Aktuelle Lage der IT-Sicherheit in KMU

Kurzfassung der Ergebnisse der Repräsentativbefragung

Annette Hillebrand
Antonia Niederprüm
Saskja Schäfer
Sonja Thiele

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

IT-Sicherheit IN DER WIRTSCHAFT

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

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 im Auftrag des Bundesministeriums 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.

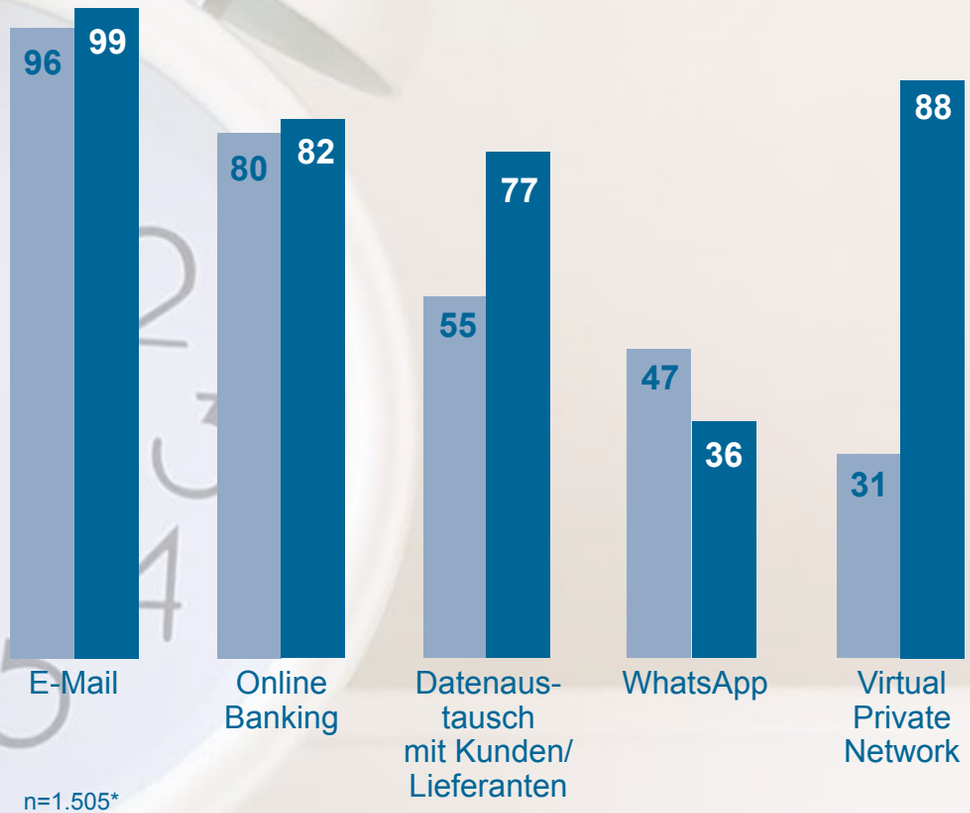
Im Vergleich zu vor fünf Jahren hat sich die Lage der IT-Sicherheit in KMU noch nicht entscheidend verbessert. Mit Blick auf die erheblich gestiegenen Anforderungen stellt sich daher die Herausforderung umso eindrücklicher, die KMU zu unterstützen, die bestehenden Defizite der Umsetzung endlich mit Nachdruck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

Dr. Iris Henseler-Unger
Geschäftsführerin

Digitalisierung erfordert erhöhte IT-Sicherheit

Weckruf: Es ist Zeit aufzuwachen

Nutzung elektronischer Kommunikation in KMU



n=1.505*

Für die meisten KMU in Deutschland sind E-Mail und Online-Banking selbstverständlich.

Komplexere IKT-Lösungen wie etwa den Datenaustausch mit Kunden oder Lieferanten nutzen mehr größere KMU als kleine.

Insbesondere kleine KMU setzen auf WhatsApp als Kommunikationsmedium.

Größere KMU ermöglichen einen externen Zugang (z.B. über VPN) deutlich häufiger als kleine Unternehmen.

kleine KMU (<50 Mitarbeiter)

größere KMU (50-499 Mitarbeiter)

*Repräsentativbefragung von KMU in Deutschland; n=1.508, davon n=1.505 Unternehmen, die das Screening-Kriterium „technische Ausstattung“ (Internet-Zugang, Mobile Endgeräte etc.) erfüllen. Alle Angaben in Prozent.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

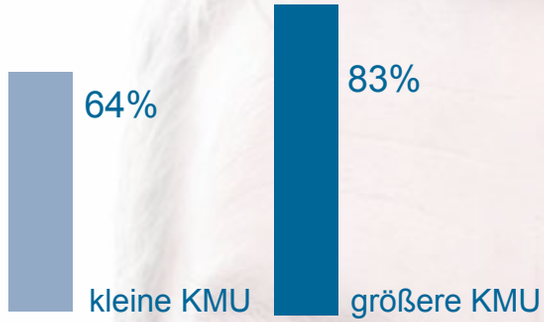
aufgrund eines Beschlusses des Deutschen Bundestages

Bedeutung von IT-Sicherheit

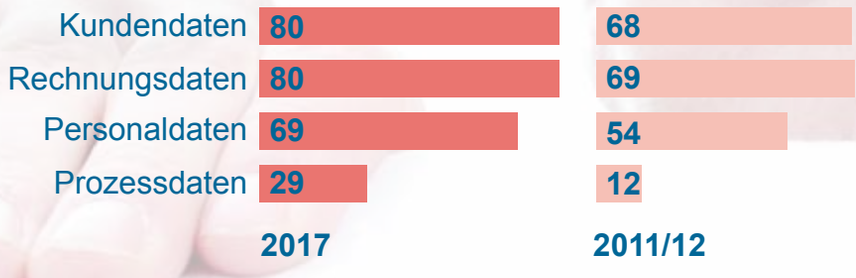
Bedeutung erkannt – Gefahr gebannt?

Für **2/3** der KMU hat **IT-Sicherheit eine „hohe“ bzw. „sehr hohe“ Bedeutung**. Dabei schätzen größere KMU IT-Sicherheit als wesentlich wichtiger ein als kleine KMU.

Welche Bedeutung hat das Thema Sicherheit der Informations- und Kommunikationstechnik in Ihrem Unternehmen?



Anteil der Unternehmen, die den Schutzbedarf ihrer Datenbestände als hoch oder sehr hoch einschätzen (2017 und 2011/12)

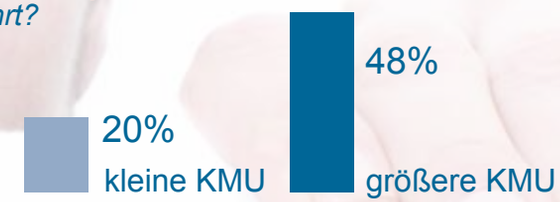


2017: n=1.505; 2011/12: n=922; alle Angaben in Prozent

Die befragten Unternehmen schätzen den Schutzbedarf ihrer Datenbestände durchweg deutlich höher ein als vor fünf Jahren. Die in der letzten Zeit bekannt gewordenen Fälle von Datenleaks sowie von Schadprogrammen wie etwa Verschlüsselungstrojanern haben zu einem erhöhten Risikobewusstsein der Unternehmen geführt. Besonders ausgeprägt ist es in Bezug auf Kunden-, Rechnungs- und Personaldaten.

