Mittelstand-
Digital

Kleine und mittlere Unternehmen mit Sicherheit digitalisieren

Chancen und Herausforderungen bei der Einführung und Zertifizierung von Informationssicherheitsmanagementsystemen (ISMS)

Eine Erhebung der Mittelstand-Digital Begleitforschung

WIK
CONSULT

Impressum

Herausgeber/Redaktion:
Begleitforschung Mittelstand-Digital
WIK-Consult GmbH
Rhöndorfer Straße 68
53604 Bad Honnef
HRB: Amtsgericht Siegburg, 7043
Tel. +49 (0)2224-9225-0, Fax +49 (0)2224-9225-68
E-Mail: mittelstand-digital@wik.org
www.mittelstand-digital.de

Verantwortlich: Martin Lundborg
Text: Pirmin Puhl
Satz und Layout: Karin Wagner

Bildquelle: Titel und Rückseite: NDABCREATIVITY-AdobeStock

August 2022

Autoren

Pirmin Puhl
Begleitforschung Mittelstand-Digital
Economist
E-Mail: p.puhl@wik.org
Tel.: +49 2224 9225-65

Martin Lundborg
Begleitforschung Mittelstand-Digital
Leiter
E-Mail: m.lundborg@wik.org
Tel.: +49 2224 9225-50

Inhalt

Executive Summary 2

1 Informationssicherheit: Notwendiges Übel oder Chance für Unternehmen? 3

2 Informationssicherheitsmanagementsysteme in KMU 4

2.1 ISMS – was ist das? 4

2.2 Wie verbreitet sind ISMS in deutschen KMU? 6

2.3 Was motiviert KMU dazu ein ISMS einzuführen und zu zertifizieren? 9

2.4 Welche Effekte haben die Einführung und Zertifizierung von ISMS in Unternehmen? 12

2.5 Was hemmt KMU bei der Einführung und Zertifizierung von ISMS? 16

3 Handlungsempfehlungen für KMU 18

4 Die Qual der Wahl – Welches ISMS ist das richtige? 20

5 Methodisches Vorgehen 23

Quellenverzeichnis 24

Executive Summary

Die zunehmende Digitalisierung führt auch dazu, dass Unternehmen mit neuen Bedrohungen für ihre IT- bzw. Informationssicherheit konfrontiert werden. Um individuell notwendige Schutzmaßnahmen strategisch ableiten und ergreifen zu können und darauf aufbauend eine passende Strategie zum Schutz des Unternehmens entwickeln zu können, eignen sich Informationssicherheitsmanagementsysteme (ISMS). Diese finden in kleinen und mittleren Unternehmen bisher noch selten Anwendung. Warum das der Fall ist, welche Vorteile Unternehmen von einem ISMS erwarten können und was die aktuellen Herausforderungen bei dieser Thematik sind, zeigt eine Expertenbefragung im Netzwerk Mittelstand-Digital.

Der Nutzen von ISMS für kleine und mittlere Unternehmen wird von der überwiegenden Mehrheit in unserer Expertenbefragung als (sehr) hoch eingeschätzt. Die meisten, der von uns befragten Expertinnen und Experten, sehen darin Mehrwerte bei der Erfüllung von vertraglichen und rechtlichen Anforderungen zur Informationssicherheit. Auch die Sicherung der Geschäftskontinuität sowie ein leichterer Zugang zu Märkten wird von unseren Expertinnen und Experten als Mehrwert durch eine ISMS-Einführung gesehen. Dabei müssen Unternehmen nicht zwingend ein ISMS zertifizieren lassen. Dies ist ein Schritt, der oft erst dann notwendig wird, wenn ein Nachweis über die Einhaltung gefordert ist.

Nach Einschätzung unserer Expertinnen und Experten implementieren KMU in der Regel ISMS nicht aus eigener Motivation. Vielmehr bedarf es meist externer Treiber, wie akute Sicherheitsvorfälle oder Vorgaben von Vertragspartnern bzw. dem Gesetzgeber, damit sie diesbezüglich tätig werden. Die Gründe dafür sind vielfältig. Die Expertenbefragung deutet darauf hin, dass ISMS in kleinen und mittleren Unternehmen noch relativ unbekannt sind. Nur für einzelne ISMS wird überhaupt eine gewisse Bekanntheit eingeschätzt. Als wichtigstes Hemmnis für eine ausbleibende Einführung und auch Zertifizierung werden die notwendigen Kosten genannt, die für externe Beratungen anfallen. Weitere wichtige Gründe, die Implementierungen und Zertifizierungen hemmen, sind nach unserer Befragung der notwendige Zeitaufwand und fehlende personelle Ressourcen in den KMU. Allerdings zeigt sich auch: Wer einmal ein ISMS eingeführt hat, ist nach Expertenmeinung häufig vom Mehrwert überzeugt. Während bei der Implementierung die Unsicherheit über den Mehrwert eines ISMS sowie die fehlende Überzeugung bzw. Motivation der Unternehmensleitung und der Mitarbeitenden noch eine große Rolle spielen, werden diese Vorbehalte von unseren Expertinnen und Experten bei einer Zertifizierung kaum noch gesehen.

Im Netzwerk Mittelstand-Digital und darüber hinaus gibt es mehrere, speziell auf die Anforderungen von kleinen und mittleren Unternehmen angepasste Unterstützungsangebote zur Verbesserung der Informationssicherheit. Diese reichen von einführenden Informationsmaterialien über Online-Angebote mit konkreten Handlungsempfehlungen bis hin zu finanziellen Zuschüssen. Um an den genannten Herausforderungen anzuknüpfen und eine sichere Digitalisierung in KMU zu ermöglichen, werden einige dieser (kostenfreien) Angebote in dieser Publikation vorgestellt.

1 Informationssicherheit: Notwendiges Übel oder Chance für Unternehmen?

Immer mehr Unternehmen profitieren von der Einführung digitaler Lösungen, Prozesse und Produkte. Zugleich entstehen mit einer zusätzlichen Digitalisierung auch neue Gefahren für die betriebliche IT-Sicherheit bzw. genauer gesagt Informationssicherheit.[1] Für die langfristige Wettbewerbsfähigkeit ist es daher zwingend erforderlich, dass sich Verantwortliche in Unternehmen auch mit potenziellen Bedrohungen sowie deren Abwehr auseinandersetzen.

Gerade in vielen kleinen und mittleren Unternehmen (KMU) sind die ergriffenen Maßnahmen unzureichend. Risiken werden zwar erkannt, noch unterbleiben aber allzu oft die notwendigen Maßnahmen.[2] Der anfallende Zeit- und Kostenaufwand sowie fehlendes qualifiziertes Personal werden häufig als Hemmnis aufgeführt. Hinzu kommt die Unübersichtlichkeit der vorhandenen Angebote, die KMU zum Schutz ihrer Sicherheit nutzen können.[3] Eine frühzeitige und intensive Auseinandersetzung mit der eigenen Informationssicherheit eröffnet Unternehmen jedoch die Möglichkeit, nachhaltig von der Digitalisierung profitieren zu können.

Um sich den Gefahren und Risiken bei der Informationsverarbeitung, -speicherung und -lagerung angemessen stellen zu können, ist es wichtig diese überhaupt erst einmal zu kennen. Darauf aufbauend können dann für das eigene Unternehmen individuell notwendige Schutzmaßnahmen abgeleitet sowie eine passende Strategie zum Schutz des Unternehmens entwickelt werden. Für dieses Vorgehen haben sich sogenannte Informationssicherheitsmanagementsysteme (= ISMS für Information Security Management Systeme) bewährt. Die aktuelle Verbreitung von ISMS und den darin genutzten Sicherheitsstandards und -maßnahmen ist noch gering. Dies spiegelt sich auch in der Studienlage wider. Erkenntnisse zu Chancen und Hürden bei der Einführung oder gar Zertifizierung von ISMS in kleinen und mittleren Unternehmen wurden bisher kaum unabhängig untersucht. Damit kommt auch zu kurz, warum Unternehmen sich bislang noch selten mit der Thematik beschäftigen.

Aus diesem Grund haben wir eine Expertenbefragung im Netzwerk Mittelstand-Digital durchgeführt, um mehr über mögliche Beweggründe von KMU zu erfahren, die bei der (ausbleibenden) Einführung und Zertifizierung von ISMS eine Rolle spielen. Die von uns befragten Expertinnen und Experten sind in ihren Institutionen nicht nur Spezialisten im Bereich Informations- und IT-Sicherheit. Sie stehen darüber hinaus durch ihre Arbeit im Netzwerk Mittelstand-Digital auch im direkten Kontakt mit kleinen und mittleren Unternehmen und können so Praxiserfahrungen aus ihrer täglichen Arbeit einfließen lassen.

Die Erkenntnisse aus dieser Erhebung sollen explizit auch Unternehmen anregen sich mit dem Thema zu beschäftigen und bei der (schrittweisen) Einführung eines ISMS unterstützen. Daher stellen wir in dieser Publikation verschiedene kostenfreie und anbieterneutrale Angebote vor, die es KMU ermöglichen, ein angemessenes Schutzniveau für ihre Informationssicherheit zu erreichen.

> *„Wenn Unternehmen den Mehrwert und Nutzen von ISMS verstehen, werden sie Standards implementieren. Die Hürde ist, die Komplexität auf ein verständliches und einfaches Niveau zu heben und den Aufwand gering zu halten."*
>
> Sandra Balz, Transferstelle IT-Sicherheit im Mittelstand (TISiM)

1 Per Definition ist IT-Sicherheit nur ein Bestandteil der Informationssicherheit. Die Begriffe werden allerdings, insbesondere außerhalb der Fachwelt, oft synonym verwendet. Da diese Publikation auch darauf abzielt Handlungsempfehlungen und -anweisungen für Personen außerhalb der Fachwelt zu liefern, ist in dieser Publikation IT-Sicherheit immer auch als Informationssicherheit zu verstehen.
2 Vgl. BSI (2017), S. 5; DsiN (2022), S. 5.
3 Vgl. Hillebrand, A., et al. (2017), S. 75 f.

2 Informationssicherheitsmanagement-systeme in KMU

2.1 ISMS – was ist das?

In vielen Unternehmen wurden Managementsysteme etabliert, um die Unternehmensleitung systematisch zu unterstützen. Mit den zunehmenden Herausforderungen im Bereich der Cyber-Sicherheit liegt es nahe, Managementsysteme auch zur Abwehr von Risiken zu nutzen. In einem **I**nformation **S**ecurity **M**anagement **S**ystem (= ISMS) stellen Unternehmen Richtlinien auf und definieren geeignete Verfahren, um ihre Bemühungen für eine angemessene Informationssicherheit zu strukturieren. Durch die Befolgung allgemein anerkannter Standards werden Unternehmen in die Lage versetzt, systematisch nach Schwachstellen zu suchen, notwendige Schutzmaßnahmen umzusetzen, den Betrieb, die Überwachung, die Aufrechterhaltung und damit die Angemessenheit umgesetzter Schutzmaßnahmen zu überprüfen sowie diese Schutzmaßnahmen fortlaufend zu verbessern. Kurz gesagt, ein ISMS ermöglicht eine individuelle Risikobewertung im Unternehmen sowie daraus abgeleitete individuelle Schutzmaßnahmen.[4] Ziel eines ISMS ist es, eine angemessene und sichere Informationsverarbeitung, -speicherung sowie -lagerung sicherzustellen. Dabei tragen ISMS maßgeblich zur Erfüllung der Schutzziele der Informationssicherheit bei:

- **Vertraulichkeit**: Informationen dürfen nur von befugten Personen mit den entsprechenden Rollen- und Rechtezuweisungen eingesehen, bearbeitet und verwaltet werden.
- **Integrität**: Informationen dürfen nicht unerkannt verändert oder manipuliert werden.
- **Verfügbarkeit**: Auf Informationen, Dienste oder Ressourcen muss jederzeit in zugesicherter Art und Weise zugegriffen werden können.

