

Datenschutz und Informationssicherheit in KMU's

In Zusammenarbeit mit

AKARION

Informationen zur Studie



Diese Studie wurde erstellt durch



Kontakt

techconsult GmbH

E-Mail: info@techconsult.de

Tel.: +49 561 8109 0

Fax: +49 561 8109 101

Web: www.techconsult.de

In Zusammenarbeit mit



Copyright

Diese Studie wurde von der techconsult GmbH im Auftrag der Akarion AG verfasst. Die darin enthaltenen Daten und Informationen wurden gewissenhaft und mit größtmöglicher Sorgfalt nach wissenschaftlichen Grundsätzen ermittelt. Für deren Vollständigkeit und Richtigkeit kann jedoch keine Garantie übernommen werden. Alle Rechte am Inhalt dieser Studie liegen bei der techconsult GmbH. Vervielfältigungen, auch auszugsweise, sind nur mit schriftlicher Genehmigung der techconsult GmbH gestattet.

Disclaimer

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen etc. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. In dieser Studie gemachte Referenzen zu irgendeinem spezifischen kommerziellen Produkt, Prozess oder Service durch Markennamen, Handelsmarken, Herstellerbezeichnung etc. bedeuten in keiner Weise eine Bevorzugung durch die techconsult GmbH.

Inhaltsverzeichnis

Vorwort.....	4
Datenschutz und Informationssicherheit stehen hoch im Kurs - aber nicht hoch genug	5
DSMS und ISMS bereits im Einsatz etabliert.....	7
Vorteile von Datenschutz- und Informationssicherheits-Management-Software.....	9
Kosten als Hemmnissfaktor Nummer 1	10
Benutzerfreundlichkeit hoch im Kurs.....	11
Fazit.....	12
Stichprobe.....	13
Weitere Informationen	14

Vorwort

Datenschutz und Informationssicherheit betreffen Unternehmen jeglicher Größe und Branche. Unternehmen müssen sicherstellen, dass sensible, personenbezogene Daten geschützt sind und IT-Prozesse und Systeme keinem Risiko ausgesetzt sind. Dafür müssen Unternehmen diesen Themen jedoch auch einen hohen Stellenwert zuweisen und die Sicherheit mit den geeigneten Werkzeugen gewährleisten.

Doch wie wichtig sehen Unternehmen Datenschutz- und Informationssicherheit tatsächlich an? Wie zufrieden sind sie mit der Umsetzung? Wie hoch ist der Verbreitungsgrad dedizierter Datenschutz- und Informationssicherheitsmanagement-Lösungen? Und welche Vorteile und Herausforderungen sehen Unternehmen im Zuge des Einsatzes solcher Spezialsoftware?

Um diese Fragen zu beantworten, wurden im Rahmen dieser Studie 200 Entscheider oder stark am Entscheidungsprozess beteiligte Personen im März 2022 zu ihrer Zufriedenheit mit Datenschutz und Informationssicherheit, den Einsatzgraden von softwaregestützten DSMS- und ISMS-Lösungen sowie zu Vorteilen und Herausforderungen, die mit dem Einsatz dieser Software korrelieren, befragt.

Datenschutz und Informationssicherheit stehen hoch im Kurs - aber nicht hoch genug

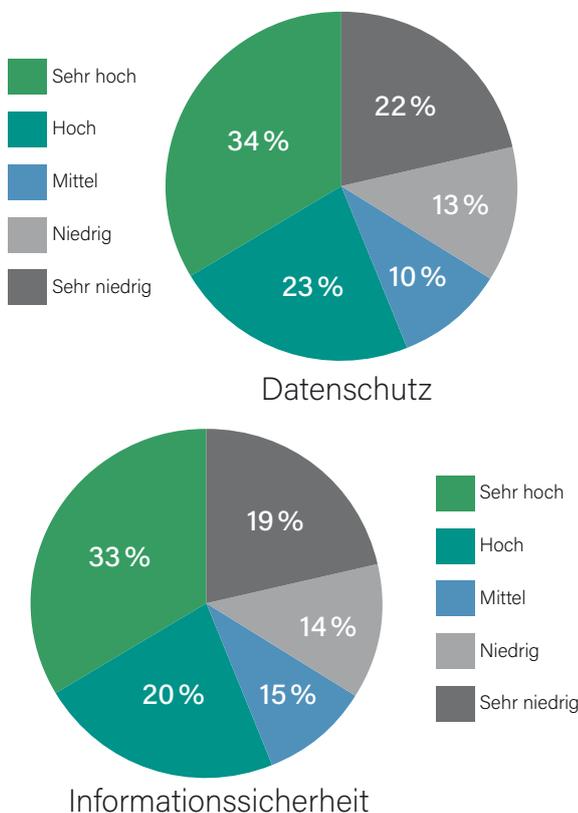
Datenschutz und Informationssicherheit sind nicht erst seit der Einführung der Datenschutzgrundverordnung (DSGVO) oder des IT-Sicherheitsgesetz 2.0 von höchster Bedeutung für Unternehmen jeglicher Art. Die DSGVO, die die Anforderungen rund um die Verarbeitung personenbezogener Daten noch einmal erhöht hat und auch das IT-Sicherheitsgesetz 2.0 sind nur die Speerspitze von zahlreichen neuen Gesetzen, Richtlinien und Empfehlungen für mehr Cybersicherheit.