Dies bedeutet jedoch nicht, dass die Unternehmen entsprechend handeln. **Es besteht eine Umsetzungslücke**. Nur jedes fünfte KMU in Deutschland hat bereits einmal eine IT-Sicherheitsanalyse durchgeführt, bei größeren Unternehmen ist es aber immerhin fast die Hälfte.

Haben Sie in Ihrem Unternehmen schon einmal eine systematische IT-Sicherheitsanalyse durchgeführt?



Gefördert durch:

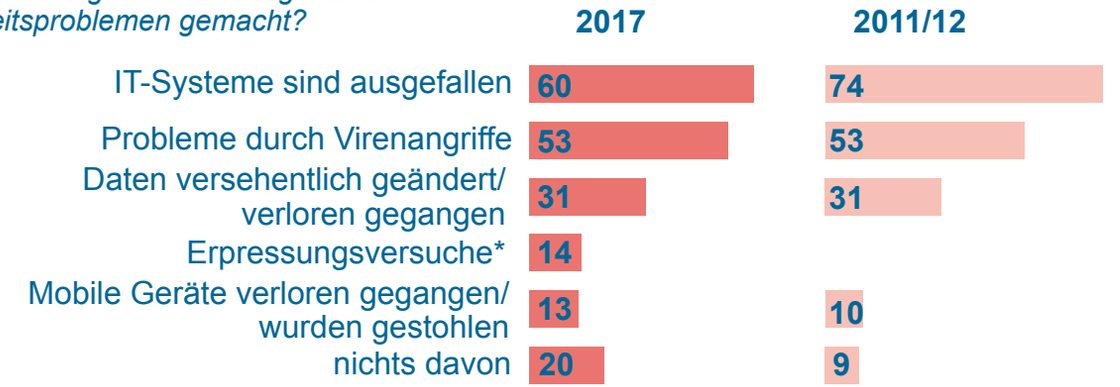
Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Erfahrungen mit IT-Sicherheits-problemen und Ursachen

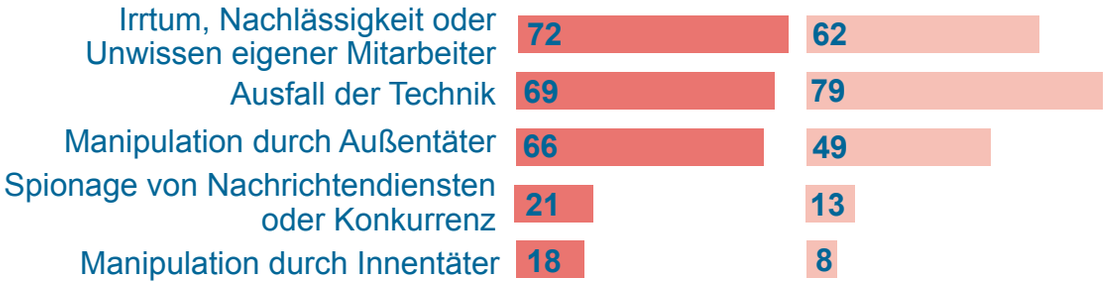
Erfahrungen mit IT-Sicherheitsproblemen

Haben Sie in Ihrem Unternehmen schon einmal konkrete Erfahrungen mit den folgenden IT-Sicherheitsproblemen gemacht?



Ursachen von IT-Sicherheitsproblemen

Wo sehen Sie die hauptsächlichen Ursachen für mögliche Probleme und Schadensfälle im Zusammenhang mit der IT?



2017: n=1.505; 2011/12: n=952; alle Angaben in Prozent; * in 2017 neu aufgenommen

Die überwiegende Mehrheit der KMU hatte schon einmal mit IT-Sicherheitsproblemen zu kämpfen. Zentrale Problembereiche bleiben Ausfall der Technik, Virenangriffe und (versehentlicher) Datenverlust oder -veränderungen. Allerdings geben aktuell deutlich weniger KMU an, dass ihre IT-Systeme ausgefallen sind. Dies spricht für Investitionen in eine erhöhte Ausfallsicherheit. Aber jedes fünfte Unternehmen hat überhaupt keine IT-Sicherheitsprobleme bemerkt – ggf. ein wichtiger Hinweis auf **Lücken in der Prävention**.

Irrtum, Nachlässigkeit oder Unwissenheit der eigenen Mitarbeiter gelten heute als Hauptursache für Schadensfälle. Angriffe mittels Social Engineering bleiben damit offensichtlich ein großes Risiko und die Information und Schulung der Mitarbeiter eine der Hauptaufgaben in KMU. Im Vergleich dazu haben technische Probleme tendenziell abgenommen. Nach Einschätzung der KMU gibt es heute aber deutlich mehr Schadensfälle durch Sabotage und Spionage. Die Unternehmensführung ist hier besonders gefragt, aktiv zu werden.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Technische Maßnahmen

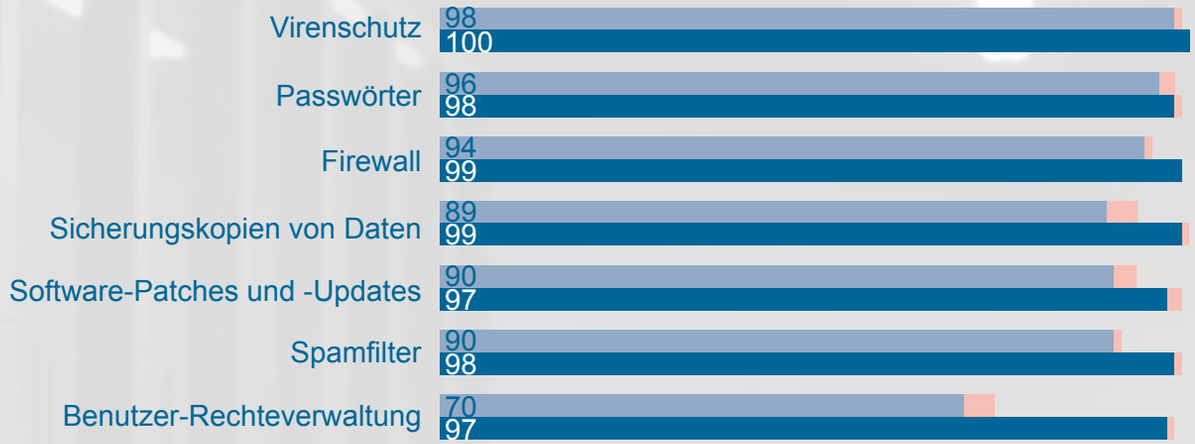
Technische Basismaßnahmen wie ein Virenschutz, die Nutzung von Passwörtern und der Einsatz von Firewalls sind sowohl in kleinen als auch in größeren KMU nahezu flächendeckend verbreitet. Kleine KMU haben noch Nachholbedarf bei der Erstellung von Sicherungskopien, Software-Patches und Updates, beim Einsatz von Spamfiltern oder der Benutzer-Rechteverwaltung.

Die Nutzung von Verschlüsselungsmaßnahmen hat in den letzten Jahren deutlich zugenommen. Heute verschlüsseln 35% der KMU ihre E-Mails und 11% halten Verschlüsselung für notwendig, haben sie aber noch nicht umgesetzt. Im Vergleich zu 2011/12 ist somit eine deutliche Zunahme zu beobachten. Damals hatten nur 17% der KMU verschlüsselt. Es zeigt sich aber, dass kleine KMU technische Maßnahmen zur Verschlüsselung immer noch deutlich seltener umsetzen als größere KMU.

