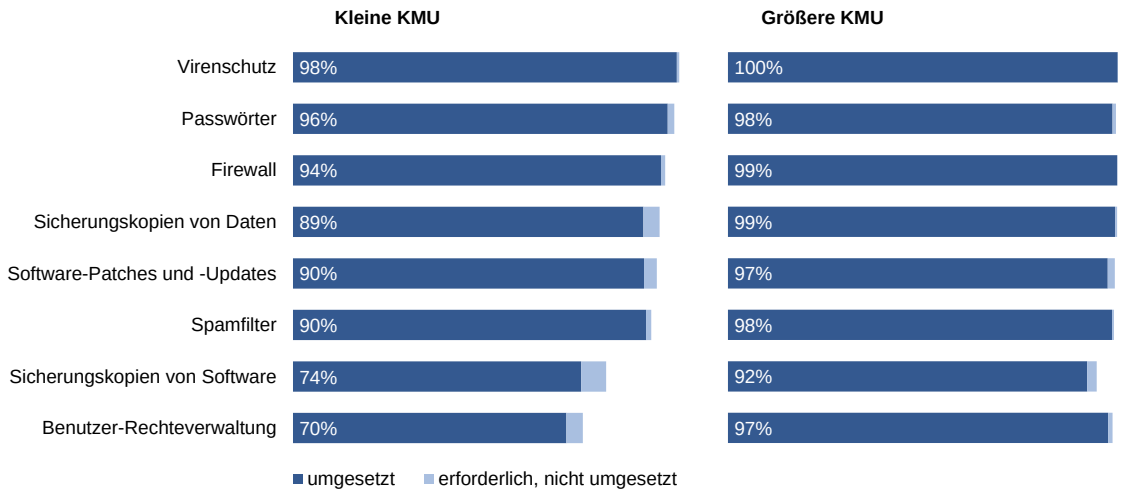
IT-Sicherheit IN DER WIRTSCHAFT

7 Umsetzung von IT-Sicherheitsmaßnahmen

7.1 Technische Maßnahmen

Die Umsetzung von technischen Basismaßnahmen befand sich bereits 2011 auf einem hohen Niveau. In größeren KMU ist in 2017 der Einsatz von Virenschutz, Passwörtern und Einsatz von Firewalls Standard (vgl. Abbildung 21). Bei den kleinen KMU besteht in einzelnen Bereichen Nachholbedarf, beispielsweise setzt jedes zehnte kleine Unternehmen keine regelmäßigen Software-Patches und Updates ein.

Abbildung 21: Technische Maßnahmen: Basisschutz



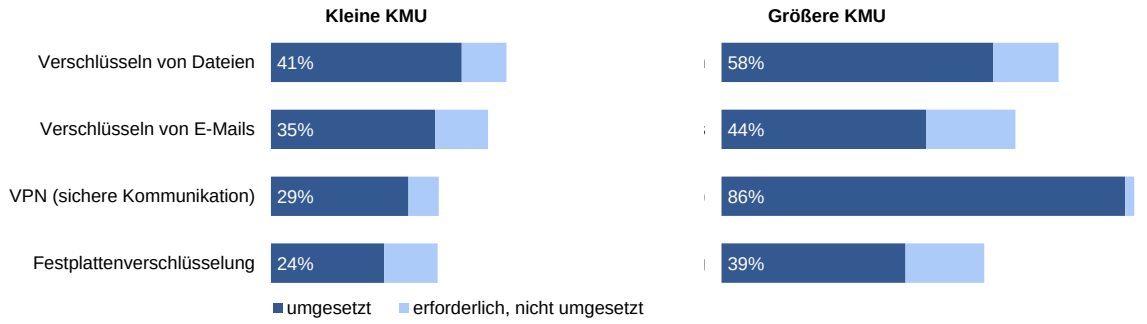
n=1.505

Frage: Halten Sie diese Maßnahmen für erforderlich und nutzen Sie sie?

Auch wenn ein Basisschutz vorhanden ist, so handelt es sich dabei meist um Einzelmaßnahmen. Eine umfassende IT-Sicherheitsanalyse hat insgesamt nur jedes fünfte Unternehmen durchführen lassen, von den größeren KMU knapp die Hälfte.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 22: Technische Maßnahmen: Verschlüsselung



2017: n=1.505

Frage: Halten Sie diese Maßnahmen für erforderlich und nutzen Sie sie?

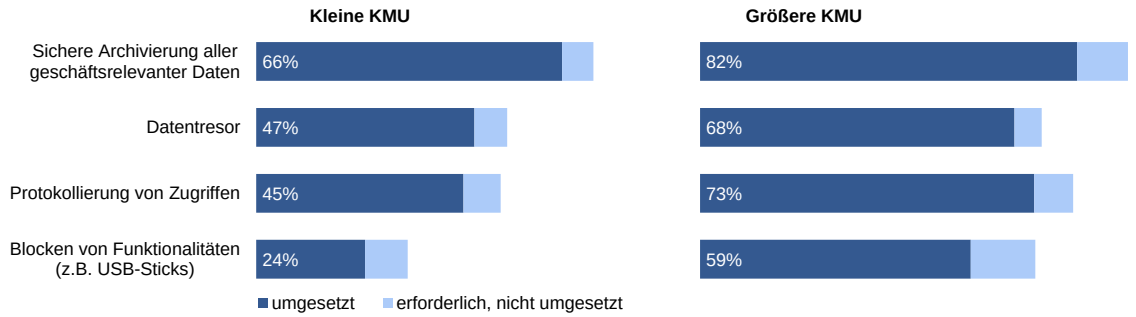
Die Nutzung von Verschlüsselungsmaßnahmen hat im Vergleich zu 2011 deutlich zugenommen. Damals hatten nur 17% der KMU ihre E-Mails verschlüsselt. Heute verschlüsseln 35% der KMU ihre E-Mails, 11% halten Verschlüsselung für notwendig, haben sie aber noch nicht umgesetzt (vgl. Abbildung 22). Festplattenverschlüsselung für Notebooks und Verschlüsselung von Dateien haben leicht zugenommen. Im Vergleich zu den technischen Basismaßnahmen zeigt sich, dass kleine Unternehmen technische Maßnahmen zur Verschlüsselung deutlich seltener umsetzen als größere KMU.

Ein ähnliches Bild zeigt sich bei den Maßnahmen zur Datensicherung (vgl. Abbildung 23). Größere KMU nutzen Datensicherungsmaßnahmen häufiger als kleine Unternehmen, aber Umsetzungslücken bestehen bei KMU aller Größen. So sind mehr als die Hälfte der kleinen Unternehmen und immerhin jedes vierte größere KMU nicht in der Lage, unberechtigte Zugriffe zu entdecken.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 23: Technische Maßnahmen: Datensicherung



n=1.505

Frage: Halten Sie diese Maßnahmen für erforderlich und nutzen Sie sie?

7.2 Organisatorische Maßnahmen

Nur in etwas mehr als jedem vierten Unternehmen sind für die verwendete IT irgendwelche eigens erstellte Dokumentationen, Anleitungen oder Anweisungen vorhanden (28%), darunter etwa gleich häufig Dokumentationen zu den IT-Systemen (21%), Notfallpläne (18%), Dokumentationen zur IT-Sicherheit sowie Netzwerkpläne (jeweils 16%). Damit wird die verwendete IT-Technik seltener dokumentiert als noch vor sechs Jahren. Während größere KMU Dokumentationen und Anleitungen genauso häufig erstellen wie zum damaligen Zeitpunkt, ist bei kleineren Unternehmen ein Rückgang zu registrieren.

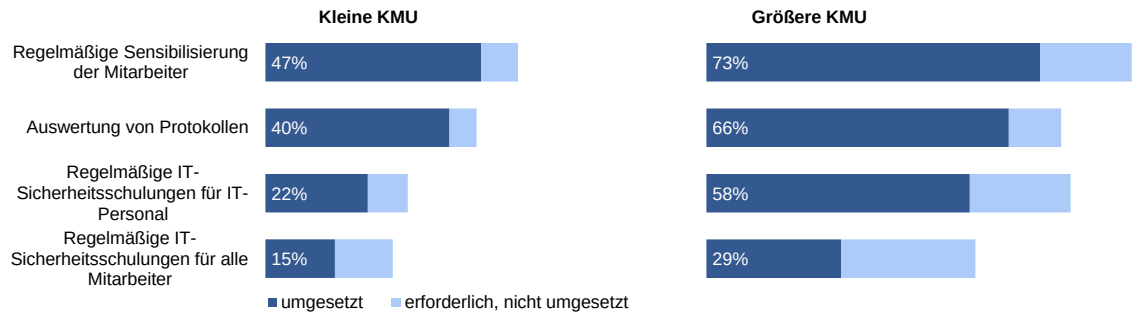
Sind allerdings Notfallpläne oder andere Dokumentationen zur IT-Sicherheit vorhanden, werden diese Konzepte von der deutlich überwiegenden Mehrheit der betreffenden Unternehmen regelmäßig aktualisiert und geübt (82%), und zwar deutlich häufiger, als es 2011 der Fall war. Diese Veränderung hat sich ausschließlich bei kleineren Unternehmen vollzogen, die sich inzwischen durch den im Vergleich aktivsten Umgang mit den Sicherheitskonzepten auszeichnen. Bei größeren KMU sind im Zeitvergleich kaum Veränderungen beim Umgang mit Notfallplänen und IT-Sicherheitskonzepten festzustellen.

KMU setzen organisatorische Maßnahmen insgesamt seltener um als technische Maßnahmen. Weniger als die Hälfte der kleinen Unternehmen sensibilisiert die Mitarbeiter für Sicherheitsrisiken, bei größeren KMU verzichten darauf immerhin noch ein Viertel der KMU (vgl. Abbildung 24). Schulungen für alle Mitarbeiter bleiben eine Lücke bei allen KMU. Sogar spezialisiertes IT-Personal wird zu wenig geschult. Dies zeigt ein geringes Bewusstsein für die Bedeutung von Schulungen. Immerhin 13% der KMU sehen hier Nachholbedarf, und rund 30 % der größeren KMU. Auf Auswertungen von Pro-

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

tokollen, wie etwa Systemzugriffe oder Firewallprotokolle, verzichten mehr als die Hälfte der kleinen Unternehmen und ein Drittel der größeren KMU.

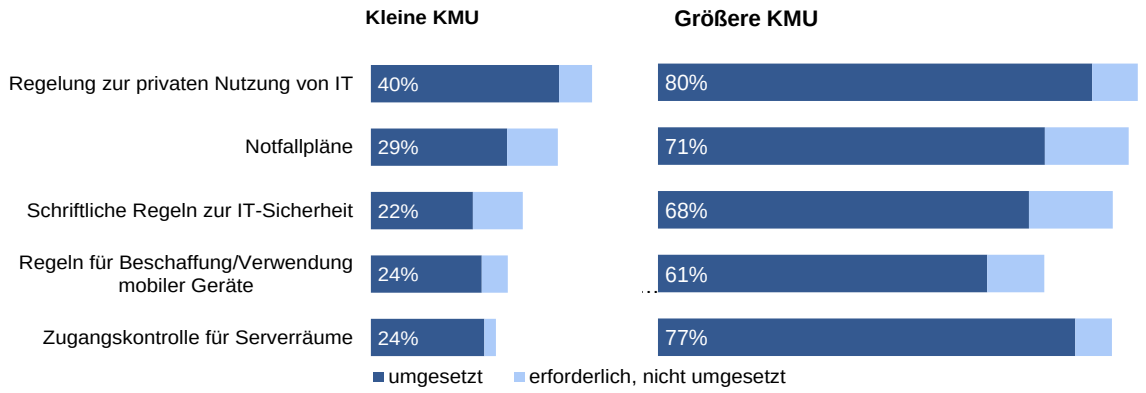
Abbildung 24: Organisatorische Maßnahmen: Schulungen und Auswertungen



n=1.505

Frage: Bitte geben Sie an, welche organisatorischen Maßnahmen im Bereich IT-Sicherheit Sie für Ihr Unternehmen für erforderlich halten und welche Sie umgesetzt haben.

Abbildung 25: Organisatorische Maßnahmen: Regeln und Kontrollen



n=1.505

Frage: Bitte geben Sie an, welche organisatorischen Maßnahmen im Bereich IT-Sicherheit Sie für Ihr Unternehmen für erforderlich halten und welche Sie umgesetzt haben.

Regeln und Kontrollen sind in den größeren KMU weit verbreitet. Inwieweit diese von allen Mitarbeitern eingehalten werden, ist angesichts des Nachholbedarfs bei Schulungen und bei Mitarbeitersensibilisierungen für IT-Sicherheit zumindest fraglich. Kleine Unternehmen implementieren Regeln und Kontrollen seltener. So dulden 60% der klei-

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

nen Unternehmen die private Nutzung von IT. Bei drei Viertel der kleinen Unternehmen fehlen einfache Regeln wir Zugangskontrollen für Serverräume oder schriftliche Regeln zur IT-Sicherheit.

Bei IT-Problemen und konkreten Schadensfällen sind nur 29% der kleinen und 71% der größeren KMU durch Notfallpläne vorbereitet.

Die Umsetzungslücke bei den organisatorischen Maßnahmen mag auch damit zusammenhängen, dass IT-Sicherheit in vielen Unternehmen noch keine Chefsache ist: in nur knapp der Hälfte der kleinen Unternehmen lässt sich die Geschäftsführung regelmäßig über den Stand der IT-Sicherheit unterrichten. Bei den größeren KMU wird die Leitung jedes vierten Unternehmens nicht regelmäßig über den Stand der IT-Sicherheit informiert. Im Vergleich zu 2011 hat das Interesse der Geschäftsführung an IT-Sicherheit sogar abgenommen.[50] Wie bereits in Kapitel 6.1 beschrieben, hat nur ein kleiner Teil der KMU (20% der kleinen Unternehmen und 48% der größeren KMU) eine systematische IT-Sicherheitsanalyse durchgeführt.

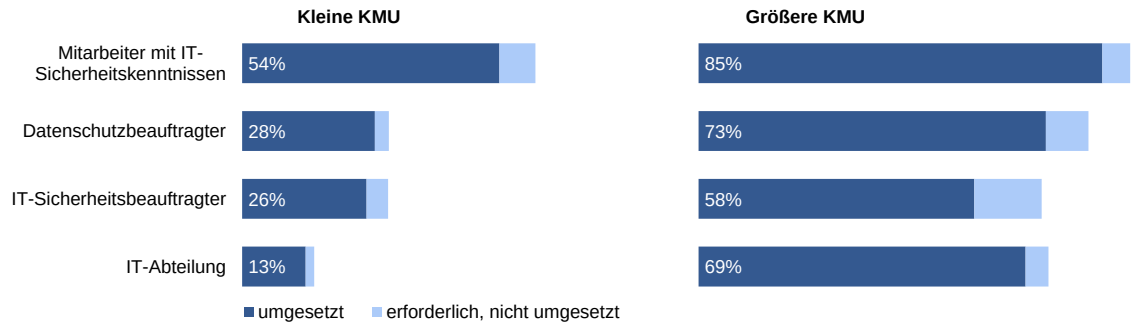
7.3 Personelle Maßnahmen

Mitarbeiter mit IT-Sicherheitskenntnissen sind in etwas mehr als der Hälfte der KMU vorhanden. Dabei haben größere KMU die Nase vorn, bei ihnen sind in 85% der Fälle Mitarbeiter mit IT-Sicherheitskenntnissen beschäftigt (vgl. Abbildung 26). Ein IT-Sicherheitsbeauftragter oder eine IT-Abteilung ist nur in 13% der kleinen Unternehmen vorhanden. Die spärliche Ausstattung mit IT-Fachpersonal ist auch auf die hohen Kosten für spezialisiertes Personal zurückzuführen. Experten zufolge liegt das Gehalt eines IT-Sicherheitsspezialisten erheblich über den jährlich (vermutlich) verursachten Schäden.

50 In 2011 ließ sich die Unternehmensleitung von 56% der KMU regelmäßig über den Stand der IT-Sicherheit berichten.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 26: Personelle Maßnahmen

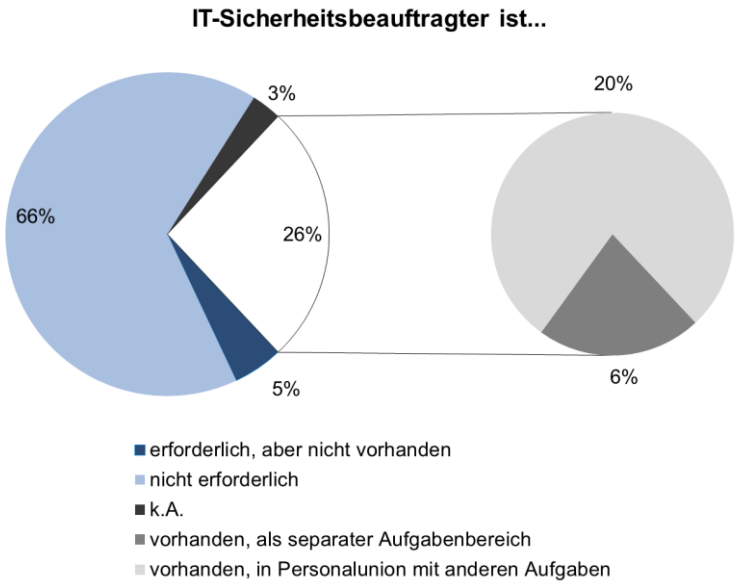


n=1.505

Frage: Welche personellen Maßnahmen im Bereich IT-Sicherheit halten Sie in Ihrem Unternehmen für erforderlich und welche sind bereits vorhanden?.

Insbesondere kleine Unternehmen haben nicht die Ressourcen, um Mitarbeiter nur für IT-Sicherheitsmaßnahmen einzustellen. Zwei Drittel der kleinen KMU halten einen IT-Sicherheitsbeauftragten nicht für erforderlich, s. Abbildung 27. Zwar ist in jedem Vierten kleinen KMU ein IT-Sicherheitsbeauftragter vorhanden, aber nur in 6% der kleinen KMU als separater Aufgabenbereich.

Abbildung 27: IT-Sicherheitsbeauftrage in kleinen Unternehmen (bis 49 Mitarbeiter)



Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

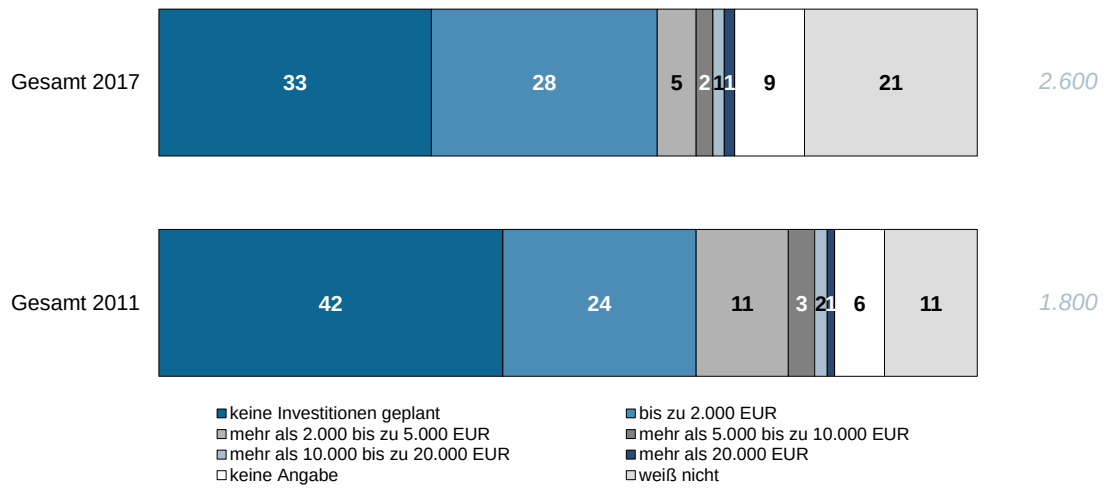
8 Investitionen in IT-Sicherheit

Für das laufende Geschäftsjahr (2017) planen die Unternehmen durchschnittlich 2.600 EUR für Ausgaben im Bereich IT-Sicherheit, wobei erwartungsgemäß mit der Unternehmensgröße auch die Investitionshöhe steigt. Die KMU investieren damit deutlich mehr als noch 2011. Allerdings beabsichtigt auch in diesem Jahr jedes dritte Unternehmen keinerlei Investitionen in diesem Bereich (33%). Der prozentuale Anteil der Ausgaben für IT-Sicherheit am IT-Budget insgesamt beträgt ca. 11% und liegt damit fast auf dem Niveau der vorausgegangenen Befragung.