50 Prozent sehen Datenschutz und Informationssicherheit als wichtig an

Wie hoch der Stellenwert tatsächlich ist, zeigen die Ergebnisse dieser Studie. Mehr als die Hälfte der befragten Unternehmen gibt an, dass Datenschutz und Informationssicherheit einen hohen bis sehr hohen Stellenwert genießen. Leider sagen auch jeweils ein knappes Drittel der Unternehmen, dass sowohl Datenschutz als auch Informationssicherheit eher wenig bis keine Relevanz haben. Ein Umstand, der den betroffenen Unternehmen zu denken geben sollte.

Stellenwert Datenschutz und Informationssicherheit

Basis: 200 Unternehmen



Als Vorreiter kann die Banken- und Versicherungsbranche angesehen werden. Mehr als 70 Prozent der Finanzdienstleister sehen in Datenschutz und Informationssicherheit Themen mit hoher Priorität. Auffällig ist die Diskrepanz zwischen Datenschutz und Informationssicherheit bei öffentlichen Verwaltungen. Während Datenschutz analog zu den anderen Branchen bei mehr als der Hälfte einen hohen Stellenwert genießt, ist es bei Informationssicherheit nur ein knappes Drittel – und damit der im Branchenvergleich mit Abstand niedrigste Wert.

Nur jedes zweite Unternehmen mit der Umsetzung zufrieden

Informationssicherheit und Datenschutz eine hohe Priorität einzuräumen ist eine Sache. Entscheidend ist aber, die Themen auch aktiv anzugehen und umzusetzen. Die reine Zuweisung eines hohen Stellenwerts führt keineswegs zum Erfolg, wenn die Umsetzung ineffektiv und fehlerhaft ist und man trotz aller theoretischer Mühen weiterhin von Datenschutzpannen oder einfachsten Informationssicherheitslücken geplagt ist.

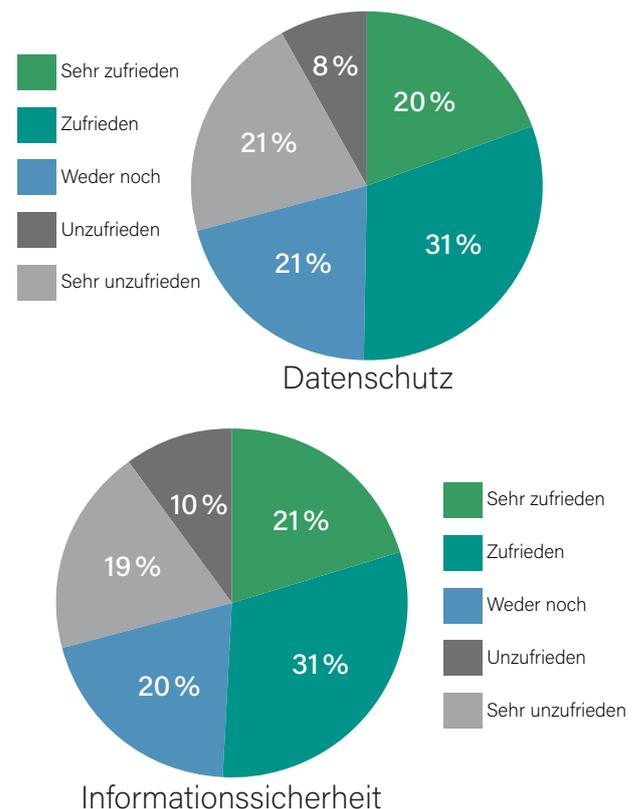
Wirklich zufrieden mit der Ausgestaltung der Maßnahmen für Datenschutz und Informationssicherheit sind jeweils nur knapp die Hälfte der Unternehmen. Fast ein Drittel bezeichnet die Umsetzung von Datenschutz und Informationssicherheit sogar als schlecht oder sehr schlecht. Dies sollte Grund zur Sorge sein. Beispielsweise können häufig auftretende Datenschutz-Pannen neben finanziellen Schäden schnell auch zu einem Vertrauensverlust bei Geschäftspartnern und Kunden führen. Solche vermeidbaren Sicherheitslücken können im schlimmsten Fall sogar die Existenz des gesamten Unternehmens bedrohen. Im Jahr 2021 stiegen einer Untersuchung von IBM zu Folge, die durchschnittlichen Kosten für Datenverstöße von 3,86 Millionen US-Dollar auf 4,24 Millionen US-Dollar – ein neuer Allzeitrekord!¹

Die tendenziell höchste Zufriedenheit mit ihren Maßnahmen weisen Finanzdienstleister auf. Während knapp zwei Drittel der Banken und Versicherungen sich mit der Umsetzung des Datenschutzes zufrieden zeigen, sind es im Bereich Informationssicherheit sogar drei Viertel. Finanzdienstleister sehen diese Themen also nicht nur als sehr wichtig an, sie setzen diese auch zufriedenstellend um.