Mit einer angemessenen Informationssicherheit können Unternehmen sich vor Gefahren schützen und diese abwehren, wirtschaftliche Schäden vermeiden sowie Risiken minimieren. Hierzu zählen nicht nur böswillige Aktionen wie Angriffe auf das Unternehmen durch Hacker, Sabotage oder Spionage, sondern z. B. auch Elementarschäden oder das versehentliche Löschen von Daten durch eigene Mitarbeitende.

Wenn Auftraggeber, Behörden, Versicherer oder der Gesetzgeber aus unterschiedlichen Gründen sicherstellen wollen, dass Sicherheitsanforderungen erfüllt sind, können ISMS als Nachweis dienen. Sobald Unternehmen ein ISMS implementiert haben, können sie sich zertifizieren lassen. Damit erfolgt eine Bestätigung durch unabhängige Dritte, dass die in der Norm oder dem Standard definierten Anforderungen erfüllt sind. Zertifikate dienen damit als Nachweis, dass versprochene Sicherheitsanforderungen tatsächlich auch eingehalten werden. Sie wirken

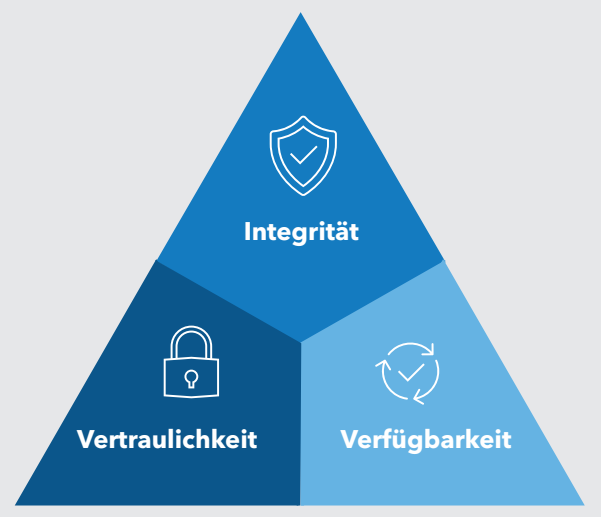


Abbildung 1: Die drei Schutzziele der Informationssicherheit

4 Vgl. ISO27000:2018 Abs. 4.2.

nach Außen somit glaubwürdiger als eine Selbsterklärung des Unternehmens zur Konformität mit den Normen und Standards.

In den vergangenen Jahren wurden verschiedene ISMS mit unterschiedlichen Ansätzen entwickelt. In dieser Erhebung konzentrieren wir uns auf ISMS, die in Deutschland eine branchenübergreifende Verbreitung finden und/oder speziell für kleine und mittlere Unternehmen geeignet sind. Aus diesem Grund werden die folgenden vier ISMS näher untersucht:

- ISO/IEC 27001,
- BSI IT-Grundschutz,
- CISIS12 sowie
- VdS 10000.

Zusätzlich nehmen wir in die Untersuchung mit VdS 10005 auch einen Ansatz auf, der aufgrund der fehlenden Managementebene kein ISMS darstellt, aber Mindestanforderungen an die Informationssicherheit für Unternehmen < 20 Mitarbeitende sowie Handwerksbetriebe definiert.[5]

Erfassen Sie Ihre Ausgangslage: Diese Online-Angebote zur Ermittlung der IT- und Informationssicherheit im Unternehmen geben auch Handlungsempfehlungen

Das kostenfrei nutzbare interaktive Online-Angebot *Sicherheitstool Mittelstand* (SiToM) ermöglicht Unternehmen mit geringem zeitlichem Aufwand ihr vorhandenes Sicherheitsniveau zu ermitteln sowie Risiken und Schwachstellen zu erkennen. Es wurde in Anlehnung an die Empfehlungen zum IT-Grundschutz des Bundesamtes für Informationssicherheit (BSI) erarbeitet. Die Ergebnisse und vorgeschlagenen Maßnahmen werden in Form einer Checkliste zur Verbesserung des Sicherheitsniveaus ausgegeben.

www.sitom.de

Mit dem Sec-O-Mat steht KMU ein kostenfreies Tool zur Verfügung, das es ermöglicht, einfach und schnell den eignen IT-Sicherheitsbedarf zu ermitteln und bedarfsgerechte Umsetzungsempfehlungen zu erhalten. Mittels einer Online-Befragung zu verschiedenen Bereichen eines Unternehmens, in denen IT-Sicherheit eine Rolle spielt, wird ein Aktionsplan mit konkreten Handlungsempfehlungen für die IT-Sicherheit erstellt. Nach Abschluss des Fragebogens führt der *Sec-O-Mat* durch die unterschiedlichen Bereiche des individuellen Aktionsplans und zeigt den Unternehmen, auf welchem Sicherheitsniveau sie mit Aktionen zur Verbesserung ihrer IT-Sicherheit beginnen sollten. So erhalten sie für sie ausgewählte Umsetzungsvorschläge, die ihrem persönlichen Stand im Bereich IT-Sicherheit entsprechen.

www.sec-o-mat.de

Informationssicherheit wird leider – insbesondere bei KMU – noch nicht ganzheitlich gedacht. Wichtige Bestandteile werden oft isoliert und losgelöst voneinander betrachtet. Allerdings stehen diese in der Realität in einem engen Zusammenhang. Das *IT-GRC-Reifegrad-Werkzeug* ermöglicht speziell für KMU einen niederschwelligen und anwendungsfreundlichen Einstieg in die Thematik. Das kostenfreie Online-Tool besteht aus einer Selbsteinschätzungs- und Auswertungskomponente. Ziel der Selbsteinschätzung ist es, den Reifegrad bezüglich des IT-Governance-, Risiko- und Compliance-Managements zu messen und wichtige Handlungsbedarfe zu erkennen. Dabei können alle Unternehmensbereiche in der gleichen Tiefe analysiert werden: Mitarbeiterinnen und Mitarbeiter eines Unternehmens können passend zu ihrer jeweiligen Rolle im Betrieb ihre individuelle Sicht in die Bewertung einfließen lassen – dadurch werden IT-GRC-Kompetenzen noch zielgenauer bewertet.

www.it-grc.th-brandenburg.de

5 Zur einfacheren Formulierung der Fragen in der Expertenbefragung wird auf die Unterscheidung verzichtet und VdS 10005 ebenfalls als ISMS bezeichnet.

2.2 Wie verbreitet sind ISMS in deutschen KMU?

Verschiedene Umfragen zeigen, dass bei weitem noch nicht alle kleinen und mittleren Unternehmen in Deutschland ein ISMS umgesetzt haben. Oft sind es Unternehmen aus spezifischen Branchen, die sich als Vorreiter mit der Thematik auseinandersetzen.

Während eine Umfrage des Bundesamts für Sicherheit in der Informationstechnik (BSI) aus 2018 davon ausgeht, dass 37 % der KMU ein ISMS umgesetzt haben, geht eine erneute Umfrage von 2020 von nur ca. 30 % der KMU aus. Um welche ISMS es sich dabei handelt, bleibt in dieser Erhebung unklar. Es wird aber deutlich: Je kleiner Unternehmen sind, desto seltener setzen sie ein ISMS auch um.[6] Auch in den DsiN-Praxisreporten 2020 und 2021 Mittelstand@IT-Sicherheit wird davon ausgegangen, dass nur eine Minderheit der deutschen KMU Standards zur Risikominimierung nutzt. Nur 20 % der Antwortenden gibt an, dass ihr KMU diese Standards und die zugehörigen, passenden Maßnahmen verwendet.[7] Laut einer repräsentativen Studie von Dreißigacker et al. (2020) zertifizieren nach eigenen Angaben 23 % der KMU mit 10 bis 49 Mitarbeitenden und jedes Dritte KMU mit 50 bis 499 Mitarbeitenden ihre IT-Sicherheit, z.B. nach ISO 27001 oder BSI Grundschutz. Die Werte hängen jedoch stark davon ab welcher Branche die Unternehmen zuzuordnen sind.[8] In einer repräsentativen Umfrage der Bundesdruckerei (2017) gaben 45 % der Unternehmen mit mindestens 20 Mitarbeitenden an, Sicherheitszertifizierungen – etwa nach ISO 27001 oder BSI-Grundschutz-Standard – umgesetzt zu haben und 28 % gaben an, ein ISMS eingeführt zu haben.[9] Laut einer Studie von Bitkom (2018) kommen in 49 % der befragten Industrieunternehmen ab 10 Mitarbeitenden Sicherheits-Zertifizierungen wie z.B. ISO 27001 oder BSI Grundschutz o. ä. zum Einsatz und 35 % haben ein ISMS eingeführt.[10]

Nicht in jeder Untersuchung werden Unterscheidungen zur Unternehmensgröße und Branche getroffen. Die zuvor genannten sowie auch weiterführende Studien und Untersuchungen legen durchweg den Schluss nahe, dass hauptsächlich größere Unternehmen sowie Unternehmen aus bestimmten Branchen ISMS einführen und zertifizieren lassen.[11] Tendenziell lassen kleine Unternehmen ohnehin seltener ihre Managementsysteme zertifizieren.[12] Dies legen auch Untersuchungen des Deutschen Instituts für Normung (DIN) auf Grundlage einer repräsentativen Datenbasis normungsaktiver und -implementierender Unternehmen nahe. Demnach haben im Jahr 2022 von den teilnehmenden Unternehmen nur 18 % die ISO/IEC 27001 implementiert. Unter diesen Unternehmen waren weniger als 10 % der kleinen und mittelgroßen Unternehmen nach ISO/IEC 27001 zertifiziert, allerdings 74 % der sehr großen Unternehmen.[13] Dieser wird seit Jahren in der DIN-Untersuchungsreihe beobachtet.

Offizielle Statistiken weisen dagegen deutlich weniger ISMS-Zertifizierungen aus. Um die Zahl der offiziell gelisteten Zertifizierungen besser einordnen zu können, muss der Unterschied zu den Zahlen in den Umfragen erläutert werden. 2020 gab es laut Internationaler Organisation für Normung (ISO) lediglich 1.281 gültige ISO/IEC 27001 Zertifikate an 3.367 Unternehmensstandorten in Deutschland.[14] 2021 gab das BSI bekannt, dass für den IT-Grundschutz innerhalb eines Jahres 87 Zertifizierungen abgeschlossen wurden, davon 31 ISO 27001 Zertifikate auf Basis von IT-Grundschutz (je hälftig Erst- und Rezertifizierungen nach Standard-Absicherung). Zusätzlich gibt das BSI an, dass 56 Überwachungsaudits durchgeführt wurden.[15] Der IT-Sicherheitscluster e. V. gibt für sein speziell für kleine und mittlere Unternehmen entwickeltes ISMS mit dem Namen CISIS12 (vormals ISIS12) eine Verbreitung von 180 Zertifizierungen und Begutachtungen im Jahr 2021 an.[16] VdS gibt 2022 an, dass 51 Zertifizierungen zu ISMS vorliegen.[17]

6 Vgl. BSI (2019), S. 18; BSI (2020), S. 11 f..
7 Vgl. DsiN (2022), S. 24; DsiN (2021), S. 26.
8 Vgl. Dreißigacker, A. et al. (2020): Cyberangriffe gegen Unternehmen in Deutschland, S. 73 ff..
9 Vgl. Bundesdruckerei (2017), S. 16 f.
10 Vgl. Bitkom (2018), S. 40.
11 Vgl. Dreißigacker, A. et al. (2020), S. 74 f. sowie Mirtsch et al. (2020b), S. 10 f.
12 Vgl. Mirtsch et al. (2020a), S. 15.
13 Vgl. Blind, K. et al. (2022).
14 Vgl. ISO (2020): The ISO Survey, https://www.iso.org/the-iso-survey.html (abgerufen am 13.05.2022).
15 Vgl. BSI (2021), S. 65.
16 Vgl. IT-Sicherheitscluster e. V. (2021): Der nächste Schritte CISIS12 – Informationssicherheits-Managementsystem https://cisis12.de/wp-content/uploads/2021/06/CISIS12-Infoveranstaltung.pdf (abgerufen am 12.07.2022).
17 Vgl. VdS (2022): Zertifikate/Verzeichnis https://vds.de/zertifikate/verzeichnis/V10031 (abgerufen am 13.07.2022).