Die Spanne der für 2017 geplanten Investitionen in IT-Sicherheit ist sehr breit und reicht von unter 100 Euro bis zu mehreren Hunderttausend Euro in der Spitze. (vgl. Abbildung 28). Unternehmen geben zu ihren Investitionen häufig keine genaue Auskunft. Daher sind die Ergebnisse der Befragung in diesem Punkt zurückhaltend zu bewerten.

Abbildung 28: Geplante Investitionen (Durchschnittsbetrag in Euro)

Angaben in Prozent



Basis: relevante technische Ausstattung vorhanden n=1.505 (2011 n=952)

Frage: In welcher Höhe planen Sie Investitionen im Bereich IT-Sicherheit im gesamten laufenden Geschäftsjahr (2017)?

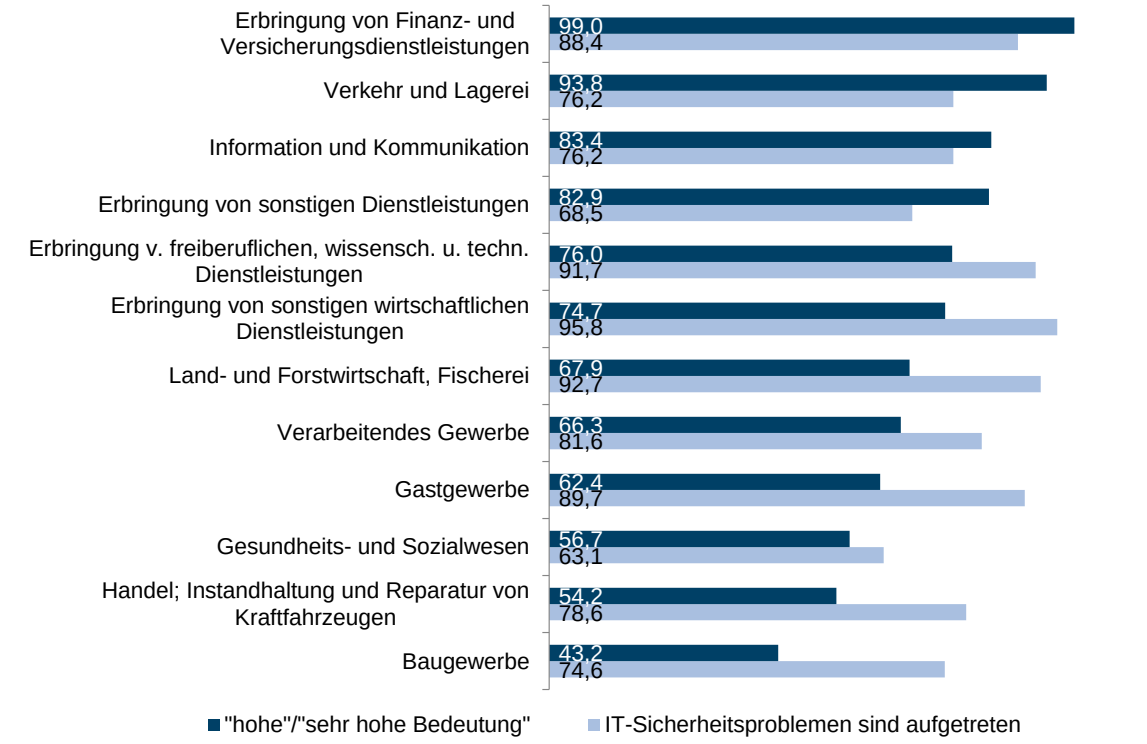
Kleine Unternehmen investieren häufiger gar nicht in IT-Sicherheit als größere KMU, was aber angesichts ihrer geringeren finanziellen Ressourcen nicht überrascht.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

9 IT-Sicherheitsniveau im Branchenvergleich

Abbildung 29 zeigt, wie unterschiedlich KMU die Bedeutung von IT-Sicherheit in Abhängigkeit der Branche einschätzen. Hochsensibel im Hinblick auf IT-Sicherheit sind Dienstleister in der Finanz- und Versicherungsbranche, während im Baugewerbe und im Handel nur etwa jedes zweite Unternehmen IT-Sicherheit eine hohe Bedeutung beimisst.

Abbildung 29: Bedeutung von IT-Sicherheit nach Branchen (in %)



n=1.505

Zusätzlich zu der allgemeinen Brancheneinteilung wurden KMU zu ihrer Zugehörigkeit zum Handwerk sowie zur Gruppe der Rechtsanwälte, Steuerberater und Wirtschaftsprüfer befragt. Handwerksbetriebe liegen bei der Bedeutung von IT-Sicherheit im unteren Mittelfeld, für 60 Prozent hat IT-Sicherheit eine hohe Bedeutung. Die Gruppe der Rechtsanwälte, Steuerberater und Wirtschaftsprüfer, die mit sensiblen Daten umgehen, misst der IT-Sicherheit hohe Bedeutung zu, gehört aber mit 79 Prozent nicht zur Spitzengruppe.

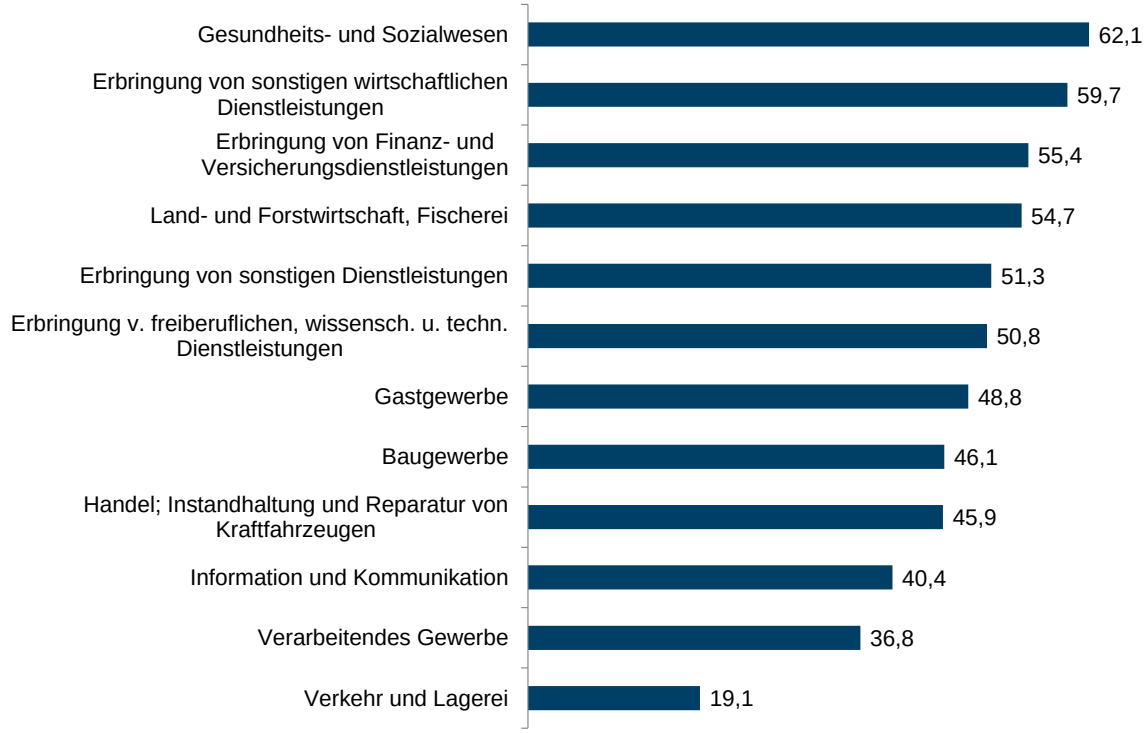
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Durchweg jede Branche hatte in der Vergangenheit bereits mit IT-Sicherheitsproblemen zu kämpfen. Sowohl KMU, für die IT-Sicherheit wichtig ist, als auch IT-sicherheitsferne KMU waren davon betroffen (vgl. Abbildung 29). Daran zeigt sich ein deutliches Missverhältnis zwischen Bewusstsein und konkreter Bedrohung bei vielen KMU.

In den Expertengesprächen wurde deutlich, wie sehr die praktische Umsetzung von IT-Sicherheit nicht nur von technischen Maßnahmen abhängt. Von besonderer Bedeutung ist die gelebte IT-Sicherheit im Arbeitsalltag aller Mitarbeiter. Technische Lösungen können umgangen oder manuell deaktiviert werden, wenn der einzelne Mitarbeiter nicht davon überzeugt ist, dass die Lösung sinnvoll ist. Experten empfehlen daher eine regelmäßige Sensibilisierung aller Mitarbeiter. Dies wird aber nur von einem Teil der KMU umgesetzt (vgl. Abbildung 30). In einigen Branchen scheinen solche Maßnahmen geradezu unüblich zu sein, z.B. Verkehr und Lagerei. Aber auch in Branchen wie der Finanz- und Versicherungsbranche, für die IT-Sicherheit eine hohe Bedeutung hat, setzen nur gut die Hälfte der KMU Mitarbeiterschulungen zur Sensibilisierung um.

Abbildung 30: Regelmäßige Sensibilisierung der Mitarbeiter umgesetzt



n=1.505

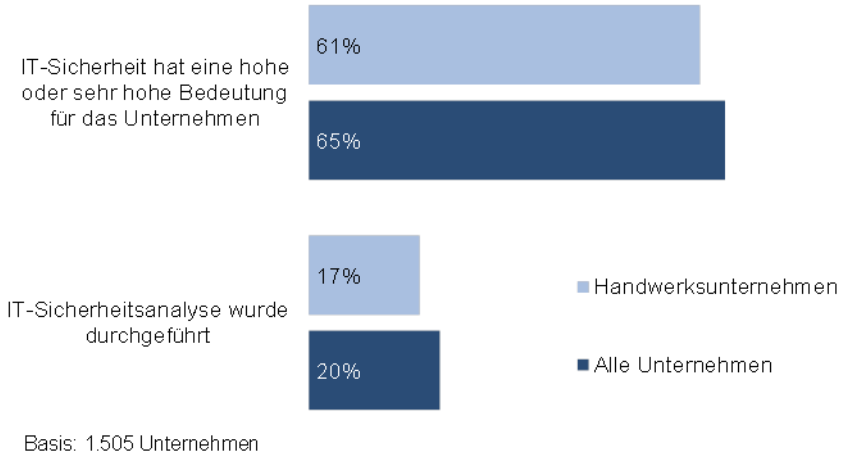
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

9.1 Handwerk

Handwerksbetriebe stehen bei der Umsetzung von IT-Sicherheit besonderen Herausforderungen gegenüber, weil die weit überwiegende Mehrheit aus sehr kleinen Betrieben besteht, gemessen an der Anzahl der Mitarbeiter. 91% aller befragten Handwerksbetriebe haben weniger als zehn Mitarbeiter, und damit nur sehr beschränkte Ressourcen für die Umsetzung von IT-Sicherheit. Dies zeigt sich auch an der Ausstattung mit Personal, das über IT-Sicherheitskenntnisse verfügt: nur 39% der befragten Handwerksbetriebe haben Mitarbeiter mit IT-Sicherheitskenntnissen.[51]

KMU im Handwerk sind IT-affin und verfügen im Vergleich zu den KMU aller Branchen über ein annähernd durchschnittliches IT-Sicherheitsbewusstsein.

Abbildung 31: IT-Sicherheitsbewusstsein im Handwerk



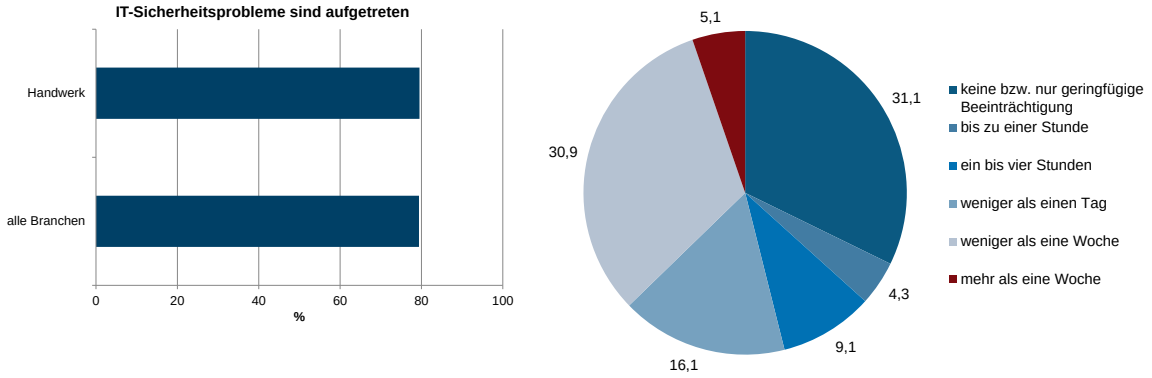
Dies steht im deutlichen Gegensatz zu den Erfahrungen, die Handwerksbetriebe mit IT-Sicherheitsproblemen haben (vgl. Abbildung 32): bei vier von fünf Handwerksbetrieben sind schon einmal IT-Sicherheitsprobleme aufgetreten. Dies entspricht dem Durchschnitt über alle Branchen. Allerdings beeinträchtigen IT-Sicherheitsprobleme die Geschäftsprozesse von Handwerksunternehmen länger als den Durchschnitt aller Branchen (vgl. Kapitel 6.3). Fast jeder dritte Betrieb mit IT-Sicherheitsproblemen war mehrere Tage dadurch beeinträchtigt.

51 Weniger als 10% haben eine eigene IT-Abteilung, was aber mit der Größe der Betriebe zusammenhängt.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 32: Erfahrungen mit IT-Sicherheitsproblemen im Handwerk



n=1.505 n=354

Handwerksbetriebe arbeiten häufig bereits sehr digitalisiert. Sie setzten computergesteuerte und teilweise vernetzte Maschinen ein, nehmen an elektronischer Auftragsvergabe teil und schreiben elektronische Rechnungen. Zudem kommunizieren sie mit Kunden, Zulieferern und Kooperationspartnern über digitale Kanäle. Dazu nutzen sie häufig neben professionellen Anwendungen (z.B. für den elektronischen Austausch von Beitrags- und Steuerdaten) auch Anwendungen, die für den privaten Einsatz entwickelt sind wie WhatsApp und soziale Netzwerke. Abhängig von der Größe und der Branche eines Handwerksbetriebs sind das Bewusstsein für IT-Sicherheit und die Ausstattung damit sehr heterogen. Als Vorreiter gelten unter Branchenkennern Sanitär- und Heizungsbauer sowie Elektroinstallateure, da diese Gewerke durch den alltäglichen Umgang mit komplexen Sicherheitsvorgaben aus dem Elektro- und Heizungsbereich ein hohes Sicherheitsbewusstsein haben. Zudem verbauen diese Gewerke bereits heute vernetzte Gebäudetechnik und müssen dabei auch für die IT-Sicherheit der Systeme sorgen.

Viele Handwerksbetriebe unterschätzen jedoch sowohl ihre eigene Bedeutung als auch den Schutzbedarf ihrer Daten. Die allgemeine Haltung „Wer soll mich schon angreifen, bei mir gibt es nichts zu holen“ ist nach Meinung von Experten weit verbreitet, und hält Betriebe davon ab, zusätzlich zu einem IT-Basisschutz ein umfassendes Sicherheitskonzept zu entwickeln. Dabei übersehen Unternehmen zwei Faktoren: zum ersten sind viele Schadprogramme sozusagen blind, unterscheiden also nicht nach lohnenden oder nicht lohnenden Zielen, sondern suchen nach Systemen mit Sicherheitslücken. Zum zweiten speichert auch das kleinste Handwerksunternehmen Daten, die für potenzielle Angreifer von Interesse sind. Dies können neben personenbezogenen Daten von Mitar-

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

beitern auch Angebotspreise in (öffentlichen) Ausschreibungen sein oder Kontoverbindungen von Kunden und Lieferanten.

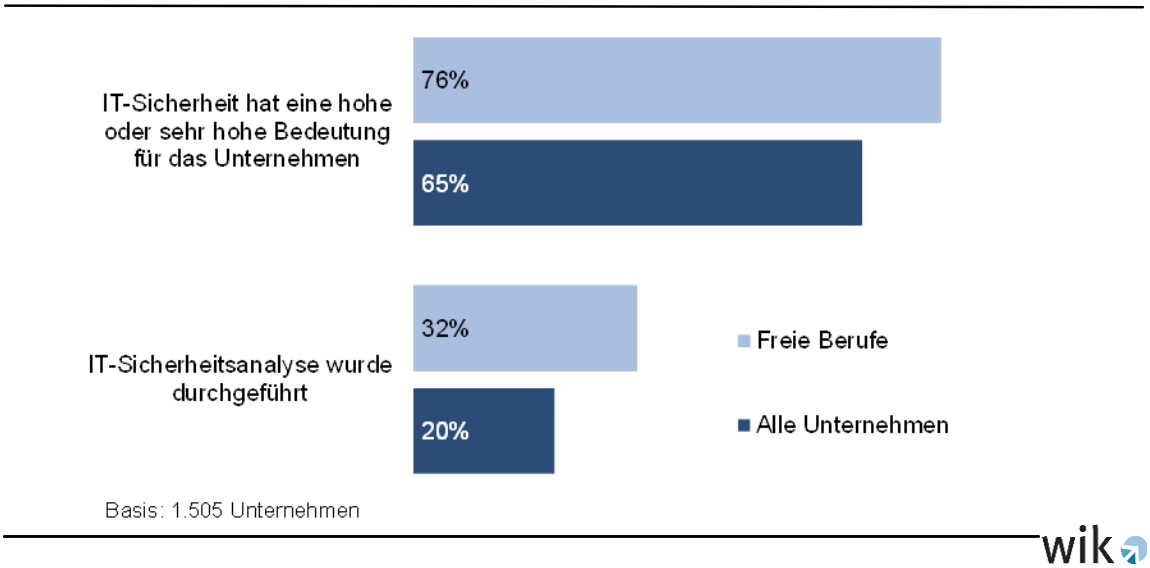
9.2 Freie Berufe

Unternehmen, die im Bereich der freien Berufe (Wirtschaftsprüfer, Rechtsanwälte, Steuerberater, Ingenieure) tätig sind, setzen weit mehr IT-Technik ein als der Durchschnitt aller Branchen und speichern zum Teil besonders sensible Daten ihrer Kunden. Von diesen Unternehmen sind daher höhere Anstrengungen zum Schutz ihrer IT-Systeme zu erwarten als in anderen Branchen.