Öffentliche Verwaltungen hingegen sind mit der Umsetzung unzufrieden. So geben weniger als 40 Prozent an, den Datenschutz und die Informationssicherheit gut oder sehr gut umzusetzen. An dieser Stelle besteht für öffentliche Verwaltungen deutlicher Nachholbedarf. Vor allem, da es nicht nur um den Schutz von personenbezogenen Daten geht, sondern auch um den Schutz von kritischer Infrastruktur. Aufgrund ihrer besonderen Stellung sind KRITIS-Unternehmen sehr attraktive Angriffsziele für Cyberkriminelle. Schäden in diesen Bereichen haben weitreichende Folgen, die von nationaler Tragweite sein können. Als mahnende Beispiele können die erfolgreichen Cyberangriffe auf die Kommunalverwaltungen von Anhalt-Bitterfeld, Schwerin oder Witten genannt werden. Auch die Cyberattacke auf den drittgrößten österreichischen Molkereibetrieb sowie ein Angriff auf die Grundwasseraufbereitungsanlage in Oldsmar (Florida) zeigen, wie stark Verwaltungen und KRITIS-Unternehmen im Fokus von Cyberkriminellen stehen.²

Zufriedenheit mit der Umsetzung

Basis: 200 Unternehmen



¹ <https://www.ibm.com/security/data-breach>

² <https://netzpalaver.de/2022/03/14/kritis-im-kontext-von-cyberangriffen>

DSMS und ISMS bereits im Einsatz etabliert

Um den hohen Anforderungen an Datenschutz und Informationssicherheit von heute gerecht zu werden, stehen Unternehmen zum Glück nicht allein dar. Praktischerweise gibt es zur Unterstützung der Maßnahmenumsetzung Softwarelösungen, die speziell darauf ausgelegt sind, das Schutzniveau zu erhöhen.

Fast alle Unternehmen werden Datenschutzmanagementsysteme nutzen

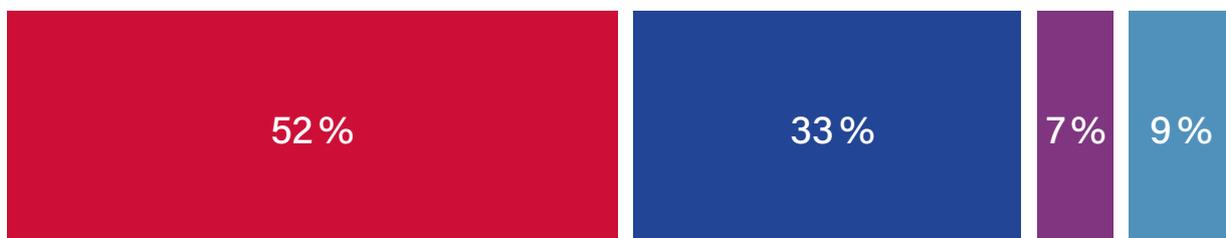
Softwaregestützte Datenschutzmanagementlösungen (DSMS) werden bisher in knapp der Hälfte der Unternehmen eingesetzt. Ein weiteres Drittel plant den Einsatz in den kommenden 12 Monaten. 6,5 Prozent wollen in den kommenden drei Jahren eine DSMS-Software einsetzen. Und noch fast 9 Prozent der Unternehmen wollen gänzlich auf eine solche Lösung verzichten. Man kann also aus gutem Grund behaupten, dass Unternehmen sich dem Einsatz von Datenschutzmanagementlösungen nicht verwehren. Innerhalb der nächsten Jahre werden 9 von 10 Unternehmen eine solche Software im Einsatz haben.

Am ehesten auf DSMS verzichten kleinere Unternehmen zwischen 200 und 499 Mitarbeitern. Zwar ist der Anteil an Unternehmen in dieser Größenklasse, die in den folgenden 3 Jahren ein DSMS einsetzen wollen, ebenfalls auf einem hohen Niveau, der Anteil an Unternehmen, die gar keinen Einsatz planen, jedoch doppelt so hoch wie im Durchschnitt (16 Prozent).

Branchenseitig sind Unternehmen aus dem Handel (64 Prozent), Banken und Versicherungen (59 Prozent) sowie Dienstleister (55 Prozent) Vorreiter beim Einsatz von DSMS. Der Anteil bei Industrieunternehmen (46 Prozent) und öffentlichen Verwaltungen (47 Prozent) ist deutlich niedriger. Darüber hinaus möchte ein knappes Fünftel der Öffentlichen Verwaltungen kein DSMS einsetzen. Das ist aufgrund der im vorherigen Abschnitt festgestellten Umsetzungsprobleme verwunderlich, würde ein DSMS doch maßgeblich zur Verbesserung des eigenen Datenschutzes beitragen und den Aufwand signifikant reduzieren.