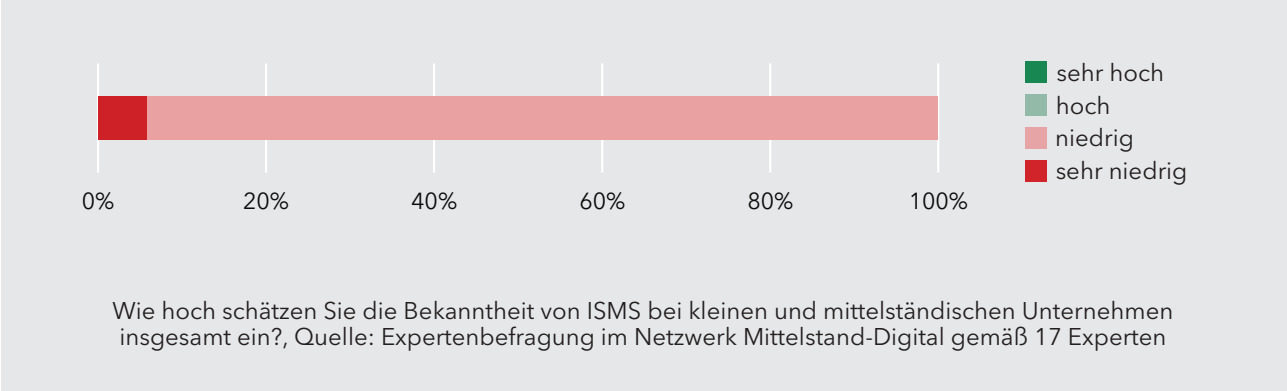


Abbildung 2: Die (fehlende) Bekanntheit von ISMS in kleinen und mittleren Unternehmen

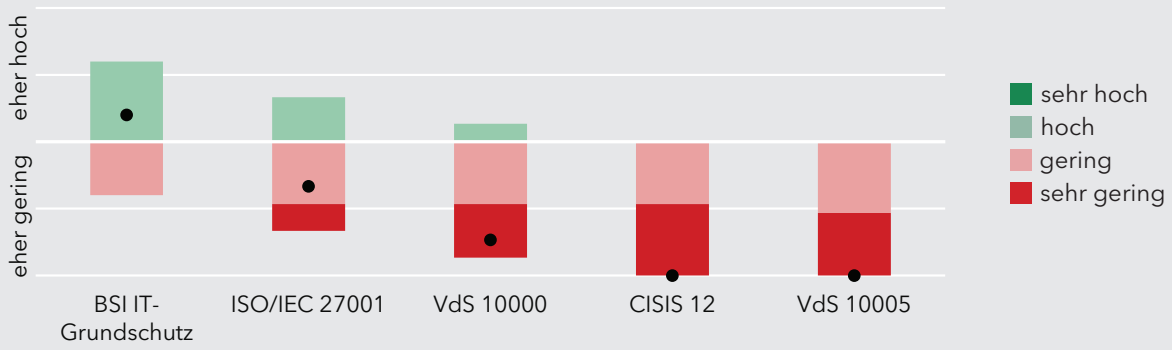
Teilweise kann die Abweichung der offiziell bekannten Zertifizierungen zu den Umfragen damit begründet werden, dass es natürlich noch weitere ISMS gibt als die hier aufgeführten. Bei vielen gibt es so gut wie keine oder nur wenige öffentliche Informationen über deren Anwendung, Zertifizierung und Verbreitung. Diese gelten meist für einzelne Branchen wie z. B. den Energiesektor oder in der Automobilindustrie sowie unter deren Zulieferern. Darüber hinaus werden in den publizierten Listen nur die ISMS-Zertifikate aufgeführt, die durch eine akkreditierte Zertifizierungsstelle ausgestellt wurden. Die Zahl der Unternehmen, die sich tatsächlich z. B. nach ISO/IEC 27001 haben zertifizieren lassen liegt vermutlich höher.[18] Viele Unternehmen wenden die Normen oder Teile davon zudem vermutlich auch an, ohne diese überhaupt zertifizieren zu lassen.[19] In der Vergangenheit haben Erhebungen gezeigt, dass sich nur etwa 1/3 der Unternehmen überhaupt zertifizieren lassen, wenn sie die ISO/IEC 27001 anwenden.[20] Dies lässt die Vermutung zu, dass es sich bei der in vielen Studien angegebenen Einführung oder Zertifizierung von ISMS durch KMU auch um Unternehmen handelt, die nur Bestandteile eines ISMS umgesetzt haben. Darüber hinaus könnte von den Befragten unter „Sicherheitszertifizierungen" auch welche verstanden werden, die nicht unter ISMS fallen.

Worin die Gründe liegen, dass nur wenige Unternehmen ein ISMS oder zumindest Bestandteile davon anwenden (oder wenn sie eines anwenden, warum sie es nicht zertifizieren lassen) bleibt in bisherigen Untersuchungen meist unberücksichtigt. Unserer Expertenbefragung nach könnte einer der Gründe für die fehlende Verbreitung die geringe Bekanntheit von ISMS in kleinen und mittleren Unternehmen sein. Alle befragten Teilnehmenden der Expertenbefragung schätzen die Bekanntheit von ISMS in KMU insgesamt als (sehr) niedrig ein (vgl. Abbildung 2).

Dabei zeigt sich in der Detailbefragung, dass nur für einzelne ISMS überhaupt eine gewisse Bekanntheit eingeschätzt wird (vgl. Abbildung 3). Am besten schneidet der BSI IT-Grundschutz ab. Etwa die Hälfte der von uns befragten Expertinnen und Experten schätzt dessen Bekanntheit unter KMU als hoch ein. An zweiter Stelle des Rankings folgt ISO/IEC 27001, bei dem zwar noch 1/3 der Expertinnen und Experten die Bekanntheit als hoch, aber bereits über die Hälfte

> *„Es gibt auf dem Markt bisher wenige wirklich KMU-gerechte ISMS. Branchenstandards wie VdS 10000 und Projekte wie CISIS12 gehen in die richtige Richtung, haben aber keinen sehr hohen Bekanntheitsgrad."*
>
> Daniel Kant, Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft

18 Auch nicht-akkreditierte Dienstleister dürfen diese Zertifizierung vornehmen. Die Zahlen hierzu werden nicht erfasst.
19 Vgl. Mirtsch et al. (2020b), S. 5.
20 Vgl. Mirtsch et al. (2020a), S. 15.



Wie hoch schätzen Sie die Bekanntheit folgender ISMS bei kleinen und mittelständischen Unternehmen ein?, Quelle: Expertenbefragung im Netzwerk Mittelstand-Digital, N = 15

Abbildung 3: Die (fehlende) Bekanntheit von BSI IT-Grundschutz, ISO/IEC 270001, VdS 10000, CISIS 12 und VdS 10005 in kleinen und mittleren Unternehmen im Detail

die Bekanntheit als (sehr) gering einschätzt. Für die anderen ISMS (CISIS 12, VdS 10000) und VdS 10005 wird von fast allen eine (sehr) geringe Bekanntheit angenommen.

Zusätzlich zu den von uns vorgegeben, haben wir nach weiteren ISMS gefragt, für die unsere Expertinnen und Experten eine (sehr) hohe Bekanntheit unter kleinen und mittleren Unternehmen vermuten. Von zwei Befragten wurde dabei TISAX genannt. Der vom Verband der Automobilindustrie (VDA) initiierte Standard soll dabei helfen ein einheitliches Informationssicherheitsniveau zwischen allen Beteiligten in dieser Branche zu gewährleisten. Dadurch müssen u. a. Zulieferer aber auch sehr kleine Unternehmen, wie z. B. Ingenieurbüros und Designer, auf externen Druck durch ihre Auftraggeber in der kommenden Zeit eine TISAX-Zertifizierung vorweisen. Dass die Verbreitung, Anwendung und Zertifizierung von ISMS auch in größerem Maße funktionieren kann, zeigt dieser spezifisch für die Automobilbranche entwickelte Standard. Für dieses ISMS, das aus der Norm ISO/IEC 27001 abgeleitet wurde, haben sich seit der Einführung 2017 mehr als 2.800 Unternehmen registriert, wobei 2.600 Prüfungen durchgeführt wurden.[21]

Verschaffen Sie sich einen Überblick: Ein Leitfaden zur Implementierung von ISMS zeigt verschiedene Möglichkeiten für KMU auf

Mit dem Leitfaden zum Informationssicherheitsmanagement wird KMU ein Einblick in das Thema ermöglicht und aufgezeigt, welche Absicherungswege im Einzelfall sinnvoll sind. Es werden unterschiedliche ISMS im Detail vorgestellt, um KMU dabei zu helfen, das passende Vorgehensmodell zu finden. Darüber hinaus wird darüber informiert, wie sie mit der Einführung eines ISMS in Ihrem Unternehmen beginnen können und was sie dabei sowie im weiteren Verlauf für Aufgaben erwarten.

https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/it-sicherheit-leitfaden-Informationssicherheitsmanagememt.html

21 Vgl. Verband der Automobilindustrie (2020), S. 162.

2.3 Was motiviert KMU dazu ein ISMS einzuführen und zu zertifizieren?

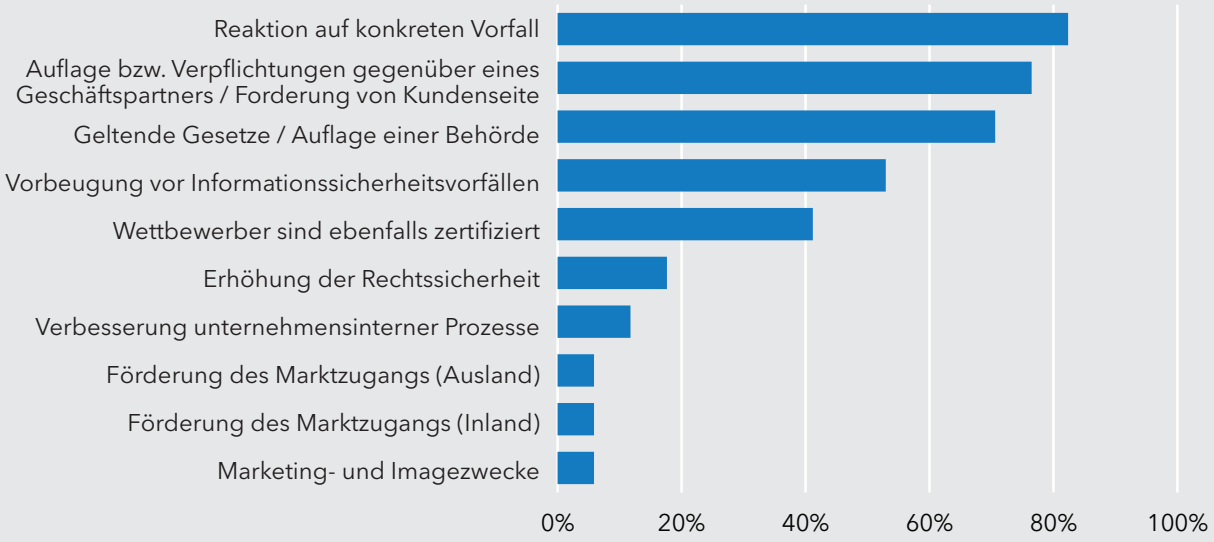
Um die Verbreitung – oder vielmehr die fehlende Verbreitung – von ISMS besser einordnen zu können, ist eine Untersuchung zur Motivationslage der Unternehmen sinnvoll. Bislang gibt es keine repräsentativen Studien, die Anreize für KMU ein ISMS zu implementieren untersuchen, wenn sie das bisher noch nicht getan haben. Wir haben diese Frage daher in unserer Expertenrunde gestellt (vgl. Abbildung 4).