Das Kommunikationsverhalten von Unternehmen in den freien Berufen unterscheidet sich deutlich von anderen Branchen. So nutzt weniger als ein Viertel der Unternehmen in freien Berufen WhatsApp zur Kommunikation - im Vergleich zu zwei Dritteln im Baugewerbe und 55% der Handwerksbetriebe. Im Hinblick auf den Zugang zu ihren Daten sind die Unternehmen vorsichtiger als der Durchschnitt aller Branchen, nur jedes zehnte nutzt Cloud Computing und nur jedes dritte erlaubt den mobilen Zugriff mit Smartphones.

Insgesamt haben Unternehmen in freien Berufen ein höheres Sicherheitsbewusstsein als andere Branchen: knapp vier von fünf Unternehmen aus den freien Berufen messen IT-Sicherheit eine hohe oder sehr hohe Bedeutung zu. Ein hoher Anteil dieser Unternehmen hat eine IT-Sicherheitsanalyse durchgeführt.

Abbildung 33: IT-Sicherheitsbewusstsein bei Freien Berufen

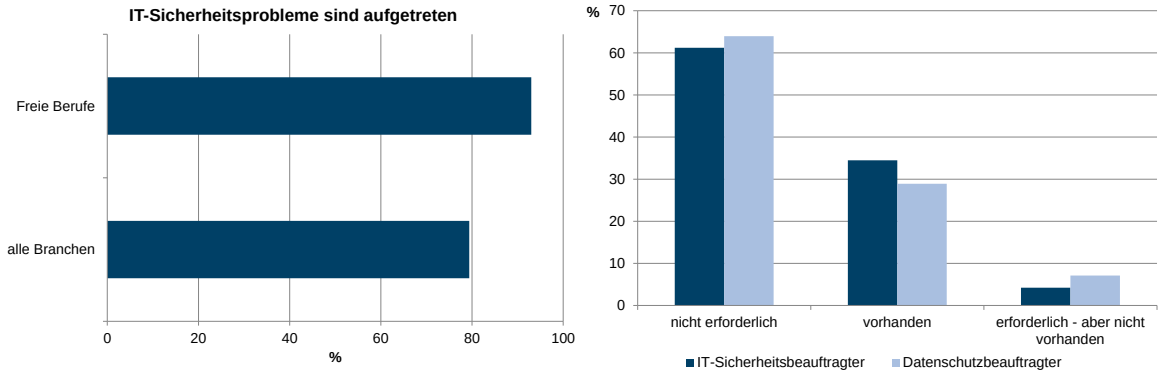


Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Dennoch sind IT-Sicherheitsprobleme in der Branche häufiger als im Durchschnitt aller Branchen aufgetreten (vgl. Abbildung 34 links).

Abbildung 34: IT-Sicherheit in den freien Berufen



n=1.505 n=165

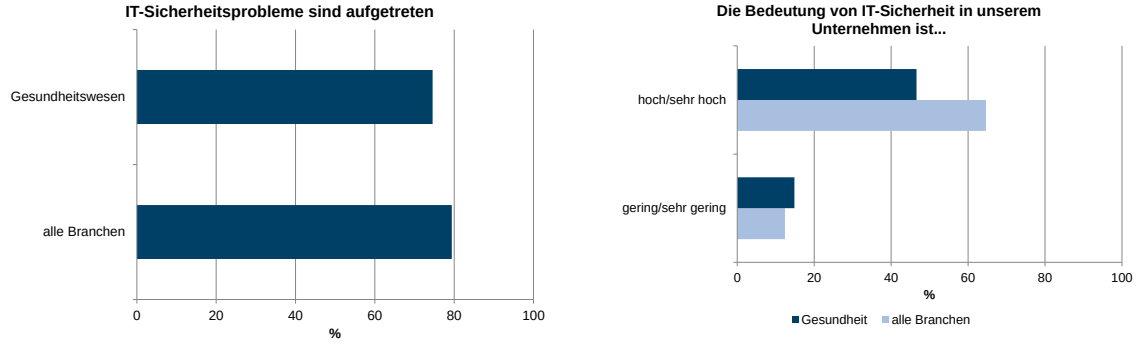
In den Unternehmen der freien Berufe hinkt die Umsetzung von IT-Sicherheit hinterher. Nur etwa jedes dritte Unternehmen in freien Berufen hat eine systematische IT-Sicherheitsanalyse durchgeführt, etwa vier von fünf Unternehmen haben keine Dokumentationen zu ihren IT-Systemen wie Netzwerk- oder Notfallpläne. Wie die rechte Grafik in Abbildung 34 zeigt, hält die Mehrheit der Unternehmen in freien Berufen die Benennung eines IT-Sicherheits- oder Datenschutzbeauftragen für nicht erforderlich. Immerhin haben bereits 42% der Unternehmen die Dienste eines IT-Sicherheitsberaters in Anspruch genommen.

9.3 Gesundheit

Der Gegensatz zwischen Anspruch an IT-Sicherheit und Realität in Praxen und Gesundheitsinstitutionen könnte kaum größer sein. Alarmierend gering ist der Anteil der Unternehmen aus dem Bereich Gesundheits- und Sozialwesen, für die IT-Sicherheit insgesamt eine hohe Bedeutung hat (vgl. Abbildung 35, rechte Seite). Während der Schutz von personenbezogenen Daten (Kunden- und Rechnungsdaten sowie Daten der Mitarbeiter) zwar in mehr als 90 % der Unternehmen in der Gesundheitsbranche eine hohe oder sehr hohe Bedeutung hat, mangelt es an der praktischen Umsetzung des Schutzes. Konkrete Probleme mit IT-Sicherheit treten mit vergleichbarer Häufigkeit in Unternehmen im Gesundheitswesen wie im Durchschnitt über alle Branchen auf (vgl. Abbildung 35, linke Seite).

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 35: Erfahrungen mit IT-Sicherheitsproblemen im Gesundheits- und Sozialwesen



n=1.505 n=1.505

Beim Anteil der Unternehmen, die eine systematische IT-Sicherheitsanalyse durchgeführt haben, liegt die Gesundheitsbranche weit zurück: nur 15% der Unternehmen haben ihre IT-Sicherheit systematisch analysiert, weniger Unternehmen haben dies nur noch in den Branchen Baugewerbe sowie Verkehr und Lagerei untersucht. Ein technischer Basisschutz durch Virenscanner und Firewall ist vorhanden. In der Gesundheitsbranche ist die Authentifizierung durch Passwörter sowie die Verwaltung von Benutzerrechten und Protokollierung von Zugriffen relativ weit verbreitet. Jedoch ist der tägliche Umgang mit diesen IT-Sicherheitstools äußerst lax: die Nutzung eines einzigen Benutzerkontos ist gängiger Standard in Praxen und Krankenhäusern, zum Teil nutzen ganze Krankenhausabteilungen ein einziges Passwort gemeinsam. Auch sind Mitarbeiter mit IT-Sicherheitskenntnissen und Datenschutzbeauftragte nur in einer Minderheit der Unternehmen vorhanden.

Experten zufolge ist die schlechte Situation der IT-Sicherheit im Gesundheitswesen auf drei Faktoren zurückzuführen. Erstens herrscht in der Branche ein starker Kostendruck, und sichere IT-Systeme haben nicht oberste Priorität bei Budgetentscheidungen. Zweitens sind sichere IT-Tools für den Arbeitsalltag in Arztpraxen oder Krankenhäusern sehr aufwändig zu handhaben. Aufgrund des Zeitdrucks könne medizinisches Personal nicht Qualität in der Patientenversorgung *und* IT-Sicherheit gewährleisten, sodass in der Realität oft IT-Sicherheit zugunsten der Patientenversorgung vernachlässigt werde. Beispielsweise fehlten einfache *single sign-on* Lösungen. Drittens verfügen Ärzte und anderes medizinisches Personal weder über IT-Sicherheitskenntnisse noch ist die Vermittlung eines Sicherheitsbewusstseins Bestandteil der medizinischen Grundausbildung. In vielen Unternehmen im Gesundheitswesen existiert kein Bewusstsein für den

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

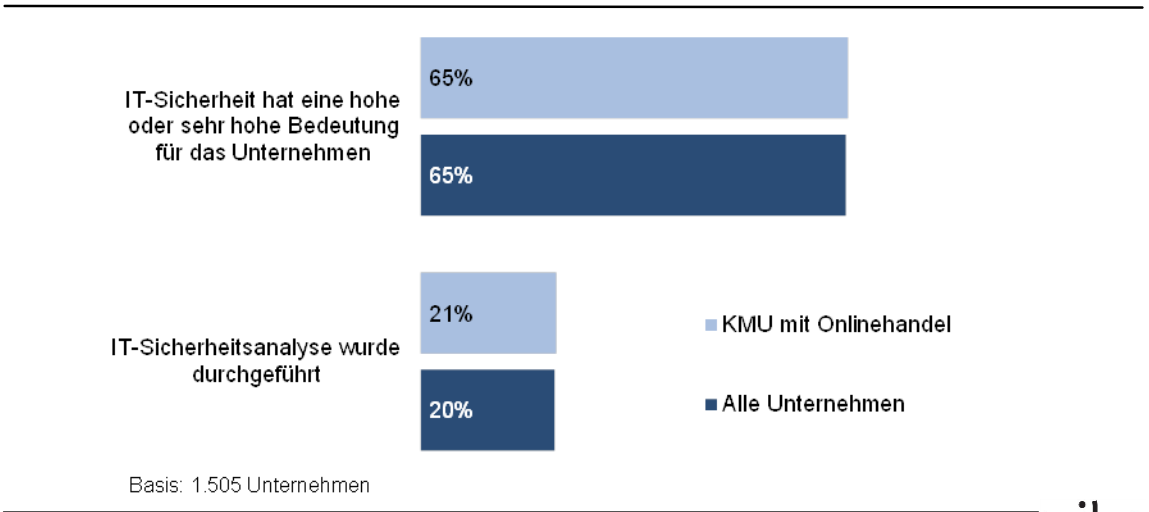
IT-Sicherheit IN DER WIRTSCHAFT

Wert von Patientendaten, oder auch von Daten über die Verschreibung bestimmter Medikamente.

9.4 E-Commerce

Das Geschäftsmodell von E-Commerce-Unternehmen ist vollständig oder zumindest teilweise digitalisiert. Als E-Commerce-Unternehmen werden in dieser Studie solche KMU definiert, die Leistungen über das Internet in einem eigenen Shop oder auf Marktplätzen anbieten, oder ein Onlinereservierungssystem für Termine oder Tickets betreiben. Aufgrund ihrer digitalen Geschäftsmodelle sind E-Commerce-Unternehmen gut mit PC-Arbeitsplätzen mit Internetzugang ausgestattet. Sie nutzen auch überdurchschnittlich häufig innovative Wearables wie z.B. Datenbrillen. Diese werden von Onlinehändlern oft zur Unterstützung der Kommissionierung und in der Lagerlogistik eingesetzt. KMU mit Online-Handel sind stark von IT abhängig, ihre Awareness ist jedoch nicht überdurchschnittlich ausgeprägt.

Abbildung 36: IT-Sicherheitsbewusstsein in Unternehmen, die Online-Handel betreiben



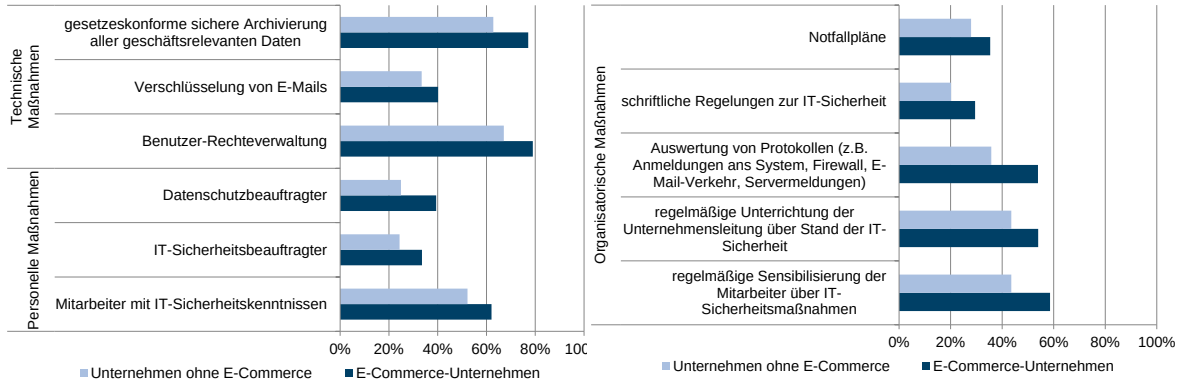
E-Commerce-Unternehmen nutzen überdurchschnittlich häufig digitale Kanäle. Insbesondere die Nutzung sozialer Netzwerke für Marketing und Vertrieb ist weit verbreitet (52% der E-Commerce-KMU). Die Unternehmen nutzen Cloud-basierte Anwendungen stärker als der Durchschnitt der KMU, und lagern mehr IT-Anwendungen aus.

Der Großteil der KMU bewertet die Bedeutung von IT-Sicherheit allgemein als hoch oder sehr hoch – aber die Unternehmen handeln nicht danach (vgl. Kapitel 6 und 7). Für E-Commerce-Unternehmen gilt dies umgekehrt: sie schätzen die Bedeutung von

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit weniger wichtig ein als der Durchschnitt, setzen aber mehr technische, organisatorische und personelle IT-Sicherheitsmaßnahmen um als andere KMU (vgl. Abbildung 37). Dieser Widerspruch muss vor dem Hintergrund der digitalen Geschäftsmodelle dieser Unternehmen betrachtet werden. E-Commerce-Unternehmen haben dadurch ein höheres Bewusstsein für IT-Sicherheit und befinden sich auf einem höheren Sicherheitsniveau als der Durchschnitt der KMU.

Abbildung 37: IT-Sicherheitsmaßnahmen im E-Commerce



n=1.505 n=1.505

wik

Bei den technischen Maßnahmen setzen E-Commerce-Unternehmen nicht nur Basismaßnahmen wie Virenscanner und Firewall ein, sondern auch weitergehende Maßnahmen wie verschlüsselte E-Mail-Kommunikation und Verwaltung unterschiedlicher (Zugriffs-)Rechte der Benutzer gehören zum Standard. E-Commerce-Unternehmen beschäftigen häufiger Fachpersonal mit IT-Sicherheitskenntnissen und benennen Verantwortliche für IT-Sicherheit und Datenschutz. Organisatorische Maßnahmen werden bereits von vielen E-Commerce-Unternehmen umgesetzt. Als besonders wichtig sind hier die regelmäßigen Sensibilisierungen der Mitarbeiter einzuschätzen, sowie das Interesse der Unternehmensleitung an IT-Sicherheit. Letzteres wirkt als starker Treiber für die Gewährleistung eines hohen IT-Sicherheitsniveaus in Unternehmen.

9.5 Industrie 4.0 – Internet der Dinge

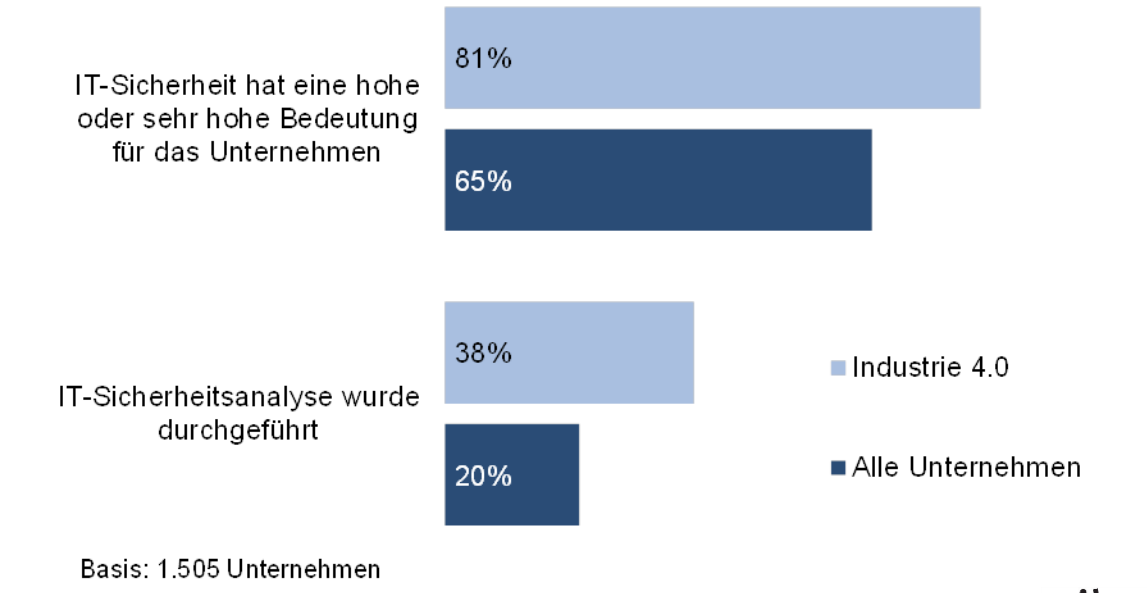
Unternehmen, die aktiv sind im Bereich Industrie 4.0, sind besser mit IT-Technik ausgestattet als der Durchschnitt und setzen mehr mobile Endgeräte jeder Art ein. Die Ausstattung mit Smartphones, Tablets und Notebooks ist bei ihnen Standard, der mobile Zugriff von unterwegs auf Unternehmensdaten und die Nutzung von Cloud-Lösungen konsequenterweise weit verbreitet.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

10% aller KMU und 29% der großen KMU (100-499 MA) sind im Bereich Industrie 4.0 aktiv. Digitalisierung von Prozessen geht in der industriellen Produktion mit einem erhöhten IT-Sicherheitsbewusstsein einher. Die Bedeutung von IT-Sicherheit ist in dieser Gruppe am höchsten.

Abbildung 38: IT-Sicherheitsbewusstsein in KMU, die im Bereich Industrie 4.0 aktiv sind



Basis: 1.505 Unternehmen

Innovative Unternehmen im Bereich Industrie 4.0 setzen überdurchschnittlich häufig IT-Sicherheitsanalysen ein.