Einsatz von Datenschutzmanagement-Lösungen

Basis: 200 Unternehmen



- Wir verwenden eine dedizierte DSMS-Lösung
- Wir verwenden derzeit keine Lösung, planen aber einen Einsatz in den nächsten 12 Monaten
- Wir verwenden derzeit keine Lösung, planen aber einen Einsatz in den nächsten 3 Jahren
- Wir verwenden derzeit keine Lösungen und planen auch keinen Einsatz

Größere Unternehmen setzen verstärkt auf Informationssicherheits-Management-Software

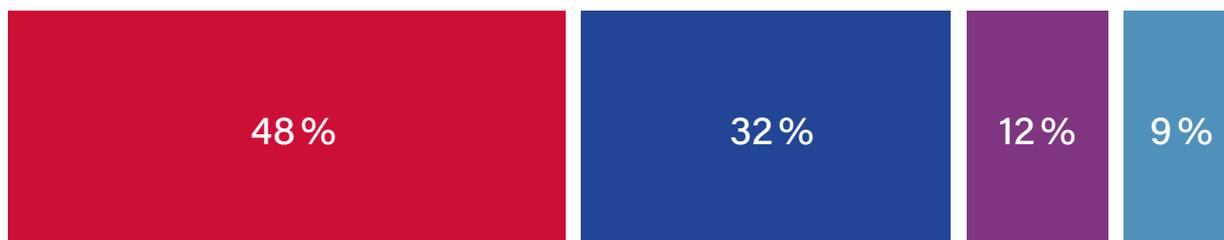
Der Einsatzgrad von Software zur Umsetzung von Informationssicherheit (ISMS) ist generell ein wenig niedriger als es bei Datenschutzmanagementsystemen der Fall ist. Weniger als die Hälfte der Unternehmen setzt ein softwaregestütztes ISMS ein. Etwas weniger als ein Drittel plant zudem den Einsatz in den kommenden zwölf Monaten. Mittelfristig, also innerhalb der nächsten drei Jahre, wollen noch weitere zwölf Prozent der Unternehmen ein softwaregestütztes ISMS einführen und für neun Prozent kommt ein Einsatz gar nicht infrage.

Die Verbreitung von ISMS-Lösungen steigt mit der Unternehmensgröße an. Während nur 36 Prozent der kleineren Unternehmen mit unter 499 Mitarbeitern ein ISMS einsetzen, sind es bei Unternehmen ab 5000 Mitarbeitern sogar 56 Prozent. Analog zu den Einsatzgraden von DSMS-Lösungen, sind es auch hier die kleineren Unternehmen, die gänzlich auf eine dedizierte Lösung verzichten wollen.

Überraschend ist branchenseitig die Tatsache, dass Banken und Versicherungen – Vorreiter in Sachen DSMS – nur einen niedrigen Einsatzgrad von 35 Prozent aufweisen. Jedoch haben diese die Handlungsnotwendigkeit erkannt und so werden jeweils 41 Prozent innerhalb der nächsten Monate und weitere 18 Prozent in spätestens drei Jahren ein ISMS aufsetzen.

Einsatz von Informationssicherheits-Management-Lösungen

Basis: 200 Unternehmen



- Wir verwenden eine dedizierte ISMS-Lösung
- Wir verwenden derzeit keine Lösungen und planen auch keinen Einsatz
- Wir verwenden derzeit keine Lösung, planen aber einen Einsatz in den nächsten 3 Jahren
- Wir verwenden derzeit keine Lösung, planen aber einen Einsatz in den nächsten 12 Monaten

Vorteile von Datenschutz- und Informationssicherheits-Management-Software

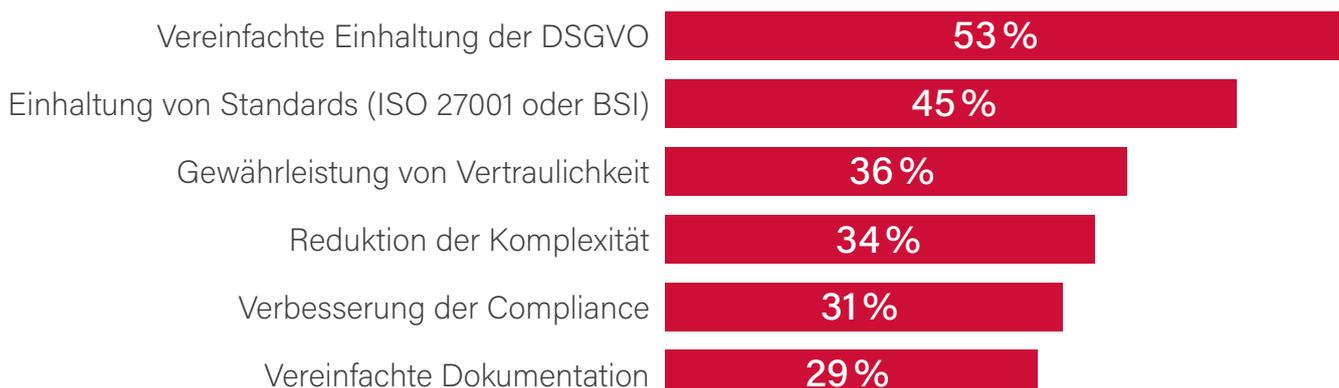
Der Einsatz einer Lösung für DSMS oder ISMS bringt für Unternehmen diverse Vorteile, die dazu beitragen, ein höheres Schutzniveau zu erreichen. Das größte Argument für den Einsatz ist dabei vor allem die vereinfachte Einhaltung der Datenschutzgrundverordnung (DSGVO). Knapp 53 Prozent der befragten Unternehmen nannten dies als Hauptgrund für den Einsatz von DSMS- und ISMS-Lösungen. Beide Systeme sorgen dafür, dass personenbezogene Daten geschützt werden. Ein ISMS ist dabei nicht primär auf den Schutz von personenbezogenen Daten ausgerichtet, sondern trägt durch die in ihm definierten Maßnahmen oder Risikobehandlungen zu besserer Informationssicherheit bei. Nur so, sind beispielsweise Zertifizierungen wie ISO 27001, TISAX oder IT-Grundschutz (BSI) ab einer gewissen Unternehmensgröße und -komplexität effizient bewältigbar. Beide Systeme schließen sich jedoch nicht aus. Ein ISMS wird meist nicht alle technischen und rechtlichen Fragen im Rahmen von Datenschutz abdecken können. Beide Systeme sollten daher zugleich in Unternehmen eingesetzt werden, um für einen optimalen Schutz zu sorgen.