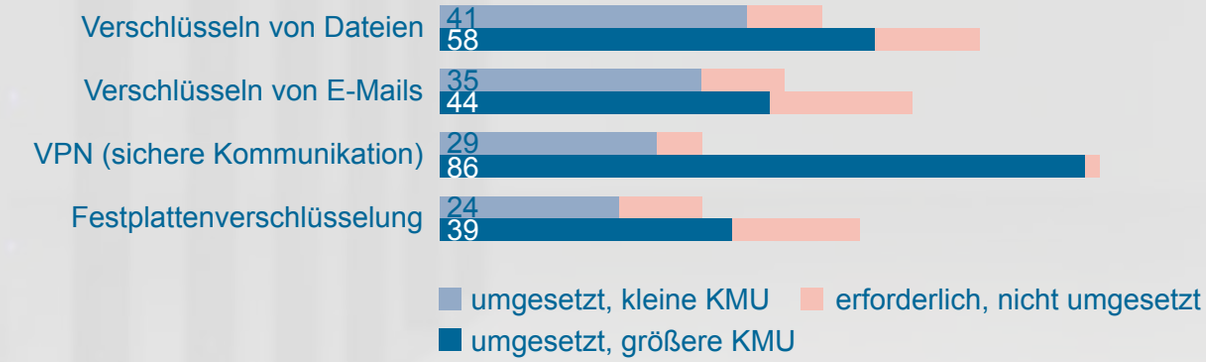
Bei der Nutzung von VPN-Verbindungen, einer Lösung für sicheren Zugriff auf Firmendaten von unterwegs, sind größere KMU den kleineren deutlich voraus. 80 Prozent der größeren KMU haben VPN im Einsatz; bei den kleineren sind es weniger als 30 Prozent.

Basisschutz zumeist vorhanden – aber kleine KMU müssen noch nachbessern

Halten Sie diese Maßnahmen für erforderlich und nutzen Sie sie?



Halten Sie diese technischen Maßnahmen im Bereich Verschlüsselung für erforderlich und nutzen Sie sie?



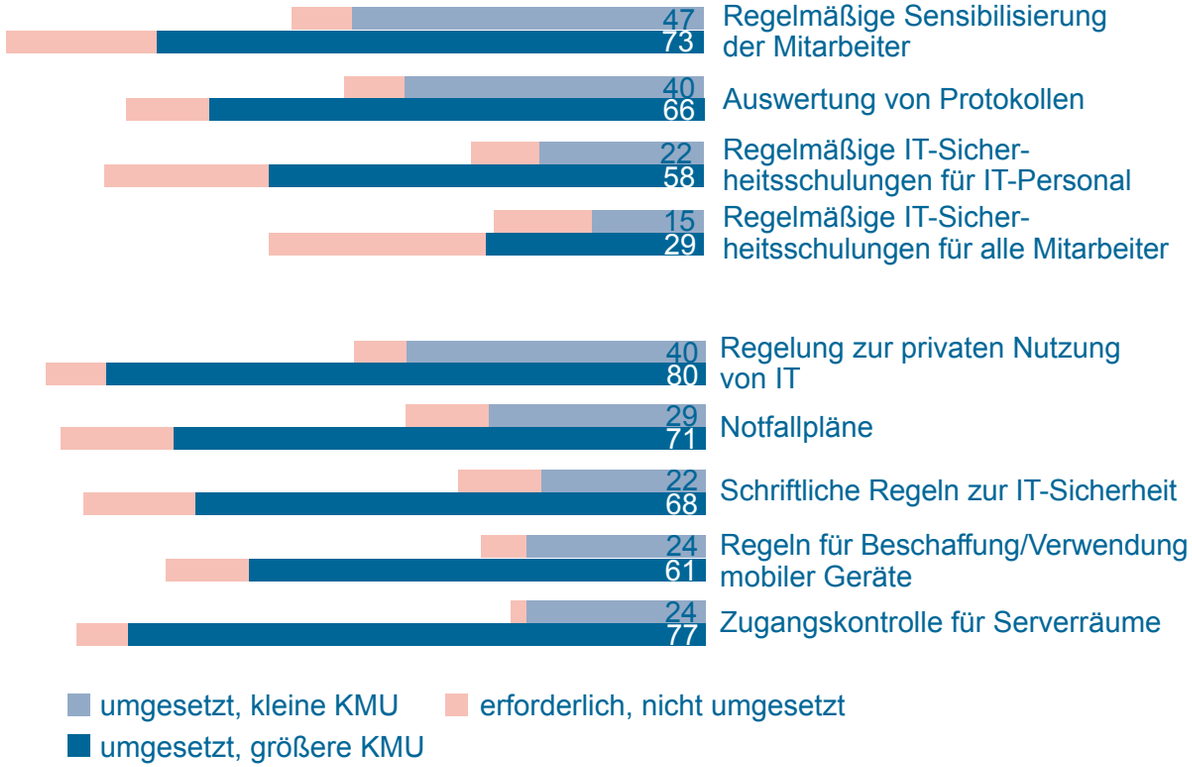
2017: n=1.505; alle Angaben in Prozent

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

Organisatorische Maßnahmen

Mitarbeiter arbeiten zunehmend vernetzt – dies erfordert ein erhöhtes Bewusstsein für IT-Sicherheit

Bitte geben Sie an, welche Maßnahmen Sie für Ihr Unternehmen für erforderlich halten und welche Sie umgesetzt haben.

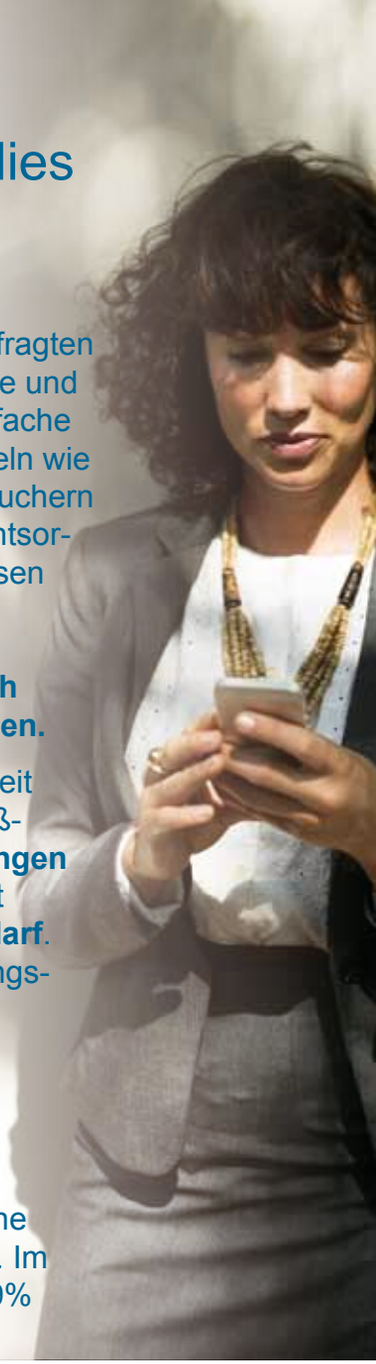


2017: n=1.505; alle Angaben in Prozent

Mitarbeiter werden von den meisten Befragten als Hauptursache für mögliche Probleme und Schadensfälle genannt. Aber schon einfache organisatorische Maßnahmen und Regeln wie die Anmeldung und Begleitung von Besuchern im Firmengebäude oder eine sichere Entsorgung von vertraulichen Druckerzeugnissen sind – so Experteneinschätzungen – unzureichend vorhanden. **KMU setzen organisatorische Maßnahmen deutlich seltener um als technische Maßnahmen.**

Um das Personal im Bereich IT-Sicherheit besser zu rüsten, sind regelmäßige Maßnahmen wie **Sensibilisierung, Schulungen und Kontrollen** unabdingbar. Hier zeigt sich bei **KMU erheblicher Nachholbedarf**. Zwar werden Informations- und Schulungsmaßnahmen für erforderlich gehalten, umgesetzt werden sie jedoch kaum. Sogar spezialisiertes Personal wird zu selten geschult.