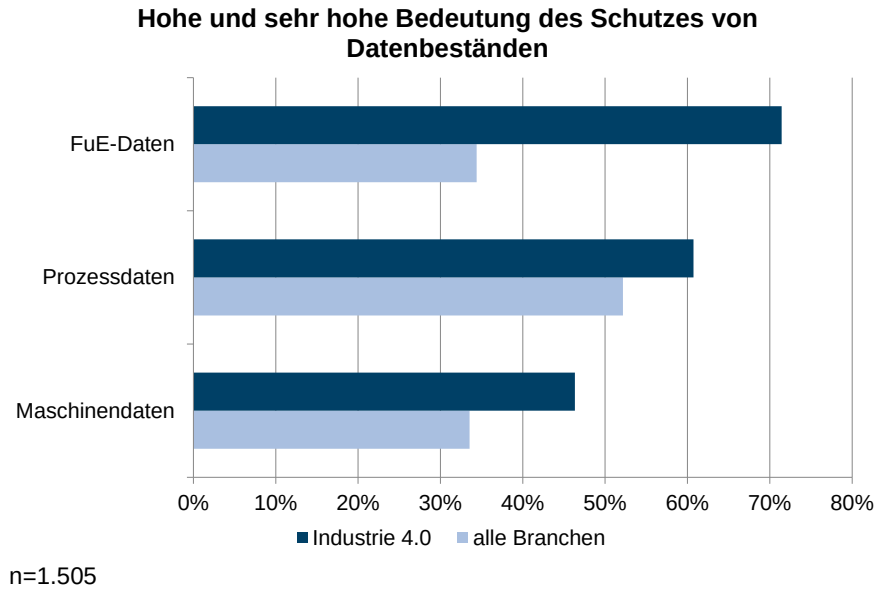
Unternehmen der Industrie 4.0 nutzen häufiger digitale Kanäle, inklusive sozialen Netzwerken und WhatsApp. Neben einfachen Anwendungen wie E-Mail und Online Banking nutzen sie auch komplizierte Anwendungen häufiger, sie tauschen Daten mit Kunden und Lieferanten auf elektronischem Wege aus oder nehmen an elektronischer Auftragsvergabe teil. Drei Viertel der KMU im Bereich Industrie 4.0 bieten ihre Leistungen im Internet an.

Insgesamt nutzen KMU aus dem Bereich Industrie 4.0 Informationstechnik häufiger und intensiver als der Durchschnitt der KMU. Ihr Bewusstsein für mögliche Risiken durch mangelnde IT-Sicherheit ist höher, für 81% der Industrie 4.0-Unternehmen ist die Bedeutung von IT-Sicherheit hoch oder sehr hoch (zum Vergleich: 65% im Durchschnitt aller Branchen).

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Die Unternehmen sind sich auch des Wertes und des Schutzbedarfs ihrer Daten bewusster als andere KMU (vgl. Abbildung 39). Das Wissen um den Wert der unternehmenseigenen Assets ist eine wichtige Voraussetzung für die Umsetzung eines individuellen Schutzkonzepts.

Abbildung 39: Bedeutung von Datenbeständen in Unternehmen der Industrie 4.0



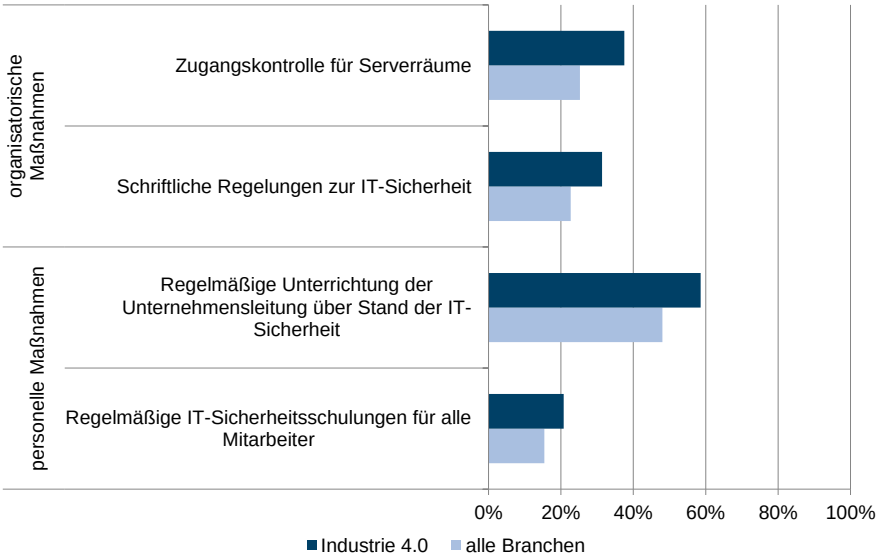
n=1.505

Durchweg haben Unternehmen der Industrie 4.0 technische Maßnahmen zum Schutz der IT häufiger umgesetzt als der Durchschnitt der KMU. Sie nutzen Verschlüsselungen von Dateien, Emails und Festplatten häufiger, und sorgen für eine sichere Archivierung geschäftsrelevanter Daten. Für den Zugriff auf Unternehmensdaten von außerhalb nutzen sie die besonders sichere VPN-Technologie (Virtual Private Networks). Auch bei der Umsetzung von personellen und organisatorischen Maßnahmen liegen KMU der Industrie 4.0 über dem Durchschnitt (vgl. Abbildung 40). Allerdings haben auch diese Unternehmen Nachholbedarf, insbesondere bei den Schulungen für Mitarbeiter und IT-Personal.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 40: Personelle und organisatorische Maßnahmen in KMU der Industrie 4.0



n=1.505

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

10 Informations- und Beratungsbedarf aus Sicht der Unternehmen

Informationsverhalten der KMU

Die Mehrheit der Befragten (80 Prozent) informiert sich über das Internet zum Thema IT-Sicherheit. Dabei informieren sich vor allem die größeren Unternehmen online. Für mehr als 90 Prozent der Befragten aus größeren Unternehmen ist das Surfen im Internet eine Möglichkeit zur Information. Bei den kleinen Unternehmen geben das verhältnismäßig wenige der Befragten, nur 81 Prozent, an. Mit deutlichen Abstand (64 Prozent) folgt die Tagespresse als Informationsmedium zum Thema IT-Sicherheit. Circa die Hälfte der Teilnehmer informiert sich mittels Herstellerinformationen oder Mitteilungen der Verbände, Innungen oder Kammern. Die Fachpresse zum Thema Informationstechnik geben 40 Prozent aller Befragten als Informationsquelle an. Online-Plattformen zum Thema IT-Sicherheit nutzt gut ein Drittel der Teilnehmer. Deutlich weniger genutzt werden von allen KMU Webinare (17 Prozent), Angebote des BMWi (12 Prozent) und externe Berater bzw. IT-Dienstleister oder Systemhäuser (5 Prozent).

Dass äußerst wenige Unternehmen auf externe Dienstleister setzen, um sich über IT-Sicherheit zu informieren, könnte auch ein Hinweis darauf sein, dass neutrale Angebote bevorzugt werden. Persönliche Kontakte, bzw. das persönliche Netzwerk, spielen bei der Information zu IT-Sicherheit nahezu keine Rolle. Nur drei Prozent der Teilnehmer nutzen diese Kanäle, um sich über IT-Sicherheit zu informieren.

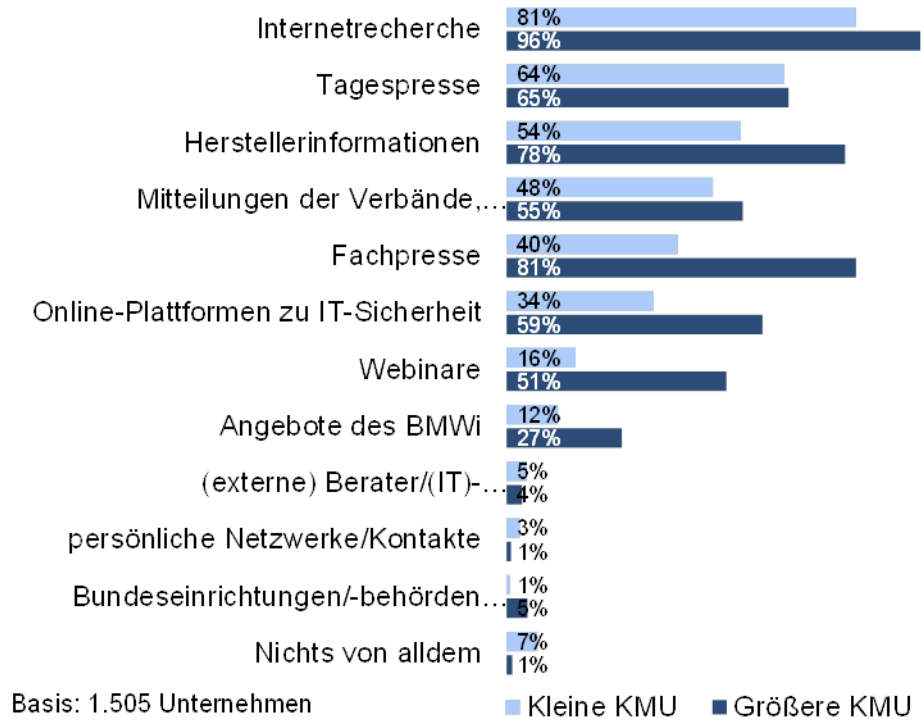
Bei den Informationsquellen Herstellerinformationen, Fachpresse zum Thema Informationstechnik, Online-Plattformen zum Thema IT-Sicherheit und bei Webinaren scheint die Nutzung stark größenabhängig. Je größer das Unternehmen, desto eher scheinen diese Kanäle attraktiv. So nutzen beispielsweise nur 16 Prozent der Kleinunternehmen Webinare als Informationsquelle während 51 Prozent der Befragten aus größeren KMU angaben, sich mit Hilfe von Webinaren zu informieren.

Insgesamt lassen die Ergebnisse vermuten, dass sich mehr größere Unternehmen zum Thema IT-Sicherheit informieren als kleinere.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 41: Nutzung verschiedener Informationsquellen zur Information über IT-Sicherheit

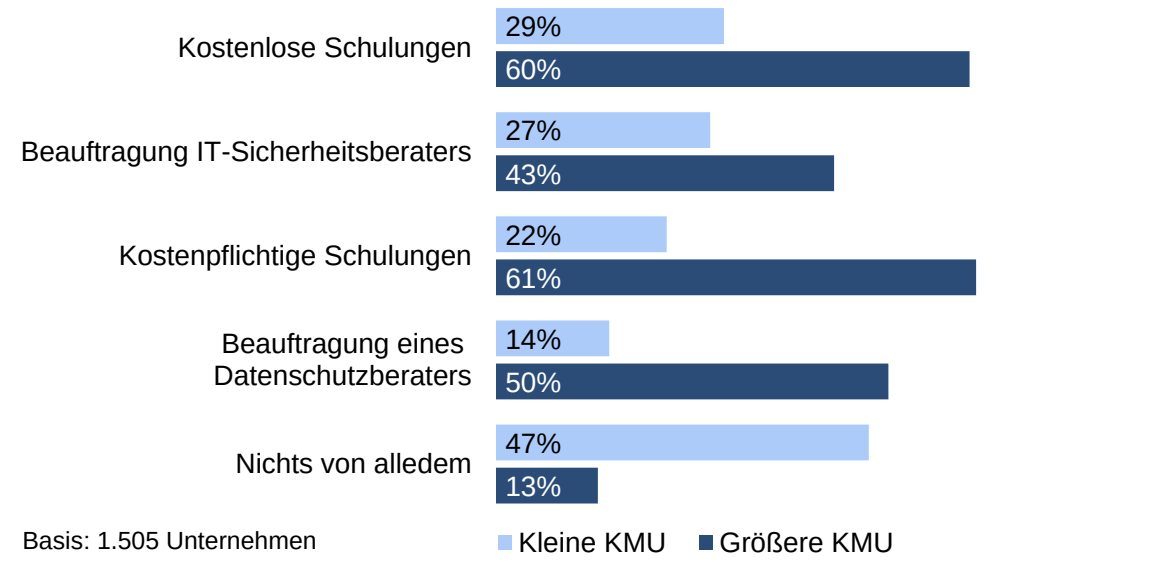


Nutzung von Schulungs- und Beratungsangebote stark größenabhängig

Die Ergebnisse zeigen, dass größere Unternehmen alle abgefragten Angebote tendenziell eher nutzen als kleinere. Knapp die Hälfte (47 Prozent) der Befragten aus kleinen KMU gibt an, keines der genannten Angebote zu nutzen. Bei den Teilnehmern aus größeren KMU antworten nur 13 Prozent so. Kostenlose Schulungen nutzen 60 Prozent der größeren KMU und 29 Prozent der kleinen KMU. Noch größer ist die Differenz zwischen größeren KMU und kleinen bei der Nutzung kostenpflichtiger Schulungen. 61 Prozent der größeren KMU geben an, kostenpflichtige Schulungen zu nutzen. Bei den kleinen sind es mit 22 Prozent deutlich weniger Befragte, die von der Nutzung kostenpflichtiger Schulungen berichten. Bei größeren Unternehmen ist damit der Anteil an Unternehmen der kostenlose Schulungsangebote nutzt nahezu gleich hoch zu dem Anteil, der kostenpflichtige Schulungen nutzt (60 Prozent bzw. 61 Prozent).

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 42: Nutzung von Schulungs- und Beratungsangeboten



Es zeigt sich allerdings, dass nicht alle Unternehmen, deren Mitarbeiter eine kostenlose Schulung besucht haben, auch eine kostenpflichtige Schulung nutzen oder umgekehrt (siehe Abbildung 43).

So haben von den 29 Prozent der Befragten aus kleineren Unternehmen, die eine kostenlose Schulung genutzt haben, nur knapp die Hälfte davon (16 Prozent) auch ein kostenpflichtiges Schulungsangebot genutzt. Das zeigt auch: Sechs Prozent der kleineren Unternehmen nutzen nur kostenpflichtige, aber keine kostenlosen Schulungsangebote. Ohne die zeitliche Reihenfolge, und damit ggf. einen Zusammenhang zwischen dem Besuch einer kostenlosen Veranstaltung und dem ggf. daraus resultierenden Anreiz in eine kostenpflichte Schulung zu investieren, zu kennen, kann durch die Repräsentativbefragung nicht geklärt werden, inwiefern ein Stufenmodell zur Heranführung von KMU an Themen der IT- bzw. Informationssicherheit funktionstüchtig erscheint. Dieses Thema wurde deshalb in den Expertengesprächen vertieft.

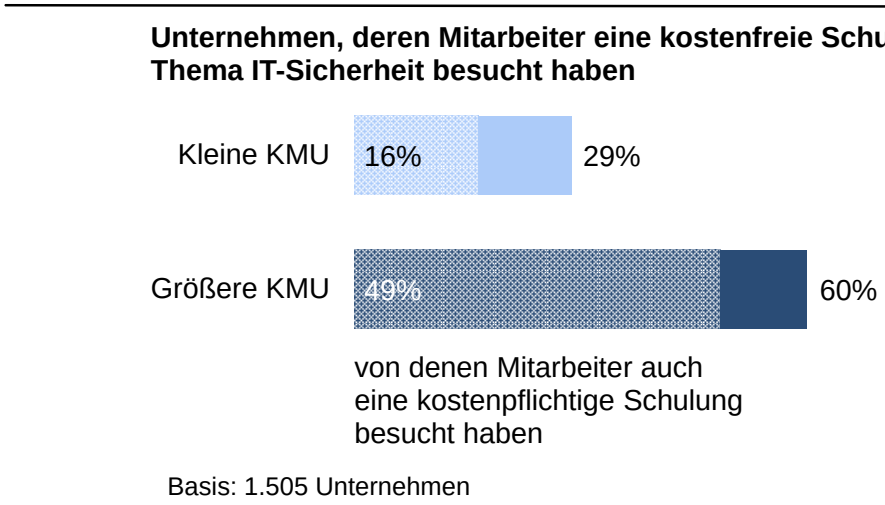
Bei den größeren Unternehmen geben 60 Prozent der Befragten an, kostenfreie Schulungsangebote zu nutzen. Mehr als 80 Prozent dieser größeren befragten Unternehmen[52] nutzen auch kostenpflichtige Schulungsangebote. Bei den größeren Unternehmen nutzen etwa 12 Prozent nur kostenpflichtige Angebote.

52 Dies entspricht 49 Prozent an der Gesamtheit der größeren Unternehmen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Abbildung 43: Nutzung sowohl kostenfreier als auch kostenpflichtiger Veranstaltungen bei Unternehmen



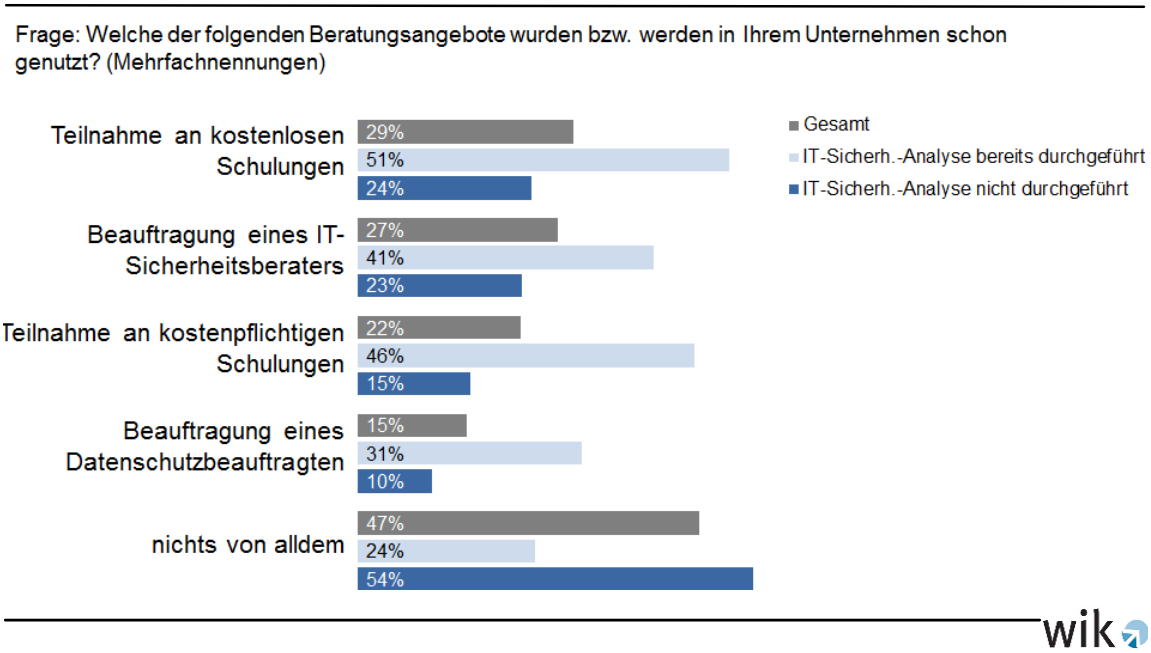
Es zeigt sich, dass die Nutzung von Schulungs- und Beratungsangeboten stark abhängig von der Unternehmensgröße ist.