Dahinter folgt die Einhaltung von Standards wie ISO 270001 oder dem BSI Standard 200-1 (Management für Informationssicherheit). Banken und Versicherungen sehen die Einhaltung von Standards sogar als wichtigsten Punkt an. 71 Prozent vergeben hier die höchste Priorität. Das verwundert wenig, denn Banken und Versicherungen müssen zu jeder Zeit ein nach ISO 27001 oder BSI zertifiziertes ISMS nachweisen können.

Ein ISO 27001 Zertifikat kann darüber hinaus auch einen ganz besonderen Wert nach Außen haben. Denn ein solches Zertifikat kann ohne Zweifel als Wettbewerbsvorteil angesehen werden. So zeigen Unternehmen, dass sie es mit der Informationssicherheit ernst meinen und sich extern auditieren lassen haben. Kunden und Partner können dank des strengen Standards darauf vertrauen, dass ihre Informationen in guten und sicheren Händen sind.

Vorteile von softwaregestütztem DSMS/ISMS

Basis: 200 Unternehmen, Mehrfachnennungen



Kosten als Hemmnissfaktor Nummer 1

Unternehmen sehen sich bei der Implementierung von DSMS- und ISMS-Lösungen mit unterschiedlichen Herausforderungen konfrontiert. Als besonders problematisch sehen 43 Prozent der Unternehmen die hohen Kosten für den Einsatz von DSMS- und ISMS-Software. Dabei fallen nicht nur die Kosten für die erstmalige Implementierung an, sondern es kommen auch Folgekosten für die Neuanschaffung von benötigter IT-Infrastruktur, Lizenzen oder Schulungen für Mitarbeiter dazu.

An zweiter Stelle folgen mit 34 Prozent IT-Sicherheitsbedenken. Insbesondere dort, wo die Verwaltung der Datenschutz- und Informationssicherheits-Software in der eigenen Hand liegt, können kleinste Fehler bereits für große Probleme sorgen. Ist eine Software selbst nicht sicher oder wird aufgrund der Komplexität falsch bedient, kann diese ihren Zweck schnell nicht mehr erfüllen. Die Folge: eine zur Verbesserung der Sicherheit gedachte Software wird selbst zum Gefahrenherd.

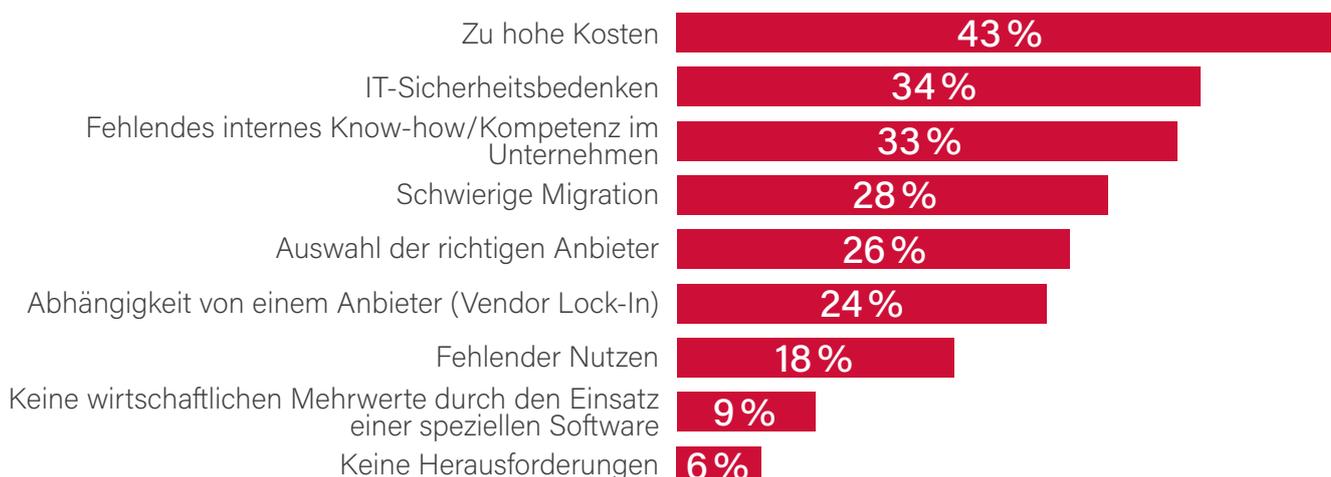
An dieser Stelle spielt auch das fehlende Know-how in den Unternehmen eine bedeutende Rolle. Knapp ein Drittel der Unternehmen geben an, nicht über die nötigen Kompetenzen zu verfügen, um ein DSMS und ISMS im eigenen Unternehmen zu implementieren und zu betreuen. Und ohne die nötigen Kompetenzen wird die Software nie so sicher eingesetzt werden können, wie es nötig ist. Anbieter von DSMS und ISMS, die selbst nach ISO 27001 zertifiziert sind, stehen für einen garantiert sicheren Betrieb.