Die meisten Befragten kommen zur Einschätzung, dass die Reaktion auf einen konkreten Vorfall sowie vertragliche und gesetzliche Verpflichtungen dazu führen, dass kleine und mittlere Unternehmen ein ISMS einführen. Mit etwas Abstand folgen die Vorbeugung von Vorfällen sowie die Tatsache, dass Wettbewerber ebenfalls zertifiziert sind. Deutlich seltener genannt werden die Erhöhung der Rechtssicherheit, die Verbesserung unternehmensinterner Prozesse, die Förderung des Marktzugangs im In- und Ausland sowie Marketing und Imagegründe.

Nach Einschätzung unserer Expertinnen und Experten beginnen KMU demnach in der Regel nicht von sich aus ein ISMS zu implementieren. Vielmehr bedarf es bisher wohl externer Treiber, wie einen akuten Sicherheitsvorfall oder der Vorgaben von Vertragspartnern bzw. dem Gesetzgeber, damit sie tätig werden. Vielen scheint daher nicht von sich aus klar zu sein, welche Vorteile ein ISMS haben kann oder ihnen ist nicht bewusst, wie sie sich sinnvoll schützen können.

Nach der Implementierung eines ISMS können sich Unternehmen die Einhaltung der Vorgaben zertifizieren lassen. Eine Zertifizierung ist allerdings nicht zwingend notwendig, um vollumfänglich von den Vorteilen eines ISMS profitieren zu können. Da sich bisherige Untersuchungen zu ISMS auf Unternehmen fokussieren, die sich auch haben zertifizieren lassen, kommen darin Erkenntnisse zum Schritt von der Implementierung zur Zertifizierung oft zu kurz.

Um zu erfahren, ob und inwiefern sich die Gründe für die Implementierung und für die Zertifizierung eines ISMS unterscheiden, haben wir unsere

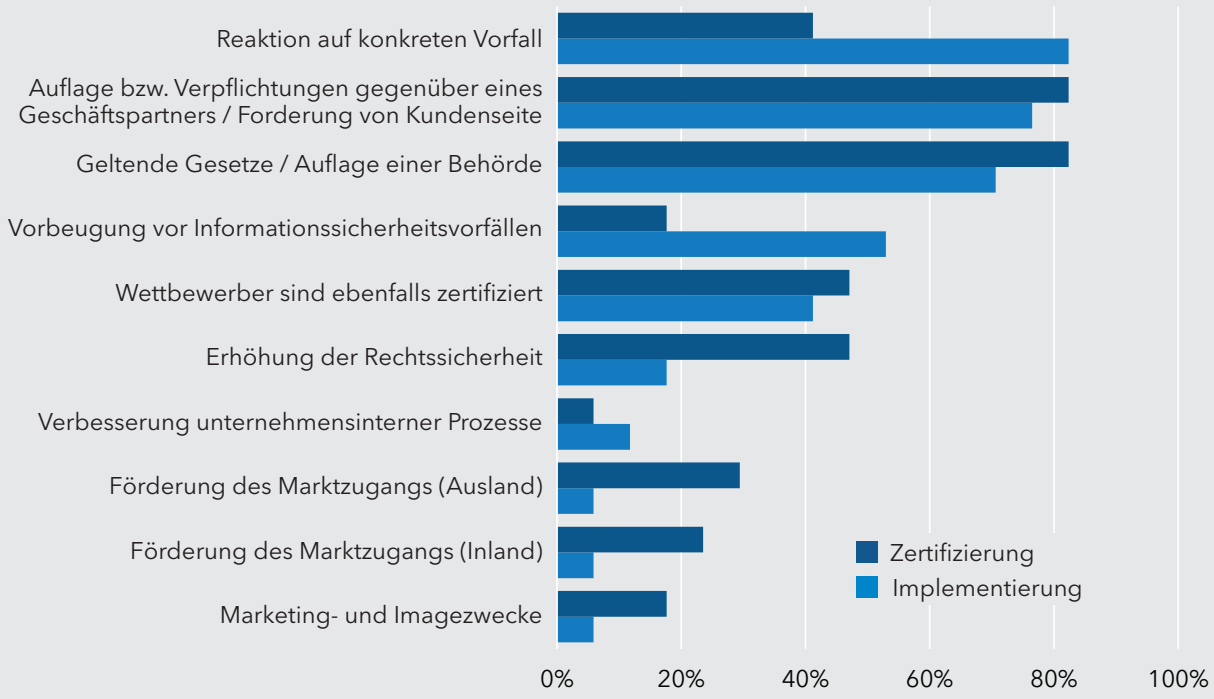


Was sind nach Ihrer Einschätzung die Gründe, die dazu führen, dass kleine und mittelständische Unternehmen ein ISMS einführen? (Mehrfachnennungen sind zulässig),
Quelle: Expertenbefragung im Netzwerk Mittelstand-Digital, N = 17

Abbildung 4: Warum führen KMU ein ISMS ein?

Expertinnen und Experten über die Beweggründe für beide Schritte befragt. Die Antworten zu diesen Fragen haben wir für den besseren Vergleich nebeneinander dargestellt (vgl. Abbildung 5). Es zeigt sich, dass sich die Gründe teilweise deutlich unterscheiden können. Als Reaktion auf konkrete Vorfälle wird aus der Erfahrung unserer Expertinnen und Experten primär die Implementierung eines ISMS angegangen, dies jedoch nicht zwingend verbunden mit dem Ziel einer anschließenden Zertifizierung. Eine Zertifizierung wird stattdessen vor allem angestrebt, um die Erfüllung von Auflagen und Forderungen von Geschäftspartnern, Kunden und Behörden nachweisen zu können. Auch die Vorbeugung von Informationssicherheitsvorfällen ist eher ein Treiber für die Implementierung statt für die Zertifizierung. Das Gegenteil ist bei der Erhöhung der Rechtssicherheit der Fall. Dies ist nach Ansicht unserer Expertinnen und Experten ein deutlich stärkerer Grund sich die Einhaltung eines ISMS zertifizieren zu lassen. Eine positive Außendarstellung gelingt ebenfalls eher mit einer Zertifizierung. Sowohl die Förderung des Marktzugangs im In- und Ausland als auch Marketing- und Imagezwecke können Treiber für eine Zertifizierung sein.

Für die Zukunft ist es zu erwarten, dass die Bedeutung von ISMS für alle Unternehmen – auch für KMU – steigen wird. Mit der zunehmenden Digitalisierung von Prozessketten in der Wirtschaft wachsen die Anforderungen an die Informationssicherheit in Zuliefer- und Partnerunternehmen. Angriffe auf einzelne, schwache Glieder in der Lieferkette können auch fatale Folgen für alle anderen beteiligten Unternehmen haben. (Groß-)Unternehmen und Akteure in Wertschöpfungsnetzwerken achten bei Zusammen- und Zuarbeiten daher bereits jetzt vermehrt auf die nachweisbare Einhaltung von gewissen Sicherheitsanforderungen, wie z. B.



Was sind nach Ihrer Einschätzung die Gründe, die dazu führen, dass kleine und mittelständische Unternehmen ein ISMS einführen?, Was sind nach Ihrer Einschätzung die Gründe, die dazu führen, dass kleine und mittelständische Unternehmen ein ISMS zertifizieren? (Mehrfachnennungen sind zulässig), Quelle: Expertenbefragung im Netzwerk Mittelstand-Digital, N = 17

Abbildung 5: Gründe, die dazu führen, dass kleine und mittlere Unternehmen ein ISMS einführen und zertifizieren lassen

Kann Zertifikaten vertraut werden? Für den Erhalt einer Zertifizierung müssen Unternehmen sich der Prüfung einer Prüfinstitutionen unterziehen. Diese können ihre Unabhängigkeit durch eine Akkreditierung bei der Deutschen Akkreditierungsstelle (DAkkS) nachweisen. Anerkannte und unabhängige Institutionen vergeben Zertifikate nur an die Unternehmen, die von ihnen geprüft wurden und die die Einhaltung von Prüfbestimmungen zu einheitlich festgelegten Kriterien erfüllen. Die Kriterien werden aus (inter-)nationalen Normen oder Standards, wie z. B. der ISO 27001, abgeleitet, die dem ISMS zugrundliegen. Ein Zertifikat bestätigt somit stichprobenartig, dass zum Prüfungszeitpunkt Konformität zu den Prüfkriterien der festgelegten Anforderungen besteht. Eine Zertifizierung zeigt den Kunden, Geschäftspartnern und Aufsichtsbehörden somit unabhängig, dass das Unternehmen (gesetzliche) Vorgaben und (vertragliche) Vereinbarungen erfüllt.

ISMS, um sich selbst als auch ihre Produktionsprozesse nicht zu gefährden.[22]

Ein Vorreiter ist die Einführung von TISAX durch die Automobilindustrie. Die Versicherungswirtschaft könnte angesichts der zunehmenden Bedrohung durch Cyber-Kriminalität und potenzielle Schäden zu einem weiteren Treiber werden, indem ein bestimmtes Sicherheitsniveau zur Voraussetzung für den Abschluss einer Cyber-Versicherung wird.

Auch vom Gesetzgeber wird zunehmend ein angemessenes Schutzniveau gefordert. Erste derartige Anforderungen und gesetzliche Regelungen finden sich beispielsweise im IT-Sicherheitsgesetz (IT-SiG) und der Datenschutz-Grundverordnung (DSGVO). Zum Teil werden auch Nachweise eines bestimmten ISMS z. B. bei öffentlichen Ausschreibungen, gefordert. Dies gilt unter anderem für Einrichtungen in kritischen Infrastrukturen (KRITIS), die durch das IT-Sicherheitsgesetz zu einem zertifizierten ISMS verpflichtet sind. Unternehmen, die unter dieses Gesetz fallen, geben diese Anforderungen auch an ihre Dienstleister weiter. Ohne Zertifikat besteht somit teilweise keine Möglichkeit diese Aufträge zu bekommen. Eine Zertifizierung kann zudem in Gerichtsverhandlungen zu Verstößen gegen die verkehrsüblichen Sorgfaltspflichten als Nachweis ihrer Einhaltung dienen. Sie können somit vor möglichen Bußgeldern schützen.