Auch bei **Regelungen und Vorgaben** im Bereich IT-Sicherheit zeigt sich: Kleine KMU sind erheblich schlechter gerüstet. Im Ernstfall stehen 71% der kleinen und 29% der größeren KMU ohne Notfallplan da.

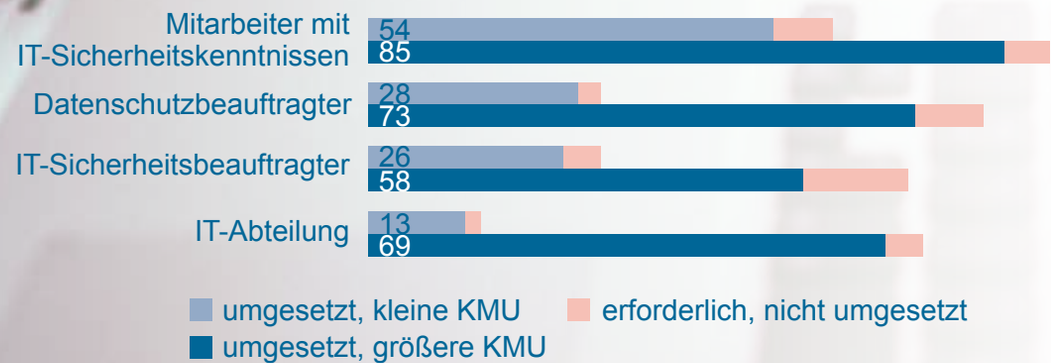


Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

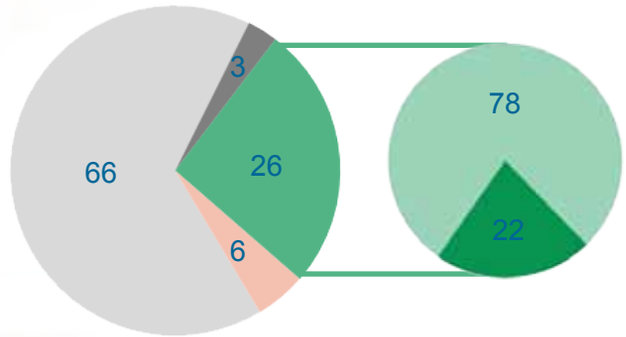
Personelle Maßnahmen

Mitarbeiter mit IT-Sicherheitskenntnissen sind in etwas mehr als der Hälfte aller KMU in Deutschland vorhanden. Dabei haben größere KMU die Nase vorn, bei ihnen sind in 85% der Unternehmen Mitarbeiter mit IT-Sicherheits-kenntnissen beschäftigt. Die spärliche Ausstattung mit IT-Fachpersonal ist auch auf die hohen Kosten für spezialisiertes Personal zurückzuführen. Experten zufolge schätzen KMU die Kosten für einen IT-Sicherheitsspezialisten erheblich höher als die jährlich (vermutlich) durch IT-Sicherheitslücken entstehenden Schäden ein.

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



IT-Sicherheitsbeauftragte in kleinen KMU



Zwei Drittel der kleinen KMU halten einen IT-Sicher-heitsbeauftragten für nicht erforderlich. Häufig werden in kleinen KMU Aufgaben wie IT, IT-Sicherheit, Datenschutz und betriebliche Organisationsaufgaben in Teilzeit, zusammen mit anderen Aufgaben, wahrgenommen.

2017: n=1.505; alle Angaben in Prozent

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

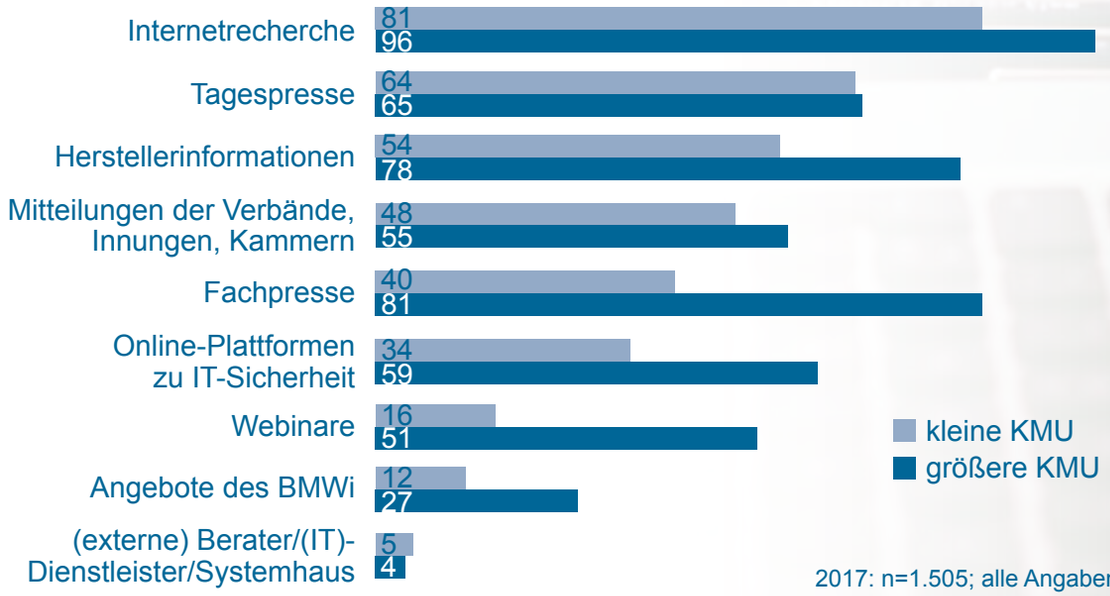
Informationen und Schulungen: Weiterbildung in KMU

Die Informationsrecherche ist im digitalen Zeitalter angekommen

Informationen werden zumeist „im Vorbeigehen“ über Massenmedien oder Internet-Recherche aufgenommen. Kleine KMU informieren sich seltener gezielt zum Thema IT-Sicherheit. Für größere KMU stellen Herstellerinformationen und die Fachpresse mehrheitlich eine wichtige Informationsquelle dar.

Externe Berater spielen eine stark untergeordnete Rolle für die Unternehmen.