Viele der Herausforderungen lassen sich durch den Einsatz einer cloudbasierten Lösung schnell und einfach meistern. Eine Lösung auf Cloudbasis hilft beispielsweise dabei, die Kosten zu senken. So fallen Anschaffungskosten sowie mögliche zusätzliche Kosten für neue Hardware weg.

Auch das Problem des fehlenden Know-hows kann mit Cloud-Lösungen umgangen werden. Die Software muss nicht aufwendig in die eigenen Systeme integriert werden, es bedarf keiner aufwendigen Installation und bei Problemen kümmert sich der Dienstleister direkt um die Fehlerbehebung. Die IT-Abteilung wird entlastet und kann sich anderen Aufgaben widmen.

Herausforderungen bei der Einführung

Basis: 200 Unternehmen, Mehrfachnennungen



Benutzerfreundlichkeit hoch im Kurs

Entscheidet sich ein Unternehmen dazu, eine dedizierte Lösung für das Datenschutz- oder Informationssicherheitsmanagement einzuführen, spielen besondere Eigenschaften eine große Rolle bei der Kaufentscheidung. Im Meer von unterschiedlichen Lösungen verschiedener Anbieter braucht es herausragende Merkmale, um sich von der Masse abzuheben.

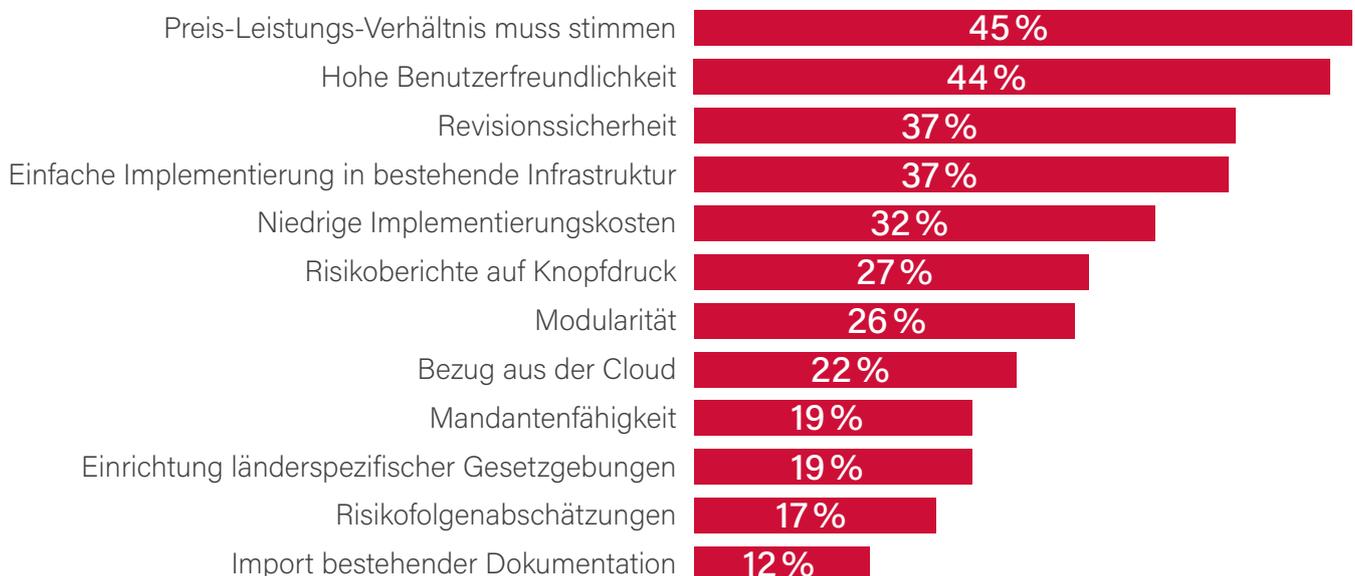
Wie so oft bei Kaufentscheidungen ist das Preis-/Leistungsverhältnis das Top-Kriterium im Zuge der Softwareauswahl. Dies sollte nicht mit einem günstigen Preis verwechselt werden. Wenn die Leistung des Produkts stimmt und die Effizienz messbar steigt, sind Kunden auch bereit, den höheren Preis für die bessere Leistung zu bezahlen. Fast auf gleichem Niveau ist die Wichtigkeit der Benutzerfreundlichkeit für die Unternehmen. In der heutigen Zeit ist die einfache Bedienbarkeit ein entscheidender Faktor bei der Auswahl von betrieblicher Software.