Viele Unternehmen werden daher vermutlich gar nicht darum herumkommen, sich in Zukunft stärker mit dieser Thematik zu beschäftigen.

Schreiben Sie Ihre eigene Erfolgsgeschichte – Teil 1: Lesen Sie, wie andere KMU ein ISMS schrittweise eingeführt haben

Für die Auswahl eines ISMS führte die Plättner Elektronik GmbH zusammen mit dem Mittelstand 4.0-Kompetenzzentrum Chemnitz eine Analyse des vorhanden IT-Sicherheitsniveaus mit Hilfe des oben vorgestellten Tools „SiToM“ durch. Um das ISMS in das bereits bestehende Managementsystem integrieren zu können, wurde die Umsetzung eines ISMS in Anlehnung an die ISO/IEC 27001 gewählt. Dafür wurde zunächst das IT-Sicherheitsniveau bewertet sowie die bestehenden Managementsysteme bezüglich ihrer Sicherheit gesichtet. Auf dieser Basis wurde eine Übersicht aller notwendigen Inhalte für den Aufbau eines ISMS erarbeitet und in einem Konzept für die Struktur innerhalb eines integrierten Managementsystems dargestellt. Darüber hinaus wurden Inhalte für Regelwerke und Richtlinien für das Notfallmanagement erarbeitet. Mit den gemeinsam gelegten Grundlagen konnte das Unternehmen selbstständig mit der Umsetzung der notwendigen Maßnahmen zur Einführung eines ISMS beginnen.

https://betrieb-machen.de/managementsystem-fuer-informationssicherheit/

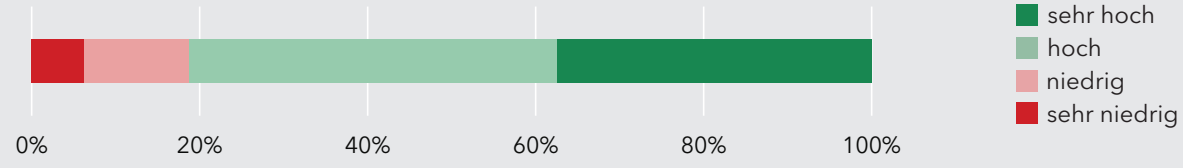
22 Vgl. ENISA (2021), S. 27.

2.4 Welche Effekte haben die Einführung und Zertifizierung von ISMS in Unternehmen?

Nach dem Nutzen von ISMS für kleine und mittlere Unternehmen gefragt, zeigt sich ein eindeutiges Bild bei den von uns befragten Expertinnen und Experten: über ¾ schätzen den Nutzen für KMU als (sehr) hoch ein (vgl. Abbildung 6). Zu diesem Ergebnis passt ebenfalls, dass 2/3 der befragten Expertinnen und Experten auf die aufbauende Frage „Welche Unternehmen sollten sich Ihrer Meinung nach mit ISMS beschäftigen?" betonten, dass dabei die Größenklasse oder Branchenzuordnung keine Rolle spielen sollte, sondern dass dies für alle Unternehmen ein wichtiges Thema ist.

Woher kommt diese Einschätzung der Expertinnen und Experten und welche Mehrwerte werden speziell für KMU durch die Implementierung eines ISMS gesehen? In unserer Befragung haben wir die Effekte einer Implementierung einschätzen lassen, die in der Literatur immer wieder im Zusammenhang mit ISMS genannt werden (vgl. Abbildung 7). Die meisten, der von uns befragten Expertinnen und Experten, sehen einen hohen Mehrwert bei der Erfüllung von Anforderungen, sowohl rechtlicher als auch vertraglicher Natur. Für die Nachweisbarkeit der Informationssicherheit sieht sogar der Großteil einen sehr hohen Mehrwert. Auch die Aufrechterhaltung der Geschäftskontinuität sowie einer Erleichterung von Marktzugängen wird von unseren Expertinnen und Experten mehrheitlich als Mehrwert gesehen, der aus der Einführung eines ISMS entsteht. Für Marketing und Imagezwecke sowie die Verbesserung unternehmensinterner Prozesse hält sich die Einschätzung in etwa die Waage. Etwa gleich viele Expertinnen und Experten sehen durch die Implementierung eines ISMS einen Mehrwert für das Unternehmen als auch keinen. Einzig für die Verbesserung der Wirtschaftlichkeit und Kostenreduzierung sieht die überwiegende Mehrheit der Expertinnen und Experten nur (sehr) geringe Mehrwerte durch die Einführung eines ISMS.

Die Implementierung eines ISMS verspricht demnach viele Vorteile. Für die anwendenden Unternehmen steht an erster Stelle natürlich ein angemessener Return on Invest, wie bei jeder anderen Investition, so auch beim Thema Informationssicherheit. Dem notwendigen Aufwand zur Implementierung, Aufrechterhaltung, stetigen Verbesserung und ggf. Zertifizierung eines ISMS muss ein entsprechender Nutzen gegenüberstehen. Die Herausforderung bei der Identifikation des finanziellen Mehrwerts eines ISMS ist, dass Nutzen und Vorteile von Informationssicherheit oft nicht ohne weiteres (monetär) messbar sind. Sinn und Zweck eines ISMS liegen ja gerade darin, Schäden zu vermeiden. Schäden und Verluste, die gar nicht erst entstehen sind hypothetische Werte. Es fällt besonders schwer diese abzuschätzen oder gar zu monetarisieren. Vor diesem Hintergrund ist der direkte (finanzielle) Mehrwert eines ISMS – neben der Erfüllung von Verträgen und Verpflichtungen – vor allem



Wie hoch schätzen Sie den Nutzen von ISMS bei kleinen und mittelständischen Unternehmen insgesamt ein?, Quelle: Expertenbefragung im Netzwerk Mittelstand-Digital, N = 16

Abbildung 6: Der Nutzen von ISMS für kleine und mittlere Unternehmen

Wie viel schätzen Sie kann die Einführung eines ISMS in kleinen und mittelständischen Unternehmen zu folgenden Punkten beitragen?, Quelle: Expertenbefragung im Netzwerk Mittelstand-Digital, N = 16

Abbildung 7: Worin liegt der Mehrwehrt bei der Einführung eines ISMS?

darin zu sehen, Risiken und negative Folgen aus Informationssicherheitsvorfällen zu vermeiden.[23] Dem Unternehmen werden durch die Implementierung eines ISMS Risiken und mögliche Schäden im Umgang mit Informationen aufgezeigt. Durch individuell auf die Organisation abgestimmte Maßnahmen können mögliche Bedrohungen für die Informationssicherheit früh erkannt und diese vorgebeugt werden. Dies bedeutet u. a. eine Reduktion der Gefahr von Informationssicherheitsvorfällen, weniger IT-Ausfälle, weniger menschliche Fehler, weniger Datenpannen sowie ein höheres Bewusstsein der Mitarbeitenden. Zusammengefasst also ein höheres Niveau an Informationssicherheit sowie die Vermeidung unnötiger Kosten.[24] Zu letzteren zählen nicht nur direkte Kosten durch Cyber-Angriffe, sondern auch indirekte Kosten durch Imageverluste, wenn Vorfälle öffentlich werden.[25]

Welche weiteren Vorteile haben Unternehmen nun konkret von einer Zertifizierung eines ISMS? Wir haben dazu die Expertinnen und Experten im Mittelstand-Digital-Netzwerk nicht nur gefragt, welche Vorteile sie in der Einführung, sondern auch der Zertifizierung eines ISMS für kleine und mittlere Unternehmen sehen (vgl. Abbildung 8). Dabei fällt auf, dass die Mehrwerte für eine zusätzliche

23 Vgl. Hsu, C. et al. (2016).

24 Vgl. Dreißigacker, A. et al. (2020), S. 36 – 39 sowie Mirtsch et al. (2020b), S. 17.

25 Vgl. Dreißigacker, A. et al. (2020), S. 36 – 39 sowie Mirtsch et al. (2020b), S. 19.

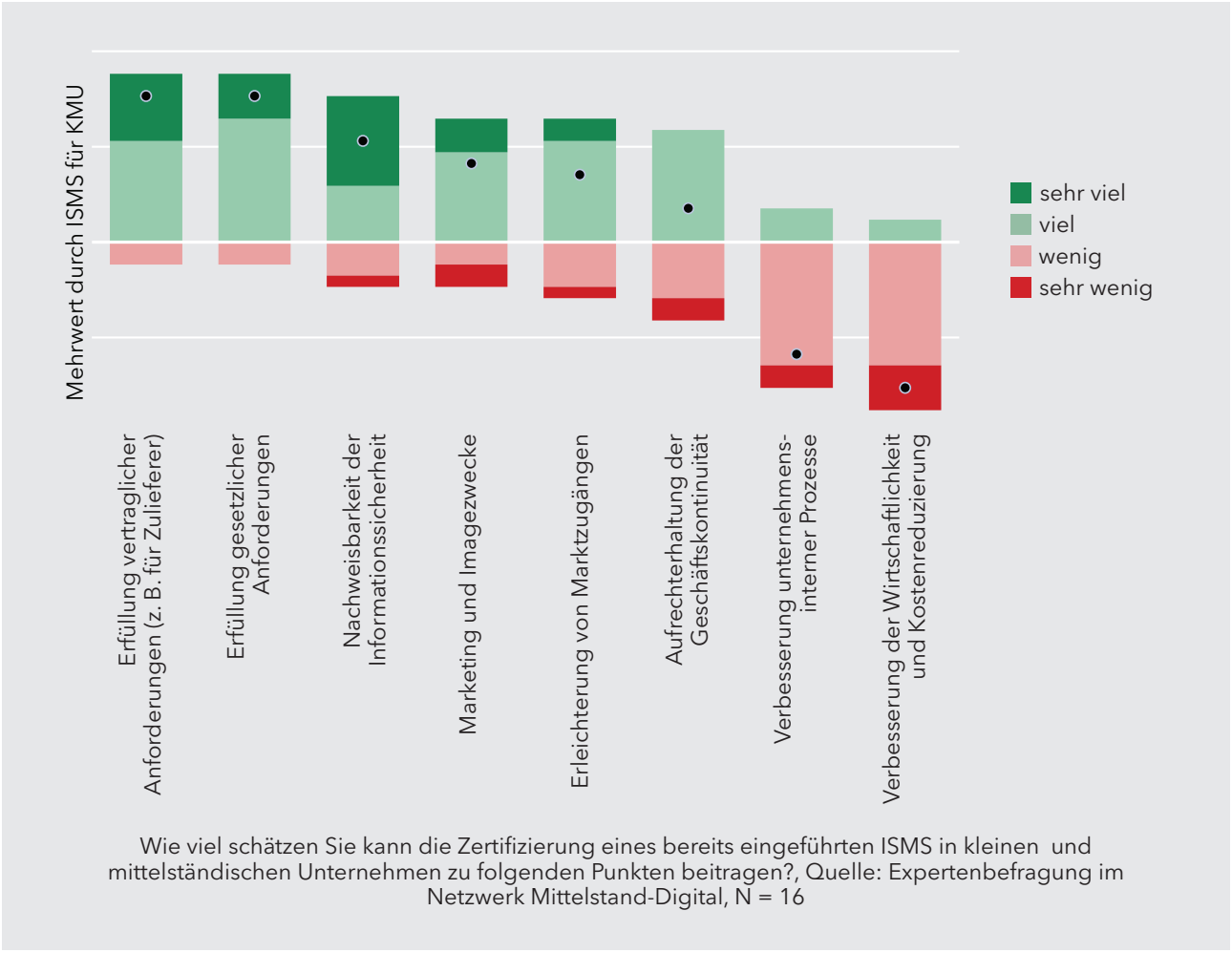


Abbildung 8: Worin liegt der Mehrwert bei der zusätzlichen Zertifizierung eines ISMS?