Unternehmen mit IT-Sicherheitsanalyse nutzen Schulungen häufiger als ohne

Betrachtet man die Nutzung von Schulungs- und Beratungsangeboten getrennt für Unternehmen, die bereits eine Sicherheitsanalyse durchgeführt haben und solche, die noch keine Sicherheitsanalyse durchgeführt haben, so zeigt sich ein Unterschied in der Nutzung für die beiden Gruppen. Es geben deutlich mehr Teilnehmer aus Unternehmen in denen bereits eine Sicherheitsanalyse durchgeführt wurde, an Beratungs- und Schulungsangebote zu nutzen als Teilnehmer aus Unternehmen, in denen bisher noch keine Sicherheitsanalyse durchgeführt wurde.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 44: Nutzung von Schulungsangeboten in Abhängigkeit von der Durchführung einer IT-Sicherheitsanalyse



Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

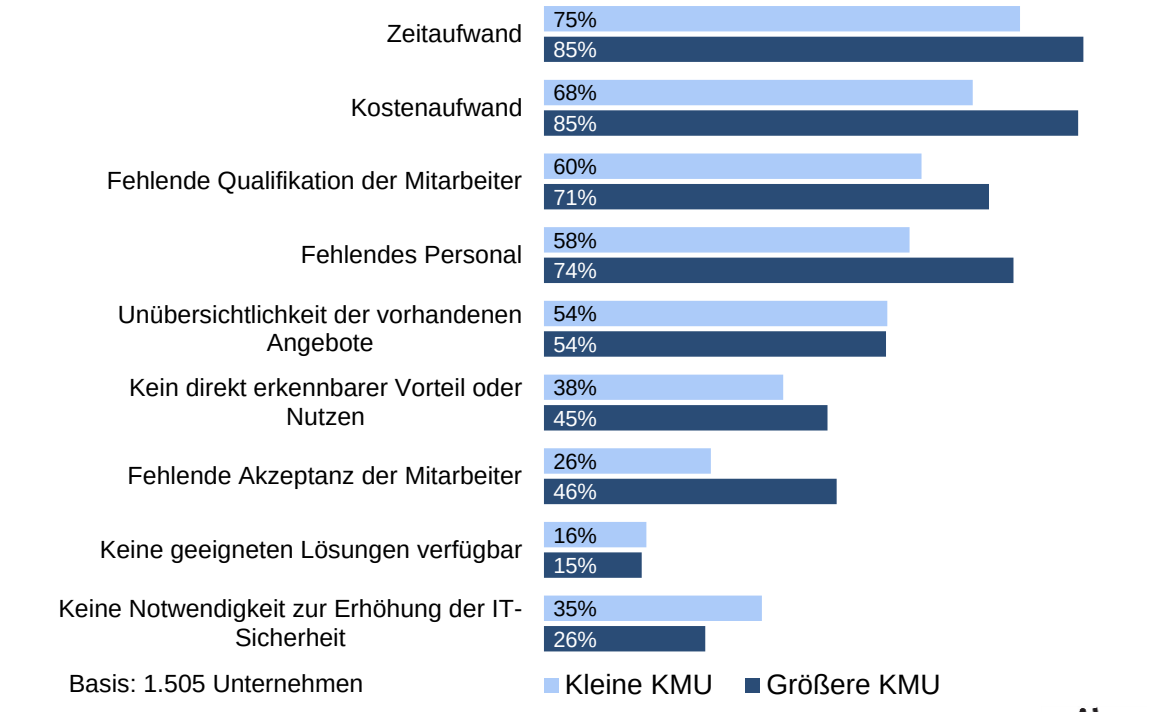
11 Handlungsbedarf aus Sicht von Unternehmen und Experten

Kosten- und Zeitaufwand als Haupthemmnis zur Verbesserung der IT-Sicherheit

Um zu einer Verbesserung des Status Quo beitragen zu können, ist es entscheidend, zu verstehen, wieso KMU trotz bekannter Risiken und steigender Bedrohungslage nicht mehr unternehmen, um ihr IT-Sicherheitsniveau zu erhöhen. Etwa ein Drittel der größeren KMU und ein Viertel der kleinen KMU sieht keine Notwendigkeit zur Erhöhung der IT-Sicherheit. Vor allem bei größeren KMU ist die fehlende Akzeptanz bei Mitarbeitern ein relevantes Thema. 46 Prozent der größeren KMU geben diese als Hürde auf dem Weg zur Verbesserung der IT-Sicherheit an. Bei den kleineren KMU sind es mit 26 Prozent deutlich weniger Befragte, die diesen Grund nennen. 38 Prozent der kleineren KMU und 45 Prozent der größeren sehen keinen erkennbaren Vorteil oder Nutzen einer Verbesserung von IT-Sicherheit. Die Unübersichtlichkeit der vorhandenen Angebote ist für etwa mehr als die Hälfte der Befragten, unabhängig von der Größe des Unternehmens, ein Problem. Fehlendes Personal und fehlende Qualifikation der Mitarbeiter sind für knapp drei Viertel der Teilnehmer aus größeren Unternehmen eine Hürde und für etwa 60 Prozent der kleineren Unternehmen. Die Haupthemmnisse stellen in dieser Erhebung wie auch in der aus dem Jahr 2012 Zeit- und Kostenaufwand dar. 85 Prozent der Befragten aus größeren KMU sehen sowohl den Zeit- als auch den Kostenaufwand als Hürde zur Verbesserung der IT-Sicherheit. Bei den kleineren sind es 75 Prozent (Zeitaufwand) bzw. 68 Prozent (Kostenaufwand).

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abbildung 45: Hemmnisse bei der Verbesserung der IT-Sicherheit aus Sicht der KMU nach Unternehmensgröße



Vorschläge zur Unterstützung aus Unternehmenssicht: Bessere Informationen und externe IT-Sicherheitsberatung

In einer offenen Frage[53] nach konkreten Unterstützungsmöglichkeiten für das eigene Unternehmen gefragt, ist die häufigste Antwort, dass „bessere“ Informationen benötigt würden. Das geben 29 Prozent der Teilnehmer aus kleinen und 23 Prozent der Teilnehmer aus größeren KMU an. Es wünschen sich also mehr kleine KMU bessere Informationen als größere. Diese alltagssprachliche Umschreibung deutet darauf hin, dass die Unternehmen die vorhandene Angebotsvielfalt als unübersichtlich und nicht zielgruppengerecht wahrnehmen könnten.

Eine externe IT-Sicherheitsberatung stell für 20 Prozent der Befragten aus kleinen KMU eine sinnvolle Unterstützung beim Thema IT-Sicherheit dar. Bei den größeren Unternehmen nennen etwas mehr, 23 Prozent der Teilnehmer die externe IT-Sicherheitsberatung als Option zur Hilfestellung.

53 Die Antworten wurden dementsprechend nachkategorisiert.

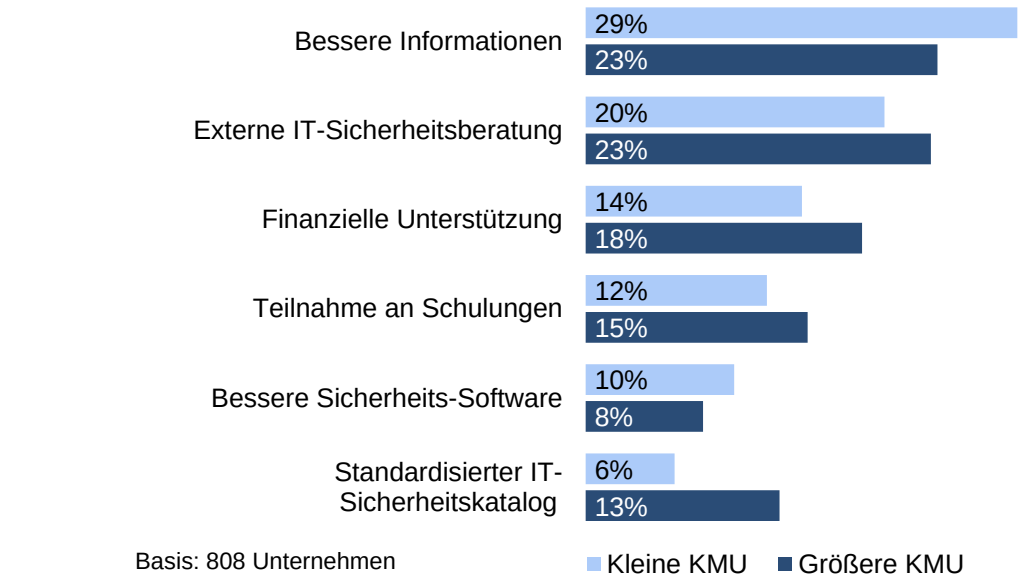
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Finanzielle Unterstützung und die Teilnahme an Schulungen nennen weniger als 20 Prozent der Befragten als mögliche Unterstützung. Dabei schlagen etwas mehr Teilnehmer aus größeren KMU dieses Maßnahmen vor als aus kleinen KMU (siehe Abbildung 46)

Die größten Diskrepanz[54] weisen kleine und größere KMU bei zwei Formaten auf. Zum einer bei der Frage nach einem standardisierten IT-Sicherheitskatalog. Bei der Erstellung eines solchen Katalogs wünschen sich nur sechs Prozent der Teilnehmer aus kleinen KMU und 13 Prozent der Befragten aus größeren KMU Unterstützung. Mehr Befragte aus kleinen KMU als aus größeren (Unterschied 6 Prozentpunkte) fordern bessere Informationen. Das deutet darauf hin, dass kleine KMU beim Thema IT-Sicherheit noch eher am Anfang der Awareness und Umsetzung stehen als größere. Kleine KMU befinden sich eher noch in der Informationsphase während größere Unternehmen sich einer möglichen Umsetzung nähern und eher in der Planungsphase sind.

Abbildung 46: Unterstützungsbedarfe der KMU



Grundsätzlich lassen die Vorschläge der KMU auf eine Lücke zwischen vorhandenem Angebot, dem Wissen über das Vorhandensein des Angebotes sowie der Bereitschaft zur Nutzung dieses Angebotes schließen. Der Unterschied zwischen kleinen und größeren KMU ist hier allerdings nicht besonders ausgeprägt.

54 Neben dem höheren Bedarf (7 Prozentpunkte) kleiner KMU nach besseren Informationen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

In den von uns durchgeführten Expertengesprächen bestätigt sich dieses Bild: Selbst bei Branchenverbänden fehlt ein strukturierter Überblick über alle im Markt verfügbaren Angebote. Wenn selbst auf dieser Ebene kein Überblick besteht, ist davon auszugehen, dass die Orientierung und schließlich die Auswahl eines Angebotes für ein KMU mit erheblichen Suchkosten verbunden ist. Diese Kosten erschweren KMU, bedenkt man ihre geringen personellen und finanziellen Ressourcen bei einer aktuell guten konjunkturellen Auslastung, die Verbesserung ihres IT- und Informationssicherheitsniveaus trotz vorhandener Angebote.

11.1 Treiber für mehr IT-Sicherheit in KMU aus Sicht der Experten

WIK hat mit Experten aus Anbieterunternehmen, Anwenderunternehmen, Verbänden, Vereinen, Industrie- und Handelskammern, Handwerkskammern sowie Vertreten aus Hochschulen und Instituten Experteninterviews geführt. So konnte WIK neben der Einschätzung der Unternehmen selbst einen breiten Blick auf das Thema IT-Sicherheit in KMU gewinnen und die Ergebnisse der Repräsentativbefragung validieren sowie die Ursachen für die derzeitige Entwicklung besser eruieren. Für die Expertengespräche wurden einheitliche Leitfäden verwendet. Die folgende Tabelle bietet einen Überblick zu den Treibern, die von zahlreichen Experten genannt und außerdem als besonders wichtig eingeschätzt wurden:

Tabelle 1: Experteneinschätzungen zu den Treibern für mehr IT-Sicherheit in KMU

Treiber für mehr IT-Sicherheit in KMU	Bedeutung
Mediale Berichterstattung zu aktuellen Vorfällen	+++
Gesetzliche Anforderungen	+++
Vorbildfunktion und hohe Awareness der Geschäftsführer und Inhaber	++
Vorfälle im eigenen oder ähnlichen Unternehmen	++
Digitalisierung, Industrie 4.0 bzw. zunehmende Vernetzung	+
Druck durch größere Unternehmen in deren Wertschöpfungsnetz das KMU eingebunden ist	+
Wettbewerbsvorteile durch IT-Sicherheit (Marketingeffekt)	-

Legende: +++ sehr hohe Bedeutung, ++ hohe Bedeutung, ++ spielt eine Rolle, - ist nicht von Bedeutung

Die zunehmenden **mediale Berichterstattung** zu aktuellen Sicherheitsvorfällen, auch in Massenmedien zur besten Sendezeit (z.B. Tagesschau) wird von den meisten Experten als Treiber von IT-Sicherheit bei KMU angeführt. Zumindest gehen viele davon aus, dass die Bedeutung des Themas für KMU dadurch gestiegen ist.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Gesetzliche Anforderungen gelten unter Experten ebenfalls als wichtiger Treiber, der in Unternehmen zu einer Beschäftigung mit dem Thema IT-Sicherheit führt bzw. führen könnte. Vorwiegend kann ein Effekt dieser Regelungen bei Unternehmen beobachtet werden, die zur Gruppe der betroffenen Unternehmen gehören. Das IT-SiG richtet sich beispielsweise vor allem an Betreiber kritischer Infrastrukturen[55]. Viele KMU sind also von den Vorgaben nicht betroffen.

Als entscheidend wird von zahlreichen Experten die **Rolle der Geschäftsführer oder Inhaber** beschrieben. Um Mitarbeiter zu mehr IT-Sicherheit im persönlichen Verhalten zu motivieren, ist es notwendig, dass Geschäftsführung und Vorgesetze das gewünschte Verhalten vorleben. Da IT-Sicherheit ein Budget zur Umsetzung von Maßnahmen benötigt, ist das Verständnis der Entscheider für den langfristigen Mehrwert solcher Ausgaben wesentlich.

Viele Experten, darunter vor allem die Dienstleister berichten, dass Unternehmen sich gerade dann an sie wenden, wenn ein **Schadensfall** eingetroffen ist. Das bedeutet, die Bereitschaft Ausgaben in IT-Sicherheit zu tätigen steigt durch bereits erlittene, eigene Verluste.

Des Weiteren berichten die Gesprächspartner die zunehmende **Digitalisierung bzw. Industrie 4.0 oder Vernetzung** führe zu höherer Sicherheitsmaßnahmen. Nichtsdestotrotz führen die Experten aus, dass die verbesserte IT-Sicherheit das erhöhte Risiko durch eine Vernetzung in den meisten Fällen keineswegs ausgleiche. So sind die Unternehmen im Endeffekt einer höheren Bedrohung ausgesetzt.

Druck größerer Unternehmen auf kleinere Zulieferer scheint nach Experteneinschätzung ein probates Mittel, um Zulieferer-KMU zu mehr Maßnahmen im Bereich IT- und Informationssicherheit zu bewegen. Nur so können die Unternehmen weiterhin als Lieferant für die Großunternehmen, beispielsweise Automobilhersteller, tätig sein.

Ein hohes IT-Sicherheitsniveau scheint den Experten nach zu urteilen in der Fläche bei den KMU **nicht als Wettbewerbsvorteil** wahrgenommen zu werden. Zeigen sich hingegen Mängel in der IT-Sicherheit eines Unternehmens, wirken sich die mittelbar oder unmittelbar nachteilig für das Unternehmen aus.

Bezüglich der Wirkung einer **medialen Berichterstattung** zu aktuellen Sicherheitsvorfällen geben die meisten Experten an, dass dies die Aufmerksamkeit für das Thema IT-Sicherheit steigert und somit als Treiber zur Verbesserung des Status Quo dienen kann. Andere Experten hingegen sehen die Berichterstattung, beispielsweise in der

55 Allerdings gelten auch für Unternehmen, die Webangebote anbieten, besondere Auflagen zum Schutz der Kundendaten.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Tagespresse, nicht als Treiber für mehr IT-Sicherheit. Die gesteigerte Aufmerksamkeit schlägt sich offensichtlich nicht in der Umsetzung von Maßnahmen im eigenen Unternehmen nieder. Die Ergebnisse der von WIK durchgeführten Repräsentativbefragung stützen diese Einschätzung. Einen negativen Effekt hat die mediale Berichterstattung dann, wenn Unternehmen aus Angst vor der aussichtslosen Lage demotiviert resignieren. Da ein effektiver Schutz ohnehin nicht möglich scheint, unternehmen sie dann gar nichts: *„Ganz im Gegenteil treibt die öffentliche Debatte um IT-Sicherheit eher das Gefühl von Fatalismus voran, nachdem Motto: „Wenn alles so schlimm ist, kann man ohnehin nichts ausrichten“.*

11.2 Hemmnisse für mehr IT-Sicherheit in KMU aus Sicht der Experten

Folgende Tabelle bietet einen Überblick zu den Hemmnissen, die von zahlreichen Experten genannt und außerdem als besonders relevant eingeschätzt wurden:

Tabelle 2: Hemmnisse für mehr IT-Sicherheit in KMU aus Sicht der Experten

Hemmnisse für mehr IT-Sicherheit in KMU	Bedeutung
Awareness für IT-Sicherheit fehlt	+++
Fehlende personelle Ressourcen bzw. fehlendes Know-how beim den vorhanden Mitarbeitern	+++
Fehlende zeitliche Ressourcen aufgrund des Tagesgeschäfts	+++
Fehlende organisatorische Maßnahmen im Unternehmen	+++
Fehlende Bereitschaft, eine fundierte Kosten-Nutzen-Analysen durchzuführen	+++
Fehlendes Wissen über schützenswerte Assets („Wir sind nicht interessant.“)	+++
Vorhandene Angebote (Informationen über Sicherheitsrisiken, Dienstleister etc.) sind unzureichend bekannt	+++
Vorhandene Angebote (Informationen über Sicherheitsrisiken, Dienstleister etc.) sind. nicht zielgruppenspezifisch	+++
Fehlende Verankerung in Schule, Ausbildung, Studium und Weiterbildung	++
Fehlende regelmäßige, sich wiederholende Schulungen für Mitarbeiter	++
Mitarbeiter als Ursache für fehlende IT-Sicherheit	+
Regionale IT-Anbieter, die ein Unternehmen über die ganze Bandbreite beraten und ausstatten können, sind nicht flächendeckend verfügbar	+
Verfügbare Sicherheitsprodukte sind wenig intuitiv und nicht nutzerfreundlich	+
Nutzung veralteter Betriebssysteme, Branchensoftware etc.	+
Technische Basisausstattung (Firewall, Spamfilter, Back-ups) fehlt	-

Legende: +++ sehr hohe Bedeutung, ++ hohe Bedeutung, ++ spielt eine Rolle, - ist nicht von Bedeutung

Zahlreiche Experten berichten von großen Schwachstellen, vor allem **im personellen Bereich**. Hauptproblem sind fehlende Mitarbeiter, sowohl mengenmäßig als auch bezüglich des passenden Know-hows. Dies führt häufig dazu, dass IT-Sicherheit von Mitarbeitern, die im Kern für etwas anders zuständig sind, mitgemacht wird Aufgaben werden durch (fachfremde) Mitarbeiter in Personalunion erledigt.

Hinzu kommt laut Experten, dass die Unternehmen aufgrund ihrer **guten Auftragslage** mit dem Tagesgeschäft schon so gebunden sind, dass die zeitlichen Ressourcen zur Beschäftigung mit dem Thema IT-Sicherheit fehlen. Vor allem aus dem Handwerk berichten die Experten über wenig Zeit für Themen außerhalb des Kerngeschäfts aufgrund der hohen Auslastung.

Selbst einfache **organisatorische Maßnahmen** und Verhaltensweisen wie die Anmeldung und Begleitung von Besuchern im Firmengebäude, die sichere Entsorgung von vertraulichen Druckerzeugnissen oder ein beschränkter Zugang zum Serverraum sind in der Fläche unzureichend vorhanden.

Die Expertengespräche haben gezeigt, dass vielfach die Bereitschaft **Kosten** für die IT-Sicherheit zu tragen bzw. Budget vorzusehen, fehlt. Dies liegt nicht etwa daran, dass per se keine finanziellen Mittel zur Verfügung stünden. Vielmehr ist es Ausdruck einer fehlenden Kosten-Nutzen-Abwägung. Die Entscheidung ob und in welchem Umfang in IT- bzw. Informationssicherheit investiert wird, wird also uninformiert getroffen.