Denn Nutzer, die mit dem Produkt tagtäglich umgehen müssen, wollen auch im beruflichen Umfeld einen ähnlich hohen Komfort haben, wie sie es mit ihrer privaten Software bereits gewohnt sind. Denn wenn eine Software im Privatbereich nicht gefällt, wird diese einfach nicht mehr genutzt. Auch bei DSMS- und ISMS-Lösungen ist die erste Nutzung bereits entscheidend. Schon in den ersten Minuten ermittelt der Nutzer, ob er die Software als gut oder schlecht erachtet.

Auch aus Kostensicht ist benutzerfreundliche Software erstrebenswert. Beispielsweise lassen sich Zeit und Kosten für etwaige Schulungen oder laufenden Support einsparen. Intuitiv bedienbare Software lässt Nutzer leichter und schneller ihre Aufgaben bewältigen, wodurch der Schulungsaufwand minimiert werden kann. Darüber hinaus liefert eine Software, die vom Nutzer akzeptiert wird, auch wenig Grund dazu, in naher Zukunft direkt wieder ausgetauscht zu werden. Und das spart Unternehmen beispielsweise unnötige Wechsel- sowie weitere Schulungskosten.

Was muss eine Lösung können

Basis: 200 Unternehmen, Mehrfachnennungen



Fazit

Daten- und Informationssicherheit stehen in der Mehrheit der Unternehmen wenig überraschend an oberster Stelle. Allerdings klaffen Theorie und Praxis hier deutlich auseinander. In vielen Unternehmen werden Datenschutz und Informationssicherheit nicht mit der nötigen Sorgfalt behandelt, wie es nötig wäre. Auch wenn die Zahl der Unternehmen, die diesen Themen keinerlei Relevanz zusprechen gering ist: In Zeiten von beinahe täglichen Angriffen auf IT-Infrastrukturen und Data Breaches ist eine geringe Professionalisierung umso erschreckender. Der 2021 von IBM veröffentlichte Bericht „Cost of a Data Breach“ zeigt beispielsweise, dass sich die durchschnittlichen Kosten für Datenverstöße auf einem Allzeithoch befinden.

Die Frage, wie sehr Datenschutz- und Informations-sicherheitsmanagement auf den Erfolg eines Unternehmens einzahlen, lässt sich einfach beantworten: Datenschutz- und IT-Sicherheitsvorfälle sorgen nicht für mehr Umsatz, tragen aber z.B. zum Schutz vor Strafen und Ransomware-Erpressungen bei. Ein Komplettausfall von IT-Systemen, wie er immer öfter durch die Medien geht, kann jede Organisation nicht nur wirtschaftlich enorm treffen. Auch die verloren gegangene Reputation ist nur schwer wiederherzustellen.

Abhilfe kann dabei der Einsatz von DSMS und ISMS-Lösungen schaffen, mit denen Unternehmen genau die Werkzeuge erhalten, mit denen sie die hohen Anforderungen an Datenschutz und Informationssicherheit bewältigen können. Denn wer heute in Compliance-Fragen Mängel aufweist, kann schnell ins Hintertreffen geraten und im schlimmsten Fall seine eigene Marktposition riskieren.

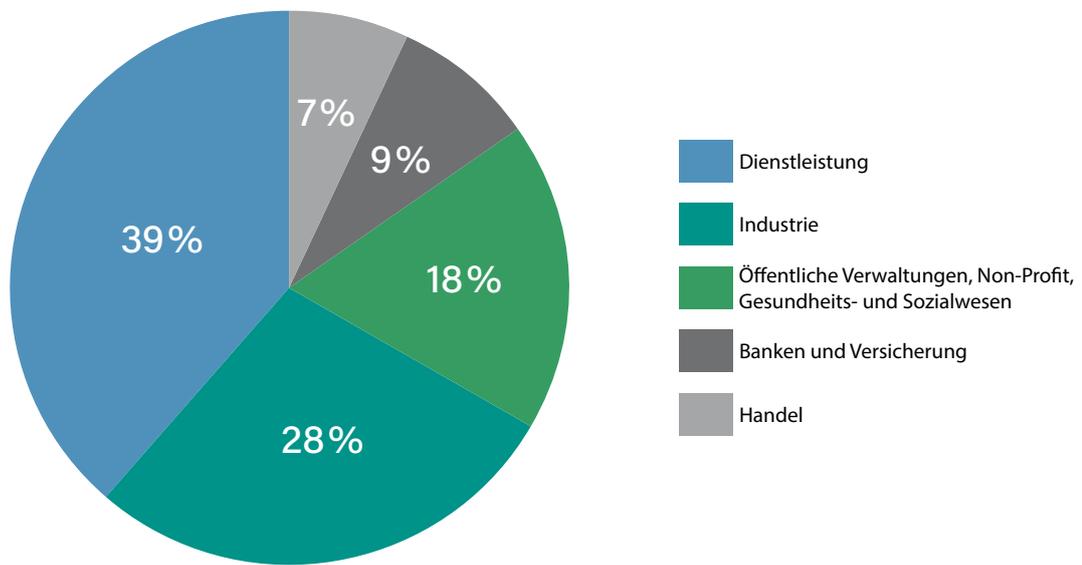
Dies zeigen auch die Nutzungszahlen von DSMS und ISMS Softwarelösungen in Unternehmen. In spätestens drei Jahren wollen nahezu sämtliche Unternehmen derartige Lösungen nutzen. Doch es gibt auch Probleme, die im Rahmen der Einführung gesehen werden. Kosten oder fehlendes internes Know-how stellen oftmals Hemmnisse beim Einsatz dieser Lösungen dar.