Zertifizierung in nahezu der gleichen Reihenfolge wie für die ursprüngliche Einführung von ISMS beurteilt werden. Lediglich für Marketing und Imagezwecke wird bei der Zertifizierung ein deutlich höherer und bei der Verbesserung unternehmensinterner Prozesse ein deutlich niedriger Mehrwert gesehen, wodurch diese in der Reihenfolge der Gründe die Plätze tauschen. Auch für die Verbesserung der Wirtschaftlichkeit und Kostenreduktion wird ein geringerer Mehrwert durch eine zusätzliche Zertifizierung gesehen.

Sollten Unternehmen ein ISMS nun also lediglich implementieren oder darüber hinaus auch zertifizieren? Dies muss jedes Unternehmen schlussendlich für sich selbst entscheiden, da sich je nach Kontext unternehmensindividuelle Mehrwerte ergeben.

Mit der unabhängigen Bestätigung, dass die Anforderungen an ein ISMS auch tatsächlich eingehalten werden, können Unternehmen sich besser vermarkten und verbindlich kommunizieren, dass sie die Anforderungen laut Prüfung auch einhalten. Mit der Werbeaussage, dass ein renommiertes Unternehmen die Prüfung durchgeführt hat, kann so bei Kunden und Auftraggebern zusätzliches Vertrauen geschaffen werden. Insbesondere kleine Unternehmen können von Verweisen auf ihre Zertifizierung profitieren.[26] Die positive Außenwirkung oder der damit mögliche Zugang zu gewissen Kundengruppen sollte daher in die Überlegungen zur Zertifizierung eines ISMS mit einbezogen werden.[27]

26 Vgl. Mirtsch et al. (2020b), S. 17.
27 Vgl. Park, C.-S. et al. (2010).

Stellen Sie grundlegende Absicherungen in Ihrem Unternehmen sicher: Ein Leitfaden mit Checklisten zum IT-Sicherheitsmanagement hilft bei den Grundlagen

Insbesondere bei kleinen Unternehmen sind kaum Mitarbeitende mit fachspezifischen IT-Kenntnissen oder gar IT-Spezialisten anzutreffen. Das birgt die Gefahr, dass diese Unternehmen bei der alltäglichen Nutzung der IT-Systeme manche Sicherheitsgefahren nicht oder nur unzureichend erkennen. Die Geschäftsführung steht jedoch in der Verantwortung, sich über die Basissicherheit im Unternehmen zu informieren und auch darüber, welche organisatorischen sowie rechtlichen Anforderungen erfüllt sein müssen.

Die im Leitfaden IT-Sicherheitsmanagement in kleinen und mittleren Unternehmen zusammengestellten Informationen und Handlungsempfehlungen bieten eine Hilfestellung zur Verbesserung eben dieser grundlegenden Sicherheitsanforderungen. Die enthaltenen Checklisten unterstützen bei der Prüfung, ob organisatorische und rechtliche Anforderungen bereits erfüllt werden und inwiefern noch Handlungsbedarfe bestehen. Setzt ein Unternehmen die im Leitfaden aufgeführten Punkte gut um, so profitiert es von verbesserten Abläufen und klaren Regeln für Mitarbeitende. Darüber hinaus wird den Unternehmen ermöglicht, sich agil auf sich verändernde Anforderungen – wie beispielsweise der Forderung eines Auftraggebers, für künftige Zusammenarbeit die IT-Sicherheit zertifizieren zu lassen – einstellen zu können.

https://betrieb-machen.de/nachgelesen_sicherheitsmanagement

Eine Befragung unter ISO/IEC 270001 zertifizierten Unternehmen in Deutschland zeigt, dass sowohl die Implementierung als auch die Zertifizierung als gute Investition in Bezug auf Kosten und Nutzen gesehen wird. In der Bewertung des Nutzens der zusätzlichen Zertifizierung zeigt sich für die Gesamtheit der Unternehmen allerdings kein spürbarer Mehrwert. Lediglich die nur im Inland tätigen Unternehmen sowie die exportierenden Unternehmen sehen einen Mehrwert in der Zertifizierung im Vergleich zur „einfachen" Implementierung.[28]

„Jeder noch so kleine Schritt in Richtung Informationssicherheit ist der richtige. Daher gilt die Devise: einfach machen!"

Alexander Bose, Mittelstand 4.0-Kompetenzzentrum Lingen

28 Vgl. Mirtsch et al. (2020b), S. 19.

Lassen Sie sich ein Sicherheitskonzept erstellen: Mit dem Grundschutz^{PLUS} Aktivator können KMU ein individuelles Informationssicherheits-Konzept entwickeln

Der Grundschutz^{PLUS} Aktivator ist eine kostenfrei nutzbare, interaktive Plattform, die KMU in die Lage versetzt, kompetente IT-sicherheitsrelevante Entscheidungen selbst zu treffen und das Verständnis für Sicherheitsfragestellungen zu stärken. Sie unterstützt produzierende KMU dabei, Hürden bei der Umsetzung von IT-Sicherheitsmaßnahmen abzubauen. Dies führt dazu, dass sie sicherer bei der Planung und Umsetzung digitalisierter Prozesse und Geschäftsmodelle werden. KMU erhalten ein speziell auf ihr Unternehmen zugeschnittenes IT-Sicherheitskonzept und Hilfestellung bei der Umsetzung.

In einem ersten Schritt werden die spezifischen IT-Sicherheitsanforderungen des KMU erfasst. Die interaktive Plattform führt in verständlicher Sprache durch einen dynamischen Dialog bis alle relevanten Informationen erfasst sind und überführt diese in ein vereinfachtes Modell des Unternehmens. Auf Basis existierender Standards (IT-Grundschutz und IEC 62443-Normen) wird ein IT-Sicherheitsmodell entwickelt und hierzu passende Resilienz- und Schutzmaßnahmen identifiziert. Auf dieser Grundlage entwickelt die Grundschutz^{PLUS} Plattform ein auf das Unternehmen zugeschnittenes IT-Sicherheitskonzept. Die Umsetzung wird durch Beispielrealisierungen, Schritt für Schritt Anleitungen und Templates unterstützt. Das daraus resultierende Informationssicherheitskonzept trägt dazu bei, Unternehmen vor Cyberangriffen zu schützen, Datendiebstahl sowie Ausfälle zu verhindern und damit das Sicherheitsniveau produzierender KMU deutlich zu steigern.

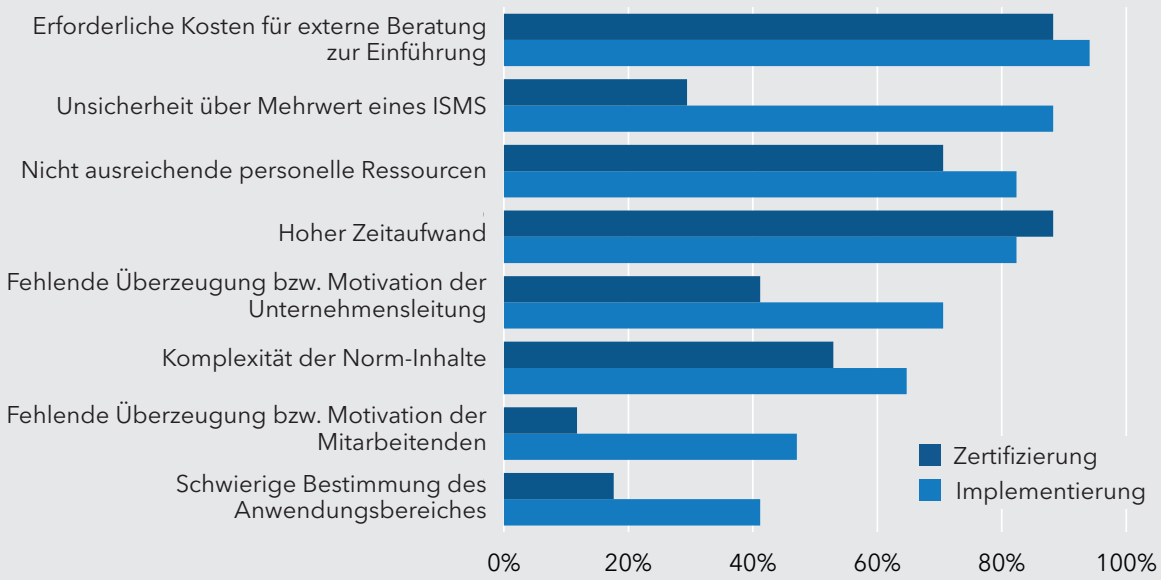
Die Grundschutz^{PLUS} Plattform bietet eine Grundlage für weitere branchenspezifische IT-Sicherheitslösungen. Der Zeitaufwand beträgt ca. 30 Minuten. Die Plattform kann beliebig oft genutzt werden; die Informationen bleiben durch den Cache des Browsers erhalten und können nach einer kostenfreien Registrierung auch auf Dauer genutzt und weiterentwickelt werden.

security4kmu.de

2.5 Was hemmt KMU bei der Einführung und Zertifizierung von ISMS?

Gemessen an den Vorteilen, die ein ISMS verspricht, sollten Unternehmen von sich aus Interesse daran habe sich mit der Thematik zu beschäftigen. Warum sind viele Unternehmen dann aber so zögerlich? Auch hierzu haben wir unsere Expertinnen und Experten befragt. Die Antworten zur Frage nach Hemmnissen bei der Einführung sowie bei der Zertifizierung haben wir für den besseren Vergleich nebeneinandergestellt (vgl. Abbildung 9).

Als wichtigstes Hemmnis für eine fehlende Implementierung und auch Zertifizierung werden die notwendigen Kosten genannt, die für externe Beratungen anfallen, die das Unternehmen dabei unterstützen. Weitere wichtige Gründe, die bei einer Implementierung und Zertifizierung Hemmnisse darstellen, sind nach unserer Befragung der notwendige Zeitaufwand und fehlende personelle Ressourcen in den KMU. Bei allen drei Gründen werden sowohl für die Implementierung als auch die Zertifizierung ähnlich hohe Hürden gesehen. Allerdings zeigt sich bei den weiteren Antworten: Wer einmal ein ISMS implementiert hat, ist nach Expertenmeinung häufig vom Mehrwert überzeugt. Während bei der Implementierung die Unsicherheit über den Mehrwert eines ISMS sowie die fehlende Überzeugung bzw. Motivation der Unternehmensleitung und der Mitarbeitenden noch eine große Rolle spielen, werden diese Vorbehalte von unseren Expertinnen und Experten bei einer Zertifizierung kaum noch gesehen. Bei der Implementierung werden diese also als deutlich größere Hürden empfunden als bei einer späteren Zertifizierung. Das Gleiche gilt auch für die schwierige Bestimmung des Anwendungsbereichs eines ISMS, die sich nach der Implementierung vereinfacht.