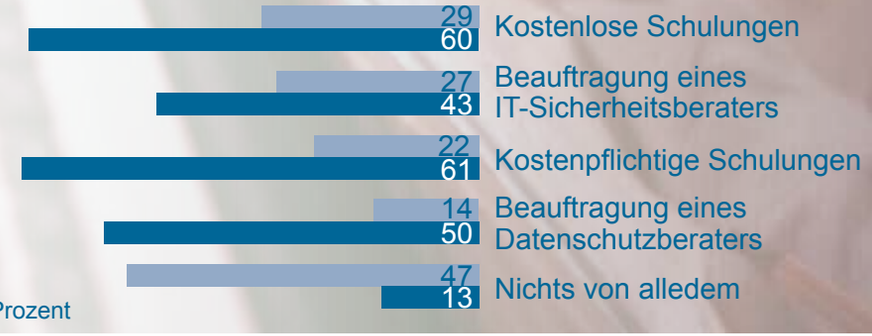
Wir informieren uns zum Thema IT-Sicherheit über ...



Kostenlose Schulungen sind wichtig, um das IT-Sicherheitsbewusstsein zu wecken.
Ob danach spezifische (kostenpflichtige) Schulungen wahrgenommen werden, ist stark abhängig von der Unternehmensgröße, so die Experteneinschätzungen.

Kostenlose Schulungen werden von kleinen KMU am ehesten genutzt. Die kostenlosen Angebote dienen laut Experten häufig als Einstieg in das Thema IT-Sicherheit. Spezielle Fragen werden dann in Beratungsgeprächen behandelt. Ist die Awareness erst einmal vorhanden, sind die KMU eher zu Investitionen bereit.

Nutzung von Schulungs-und Beratungsangeboten

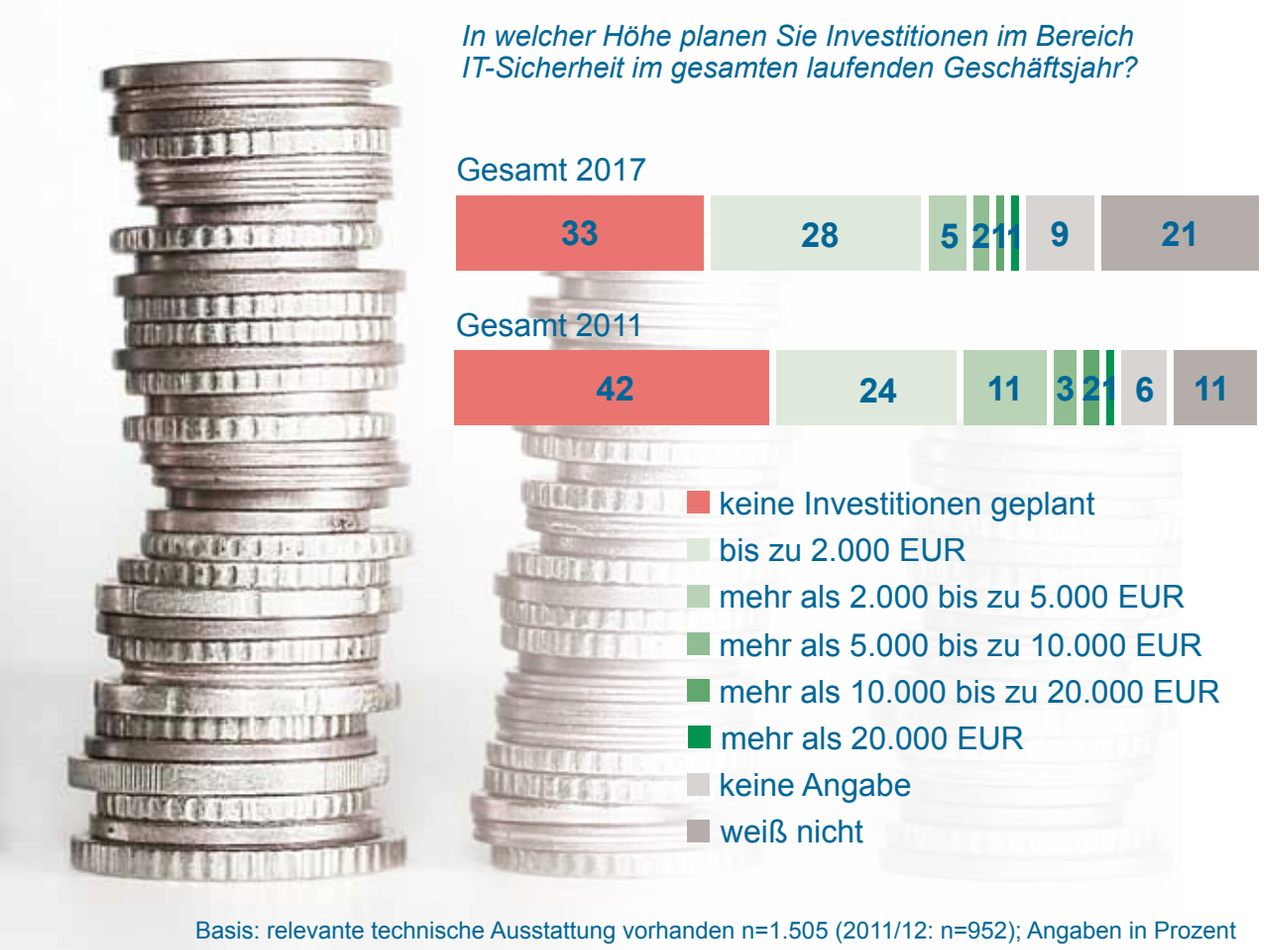


2017: n=1.505; alle Angaben in Prozent

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

Investitionen in IT-Sicherheit

Ein Drittel der KMU hat für das Jahr 2017 keine Investitionen in IT-Sicherheit geplant



In welcher Höhe planen Sie Investitionen im Bereich IT-Sicherheit im gesamten laufenden Geschäftsjahr?

Basis: relevante technische Ausstattung vorhanden n=1.505 (2011/12: n=952); Angaben in Prozent

Die Ergebnisse der Befragung zeigen eine **breite Spanne der für 2017 geplanten Investitionen in IT-Sicherheit**. Sie reicht von unter 100 Euro bis zu mehreren Hunderttausend Euro in der Spitze. Im Durchschnitt investieren KMU heute deutlich mehr und häufiger als zuvor. Kleine Unternehmen investieren häufiger gar nicht in IT-Sicherheit, was angesichts ihres Digitalisierungsgrads mit erheblichen Risiken einhergeht.

Vielen KMU ist laut Experten nicht klar, was ein angemessener Schutz kosten könnte. Hier eignen sich Beispiele anderer Unternehmen, um erste Kosten-Nutzen-Abwägungen anzustellen.

Unternehmen geben zu ihren Investitionen häufig keine genaue Auskunft. Daher sind die Ergebnisse der Befragung in diesem Punkt zurückhaltend zu bewerten. Im gesamten laufenden Geschäftsjahr 2017 waren Investitionen in IT-Sicherheit von durchschnittlich 2.600 Euro pro Unternehmen geplant. In 2011 waren es nur 1.800 Euro.

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

Hemmnisse: Warum werden kaum IT-Sicherheitsmaßnahmen ergriffen?