Eine elegante und kosteneffiziente Lösung kann hier der Einsatz von cloudbasierter DSMS- und ISMS-Software sein, mit denen viele der Hürden gar nicht erst auftauchen. Ohne komplizierte Installation, zusätzliche Kosten für Infrastruktur und erhöhte Schulungsaufwände lassen sich mit cloudbasierten Lösungen Datenschutz und Informationssicherheit praktisch sofort verbessern.



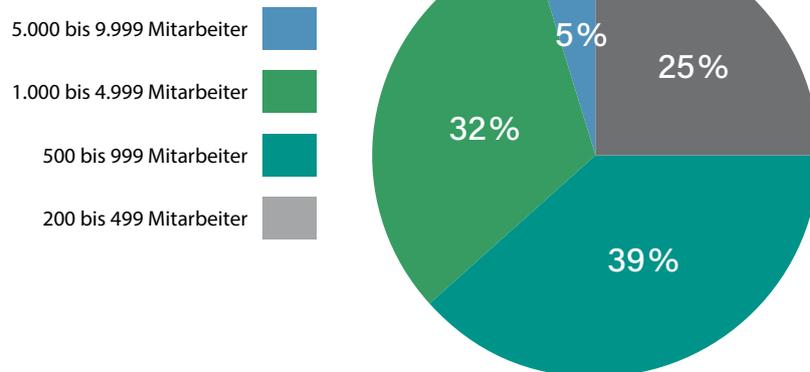
Stichprobe

Branche



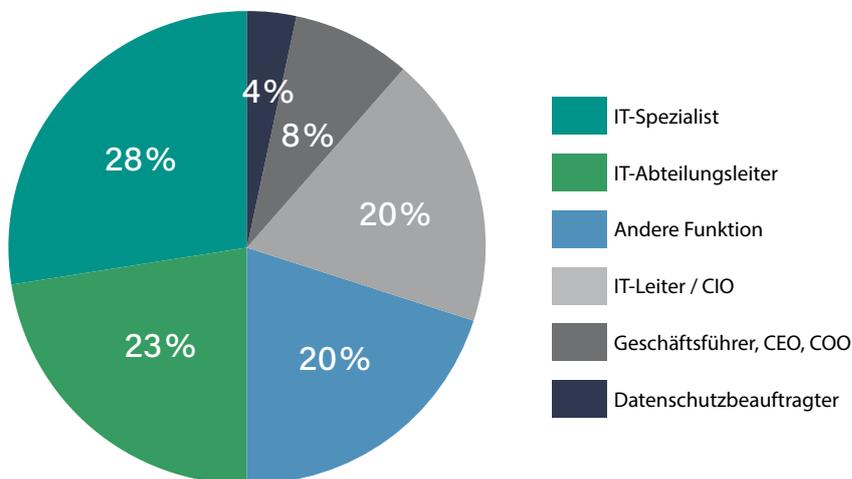
Basis: 200 Unternehmen

Mitarbeiter



Basis: 200 Unternehmen

Position



Basis: 200 Unternehmen

Weitere Informationen

Kontakt für mehr Informationen

Raphael Napieralski

Analyst

Telefon: +49 561 8109 0

E-Mail: raphael.napieralski@techconsult.de

Baunsbergstr. 37

techconsult GmbH

D-34131 Kassel

Über techconsult GmbH

Die techconsult GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Über Akarion

AKARION entwickelt seit 2017 herausragende und einzigartige Software-Lösungen für die Bereiche Compliance & GRC.

Mit der AKARION Compliance Cloud bewältigen Unternehmen und Berater:innen zahlreiche regulatorische Anforderungen mit nur einer einzigen Lösung. Sie vereint dabei bewährte Best Practices, innovatives Design und modernste Softwareentwicklung. Zahlreiche Organisationen jeder Größe nutzen die intuitive SaaS-Plattform, um gesetzlich erforderliche Dokumentationen für unterschiedlichste Fachgebiete zu erstellen. Die 3 Hauptmodule Datenschutz, Informationssicherheit und Whistleblowing sind kombinierbar mit aktuell 4 Nebenmodulen. Alle verwenden eine intuitive Nutzeroberfläche und eine gemeinsame Datenbank, um Redundanzen zu vermeiden. Ergänzt durch den einzigartigen Trust Layer für manipulationsfreie und revisionssicher Datendokumentation erhalten Unternehmen und Berater:innen die einfachste, schnellste und kosteneffizienteste Compliance-Lösung am Markt.



Eine Studie von

30 YEARS
ANNIVERSARY

techconsult
TECHNOLOGY MARKET ANALYSTS

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de

Telefon: +49 561 8109 0

Telefax: +49 561 8109 101

Web: www.techconsult.de

In Zusammenarbeit mit