Welche Hemmnisse stehen nach Ihrer Einschätzung kleinen und mittelständischen Unternehmen bei der Einführung von ISMS im Weg?, Welche Hemmnisse stehen nach Ihrer Einschätzung kleinen und mittelständischen Unternehmen bei der Zertifizierung von bereits eingeführten ISMS im Weg?, Quelle: Expertenbefragung im Netzwerk Mittelstand-Digital, N = 17

Abbildung 9: Welche Hemmnisse stehen kleinen und mittleren Unternehmen bei der Einführung und Zertifizierung eines ISMS im Weg?

Schreiben Sie Ihre eigene Erfolgsgeschichte – Teil 2: Erfolgsbeispiele zeigen, wie andere KMU eine zertifizierte IT-Sicherheit umgesetzt haben

Durch die negativen Erfahrungen eines benachbarten Betriebes, der Opfer eines Cyber-Angriffs wurde, hat sich die Thormählen GmbH intensiv mit den Themen Datensicherheit und Datenschutz auseinandergesetzt. Um für eine geplante Cyber-Versicherung eine solide Basis zu schaffen, sollte eine zertifizierte Überprüfung der IT-Sicherheit durchgeführt werden. Zusammen mit dem Kompetenzzentrum Digitales Handwerk wurde ein Verfahren ausgewählt, mit dem ein Handwerksbetrieb seine IT-Sicherheit auf den Prüfstand stellen und dies durch ein abschließendes Audit auch zertifizieren lassen kann. Das Projekt aus der Praxis zeigt beispielhaft auf, wie KMU an die Umsetzung in einzelnen Schritten herangehen können – und dass eine Implementierung und Zertifizierung von Sicherheitsstandards auch in KMU funktionieren kann.

https://handwerkdigital.de/cgi-bin/scgi?sid=1&se=1&kd=0&sp=deu&artikellfd=100626&bef=oeffneartikel

3 Handlungsempfehlungen für KMU

Die Expertenbefragung zeigt, dass auch für kleine und mittlere Unternehmen viele Mehrwerte durch die Implementierung und gegebenenfalls auch Zertifizierung eines ISMS gesehen werden. Sie zeigt aber auch, dass KMU dabei vor Herausforderungen stehen, für die sie mitunter Unterstützungsangebote benötigen. Es sind bereits zahlreiche Unterstützungsangebote vorhanden, die auf dem Weg zu einer verbesserten Informationssicherheit dienlich sein können – und damit auch bei der Implementierung eines ISMS. Verantwortliche in KMU sollten sich vor dem Hintergrund der zunehmenden Bedeutung von Informationssicherheit die Zeit nehmen und sich mit der Thematik zu beschäftigen. Nicht nur können sie sich damit selbst vor Gefahren adäquat schützen. Sie bereiten sich damit auch frühzeitig auf mögliche Anforderungen vor, die ihnen von ihren Kunden oder Auftraggebern herangetragen werden. Die kostenfreien Angebote, die in dieser Publikation in den Info-Boxen zu finden sind, können ein Anfang sein sich mit überschaubarem Aufwand dem Thema zu nähern. Sie bieten insbesondere dann eine gute Hilfestellung, wenn sich über den möglichen Mehrwert und den anfallenden Aufwand informiert werden soll. Viele der Angebote gehen sogar einen Schritt weiter. Sie liefern allgemeine und auch konkret auf die Bedarfe der einzelnen KMU abgestimmte Handlungsempfehlungen und -anweisungen, mit denen die Informationssicherheit im Unternehmen – in Anlehnung an ein ISMS – verbessert werden kann.

„Informationssicherheitsmanagementsysteme sind für verschiedene Anwendungsfelder sowie Unternehmenstypen verfügbar und erhöhen nachhaltig das IT-Sicherheitsniveau. KMU sollten nicht vor der Komplexität zurückschrecken, sondern bei Bedarf entsprechende externe Expertinnen und Experten zur Unterstützung hinzuziehen. Die Leistungen autorisierter Beratungsunternehmen sind mitunter förderfähig, z. B. durch go-digital."

Andreas Neuenfels, Mittelstand-Digital Zentrum Chemnitz

Kleine und mittlere Unternehmen, die zur Überzeugung gekommen sind, ein ISMS in ihrem Betrieb zu implementieren, sollten sie sich nicht von möglichen Kosten abschrecken lassen. Eine gut abgestimmte Informationssicherheit zahlt sich aus. Anfallende Investitionen sollten daher vielmehr vor dem Hintergrund gesehen werden, dass dieser wichtige Bestandteil bisher womöglich vernachlässigt wurde. Dabei können KMU auch auf verschiedene finanzielle Fördermöglichkeiten zurückgreifen. Mittlerweile gibt es von verschiedenen Ministerien auf Bundes- sowie Landesebene Fördermöglichkeiten, die Unternehmen bei der Einführung einer guten Informationssicherheit auch finanziell unterstützen.

Lassen Sie sich auf dem Weg zu einem ISMS finanziell unterstützen: Kleine und mittlere Unternehmen der gewerblichen Wirtschaft oder des Handwerks können ohne großen formellen Aufwand von staatlichen Förderungen profitieren

Im Programm *go-digital* können kleine und mittelständische Unternehmen sowie Handwerksbetriebe eine Förderung für alle notwendigen Beratungs- und Umsetzungsmaßnahmen erhalten, um ihre Cyber- und Datensicherheit im Unternehmen zu verbessern. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) hat dazu über 1.000 kompetente Beratungsunternehmen autorisiert, die sie bei der Suche nach individuellen Lösungen unterstützen. Die Beratungsunternehmen übernehmen dabei die Antragstellung für die Fördermittel, die Abrechnung und das Berichtswesen. Gefördert werden dabei:

- Risiko- und Sicherheitsanalysen (Bewertung von Bedrohungen und möglichen Schwachstellen) der bestehenden oder neu geplanten betrieblichen IKT-Infrastruktur
- Maßnahmen zur Initiierung / Optimierung von betrieblichen IT-Sicherheitsmanagementsystemen.

https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/go-digital/go-digital.html

Das Investitionszuschussprogramm *Digital Jetzt* unterstützt mittelständische Unternehmen mit 3 bis 499 Beschäftigten branchenübergreifend bei Investitionen in digitale Technologien und digitale Anwendungen sowie die Qualifizierung ihrer Mitarbeitenden zu Digitalthemen. Abhängig von der Beschäftigtenzahl und dem inhaltlichen Schwerpunkt des Vorhabens kann *Digital Jetzt* einen wesentlichen Anteil der Investitionskosten übernehmen – auch für die Informationssicherheit.

https://www.bmwk.de/Redaktion/DE/Dossier/digital-jetzt.html

4 Die Qual der Wahl – Welches ISMS ist das richtige?

Natürlich gibt es über die in dieser Erhebung aufgeführten hinaus noch zahlreiche weitere ISMS oder Möglichkeiten Sicherheitsmaßnahmen zertifizieren zu lassen. Wir haben uns in dieser Publikation darauf beschränkt das weltweit meist verbreitete ISMS (ISO/IEC 27001), das von der Cyber-Sicherheitsbehörde des Bundes entwickelte ISMS (BSI IT-Grundschutz) zwei speziell für deutsche kleine und mittlere Unternehmen entwickelte ISMS (CISIS12, VdS 10000), VdS 10005 mit Mindestanforderungen an die Informationssicherheit für Unternehmen < 20 Mitarbeitende und Handwerksbetriebe sowie den speziell für Handwerksunternehmen entwickelten E-Check IT aufzunehmen.[29]

Eine Aussage welches ISMS das richtige für ein Unternehmen ist, kann pauschal nicht getroffen werden. Wenn Unternehmen keine Vorgabe haben, welches ISMS sie zu wählen haben, ist eine individuelle Abwägung notwendig. Eine Hilfestellung dabei soll die nachfolgende Tabelle mit weiteren Informationen liefern (vgl. Tabelle 1).[30]

29 "E-Check IT" wurde vom BFE Oldenburg für den ZVEH (Zentralverband der deutschen Elektro- und Informationstechnischen Handwerke) entwickelt und basiert auf den BSI IT-Grundschutz. Neben den erforderlichen Dokumenten und Dokumentation spielt dabei die ca. 60 Seiten umfassende Checkliste eine zentrale Stelle, die mit den einzelnen Bausteinen des IT-Grundschutz vergleichbar ist und nur auf einen Kleinbetrieb abgebildet wird.

30 Angelehnt an BITMi (2021), S. 18 f.; eco (2019); Deutscher Landkreistag (2017), S. 9.

Standard	ISO/IEC 27001	BSI IT-Grundschutz Standard-absicherung	BSI IT-Grundschutz Basis-absicherung	CISIS12	VdS 10000	VdS 10005	E-Check IT
Herausgeber	International Standards Organisation	Bundesamt für Sicherheit in der Informationstechnik		IT-Sicherheitscluster e.V.	VdS Schadenverhütung GmbH	VdS Schadenverhütung GmbH	Zentralverband der Deutschen Elektro- und Informations-technischen Handwerke
Zielgruppe	Organisationen jeder Größenordnung	Organisationen jeder Größenordnung, öffentliche Verwaltung	kleine und mittlere Unternehmen	kleine und mittlere Unternehmen	kleine und mittlere Unternehmen	Klein- und Kleinstunternehmen < 20 Mitarbeitende, Handwerksbetriebe	Handwerksbetriebe (Klein- und Kleinstbetriebe)
Umfang des Standards im Vergleich	ISMS	ISMS		ISMS	ISMS	Mindestanforderungen an die Informationssicherheit	IT-Sicherheitscheck
	groß (ca. 400 Seiten)	sehr groß (ca. 5.000 Seiten)	klein bis mittel (ca. 90 Seiten)	mittel (ca. 170 Seiten)	klein (ca. 40 Seiten)	sehr klein (ca. 15 Seiten)	klein (ca. 60 Seiten)
	Generisch formulierte Maßnahmen	Konkret formulierte Maßnahmen		Konkret formulierte Maßnahmen	Generisch formulierte Maßnahmen	Generisch formulierte Maßnahmen	Konkret formulierte Maßnahmen
Aufwand der Implementation	Externer Aufwand: 30 - 300 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	Externer Aufwand: 30 - 300 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	Verhältnismäßig geringer Aufwand im Vergleich zur Standardabsicherung	Externer Aufwand: 5 - 40 PT Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	Ca. 20 – 30 % des Aufwandes im Vergleich zu ISO/IEC 27001	-	-
	Interner Aufwand: Faktor 1,5 - 2	Interner Aufwand: Faktor 2 - 4	15 – 20 Tage Aufwand für einen erfahrenen Informationssicherheitsbeauftragten	Interner Aufwand: angepasst an KMU und damit geringer im Vergleich zu ISO/IEC 27001 und BSI IT-Grundschutz, aber abhängig vom individuellen Umfang	angepasst an KMU, ca. 20 – 30 % des Aufwandes im Vergleich zu ISO/IEC 27001	-	Aufwand für den Betrieb abhängig vom Ist-Stand der IT-Sicherheit im Unternehmen. Mindestens 14 PT.
Audit	Voraussetzung für die Vergabe eines ISO 27001-Zertifikats ist eine Überprüfung (Zertifizierungsaudit) durch einen unabhängigen Auditor. Der externe Auditor prüft in zwei Stufen, ob die Anforderungen der Norm ISO/IEC 27001 im Managementsystem umgesetzt sind.	Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz (Standardabsicherung) ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Der externe Auditor prüft in zwei Phasen, ob die Anforderungen von ISO/IEC 27001 und BSI IT-Grundschutz umgesetzt sind.	Voraussetzung für die Vergabe eines Testats nach der Basis-Absicherung gemäß IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Der externe Auditor prüft in zwei Phasen, ob die Anforderungen an die Erfüllung der Basis-Anforderungen nach dem Prüfschema für die Erteilung eines Testats nach der Basis-Absicherung gemäß IT-Grundschutz umgesetzt sind.	Voraussetzung für die Vergabe eines CISIS12-Zertifikats ist eine Überprüfung durch einen vom IT-Sicherheitscluster e.V. gelisteten Auditor oder Auditoren der Zertifizierungsstellen. Der externe Auditor prüft in zwei Stufen, ob die Anforderungen von CISIS12 umgesetzt sind.	Voraussetzung für die Vergabe eines VdS 10000-Zertifikats ist die Durchführung des VdS Quick-Checks für Informationssicherheits-Managementsysteme sowie eine Überprüfung durch einen von VdS benannten Auditor. Der Auditor prüft, ob die getroffenen Maßnahmen zur Cyber-Security im Unternehmen umgesetzt sind.	Basierend auf dem Ergebnis des VdS Quick-Checks und eines Auditfragebogens führen Auditoren eine Überprüfung aus der Ferne („Remote Auditierung") durch.	Voraussetzung für die Vergabe eines E-Check IT-Zertifikats ist eine Überprüfung durch einen Auditor.