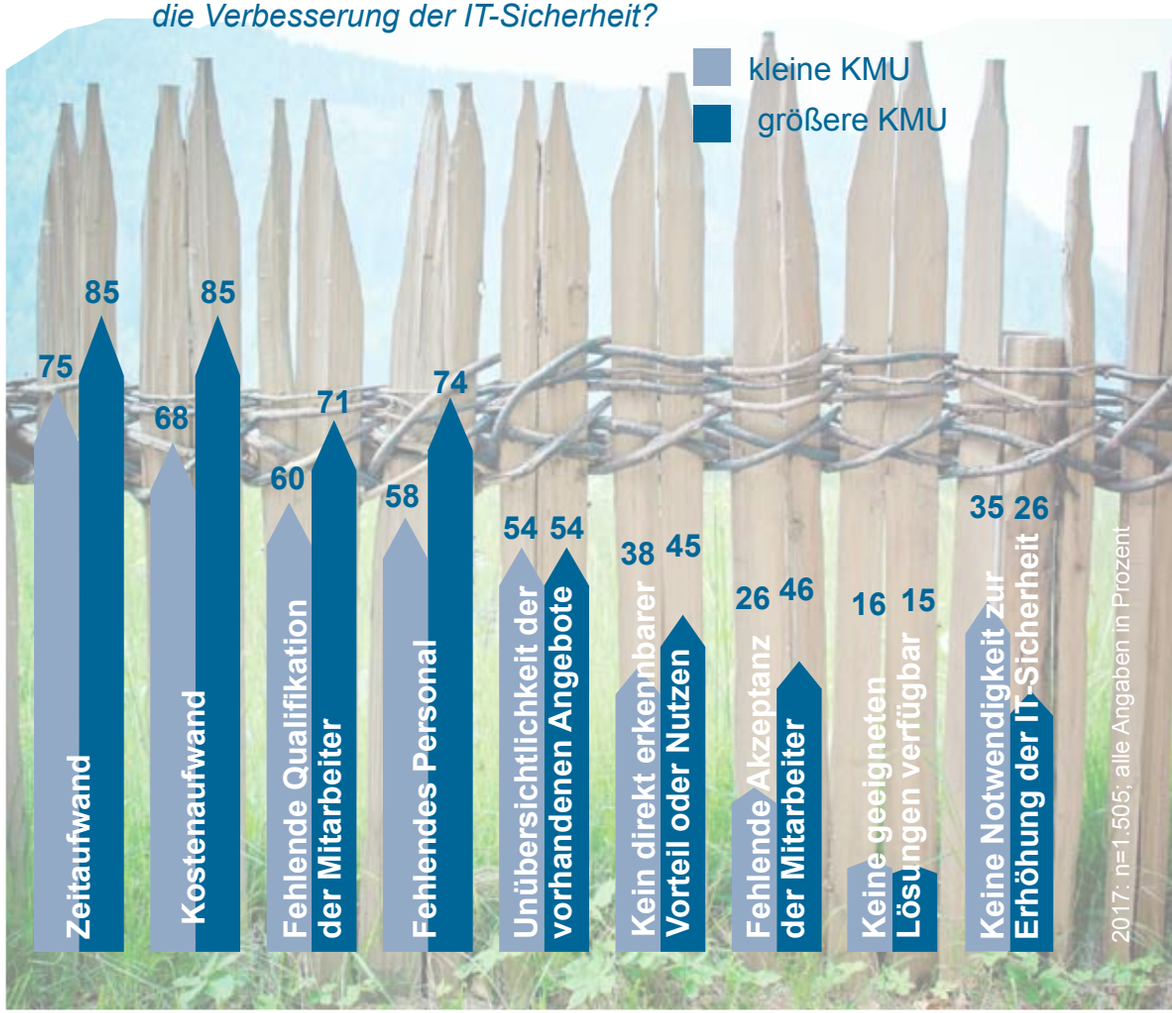
Sowohl für größere als auch kleine KMU ist der Zeitaufwand laut Befragung ein Hauptfaktor.

Kostenaufwand, fehlende Qualifikation der Mitarbeiter oder Mangel an einschlägigem Personal nennen mehr als die Hälfte der KMU als Grund für die aktuell unzureichende IT-Sicherheitslage bei KMU in Deutschland. Angebote wie Informationsbroschüren oder kostenlose Schulungen sind zwar vorhanden, oftmals allerdings fehlt die Übersicht, was für das eigene Unternehmen passt und wer diese Angebote, eventuell sogar kostenlos, verbreitet. Unübersichtlichkeit und eine komplexe Technik-Sprache schrecken KMU ab.

Allem voran fehlt es aus Sicht vieler Experten trotz Digitalisierung und Vernetzung in KMU jeder Größe immer noch an Awareness für das Thema IT-Sicherheit im eigenen Unternehmen.

Viele Experten gehen davon aus, dass KMU keine fundierte Kosten-Nutzen-Analyse durchführen und sowohl das Wissen über mögliche Kosten als auch das Wissen über schützenswerte Assets fehlt. Schon eine einfache, durch Berater angeleitete IT-Sicherheitsanalyse mit wenigen gezielten Fragestellungen kann hier Abhilfe schaffen, und dies ohne hohe zeitliche und kostenmäßige Belastung. **Regionale IT-Dienstleister, Kammern und Verbände sowie neutrale Beratungseinrichtungen spielen dabei eine wichtige Rolle.**

Welche Hürden sehen Sie bei KMU insgesamt in Bezug auf die Verbesserung der IT-Sicherheit?



Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Fokus **Handwerk**

Kommunikation ist längst digitalisiert

37% greifen mit Smartphones auf Unternehmensdaten zu.

55% nutzen WhatsApp.

60% tauschen Daten mit Kunden/Lieferanten aus.

…und oft auch die Produktion

Handwerksbetriebe besitzen schützenswerte Daten über Kunden, Lieferanten und Mitarbeiter – ein lohnendes Ziel für Angreifer.

Das Internet der Dinge ist im Handwerk angekommen: Viele Handwerksbetriebe setzen vernetzte Maschinen ein, sichern diese aber nicht ausreichend gegen Angriffe ab.

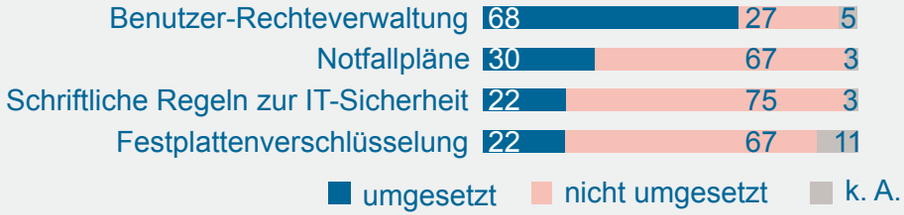
Schwachstellen bei IT-Sicherheit im Handwerk

Umfassende IT-Sicherheitskonzepte fehlen:

79% der Handwerksbetriebe haben keine IT-Sicherheitsanalyse durchgeführt.

60% haben keine Mitarbeiter mit IT-Sicherheitskenntnissen.

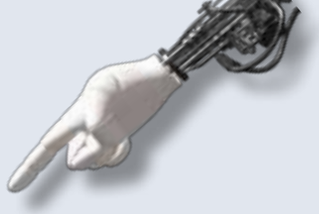
Technische und organisatorische Maßnahmen im Handwerk



Basis: 354 Handwerksunternehmen

Alle Angaben in Prozent

Fokus **Industrie 4.0**



Industrie 4.0-Unternehmen: Erhöhte Digitalisierung erfordert mehr IT-Sicherheit

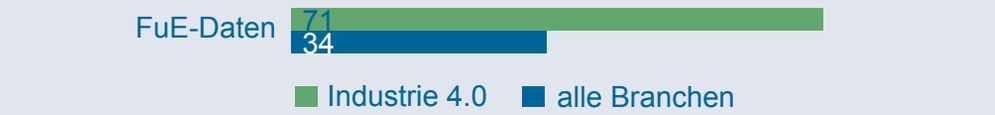
Unternehmen, die im Bereich Industrie 4.0 aktiv sind, sind besser mit IT-Technik ausgestattet als der Durchschnitt der KMU, setzen mehr mobile Endgeräte ein, nutzen häufiger digitale Kanäle und tauschen Daten mit Kunden und Lieferanten auf elektronischem Wege aus. Kurz gesagt: Sie sind **stärker digitalisiert und dadurch angreifbarer.**

Diese KMU scheinen sich jedoch der **gestiegenen Sicherheitsanforderungen bewusst** zu sein. Im Vergleich zum Durchschnitt über alle Branchen schätzen sie die Wichtigkeit des Schutzes der Datenbestände deutlich häufiger als hoch oder sehr hoch ein.

Für diese Unternehmen gelten aufgrund der engen Vernetzung zwischen Partnern in der Wertschöpfungskette, wie z.B. zwischen Zulieferern und Herstellern, gesteigerte Anforderungen an IT-Sicherheit. Im besten Fall üben große Unternehmen Druck zur Umsetzung von IT-Sicherheitsvorkehrungen auf Partner aus. Oftmals beobachtet man allerdings auch in solchen Konstellationen weiterhin eine Umsetzungslücke zwischen erforderlichem und bestehendem Schutzniveau.

Personelle und organisatorische Maßnahmen in KMU der Industrie 4.0

Hohe und sehr hohe Bedeutung des Schutzes von Datenbeständen

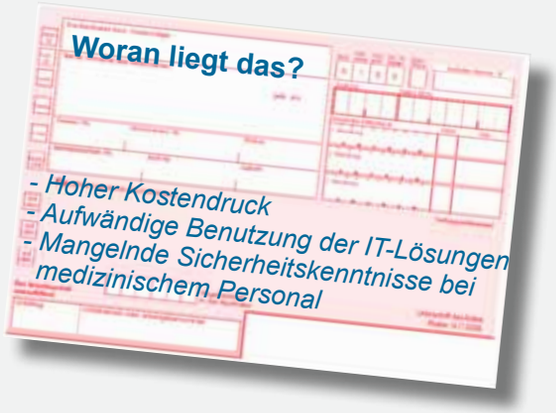


Basis: 77 Unternehmen, die im Bereich Industrie 4.0 aktiv sind

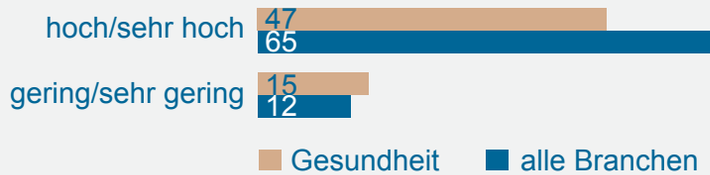
Fokus **Gesundheit**

Der Gegensatz zwischen Anspruch an IT-Sicherheit und Realität in Praxen und Gesundheitsinstitutionen könnte kaum größer sein. Alarmierend gering ist vor allem das Risikobewusstsein der Unternehmen aus dem Bereich Gesundheits- und Sozialwesen. Diese Unternehmen mit hochsensiblen personenbezogenen Daten messen der IT-Sicherheit durchschnittlich eine geringere Bedeutung zu, als das Unternehmen anderer Branchen tun. Auch beim Anteil der Unternehmen, die eine systematische **IT-Sicherheitsanalyse** durchgeführt haben, liegt die Gesundheitsbranche weit zurück: Nur 15% haben ihre IT-Sicherheit systematisch analysiert.

Nicht einmal **1** aus **5** KMU der Gesundheitsbranche hat eine Sicherheitsanalyse durchgeführt.



Die Bedeutung von IT-Sicherheit in unserem Unternehmen ist



Basis: 98 Unternehmen der Gesundheitsbranche

Fokus **E-Commerce**

Aufgrund ihrer digitalen Geschäftsmodelle sind E-Commerce-Unternehmen sehr gut mit IKT ausgestattet. Sie nutzen auch überdurchschnittlich häufig innovative Wearables wie z.B. Datenbrillen und digitale Kanäle. Insbesondere die Nutzung sozialer Netzwerke für Marketing und Vertrieb ist weit verbreitet. Jedes zweite E-Commerce-Unternehmen ist hier aktiv.

Der Großteil der KMU in Deutschland bewertet die Bedeutung von IT-Sicherheit allgemein als hoch oder sehr hoch – handelt aber nicht danach. Für E-Commerce-Unternehmen gilt dies umgekehrt: Sie schätzen die Bedeutung von IT-Sicherheit weniger wichtig ein als der Durchschnitt, setzen aber mehr technische, organisatorische und personelle IT-Sicherheitsmaßnahmen um.

Einsatz technischer, personeller und organisatorischer Maßnahmen bei E-Commerce-Unternehmen

Basis: 428 Unternehmen, die E-Commerce betreiben

Alle Angaben in Prozent

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

IT-Sicherheit in KMU 2011/12 und heute

Digitalisierung bedeutet noch größere Herausforderungen für die IT-Sicherheit

Die Nutzung von IKT in KMU hat seit 2011/12 stetig zugenommen. Deutlich mehr Unternehmen nutzen Outsourcing von IT-Anwendungen und Cloud Computing.

IT-Sicherheit kann heute kein Randthema mehr sein, sondern sollte zum integralen Bestandteil der Unternehmensstrategie werden.

Die Anstrengungen für mehr IT-Sicherheit haben sich 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 Lichtblicke. Personelle und organisatorische Maßnahmen bleiben dagegen weiterhin sogar hinter der eigenen Risikoeinschätzung und dem objektiven Schutzbedarf zurück.

Auffällig ist, dass die Unternehmen, die bereits stark digitalisiert sind, also zum Beispiel Industrie 4.0-Projekte verfolgen oder im E-Commerce aktiv sind, umfassendere IT-Sicherheitsmaßnahmen einsetzen. Für die große Mehrheit der KMU gilt allerdings, dass den gestiegenen Anforderungen an IT-Sicherheit unzureichende Schutzmaßnahmen gegenüberstehen.

Daher ist es unerlässlich, das Thema jetzt erst recht mit Nachdruck anzugehen.

Schritt für Schritt

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.

- Vorhandene Regeln zum Umgang mit IT und Daten schriftlich festhalten und immer wieder in Erinnerung rufen.
- Kostenlose Angebote neutraler, regionaler Anbieter zur Erstinformation nutzen.
- Vorbildfunktion als Führungskraft annehmen: Sicherheitskultur im Unternehmen etablieren.
- Notfallplan für den Ernstfall erarbeiten.
- IT-Sicherheitsanalyse durchführen: Was sind schützenswerte Datenbestände in meinem Unternehmen?