Experten berichten außerdem, dass **vorhandene Angebote** zur Unterstützung im Bereich IT- bzw. Informationssicherheit vielen KMU **nicht bekannt** sind oder aber sie sich von diesen nicht angesprochen fühlen. Angebote, vor allem von Dienstleistern, scheinen zu technisch aufbereitet und daher sprachlich wenig verständlich für KMU. Darüber hinaus sind die Veranstaltungen teilweise auch hinsichtlich der Länge und der Tageszeit für KMU, gerade Handwerksbetriebe, nicht passend.

Die fehlende, bzw. verzerrte Kosten-Nutzen-Analyse, also einen Kostenansatz für IT-Sicherheit ohne einen dem gegenüberstehenden Nutzen, zeugt vom **fehlenden Wissen** der Unternehmen über ihre **schützenswerten Assets**.

Die **Rolle von IT-Sicherheit in der Ausbildung**, von der Schule bis hin zum Informatikmaster und schließlich im Bereich der inner- und außerbetrieblichen Weiterbildung, ist mehr als untergeordnet. Selbst in Informatikstudiengängen ist IT-Sicherheit in den meisten Fällen nicht mit einem einzigen Pflichtmodul zu belegen. Schulen nähern sich laut Experten aktuell dem Thema IT und neue Medien. IT-Sicherheit wird dabei kaum beleuchtet.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Die Experten berichten davon, ob im eigenen Unternehmen oder bei anderen, dass sich **wiederholende Mitarbeiterschulungen**, beispielsweise zur Verwendung von sicheren Passwörtern oder dem Erkennen von gefälschten E-Mails, häufig nicht stattfinden.

Mitarbeiter gelten oftmals als Ursache für fehlende IT-Sicherheit. Absichtliche oder unbeabsichtigte Handlungen von Mitarbeitern, wie beispielsweise im Falle eines CEO-Frauds, machen den Mitarbeiter unter Umständen zu einer Schwachstelle in einem auf technischer Ebene sicheren System.

Auf der **Anbieterseite** sind aus Sicht der Experten vor allem **keine, regionale Anbieter**, die dennoch in der Lage sind, ein KMU über die Bandbreite der benötigten Dienstleistungen zu bedienen in der Fläche nicht verfügbar. Experten berichten, dass von Anbieterseite aus Dinge „mitgemacht“ werden, die über Kernkompetenzen des Anbieters hinausgehen.

Am Markt befindliche **Sicherheitsprodukte** sind **wenig intuitiv und nutzerfreundlich**. So besteht die Gefahr, dass trotz vorhandener technischer Ausstattung die Nutzung der Schutzmechanismen nicht oder nicht wie vorgesehen umgesetzt wird.

Die Experten nennen als weiteres Hemmnis für mehr IT-Sicherheit in KMU die **Nutzung alter Betriebssysteme** im Unternehmen. Der WannaCry-Angriff beispielsweise konnte u.a. deshalb so erfolgreich sein, weil Unternehmen trotz jahrelanger Warnungen von Microsoft immer noch das Betriebssystem Windows XP im Einsatz haben. In einigen Fällen ist es für die Unternehmen in der Praxis allerdings schwer, ohne das alte System auszukommen. So gibt es Maschinen oder Anlagen, die auf anderen Betriebssystemen nicht zu verlässig laufen. Hier entstünde den Unternehmen ein wirtschaftlicher Nachteil, bei Nutzung eines neuen Systems. Dann ist es unerlässlich, die Maschine nicht mehr ans Internet und den Rest des Netzwerkes anzuschließen.[56]

Die **technische Basisausstattung** wie eine Firewall und ein Spamfilter ist in der Mehrheit der Unternehmen vorhanden. Ebenso hat die Erstellung von Back-ups bereits Verbreitung gefunden. An der absoluten technischen Basisausstattung mangelt es also aus Sicht der Experten nicht. Dies kann allerdings keinesfalls über die großen Missstände im Bereich der organisatorische und personellen Maßnahmen hinweg täuschen, die ein Unternehmen über seine Mitarbeiter verwundbar machen. Dies gilt insbesondere für Mitarbeiter, die aufgrund von Konflikten ausscheiden.

56 Siehe auch: Kaps, Reiko (2014): Quarantäne - Windows XP im LAN absondern. In: Heise.de, 22.02.2014, URL: https://www.heise.de/ct/ausgabe/2014-6-Windows-XP-im-LAN-absondern-2118704.html.

11.3 Branchen mit besonders geringem IT-Sicherheitsbewusstsein

Inwiefern einzelne Branchen besonders wenig oder besonders viel Wert auf IT-Sicherheit legen, werden kontrovers diskutiert. Die Bedeutung des Thema und die Umsetzung von Schutzmaßnahmen scheint weniger von der Branche und mehr von der Größe des Unternehmens, dem Grad der Digitalisierung und der Einbindung in ein Netzwerk mit größeren Herstellern bzw. dem Grad der Vernetzung abzuhängen.

Einzig Akteure der Gesundheitsbranche, also vor allem Praxen und Krankenhäuser scheinen laut Experten flächendeckend wenig gerüstet gegenüber Angriffen auf IT- und Informationssysteme.

Die meisten Experten betätigen den Eindruck der Repräsentativbefragung, dass die IT-Sicherheitslage im Gesundheitssektor[57] weitaus schlechter ist als in anderen Branchen.

„In der Gesundheitsbranche gibt es ein Dilemma zwischen Sicherheit und Produktivität“

„Große Krankenhäusern sind oftmals „offene Labore““

„IT ist ein Werkzeug und liegt rum wie ein Stethoskop.“

Experten sehen die Hauptursache darin, dass der medizinische Bereich dem der Informatik **inhaltlich sehr fern** sei. Entsprechend schwer tun sich Angestellte, die oftmals wenig nutzerfreundlichen Sicherheitslösungen, so sie denn verfügbar sind, ordnungsgemäß zu verwenden. Hinzu kommt, dass die Versorgung teils lebensbedrohlicher Patienten verglichen mit der Notwendigkeit, sich Zeit zur Absicherung von Daten und Systemen zu nehmen, deutlich wichtiger scheint. Diese Sichtweise wird in einer Zeit der zunehmenden Vernetzung dann relativiert, wenn die Patientenversorgung unmittelbar von der Absicherung der IT abhängt. Das ist zum Beispiel dann der Fall, wenn der Zugriff auf benötigte Patienteninformationen blockiert wird, Herzschrittmacher von der Ferne aus manipuliert oder Überwachungsmonitore auf Intensivstationen lahmgelegt werden.

Dieser unmittelbare **Zusammenhang zwischen Patientenversorgung und IT- bzw. Informationssicherheit** scheint aktuell für das betreffende medizinische Personal gedanklich noch nicht zu bestehen. Das Lukas Krankenhaus in Neuss mit seinem prominenten Sicherheitsvorfall ist das mit Abstand meist genannte Sicherheitsereignis im Rahmen der 30 geführten Interviews.

57 Ausgenommen sind Hersteller von medizinischen Geräten.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Laut Experten besteht in der Gesundheitsbranche ein hoher **Zeit- und Kostendruck**. Dies führt zu sicherheitskritischen Praktiken wie die nicht-Verwendung von Single Sign-on an den Rechnern oder die Nutzung ursprünglich privater Kommunikationskanäle für dienstlich Zwecke, beispielsweise WhatsApp.

Aufklärungsarbeit könnte im Gesundheitsbereich über Ärztekammern und die kassenärztlichen Vereinigungen stattfinden.

Gesetzliche Vorgaben können den Druck auf Akteure im Gesundheitswesen erhöhen. Diese sollten allerdings passend gestaltet sein. Das setzt voraus, dass in der Politik sowohl ein Bewusstsein für die Lage im Gesundheitssektor vorhanden ist als auch dass die vom Gesetzgeber geforderten Vorgaben erfüllbar sind, dass also die Hardware verfügbar ist.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

11.4 Handlungsempfehlungen der Experten

Die folgende Tabelle bietet einen Überblick zu den Treibern, die von zahlreichen Experten genannt und außerdem als besonders wichtig eingeschätzt wurden:

Tabelle 3: Handlungsempfehlungen aus Sicht der Experten für mehr IT-Sicherheit in KMU

Handlungsempfehlungen der Experten für mehr IT-Sicherheit in KMU
Übersichtlichkeit schaffen und Transfer verbessern, denn das Angebot ist im Prinzip vorhanden, aber die Awareness fehlt.
Informationsbasis verbreitern und verbessern, Eingriffstiefe: gering
Weiterhin neutrale Angebote zur Verfügung stellen
Konkrete Beratungsleistungen
Sicherheitsanalyse/ Testate/ Audits/ Penetrationstest zum Einstieg und einer ersten Lage- und Kostenabschätzung fördern beispielsweise über Beratungsgutschein .
Gesetzliche Maßnahmen und Anpassung der Curricula, Eingriffstiefe: stark
Durchgängige Verankerung in Schule, Ausbildung , Studium und Betrieb
Kontrolle gesetzlicher Vorschriften
Rahmenbedingungen für alle Maßnahmen
Zusammenbringen von Angebot (IT-Dienstleister) und Nachfrage (KMU)
Angebote auf die Sprache und Bedürfnisse der KMU abstimmen.
Regionale Angebote entsprechend den Bedürfnissen der KMU machen.
Praxisbeispiele verwenden.
Positiver Umgang mit dem Thema. Angst machen hilft nicht weiter. Besser kleine Schritte aufzeigen, damit es nicht zur Überforderung kommt.
Vertrauen schaffen und sensibel agieren: Keine Schließung des Betriebs bei Meldung von Angriffe oder Beschlagnahmung von Geräten.
Versicherungen
Cyberversicherungen mit günstigeren Tarifen bei besserer Ausstattung

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

- **Awareness steigern, Eingriffstiefe: gering**

Die Experten betonen, dass weiterhin Angebote zur Awareness-Steigerung für KMU bereitgestellt werden sollten. Da bereits viele Angebote im Markt vorhanden sind, scheint der Ansatz nicht unbedingt ein Mehr an Angeboten zu sein. Vielmehr sollten die vorhandenen Angebote so aufbereitet werden, dass KMU sich angesprochen fühlen und **Angebot** und ggf. geweckte **Nachfrage zusammen kommen**. Das betrifft vor allem den **Transfer** hin zu KMU. Nur wenn die verfügbaren Informationen zu KMU durchdringen, kann ein Verständnis für die Wichtigkeit des Themas entstehen und ein Interesse für tiefere Veranstaltungen und ggf. kostenpflichtige Angebote hervorgerufen werden.

- **Informationsbasis verbreitern und verbessern, Eingriffstiefe: gering**

Um die Informationsbasis zu verbreiten sollten weiterhin **neutrale Angebote** zur Verfügung gestellt werden.

- **Konkrete Beratungsleistungen**

Experten geben an, dass **Sicherheitsanalysen** auch bezeichnet als Testate, Audits oder Penetrationstest **zum Einstieg** und einer ersten Lage- und Kostenabschätzung gefördert werden könnten, beispielsweise über **Beratungsgutscheine**.

- **Gesetzliche Maßnahmen und Anpassung der Curricula, Eingriffstiefe: stark**

Im Grundsatz können **Gesetze** dazu führen, dass Unternehmen sich vermehrt mit dem Thema IT-Sicherheit beschäftigen und Maßnahmen implementieren. So berichten Experten aktuell zum Beispiel von einer erhöhten Nachfrage nach Veranstaltungen zur DSGVO. Gesetzliche Vorschriften haben, wie an anderer Stelle in diesem Bericht bereits erläutert, allerdings auch Nachteile (siehe 11.1). Gerade dann, wenn der Markt relativ unvorbereitet mit Blick auf die neuen Vorgaben ist (DSGVO), besteht das Risiko blinden Aktionismus.

Eine durchgängige **Verankerung** des Themas in **Schule, Ausbildung, Studium und Betrieb** könnte von Grund zu mehr Verständnis und Know-how im Bereich IT-Sicherheit führen.

- **Rahmenbedingungen für alle Maßnahmen**

Folgende Rahmenbedingungen gilt es bei Angeboten aus Expertensicht zu berücksichtigen:

- Die **zeitliche Verfügbarkeit** der KMU sollte bei der Konzeption der Veranstaltung berücksichtigt werden. Hier gilt auch, die Inhalte auf das wirklich für

KMU relevante zu reduzieren und beispielsweise auf lange Grußworte zu verzichten.

- **Veranstaltungen** sollten **regional** durchgeführt werden, um möglichst auch für KMU mit hoher Arbeitsauslastung erreichbar zu sein.
- Die Ansprache sollte so gewählt werden, dass die **Zielgruppe** sich inhaltlich angesprochen fühlt und die technischen Inhalte verstehen kann. Dazu gibt es aus anderen Bereichen Konzepte zur Definition von Rollen, um eine heterogene Zielgruppe zu erreichen. Mehr als die technischen Lösungen sollten die Mehrwerte, die die Lösungen bringen, herausgestellt werden. Es könnte zudem sinnvoll sein, wie dies bereits in Förderprojekten umgesetzt wird, bei geförderten Projekten Budget für **Didaktik und Pädagogik** vorzusehen. So müssen diese Bereiche nicht von Techniker mit- bzw. nicht gemacht werden.
- **Aktive Bewerbung** von Veranstaltungen und anderen Angeboten, regional und auch auf fachfremden Veranstaltungen, die KMU bzw. Menschen ohnehin besuchen.
- **Neutralität** des Angebotes gewährleisten und damit werben.
- **Praxisbezug** deutlich machen. Unternehmer lernen am besten von anderen Unternehmern. So kann eine Vorstellung entstehen, was zum Beispiel ein guter Basisschutz bei einem vergleichbaren Unternehmen gekostet hat.
- **Positiver Umgang** mit dem Thema um Angst und daraus resultierenden Fatalismus zu vermeiden.

Es wurde an verschiedenen Stellen deutlich, wie wichtig **Diskretion und Vertrauen** beim Thema IT-Sicherheit ist. Wendet sich ein Unternehmen beispielsweise an eine Zentrale Ansprechstelle im Bereich Cybercrime der Polizeien, der Länder und des Bundes muss es sich darauf verlassen können, dass der laufende Betrieb nicht durch Beschlagnahmung von Infrastruktur gestört wird. Zudem ist zum Schutz des Rufes eines KMU so zu verfahren, dass die Presse nicht auf den Vorfall aufmerksam wird.

➢ **Versicherungen**

Bisher noch weniger im Markt präsent, aber durchaus bekannt bei Experten, sind **Cyberversicherungen**. Hier fehlt allerdings aktuell die Erfahrung, inwiefern diese zu mehr IT-Sicherheit führen. Auflagen der Versicherer führen hier zu einer gesteigerten Awareness bei den Unternehmen und auch zum Einsatz von Maßnahmen, die Bedingung für den Versicherungsschutz sind.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

12 Fazit und Handlungsoptionen

12.1 Fazit: Zusammenfassung der zentralen Ergebnisse

Die Untersuchung „Aktuelle Lage der IT-Sicherheit in KMU“ zeigt einen nachhaltig hohen Nutzungsgrad von IT und Internet für alle Bereiche in KMU. Mobile Endgeräte und Outsourcing spielen eine immer wichtigere Rolle. Die Gesamtbedeutung von IT-Sicherheit ist hoch und im Vergleich unverändert zu der Untersuchung von 2011/12. Weiterhin sind deutliche Branchenunterschiede (Handwerk, Freie Berufe, Gesundheitswesen, Industrielle Produktion) sichtbar. Unternehmen mit einer höheren IT-Affinität oder hohem Koordinierungsbedarf wie etwa Freie Berufe, Handwerk und industrielle Produktion setzte IT stärker ein und sind auch eher für Sicherheitsbelange sensibilisiert, da IT-Sicherheit eine wichtige Bedeutung für die Absicherung ihrer Geschäftstätigkeit bietet. Angesichts der hohen Bedeutung von Datenschutz und Datensicherheit im Gesundheitswesen ist der vergleichsweise zu anderen Branchen deutlich geringere Einsatz von IT-Sicherheitsmaßnahmen besorgniserregend. Vor allem die Experten haben deutlich auf den Verbesserungsbedarf hingewiesen und die Situation als prekär dargestellt.

Eine hohe Awareness bedeutet aber nicht immer, dass Unternehmen auch entsprechend handeln – die Umsetzungslücke im organisatorischen und personellen Bereich bleibt sowohl bei kleinen als auch bei größeren KMU bestehen. Auch risikoreiche Anwendungen werden nicht immer ausreichend abgesichert bzw. trotz Risiken eingesetzt (WhatsApp, Soziale Netzwerke).

Eigene Mitarbeiter gelten weiter als Hauptursache für Schadensfälle, aber auch „Sabotage“, d.h. absichtliche Manipulation durch Außen- und Innentäter sowie Spionage hat in der Wahrnehmung der KMU deutlich zugenommen. 20% der KMU haben keine konkreten IT-Sicherheitsprobleme bemerkt, ein Drittel sieht keine Notwendigkeit zur Erhöhung der IT-Sicherheit.

Technischer Schutz ist mittlerweile ausreichend vorhanden (>90%), muss aber noch weiteren Maßnahmen flankiert werden, um wirksam zu sein. Nur 55% der KMU verfügen über Personal mit IT-Sicherheitskenntnissen. Der Einsatz von Verschlüsselung hat im Vergleich zu vor fünf Jahren deutlich zugenommen, auch bei kleinen KMU, aber weniger als die Hälfte der Unternehmen dieser Größenklasse ist in der Lage, unbefugte Zugriffe zu entdecken.

Informationen werden zumeist „im Vorbeigehen“ über Massenmedien oder Internet-Recherche wahrgenommen. Die Information wird damit weniger gezielt aufgenommen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

Kostenlose Schulungen bilden einen wichtiger Einstieg in das Thema IT-Sicherheit, die Nutzung von spezifischen (kostenpflichtigen) Schulungen und Beratungsleistungen sind stark abhängig von der Unternehmensgröße.

Die Anstrengungen für mehr IT-Sicherheit haben sich demgegenüber in den letzten fünf Jahren wenig erhöht. Einzige Ausnahme ist der technische Bereich. Basislösungen sind hier flächendeckend vorhanden und beim Einsatz von Verschlüsselungslösungen gibt es immerhin Fortschritte. Personelle und organisatorische Maßnahmen bleiben dagegen weiterhin sogar hinter der eigenen Risikoeinschätzung und dem objektiven Schutzbedarf zurück.

Der Grund für diese weiterhin bestehende **Umsetzungslücke zwischen Risikowahrnehmung und der Bereitschaft, in IT-Sicherheitsmaßnahmen zu investieren** ist offenkundig in der **Unternehmensstruktur der KMU** selbst zu suchen. Fehlende Größenvorteile in Kleinst- und Kleinunternehmen, mangelnde IT-Sicherheitsaffinität und geringes IT-Know-how der Mitarbeiter und Leitungsebene bei gleichzeitig hoher Verbreitung von IKT in den Unternehmen, Zeitmangel und Kostenvorbehalte bei der Durchführung von Projekten und Vorhaben außerhalb der unmittelbaren Geschäftsziele sind als Hauptursache für diese Umsetzungslücke anzusehen.

Die Digitalisierung bedeutet jedoch noch größere Herausforderungen für die IT-Sicherheit als vor fünf Jahren. Die Nutzung von IKT in KMU hat seit der WIK-Untersuchung im Jahr 2011/12 stetig zugenommen. IT-Sicherheit kann somit heute kein Randthema mehr sein, sondern sollte zum **integralen Bestandteil der Unternehmensstrategie und –kultur** werden.