Standard	ISO/IEC 27001	BSI IT-Grundschutz Standard-absicherung	BSI IT-Grundschutz Basis-absicherung	CISIS12	VdS 10000	VdS 10005	E-Check IT
	Externer Aufwand ist abhängig von Zahl der Mitarbeitenden und weiteren Faktoren (z. B. Komplexität des ISMS, Anzahl der Standorte, …). Für KMU zwischen ~ 5 und 16,5 Tage	ca. 15 bis 30 Tage	-	-	Externer Aufwand ist individuell abhängig vom Ergebnis des Quick-Checks sowie der Größe, Struktur und Tätigkeitsfelder des Unternehmens. Je nach Unternehmensgröße dauert ein Zertifizierungsaudit gemäß VdS 10000 zwischen ein und zwei Tagen.	Externer Aufwand: ½ Tag	Externer Aufwand: 1 Tag
Zertifizierung / Testat	Möglich, nach positivem Abschluss des Audits	Möglich, für die Standard- und Kern-Absicherung, nach positivem Abschluss des Audits	Testat nach positivem Abschluss des Audits möglich. Die Ausstellung der Auditoren-Testate erfolgt nicht durch die Zertifizierungsstelle und liegt allein in der Verantwortung des zertifizierten Auditors.	Möglich, nach positivem Abschluss des Audits	Möglich, nach positivem Abschluss des Audits und dessen Prüfung durch Mitarbeitenden der VdS Zertifizierungsstelle, der/die nicht an der Auditierung teilgenommen hat.	VdS-Testat nach positivem Abschluss des Audits möglich.	Möglich, nach positivem Abschluss des Audits.
	ISO-Zertifizierung durch verschiedene Anbieter; Akkreditierung durch DAkkS von ISO empfohlen	ISO-Zertifizierung auf Basis IT-Grundschutz durch verschiedene Anbieter; Akkreditierung / Zertifizierung des Anbieters durch BSI ist Voraussetzung	Testat durch verschiedene Anbieter; Akkreditierung / Zertifizierung des Anbieters durch BSI ist Voraussetzung	Zertifizierung durch datenschutz cert GmbH und DQS GmbH; Akkreditierung durch DAkkS ist gegeben	VdS-Zertifizierung durch VdS Zertifizierungsstelle, aber unabhängiger Audit	-	Zertifizierung durch ZVEH
Kosten*	Dokumente < 200 EUR; Weitere Kosten für Beratung, Audit und Zertifizierung hängen von der Komplexität des Untersuchungsgegenstands ab.	Dokumente kostenfrei erhältlich; Weitere Kosten für Beratung, Audit und Zertifizierung hängen von der Komplexität des Untersuchungsgegenstands ab.		Dokumente (CISIS12-Norm, -Handbuch und Katalog): < 200 EUR; Weitere Kosten für Beratung, Audit und Zertifizierung hängen von der Komplexität des Untersuchungsgegenstands ab.	Quick Check, Dokumente (Richtlinien, Leitfaden): < 100 EUR; Weitere Kosten für Beratung, Audit und Zertifizierung hängen von der Komplexität des Untersuchungsgegenstands ab.	Quick Check, Dokumente (Richtlinien, Leitfaden), Audit und VdS-Testat < 1.000 EUR	Kosten für Beratung und Audit ca. 1.000 EUR. Abhängig vom Aufwand.
Gültigkeit der Zertifizierung / des Testats	3 Jahre, jährlich Monitorings	3 Jahre, jährlich Monitorings	2 Jahre	3 Jahre, jährlich Monitorings	3 Jahre, jährlich Monitorings	Unbegrenzt, aber Wiederholung der Testierung in geeigneten Zeitabständen empfohlen	3 Jahre, jährliche "Digitale" Mitarbeiterschulungen zur Sensibilisierung erforderlich
Aufwärts-kompatibel zu	-	ISO/IEC 27001	BSI IT-Grundschutz Standardabsicherung	ISO/IEC 27001 und BSI IT-Grundschutz	ISO/IEC 27001	VdS 10000	BSI IT-Grundschutz

*Kosten für Beratung, Audit und Zertifizierung sind je nach Anbieter unterschiedlich. In der Regel fallen ~ zwischen 800 und 1.500 EUR pro PT an.

Tabelle 1: Übersicht zu gängigen, ausgewählten Informationssicherheitsstandards

5 Methodisches Vorgehen

Die Umfrageergebnisse der Studie basieren auf der Auswertung einer Expertenumfrage, die von der WIK-Consult GmbH im Rahmen der Begleitforschung Mittelstand-Digital vom 01.06.2021 bis 21.06.2022 durchgeführt wurde. Befragt wurden die Expertinnen und Experten mit Schwerpunkt Informationssicherheit des Netzwerks Mittelstand-Digital. 17 Expertinnen und Experten haben an der Umfrage teilgenommen, darunter sind u.a. Vertreterinnen und Vertreter von Universitäten, Hochschulen, Verbänden sowie aus der Praxis mit Fokus auf den Aufbau von Managementsystemen.

Da ISMS im Mittelstand bisher nur selten zum Einsatz kommen, können Expertinnen und Experten einen umfassenderen Überblick geben als Umfragen unter KMU. Die Befragten stammen aus dem Transferbereich an der Schnittstelle zwischen Wissenschaft und Implementierung in der Praxis. Entsprechend sind die Befragten mit den unternehmerischen Herausforderungen gut vertraut. Es wird kein Anspruch auf Repräsentativität erhoben. Vielmehr handelt es um die fundierte fachliche Einschätzung von Expertinnen und Experten.

Quellenverzeichnis

Bitkom (2018): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, Studienbericht 2018

Blind, K., Kromer, L., Heß, P. (2022): Deutsches Normungspanel 2022 – Jährlicher Indikatorenbericht zur Bedeutung von Normen und Standards sowie Normungsaktivitäten deutscher Unternehmen, Herausgeber DIN Deutsches Institut für Normung e. V.

Bundesamt für Sicherheit in der Informationstechnik – BSI (2017): Leitfaden zur Basis-Absicherung nach IT-Grundschutz

Bundesamt für Sicherheit in der Informationstechnik - BSI (2019): Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen

Bundesamt für Sicherheit in der Informationstechnik - BSI (2020): IT-Sicherheit im HOME-OFFICE – UNTER BESONDERER BERÜCKSICHTIGUNG DER COVID-19 SITUATION

Bundesamt für Sicherheit in der Informationstechnik – BSI (2021): Die Lage der IT-Sicherheit in Deutschland 2021

Bundesdruckerei (2017): Digitalisierung und IT-Sicherheit in deutschen Unternehmen – Eine repräsentative Untersuchung, erstellt von der Bundesdruckerei GmbH in Zusammenarbeit mit KANTAR EMNID

Bundesverband IT-Mittelstand - BITMi (2021): So werde ich sicher – Eine einfache Anleitung zur IT-Sicherheit für den Mittelstand

Deutscher Landkreistag (2017): Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, erschienen in Schriften des Deutschen Landkreistages, Band 129 der Veröffentlichungen des Vereins für Geschichte der Deutschen Landkreise e.V, Herausgeber Deutscher Landkreistag

Deutschland sicher im Netz (2021): DsiN-Praxisreport 2020 Mittelstand@IT-Sicherheit

Deutschland sicher im Netz (2022): DsiN-Praxisreport 2021/22 Mittelstand@IT-Sicherheit

Dreißigacker, A., von Skarczinski, B., Wollinger, G. R. (2020): Cyberangriffe gegen Unternehmen in Deutschland – Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019, Kriminologisches Forschungsinstitut Niedersachsen e.V

eco - Verband der Internetwirtschaft (2019): Kompetenzgruppe Sicherheit Arbeitskreis ISMS, https://www.eco.de/wp-content/uploads/2019/07/eco_Sicherheit_Vergleich_ISMS-2.pdf (abgerufen am 19.07.2022, 11:43 Uhr)

European Union Agency for Cybersecurity - ENISA (2021): ENISA Threat Landscape for Supply Chain Attacks, July 2021

Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele, S., Henseler-Unger, I. (2017): Aktuelle Lage der IT-Sicherheit in KMU, WIK-Studie im Auftrag des BMWi

Hsu, C., Wang, D., Lu, A. (2016): The Impact of ISO 27001 Certification on Firm Performance, erschienen in Proceedings of the 49th Hawaii International Conference on System Sciences (2016), Herausgeber IEEE Computer Society

International Organization for Standardization - ISO (2018): ISO/IEC 27000:2018-02 Informationstechnik - Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie

International Organization for Standardization - ISO (2020): The ISO Survey, https://www.iso.org/the-iso-survey.html (abgerufen am 13.05.2022)

IT-Sicherheitscluster e. V. (2021): Der nächste Schritte CISIS12 – Informationssicherheits-Managementsystem, https://cisis12.de/wp-content/uploads/2021/06/CISIS12-Infoveranstaltung.pdf (abgerufen am 12.07.2022 um 11:18 Uhr)

Jeliazkov, N. et al (2020): Bewertung der Leistung eines ISMS durch Schlüsselindikatoren, Praxisleitfaden für ein zielorientiertes IS-Kennzahlensystem nach ISO/IEC 27004:2016, Herausgeber ISACA Germany Chapter e.V

Mirtsch et al (2020a): Die Nutzung und Wirkung genormter Managementsysteme – Eine Studie im Rahmen der Initiative QI-FoKuS, Vol. 1, Herausgeber Bundesanstalt für Materialforschung und -prüfung (BAM)

Mirtsch et al (2020b): Die Nutzung und Wirkung der Norm ISO/IEC 27001 für Informationssicherheit in Unternehmen in Deutschland – Eine Studie im Rahmen der Initiative QI-FoKuS Vol. 2, Herausgeber Bundesanstalt für Materialforschung und -prüfung (BAM)

Park, C.-S., Jang, S.-S., Park, Y.-T. (2010): A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance, erschienen in IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.3, March 2010

VdS Schadenverhütung GmbH (2022): Zertifikate/Verzeichnis, https://vds.de/zertifikate/verzeichnis/V10031 (abgerufen am 13.07.2022 um 15:19 Uhr)

Verband der Automobilindustrie (2020): VDA Jahresbericht 2020 – Die Automobilindustrie in Daten und Fakten

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit.
Weitere Informationen finden Sie unter *www.mittelstand-digital.de*.

www.mittelstand-digital.de