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

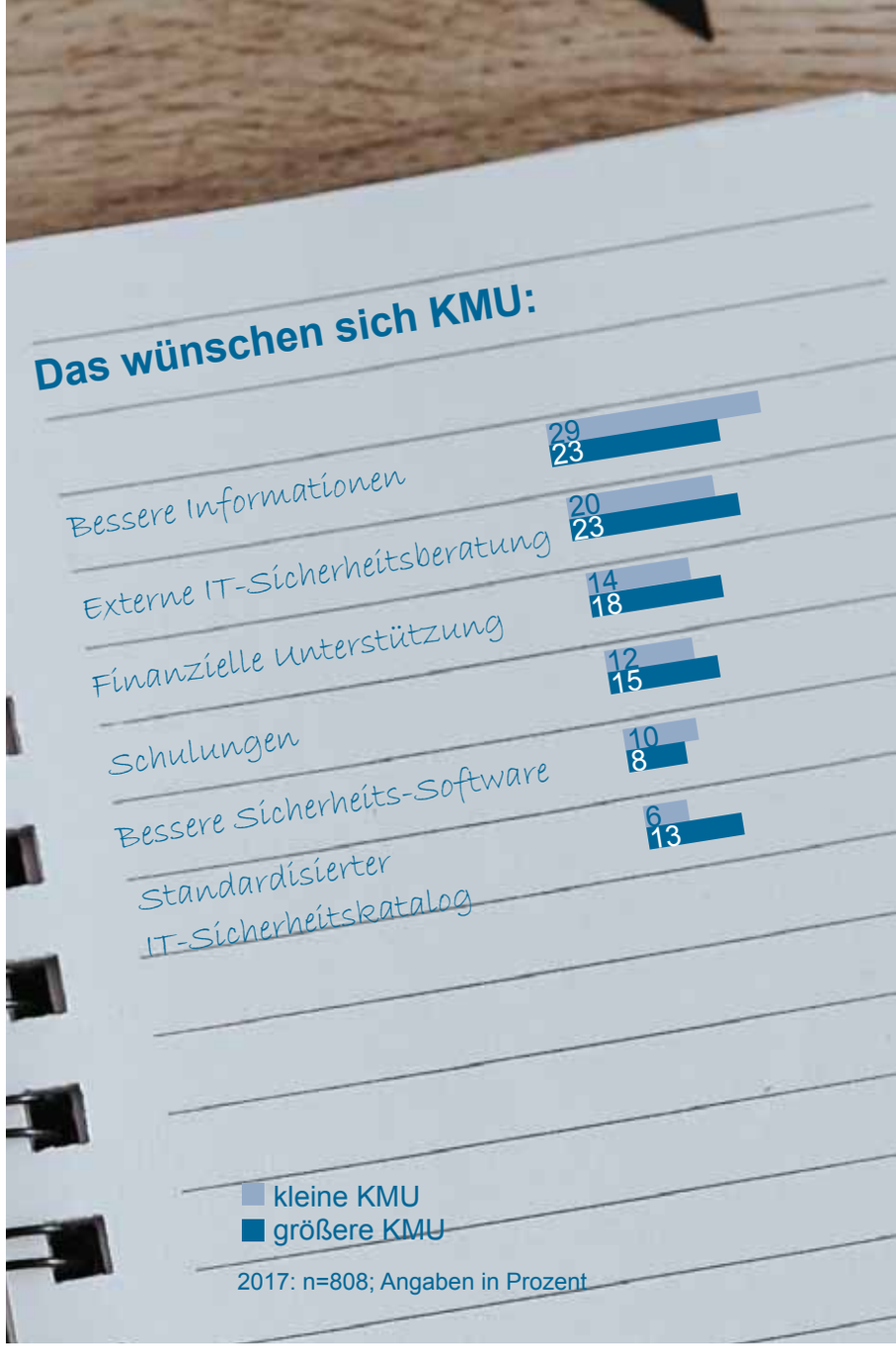
Was kann getan werden, um KMU auf dem Weg zu mehr IT-Sicherheit zu unterstützen?

Was weiterhin wichtig ist:

1. **Bewusstsein wecken:** Awarenesskampagnen initiieren und unterstützen; Themen wie Digitalisierung oder die Datenschutz-Grundverordnung (DSGVO) nutzen, um KMU für IT-Sicherheit zu sensibilisieren
2. **Beispiele zeigen:** Best-Practices und Fallbeispiele verbreiten, die zeigen, wie vergleichbare Unternehmen IT-Sicherheit angehen
3. **Verständlich anleiten:** Didaktische Aufbereitung der Angebote fördern, damit die Inhalte von KMU verstanden werden
4. **Regionale Präsenz stärken:** Neutrale Beratungseinrichtungen bereithalten, denn KMU bevorzugen Angebote vor Ort
5. **Hilfe bei Kosten-Nutzen-Abwägungen:** Informations- und Schulungsangebote als Einstieg und zur ersten IT-Sicherheitsanalyse anbieten
6. **Lotsenfunktion:** KMU beim Finden von neutralen IT-Beratern und IT-Produkten unterstützen
7. **Aufklärung:** Neutral über aktuelle Sicherheitsvorfälle, ihre Einfallstore und mögliche Schäden und Kosten berichten

Heute im Vergleich zu 2011 insbesondere vor dem Hintergrund der Digitalisierung wichtig:

8. **Nachhaltigkeit der Angebote sichern:** KMU im Wandel brauchen immer wieder IT-Sicherheitsinformationen und -schulungen
9. **Schule, Aus- und Weiterbildung stärken** und an die neuen, sich verändernden Herausforderungen der Digitalisierung und IT-Sicherheit anpassen
10. **Security by Design:** Von Anfang an nutzerfreundliche Sicherheitsfunktionen mitdenken und in Unternehmensprozesse integrieren



Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Über diese Publikation

Das Bundesministerium für Wirtschaft und Energie (BMWi) fördert im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ Projekte zur Stärkung der IT-Sicherheit, insbesondere in kleinen und mittleren Unternehmen. Das WIK – Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste hat im Rahmen dieser Initiative das vom BMWi geförderte Projekt „Aktuelle Lage der IT-Sicherheit in KMU“ durchgeführt. Die Ergebnisse basieren neben einer umfassenden Literaturauswertung auf der Durchführung einer repräsentativen Befragung (CATI) bei 1.508 KMU in Deutschland und 30 vertieften Experteninterviews. Die Langfassung der Studie ist unter *www.wik.org* abrufbar. Bezugspunkt ist die WIK-Studie „IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie“, September 2012, mit zwei Repräsentativbefragungen 2011 und 2012.

Über die 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.

Über das WIK – Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) in Bad Honnef berät seit mehr als 30 Jahren öffentliche und private Auftraggeber weltweit in den Bereichen Telekommunikation, Internet, Post und Energie. Zu den Schwerpunktthemen gehören Politik, Regulierung, Wettbewerb und Strategie. Weitere Informationen finden Sie unter: *www.wik.org*.

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@wik.org
www.wik.org

Umsatzsteueridentifikations Nr.: DE 123 383 795
Vertretungs- und zeichnungsberechtigte Personen
Geschäftsführerin und Direktorin: Dr. Iris Henseler-Unger
Direktor und Abteilungsleiter
Post und Logistik: Alex Kalevi Dieke
Direktor und Abteilungsleiter
Netze und Kosten: Dr. Thomas Plückebaum
Leiter Verwaltung: Karl-Hubert Strüver

Vorsitzender des Aufsichtsrates: Winfried Ulmen
Handelsregister: Amtsgericht Siegburg, HRB 7225
Steuer Nr.: 222/5751/0722

Dezember 2017

Bildnachweis: S. 1, 16: Unsplash.com–Jason Blackeye; S. 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14: Pixabay.com; S. 15: Kaboompics.com

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

IT-Sicherheit IN DER WIRTSCHAFT

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