Als Schlussfolgerung und Handlungsmaxime für die Zukunft kann aus der Untersuchung zur aktuellen Lage der IT-Sicherheit in KMU festgehalten werden:

- Die **Awareness bei den KMU für IT-Sicherheitsrisiken ist in den letzten Jahren zwar gewachsen**, diese Bewertung wird aber **zu wenig in konkrete Maßnahmen** umgesetzt

- Ein **Qualitätssprung bei den Angriffen** auf die IT-Sicherheit stellt KMU, aber auch politische Akteure, vor **neue Herausforderungen**

- Die Bedeutung der Digitalisierung wird weiter steigen. IT-Sicherheit wird damit ein immer zentralerer Baustein der Geschäftsmodelle von KMU. Das Schaffen eines hohen IT-Sicherheitsniveaus erfordert angesichts des starken **Wandels im Markt** (Innovationen, Neugründungen, Expansion) und der **Digitalisierung permanenten Dialog mit den Unternehmen**

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

- IT-Sicherheit ist aus der Unternehmensperspektive, aber auch aus volkswirtschaftlicher Sicht als **rekursiver Prozess** zu verstehen

Aus diesen Ergebnissen lassen sich für die Unternehmen selbst, aber auch für politische Akteure, Interessensverbände und Unternehmensorganisationen Handlungsempfehlungen ableiten, die für die Zukunft wichtig sind, um den Herausforderungen der weiteren IT-Nutzung und Digitalisierung zu begegnen.

12.2 Schritt für Schritt: Was Unternehmen selbst tun können

Sicherheitskultur im Unternehmen etabliert sich eher, wenn sie „von oben“ vorgelebt wird, so die Erfahrungen der befragten Unternehmer und Experten. Geschäftsführer sollten ihre Vorbildfunktion als Führungskraft im Bereich IT-Sicherheit annehmen. Bereits kleine Schritte können schon einen entscheidenden Unterschied zur Verbesserung der IT-Sicherheit im Unternehmen leisten. Eine einfache, intern durchgeführte IT-Sicherheitsanalyse auf Basis vorhandener Checklisten bildet einen ersten Startpunkt. Notfallpläne für den Ernstfall können auch intern erarbeitet und geprobt werden. Wichtig ist zum Beispiel, das regelmäßige Back-up auch einmal auf seine Zuverlässigkeit zu überprüfen. Eine erste IT-Sicherheitsanalyse im Rahmen einer unternehmensinternen Strategieplanung ist ebenfalls sinnvoll, auch wenn spezielle Probleme mit Hilfe von Fachleuten gelöst werden sollten. Die interne Beantwortung von Fragen wie „Was sind schützenswerte Datenbestände in meinem Unternehmen?“ und „Was können wir tun, wenn die IT ausfällt, wenn wichtige Daten plötzlich nicht mehr vorhanden sind oder wenn ein Mitarbeiter aus dem Unternehmen ausscheiden soll, der Zugang zu wichtigen Daten hat?“ können ein Start für erste Überlegungen zur Erhöhung der IT-Sicherheit im Unternehmen sein.

Vorhandene Regeln zum Umgang mit IT und Daten können die Unternehmen selbst schriftlich festzuhalten und immer wieder bei den Mitarbeitern in Erinnerung rufen. Kurze Informationen vor z.B. regelmäßig stattfindenden Besprechungen können Routine in die Informations- und Schulungsbemühungen bringen.

Kostenlose Angebote neutraler, regionaler Anbieter können zur Erstinformation genutzt werden. Viele den Unternehmen bekannte Organisationen vor Ort wie etwa die IHKs, Handwerkskammern oder andere lokale Initiativen widmen sich mittlerweile dem Thema. Eine Erfahrungsaustausch unter Unternehmern könnte im Rahmen eines regelmäßigen Treffens organisiert werden. Persönliche Empfehlungen zu Vorgehensweisen und Austausch von Tipps zu Dienstleistern gelten immer noch als wichtigster Einstieg in das Thema, wie in den Experteninterviews immer wieder versichert wurde.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Angebote an KMU für erste Informationen, Schulung und Beratung

Unterstützung bieten heute vor allem auch vorhandene Institutionen wie zum Beispiel die Industrie- und Handelskammern, die Handwerkskammern oder auch die Kompetenzzentren von Mittelstand-Digital (www.mittelstand-digital.de), die regional aufgestellt sind und zum Teil auf eine jahrzehntelange Erfahrung in der Beratung von KMU vor Ort zurückblicken können. Es darf aber auch nicht vergessen werden, dass Information auch eine „Holschuld" der Unternehmen darstellt und eine gewisse Awareness und Bereitschaft, aktiv zu werden erwartet werden kann.

Im Rahmen der Initiative des Bundesministeriums für Wirtschaft und Energie „IT-Sicherheit in der Wirtschaft"[58] sind wichtige Unterstützungsprojekte für KMU entstanden, die konkreten Nutzen für die Unternehmen bieten und unmittelbar eingesetzt werden können, zum Beispiel

- Webseiten-Check der Initiative-S www.initiative-s.de: Mit Schadprogrammen infizierte Unternehmens-Webseiten bilden eine Gefahr im Internet. Der eco-Verband der Internetwirtschaft hat einen Sicherheitsservice entwickelt, über den die Unternehmen ihren Internet-Auftritt kostenfrei von den Experten der Initiative-S online prüfen lassen können. Unternehmen, die die Sicherheit ihrer Webseiten regelmäßig prüfen lassen, können ihren Internetauftritt mit einem Sicherheits-Siegel versehen.

- Bildungsangebot Bottom-Up: Berufsschüler für IT-Sicherheit: www.dsin-berufsschulen.de: Auf Basis dieser Lehrmaterialien, entwickelt von Deutschland sicher im Netz e.V. erhalten Lehrkräfte kostenfrei praxisnahe Unterrichtsmaterialien zum Thema IT-Sicherheit in Unternehmen (Lehrfilme, Online-Quizspiele, Rollenspiele und Gruppenarbeitsaufträge), die sich im Unterricht nutzen lassen. Künftige Mitarbeiter werden so bereits in der dualen Ausbildung zu IT-Sicherheitsfragen geschult und dienen als Multiplikatoren, indem sie Transfermaterialien wie praktische Checklisten in den Betrieben einsetzen können. Eine Erprobung an Pilotschulen fand von 2015 bis 2016 statt.

- SIWECOS - Sichere Webseiten und Content Management Systeme www.siwecos.de: SIWECOS hilft KMU dabei, Sicherheitslücken auf Webseiten zu erkennen und zu beheben. Ein Vulnerability Scanner überprüft in regelmäßigen Abständen die Serversysteme auf bekanntgewordene Schwachstellen oder die darauf installierten Webanwendungen auf Sicherheitslücken hin. SIWECOS wurde unter der Prämisse Secure by Design entwickelt. Ein Service für Webhos-

58 Weitere Hinweise finden sich auch unter www.it-sicherheit-in-der-wirtschaft.de.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

ter informiert aktiv über Sicherheitslücken und bietet Filtermöglichkeiten an. So können Cyberangriffe rechtzeitig gestoppt werden.

- KMU AWARE - Awareness im Mittelstand www.awareness-im-mittelstand.de: Das Projekt bietet Veranstaltungen und Trainingsangebote, z.B. Online-Trainingsmodule zum Schwerpunkt Phishing und zum Passwortsicherheitstraining sowie Awareness-Module, die die Prinzipien des Darknet erläutern und in Live Hackings aufzeigen, welchem IT-Sicherheitsrisiko die KMU ausgesetzt sind. Weitere Trainings der Projektpartner usd AG Forschungsgruppe SECUSO der TU Darmstadt sind in der Entwicklung.

- Cyber Security Challenge Germany www.cscg.de: Die Cyber Security Challenge Germany sucht junge IT-Fachleute und Talente, sich für einen europaweiten Wettbewerb qualifizieren können. Auf eine Qualifikationsrunde mit neun Online-Aufgaben (www.hacking-lab.com) folgt ein Landesfinale in Düsseldorf mit Möglichkeit zur Qualifikation für die European Cyber Security Challenge (www.ecsc.eu).

- Kompass zur IT-Verschlüsselung: Auf Basis einer Studie im Auftrag des BMWi, die den Nachholbedarf bei KMU in diesem Bereich aufzeigt, haben die Auftragnehmer Goldmedia GmbH zusammen mit dem Institut für Internet-Sicherheit – if(is) und dem Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie, IRNIK, einen Leitfaden[59] für die Anwendung von Verschlüsselung im Unternehmen erstellt.

- IT-Sicherheitsnavigator: Der IT-Sicherheitsnavigator hilft dabei, das passende Informations- und Beratungsangebot zu finden. Er listet Beratungsstellen in der Region sowie kostenlose Checklisten, Broschüren und andere multimedialen Informationsangebote.[60]

- IT-Sicherheitscheck www.dsin-sicherheitscheck.de: Der DsiN-Sicherheitscheck bietet eine erste Ermittlung des IT-Sicherheitsniveaus individuell für ein KMU mit ersten passenden Handlungsempfehlungen. Der DsiN-Sicherheitscheck greift zum Beispiel Herausforderungen von Industrie 4.0 bis zur EU-Datenschutzgrundverordnung auf und informiert über die Versicherbarkeit von IT-Risiken. Der Test umfasst bis zu 24 Fragen und kann in kurzer Zeit online absolviert werden. Er dient auch als Einstiegstest für die Workshop-Reihe IT-Sicherheit@Mittelstand, der gemeinsamen Workshop-Reihe des DIHK mit DsiN.

59 Siehe http://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompass-it-verschluesselung.html
60 Der Navigator ist nutzbar unter: http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Angebote/IT-Sicherheitsnavigator/it-sicherheitsnavigator-suche.html

Die Allianz für Cybersicherheit, gegründet vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Branchenverband Bitkom im Jahr 2012 bildet ebenfalls eine Anlaufstelle für Unternehmen, die im Bereich IT-Sicherheit aktiv sind und zum Wissenstransfer für Unternehmen beitragen wollen.[61] Hier können auch Sicherheitsvorfälle und Cyber-Angriffe mittels Online-Meldeformular gemeldet werden. Das BSI bietet auch auf vielen Themengebieten Hilfestellungen, z. B. durch die Veröffentlichung von Leitfäden und von praxisorientierten Hintergrundinformationen, mit denen die Sicherheit in Institutionen geprüft werden kann, an. Für Unternehmen steht damit nicht nur der IT-Grundschutz, sondern auch weitere Anleitungen zur Verfügung wie etwa der „Leitfaden zur Basis-Absicherung nach IT-Grundschutz: In 3 Schritten zur Informationssicherheit“, der sich an kleine und mittlere Unternehmen sowie kleinere Behörden richtet und einen kompakten Einstieg zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) beinhaltet.[62]

12.3 Handlungsoptionen und Unterstützungsmaßnahmen: Was kann getan werden, um KMU auf dem Weg zu mehr IT-Sicherheit zu unterstützen?

Was weiterhin wichtig ist

Weiterhing wichtig ist es daher, **Bewusstsein zu wecken.** Awarenesskampagnen zu initiieren und bestehende zu unterstützen bleibt eine Daueraufgabe. Die Initiative IT-Sicherheit in der Wirtschaft des BMWi hat hier bereits durch zahlreiche Projekte eine Grundlage gelegt. Diese sollten verstetigt werden, um KMU im digitalen Wandel nachhaltig bewusst zu machen, dass Digitalisierung ohne IT-Sicherheit ein Risiko darstellt.

Themen wie die Umsetzung der Datenschutz-Grundverordnung (DSGVO) können genutzt werden, um KMU auch für IT-Sicherheit zu sensibilisieren.[63] Im Rahmen der Interviews wurde wiederholt von den Experten berichtet, dass die DSGVO aktuell ein relevantes und damit gefragtes Thema ist und die Unternehmen im Zusammenhang mit den Anforderungen an den Datenschutz auch ihre technischen, organisatorischen und personellen IT-Sicherheitsmaßnahmen überdenken.

---

61 Siehe https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html. Derzeit hat die Organisation über 2.500 Mitgliedsunternehmen. Die Ergebnisse der Meldungen von Sicherheitsvorfällen wird jährlich veröffentlicht.

62 Download unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3.

63 So zum Beispiel auf der Mittelstand 4.0-Regionalkonferenz des BMWi am 15. März in Chemnitz, wo es um die rechtssichere Gestaltung der Digitalisierung geht. Unter dem Motto „Sicher Betrieb Machen! – Datenhoheit, Datensicherheit, Datenschutz in der Praxis“ werden einen Tag lang Praxisbeispiele vorgestellt und diskutiert, wie die Digitalisierung (rechts-)sicher (und u.a. DSGVO-konform) gelingt.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Dennoch befürchten viele Experten, dass die Vorbereitungen hinsichtlich der Umsetzung bis zum Inkrafttreten im Mai 2018 nicht bzw. zu selten stattfinden. Das Gesundheitswesen scheint laut Einschätzung der Interviewpartner weniger weit in der Umsetzung als andere Branchen. Ein Experte formulierte es so: *„Die DSGVO wird die Praxen eiskalt erwischen. Nach der Umsetzungsfrist besteht die Gefahr für blinden Aktionismus“.*

Nach Aussagen von Experten ist es unabdingbar, den Entscheidern in den KMU vor Augen zu führen, wie vergleichbare Unternehmen IT-Sicherheit angehen. **Beispiele zu zeigen,** Best-Practices und Fallbeispiele zu verbreiten, bei Treffen vor Ort „unter sich“ Tipps und Anregungen auszutauschen stellt eine nicht zu unterschätzende Hilfestellung dar, wenn erste Hürden zur Umsetzung von IT-Sicherheitsmaßnahmen überwunden werden sollen. Aktivitäten in diesem Bereich initiiert das BMWi vor allem mit der Förderinitiative Mittelstand-Digital, die zahlreiche Praxisbeispiele veröffentlicht.[64]

In der Repräsentativbefragung wurde deutlich, dass sich Unternehmen vor allem „bessere Informationen“ wünschen. 20% aller Unternehmen, die Unterstützungsmaßnahmen für sinnvoll erachten, gaben dies als Antwort auf die offen gestellte Frage an. Dieser umgangssprachliche Ausdruck verdeutlicht vor allem eins: Unternehmen sehen, dass Informationen zu IT-Sicherheit verfügbar sind, sie treffen aber häufig nicht die Sprache und die Problemlage der Unternehmen. Um „bessere“ Informationen, d.h. zielgruppengerechte Angebote zu erarbeiten, ist eine didaktische Aufbereitung der Angebote zu fördern, damit die Inhalte von KMU verstanden werden. KMU **verständlich anzuleiten** ist eine Grundvoraussetzung, um Awareness zu wecken und Umsetzungsbeispiele und Leitfäden der Zielgruppe nahe zu bringen.

Im Zusammenhang mit KMU ist es außerdem erforderlich, den Aktionsradius insbesondere von kleineren KMU mit weniger als 50 Mitarbeitern zu berücksichtigen. Es geht vor allem darum, die **regionale Präsenz zu stärken.** KMU benötigen neutrale Beratungseinrichtungen und bevorzugen Angebote vor Ort, da der Zeit- und Kostenaufwand für den Besuch von Veranstaltungen und Beratungen den Ressourcen angepasst sein muss. Die vom BMWi geförderten IT-Sicherheitsworkshops in der Fläche, wie sie z. B. von DsiN und DIHK durchgeführt werden, leisten dazu einen Beitrag. Diese Bemühungen sollten weiter verstärkt werden, wozu sich auch die Kompetenzzentren von Mittelstand-Digital eignen. Ziel sollte es sein, auch Regionen abseits der vorhandenen Zentren zu erreichen, auch wenn dies einen hohen Aufwand für ggf. wenige Teilnehmer und Interessierte bedeutet.

64 Zum Beispiel in der Reihe „Wissenschaft trifft Praxis“, zu finden unter http://www.mittelstand-digital.de/DE/Presse/Downloads/magazin.html. Im Jahr 2018 werden im Themenschwerpunkt IT-Sicherheit weitere Umsetzungsbeispiele veröffentlicht.

Informations- und Schulungsangebote als Einstieg und zur ersten IT-Sicherheitsanalyse können eine wichtige **Hilfe bei Kosten-Nutzen-Abwägungen** im Hinblick auf IT-Sicherheitsmaßnahmen der KMU sein. Das neu gestartete Förderprogramm „go-digital" richtet sich z. B. gezielt an kleine und mittlere Unternehmen der gewerblichen Wirtschaft und an das Handwerk und bietet Beratungsleistungen an, um mit „dem steigenden Sicherheitsbedarf bei der digitalen Vernetzung" Schritt zu halten.[65] Autorisierte Beratungsunternehmen übernehmen die Antragstellung für die Förderung.[66] Wenn diese Angebote nachhaltig in der Fläche bekannt werden, auch beworben durch die registrierten Dienstleister, kann dies ein wichtiger Beitrag zur Verminderung der Kostenlast bei IT-Sicherheitsberatungen in KMU sein.

Den öffentlichen Akteuren im Bereich IT-Sicherheit kommt zentrale **Lotsenfunktion** zu, wenn es darum geht, KMU beim Finden von neutralen IT-Beratern und IT-Produkten zu unterstützen. Die Kompetenzzentren Mittelstand-Digital und der IT-Sicherheitsnavigator der Initiative IT-Sicherheit in der Wirtschaft tragen dazu bei, letztere ist jedoch möglicherweise noch nicht bekannt genug.

Das Vorhandensein zahlreicher Angebote und Initiativen macht vor allem deutlich, dass die KMU zum Teil mit der **Fülle an Informationen überfordert** sein könnten und die **Vielzahl der Angebote auch zu Intransparenz führen** kann. Daher sollte die **Lotsenfunktion** auch so verstanden werden, dass kontinuierlich die verschiedenen Akteure untereinander über ihre Angebote kommunizieren, sich vernetzen und Erfahrungen austauschen.

Eine notwendige **Aufklärung**, die neutral über aktuelle Sicherheitsvorfälle, ihre Einfallstore und mögliche Schäden und Kosten berichtet, ohne Führungskräfte in KMU dazu zu verleiten, die Vorkommnisse zu ignorieren und zu resignieren erscheint als eine ebenfalls wichtige, flankierende Maßnahme, um die Relevanz kontinuierlicher Anstrengungen in den Unternehmen zu verdeutlichen. Den Akteuren kommt die schwierige Aufgabe zu, immer wieder auf die Bedrohungen und neue Angriffsszenarien hinzuweisen und die Erforderlichkeit für stetige Überprüfungen und Modernisierungen der IT-Sicherheitsmaßnahmen nachdrücklich aufzuzeigen. Das BSI hat mit der Allianz für Cybersicherheit und der Online-Meldung von Vorfällen dazu eine Struktur geschaffen, die der Masse der KMU nahegebracht werden könnte.

65 https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/foerderprogramm-go-digital.html.

66 Kriterien für zu fördernde Unternehmen: Unternehmen der gewerblichen Wirtschaft einschließlich des Handwerks mit technologischem Potenzial, Beschäftigung von weniger als 100 Mitarbeitern, Jahresumsatz oder eine Jahresbilanzsumme des Vorjahres von höchstens 20 Millionen Euro.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Heute im Vergleich zu 2011/12 besonders wichtig

Heute ist im Vergleich zu 2011/12 insbesondere vor dem Hintergrund der Digitalisierung wichtig, die **Nachhaltigkeit der Angebote zu sichern.** KMU im Wandel brauchen immer wieder IT-Sicherheitsinformationen und –schulungen, um ihre IT-Sicherheitsmaßnahmen an den Einsatz von IKT anzupassen. Die Untersuchung hat gezeigt, dass PC-Arbeitsplätze, Internet-Zugang und der Umgang mit mobilen Endgeräten auch in KMU aller Größenklassen selbstverständlich geworden ist. E-Commerce, IoT-Anwendungen oder Industrie 4.0 Unternehmen benötigen aber Angebote auf höherem Niveau und Unternehmen, die in diesen Bereichen erst noch investieren wollen, stehen vor der Aufgabe, die richtigen Maßnahmen und Beratungsleistungen auszuwählen.

Parallel zu den oben genannten Handlungsoptionen erscheint die Anpassung von **Schule, Aus- und Weiterbildung** an die neuen, sich verändernden Herausforderungen der Digitalisierung und IT-Sicherheit als übergreifende, zentrale Aufgabe für die Zukunft, die über die Erhöhung von IT-Sicherheit in Unternehmen weit hinausgeht. KMU leiden aufgrund ihrer begrenzten Ressourcen besonders unter Fachkräftemangel. 40% der Industriebetriebe sehen im Fachkräftemangel eines der Hauptrisiken (DIHK Industriereport 2016/17). Sie fordern den Ausbau der Digitalen Bildung (BITMi 2017). Erste Schritte wurden mit dem Projekt „Bottom-Up: Berufsschüler für IT-Sicherheit“ gemacht. Die Erneuerung von Verordnungen über die Berufsausbildung, wie sie z. B. im Bereich IT-Systemelektroniker/in, Fachinformatiker/in, IT-System-Kaufmann/frau, Informatikkaufmann/frau erfolgt sind unter der Berücksichtigung von IT-Sicherheit, Datenschutz und Urheberrechtsbelangen, ist eine wichtige Zukunftsaufgabe, die lange Zeit zur Umsetzung benötigen wird. Die Barrieren für eine rasche Umsetzung sind jedoch in der Struktur des Bildungs- und Ausbildungssystems im Allgemeinen zu suchen und sind nicht IT- oder IT-sicherheitsspezifisch.

Schließlich ist eine zentrale Herausforderung für die Unternehmen, IT-Sicherheit nicht als nachträgliche Maßnahme zu verstehen, die erst bei Auftreten von Sicherheitsprobleme in Angriff genommen wird, sondern von Anfang an nutzerfreundliche Sicherheitsfunktionen mitzudenken und in Unternehmensprozesse zu integrieren. **Security by Design** bzw. die Auswahl von IKT unter Berücksichtigung der benötigten IT-Sicherheitsmaßnahmen und die Implementierung in organisatorische Prozesse ist eine Voraussetzung dafür, dass erarbeitete IT-Sicherheitskonzepte und ISMS (Managementsysteme für Informationssicherheit) in den KMU auch effektiv greifen können.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheit IN DER WIRTSCHAFT

13 Ausblick und weitere Fragestellungen

Blockchain: Potentiale für mehr Sicherheit bei (online) Transaktionen

Bei **Blockchain** handelt es sich um eine Technologie, die Transaktionen transparent und manipulationssicher erfassen kann. Kommunikationspartner können mit Hilfe von Blockchain ohne ein Intermediär, wie beispielsweise eine Bank, miteinander agieren. Die Blockchain kann nicht bzw. nur schwer manipuliert werden. Das liegt zum einen daran, dass die Transaktionen verteilt gespeichert werden. Es gibt also unzählige Kopien der Transaktionen auf den verteilten Geräten aller Teilnehmer. Außerdem erhält jeder Teilnehmer einen individuellen (Private Key) und einen öffentlichen Schlüssel (Public Key). Um neue Informationen in die Blockchain aufzunehmen, müssen die Transaktionen von allen bestätigt werden. Dazu gibt es verschiedenen Verfahren. Bekannte Verfahren sind der Proof of Work (PoW), wie er bei Bitcoin verwendet wird oder der Proof of Stake.[67]

Die bekannteste **Anwendung** auf einer Blockchain ist die Kryptowährung Bitcoin. Sie bildet allerdings lediglich einen spezifischen Anwendungsbereich der Blockchain ab. Es gibt zahlreiche Anwendungen bei denen Experten hohes Potential für eine gesteigerte Sicherheit durch Blockchain sehen.[68] Im Bereich digitaler Güter kann die Blockchain beispielsweise für einen sogenannten „Proof of ownership“ eingesetzt werden. Hierdurch können Urheber von z.B. Musik, Fotos oder Filmen transparent erfasst und Copyright Fragen gelöst werden. Außerdem könnte die Blockchain dazu eingesetzt werde, die Echtheit von Zeugnissen zu bestätigen, um Fälschungen auch bei einem ausschließlich digitalen Bewerbungsverfahren aufzudecken. Mit Hilfe von auf Blockchain basierenden Smart Contracts können Regeln im Geschäftsprozess automatisiert ausgeführt werden. Blockchain bietet laut Experten somit das Potential für mehr Sicherheit im Bereich der additiven Fertigung. Hier besteht das Problem, dass jeder, der die Konstruktionsdaten besitzt, die Teile in beliebiger Losgröße produzieren kann.[69] Im Bereich 3D-Druck könnte der Prozess mit Blockchain dabei so aussehen, dass Unternehmen A von Unternehmen B eine Zeichnung bzw. die Konstruktionsdaten für ein Ersatzteil über die Blockchain erhält. Der Empfänger erhält dabei das Recht, diese Daten einmal zu verwenden (Lizenzierung). In einem Service Center, was nach Nutzung abrechnet, wird das Teil mittels 3D-Druck hergestellt (Produktion). Nach Abschluss des Drucks wird die

67 Kaltofen, Thomas (2017): Blockchain-Technologien im Detail - Kryptowährungen verstehen, selbst kreieren. URL: https://www.computerwoche.de/a/blockchain-technologien-im-detail,3330877,2.

68 Siehe dazu beispielsweise: TeleTrusT Bundesverband IT-Sicherheit e.V. (2017): Blockchain ist Chance für die IT-Sicherheitsindustrie. Pressemitteilung vom 01.03.2017, URL: https://www.teletrust.de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=1021&cHash=c280b4cfd15f9c359751c5aa97858b54.

69 Giese, Philipp (2017): SAMPL – sicherer 3D-Druck auf der Blockchain. 25.06.2017, URL: https://www.btc-echo.de/sampl-sicherer-3d-druck-auf-der-blockchain/.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Zahlung von Unternehmen A an Unternehmen B automatisch ausgelöst.[70] Wie genau sichergestellt werden soll, dass reale Objekte zuverlässig in die Blockchain integriert werden, erforscht das vom BMWi geförderte Projekt SAMPLE (Secure Additive Manufacturing Platform).

Welche Anwendungen sich auf Basis von Blockchain entwickeln und letztlich durchsetzen, ist aktuell noch nicht absehbar. Die Berichterstattung der vergangenen Monate zeigt allerdings das große Potential und die Bandbreite von Anwendungsmöglichkeiten auch für KMU.[71]

Weiterführende Untersuchungsbereiche für mehr IT-Sicherheit in KMU

Im Rahmen dieser Studie stellte sich heraus, dass ein weiterer Bedarf zur Analyse der Strukturen im Bereich der Spezialanbieter von IT-Sicherheit hinsichtlich der Schnittstellen zu KMU vorhanden ist.

- Struktur und Ausgestaltung von Wertschöpfungskette von IT-Spezialisten und möglichen regionalen Partnern (B2B)

Im Bereich der Anbieter von IT-Sicherheit zeichnet sich eine Arbeitsteilung zwischen den Herstellern der Lösungen und Vertriebspartnern ab. Dieses in der Vergangenheit freilich nicht unbekannte Modell bietet Potentiale zum Ausbau. Gezielte Schulungen großer Unternehmen für kleine Anbieter, die regional vor Ort sind, können eine nahezu vollständige Information bei regionaler Betreuung sicherstellen. Dazu könnte auch eine flächendeckende Etablierung von Notfallstellen angeboten von großen Spezialisten für regionale Anbieter (also B2B) gehören.

70 Stommel, Sebastian (2017): Blockchain-basiertes Supply Chain Management. Vortrag im Rahmen des TeleTrusT-Informationstag „Blockchain", 13.07.2017.

71 Nördinger, Susanna (2017): Darum passen Blockchain und Industrie 4.0 zusammen. 25.08.2017, URL: https://www.produktion.de/revolution-blockchain-archiv/darum-passen-blockchain-und-industrie-4-0-zusammen-278.html. O.V. (2017): If blockchains ran the world - Disrupting the trust business. In: The Economist.com, 15.07.2017, URL: https://www.economist.com/news/world-if/21724906-trust-business-little-noticed-huge-startups-deploying-blockchain-technology-threaten. Deutsche Bundesbank (2016): Gemeinsamer Blockchain-Prototyp von Deutscher Bundesbank und Deutscher Börse. Pressemitteilung vom 28.11.2016, URL: http://docs.dpaq.de/11581-2016_11_28_blockchain_prototyp.pdf. Schmitz, Peter (2017): Blockchain als Chance für die IT-Sicherheitsindustrie. In: Security Insider.de, 22.03.2017, URL: http://www.security-insider.de/blockchain-als-chance-fuer-die-it-sicherheitsindustrie-a-592079/.Wiebe, Frank (2017): Blockchain - Der stromfressende Alleskönner. In: Handelsblatt.com, 02.07.2017, URL: http://www.handelsblatt.com/my/finanzen/maerkte/devisen-rohstoffe/blockchain-der-stromfressende-alleskoenner/20007958.html. „Blockchain Could Make the Insurance Industry Much More Transparent"¬¬, Harvard Business Review, Dante Disparte, 12.07.2017 https://hbr.org/2017/07/blockchain-could-make-the-insurance-industry-much-more-transparent.

- Struktur und Umfang eigner und fremder Leistungen bei KMU

Zum anderen scheinen viele KMU vor der Frage zu stehen, ab wann und für welche Aufgaben sich eine Vollzeitstelle für das Thema IT-Sicherheit im eigenen Unternehmen lohnt. Diverse Experten der Anwenderseite schätzen die Bündelung aller Aufgaben im Bereich IT- und Informationssicherheit in nur einer Person als unzureichend und ineffizient ein. Weiterführende Analysen könnten Fragen nach kritischen Schwellwerten bezüglich eigener Vollzeitstellen als auch Fragen nach Arbeitsteilungsmodelle im Bereich IT-Sicherheit nachgehen. Zu denken ist hierbei an Outsourcing-Modelle, die in Umfang, Zeitraum und im Grad der Abgabe von Verantwortung stark variieren können. Cloud-Anwendungen bieten dabei neue Möglichkeiten (Security as a Service).

Regelmäßiger Informationsbedarf zur aktuellen Lage der IT-Sicherheit in KMU

Natürlich kann die vorliegende Studie das Themenfeld IT-Sicherheit und KMU nicht erschöpfend und ein für allemal abhandeln. Insbesondere durch die Dynamik der Digitalisierung, die 4. Industrielle Revolution und viele Smart-Anwendungen, die auch für KMU als Nutzer oder Anbieter relevant sind, wird die Frage zur aktuellen Lage der IT-Sicherheit in KMU in regelmäßigen Abständen zu stellen sein, auch um die Veränderungen in der Zeit zu analysieren. Letztlich wird es darum gehen, Handlungsempfehlungen zu aktualisieren, neue zu entwickeln und Korrekturen an wenig effizienten Maßnahmen durchzuführen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Expertengespräche

WIK dankt allen, die für Experteninterviews zur Verfügung standen, namentlich den folgenden Experten:[72]

Angela Baudach, Security Awareness Consultant, DXC Technology

Stefan Becker, Referatsleiter Referat B25 Cyber-Sicherheit für die Wirtschaft, Bundesamt für Sicherheit in der Informationstechnik

Dr. Christina Czeschik, Beratung und Fachredaktion in den Bereichen E-Health, Datenschutz und Informationssicherheit, Serapion, Ärztin für Medizinische Informatik

Oliver Dehning, Hornetsecurity GmbH, CEO, Hannover (TH)

Dipl.-Wirt.-Ing. Wolfgang Diebke, HWK Dortmund, Technologieberater Beauftragter für Technologie und Innovation (BIT)

Dr. Michael Dolny, Multimedia & E-Business, Südwestfälische Industrie- und Handelskammer zu Hagen

Sebastian Feik, Fachgruppensprecher der Gruppe IT-Sicherheit beim Bundesverband IT-Mittelstand e.V. (BITMi) sowie Geschäftsführer der legitimis group GmbH

Mathias Gärtner, Stellv. Vorsitzender, Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS e.V.)

Prof. Dr. Rainer W. Gerling, IT-Sicherheitsbeauftragter, Max-Planck-Gesellschaft, Hochschule München

Dr. Christoph F-J Goetz, Leiter der TeleTrusT-Arbeitsgruppe „Gesundheitstelematik"

Roland Hallau, Projektmanager, tti Technologietransfer und Innovationsförderung Magdeburg GmbH, Projektleiter Mittelstand 4.0-Agentur Prozesse

Prof. Dipl.-Phys. Till Hänisch, Dozent für Wirtschaftsinformatik, Duale Hochschule Baden-Württemberg

Alexandra Horn; Bundesverband mittelständische Wirtschaft e.V. (BVMW), Leiterin Verbandskooperationen und Projekte, Mittelstand 4.0-Kompetenzzentrum Berlin

72 Es sind diejenigen Experten gelistet, die der Nennung zugestimmt haben.

Harald Kesberg, Projektentwicklung, Kommunikation & Kooperation, Kesberg Consulting

Henrik Klohs, Beauftragter für Innovation und Technologie, Handwerkskammer Frankfurt (Oder) - Region Ostbrandenburg

Dipl.-Ing. Helko Kögel, Director Consulting, Rhode und Schwarz

Dr. Michael Littger, Geschäftsführer, Deutschland sicher im Netz e.V. (DsiN)

Dr. Norbert Niederprüm, Geschäftsführung, dnb Systemberatung

Markus Schaffrin, Geschäftsbereichsleiter Mitglieder Services, Eco - Verband der deutschen Internetwirtschaft e.V.

Hartmut Schmitt, Koordinator Forschungsprojekte, HK Business Solutions (HKBS), Mittelstand –Digital Projekt USecureD

Ulrich Schölermann, Geschäftsführer, Schölermann Werbung und Druck

Jürgen Schüler, Fachbereich Kompetenzzentrum, Technologie- und Innovationsberatung, IT-Sicherheit, Handwerkskammer Rheinhessen

Dr. Christian Schwartz, Senior Security Management Consultant, usd AG, Projekt KMU AWARE

Dr. Katrin Sobania, Leiterin des Referats Informations- und Kommunikationstechnologie, E-Government, Postdienste, DIHK - Deutscher Industrie- und Handelskammertag e. V.

Felix Struve, Ansprechpartner zu den Themen ISIS12, ISA+ Informations-Sicherheits-Analyse, DGO, Bayerischer IT-Sicherheitsclusters e.V.

Thomas Uhlmann, Security Specialist/ Evangelist, ESET

Veiko Ullmann, Leiter Firmengeschäft der Vertriebsdirektion Berlin, Filialdirektor, Allianz Beratungs- und Vertriebs-AG

Reiner Wolf, Herstellungsleiter, Verlag Kirchheim

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Anhang

Tabelle 4: Übersicht relevante Studie zum Thema IT-Sicherheit in KMU

Nr.	Titel	Autor/ Institution	Anzahl der Befragten	KMU Fokus	Methode	Repräsentativ für KMU	Fragt nach Unterstützungsbedarfen	Beinhaltet Handlungsempfehlungen	Auswertung der Ergebnisse nach Branchen	Untersucht Investitionen	Betrachtet Personalfragen im Bereich IT-Sic	Abfrage Bedrohungslage	Betrachtet Schäden	Abfrage technischer Maßnahmen	Sonderthemen	Begleitende Tools oder Leitfäden	Summe inhaltlicher Aspekte (Spalte 8-17)
1	Cyber-Sicherheits-Umfrage 2016	BSI, Allianz für Cybersicherheit	331	✓	selbstselektiv, online, Anwender	×	×	×	×	×	✓	✓	✓	✓	×	× Nicht direkt, generell BSI	4
2	Im Visier der Cybergangster - So gefährdet ist die Informationssicherheit im deutschen Mittelstand	PwC	400	×	CATI, 200-1000 MA, Anwender	×	×	✓	×	✓	✓	✓	×	×	- Industrie 4.0 - IT-SiG	×	5
3	Studienbericht zur Security Bilanz Deutschland 2016: IT- und Informationssicherheit: Technische Maßnahmen und Lösungen in Mittelstand und öffentlichen Verwaltungen	Techconsult und Unterstützer	500	✓	online, Experten	×	×	✓ Gesonderte Publikation für Unternehmen	✓	× Siehe gesonderte Publikation	×	×	×	✓ (nur nach Problemen, nicht nach Vorhandensein)	×	✓ Security Consulter Self Check Tool	4
4	Sicherheitsmonitor Mittelstand 2016	DsiN, Testentwicklung mit Partnern	1.320	✓	selbstselektiv, online, Anwender	×	×	✓	×	×	✓	×	×	✓	- Nutzung von Online-Banking, Cloud-Computing und Co. - Rechtl. Anford. Cloud etc.	✓ DsiN-Sicherheitscheck	5

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Nr.	Titel	Autor/ Institution	Anzahl der Befragten	KMU Fokus	Methode	Repräsentativ für KMU	Fragt nach Unterstützungsbedarfen	Beinhaltet Handlungsempfehlungen	Auswertung der Ergebnisse nach Branchen	Untersucht Investitionen	Betrachtet Personalfragen im Bereich IT-Sic	Abfrage Bedrohungslage	Betrachtet Schäden	Abfrage technischer Maßnahmen	Sonderthemen	Begleitende Tools oder Leitfäden	Summe inhaltlicher Aspekte (Spalte 8-17)
5	eco Studie IT-Sicherheit 2017	Eco-Verband	590	Nicht erhoben	Selbstselektiv, Experten	×	×	×	×	✓	(✓)	✓	×	(×)	- Treiber für Veränderungen der IT-Sic. - Cloud-Sic. - Smart Home - Connected Car	×	4
6	Digitalisierung und IT-Sicherheit in deutschen Unternehmen	Im Auftrag der Bundesdruckerei	500	✓	CATI, >20 – 2.000 MA, Anwender	×	×	×	✓	✓	✓	×	×	✓	- Cloud-Angebote - Einsatz von Mitarbeiterausweisen - IT-Sic. und Digitalisierung	×	5
7	Cybersicherheitsstrategie	PwC Strategy& (i.A. BMI)	300	✓	Sebstselektiv, online, Anwender	× (ab 20 MA)	✓	✓ indirekt	×	✓	✓	✓	×	(×)	- Stresstests - Zusammenarb. Staat und Wirtschaft - Verfügbarkeit IT-Sic.-DL - Staatliche Förderunug - Gütesiegel	×	6
8	Wirtschaftsschutz in der digitalen Welt	Bitkom Research	1.069	?	CATI, Anwender	× (ab 20 MA)	×	✓ (PM)	×	×	×	✓	✓	✓	- Täterkreis - Ursprungsländer der schädl. Handlungen - Einschalten staatlicher Stellen - Schadensfeststellung	×	6
	Summe Häufigkeit des Vorkommens des Themas in allen betrachteten Studien						1	5	2	4	6	5	2	5	6	3	/

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages