gfs-zürich | MARKT- & SOZIALFORSCHUNG

Schlussbericht 2017:

Cyberrisiken in Schweizer KMUs

Befragung von GeschäftsführerInnen Schweizer KMUs

Studie im Auftrag von:

Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit, Arié Malz
ICTswitzerland, Andreas Kaelin
ISB Informatiksteuerungsorgan des Bundes, Manuel Suter
ISSS Information Security Society Switzerland, Umberto Annino
SQS Schweizerische Vereinigung für Qualitäts- und Managementsysteme, Felix Müller
SVV Schweizer Versicherungsverband, Gunthard Niederbäumer

gfs-zürich, Markt- und Sozialforschung

Karin Mändli Lerch (Projektleitung)
Aleksandar Repic (Projektmitarbeit)

Zürich, 12. Dezember 2017

SCHWEIZER MARKTFORSCHUNG
Verband Schweizer Markt- und Sozialforschung
Mitglied swiss interview institute®

Riedtlistrasse 9
CH 8006 Zürich

Tel. +41 44 360 40 20
Fax. +41 44 350 35 33

E-mail: gfs@gfs-zh.ch
Internet: www.gfs-zh.ch

Inhaltsverzeichnis

1 Management Summary

Vom 13. bis 27. September 2017 führte das Markt- und Sozialforschungsinstitut gfs-zürich 301 Interviews mit GeschäftsführerInnen von Schweizer KMUs durch. Ziel war deren Kenntnisse, Einstellungen und getroffene Massnahmen zum Thema Cyberrisiken zu erheben.

Cyberrisiken in Schweizer KMUs
gfs-zürich, Karin Mändli Lerch
Veröffentlicht: 12. Dezember 2017

1.1 Risikofaktoren in KMUs

Das kontinuierliche Funktionieren der IT wird von rund zwei Dritteln der Befragten (62%) als sehr wichtig bezeichnet, was bedeutet, dass ein erfolgreicher Cyberangriff und ein damit einhergehender Betriebsausfall bereits einen gewissen Schaden anrichten kann.

Einen weiteren Risikofaktor bilden sensitive Daten, die bei einem Angriff gestohlen werden können. Knapp die Hälfte der befragten Firmen bewirtschaftet Geschäftsgeheimnisse (47%) und drei von fünf Firmen verwalten personenbezogene Kundendaten (60%). In rund drei Vierteln der Fälle (79% bzw. 74%) werden diese intern gespeichert.

Bei über der Hälfte der KMUs (55%) ist der/die GeschäftsführerIn selber für die IT-Sicherheit verantwortlich, davon wiederum fühlt sich rund die Hälfte (51%) gut bis sehr gut über die Cyberrisk-Thematik informiert. Dieser eher tiefe Informationsgrad dürfte ein weiterer Risikofaktor sein.

1.2 Risiko-Einschätzung und Betroffenheit

Das Risiko, Opfer eines Cyberangriffs zu werden, wird als tief eingeschätzt: Einen Tag lang ausser Gefecht gesetzt oder gar in der Existenz gefährdet zu werden, empfindet nur jeder zehnte bzw. nur jeder 25ste Befragte als grosse oder sehr grosse Gefahr (10 bzw. 4%).

Die Betroffenheitszahlen hingegen sind hoch: Auf Basis der 301 befragten KMUs kann die Anzahl an von Erpressung betroffenen Firmen auf 23'000 (4%) geschätzt werden, und ca. 209’000 Unternehmen (36%) dürften von Malware wie Viren oder Trojanern betroffen gewesen sein.

1.3 Umsetzung von Massnahmen

Drei von fünf Befragten geben an, Grundschutzmassnahmen wie Malware-Schutz, Firewall, Patch-Management und Backup voll und ganz umgesetzt zu haben. Erkennungssysteme und Prozesse zur Behandlung von Cyber-Vorfällen wurden nur von rund jedem fünften Unternehmen vollständig

eingeführt (20 bzw. 18%), Mitarbeiter-Trainings über den sicheren Gebrauch von IT noch lediglich von rund jedem siebten Unternehmen (15%).

Die Verbesserungsbereitschaft ist hoch; fast die Hälfte der Befragten (45%) plant in den nächsten 2-3 Jahren ihren Schutz gegen Cyberangriffe zu verbessern.

Ein Drittel der Befragten (33%) verwendet nach eigenen Angaben Standardrichtlinien für die IT-Sicherheit, wobei es sich vorwiegend um Branchenstandards (38%) oder Konzern- und interne Standards (35%) handelt.

1.4 Mindeststandards und Meldepflicht

Verpflichtende Mindeststandards werden nur von etwas mehr als einem Viertel der Befragten (29%) befürwortet. Die Zustimmung ist höher bei Unternehmen, welche das Risiko eines Cyberangriffs hoch einschätzen (46%) bzw. schon einmal betroffen waren von einem Cyberangriff (39%). Zuständig für solche verpflichtenden Mindeststandards müssten gemäss den Befragten die Branchenverbände (38%) oder der Bund (37%) sein.

Eine Meldepflicht, welche verlangen würde, dass Firmen und Verwaltungen Cyberangriffe melden müssten, wurde bei den Befragten mit je zwei Pro- und Kontra-Argumenten überprüft. Dabei haben die Pro-Argumente mehr Zustimmung erhalten als Ablehnung; bei den Kontra-Argumenten hielten sich die zustimmenden und ablehnenden Haltungen in etwa die Waage:

- Dem Argument, dass die Meldepflicht ein Warnsystem ermöglicht und somit die Sicherheit für alle erhöht, stimmen drei von fünf Befragten zu (60%).

- Dem Argument, dass die Meldepflicht zu einer vollständigeren Kenntnis der Bedrohungslage führt und damit die Bekämpfung von Cyberangriffen gefördert wird, wird von etwas mehr als der Hälfte der Befragten (56%) zugestimmt.

- Dass Betroffene ihre Cyberangriffe aus Angst vor Reputationsschäden nicht melden möchten, bestätigt eine knappe Mehrheit der Befragten (52%).

- Dass eine Meldepflicht nur eine weitere unnötige Belastung der KMUs ist, empfinden rund zwei von fünf Befragten als korrekte Aussage (42%).

Wichtig dürfte bei den Pro-Argumenten sein, dass die Sicherheit durch die Meldepflicht tatsächlich und glaubwürdig erhöht bzw. die Bekämpfung gestärkt würde.

1.5 Versicherung

Rund jeder achte Befragte (12%) gibt an, seine Cyberrisiken versichert zu haben. Allerdings ist dabei nicht klar, ob es sich dabei um eine ausdrückliche Cyberversicherung handelt oder ob vielleicht einzelne Befragte von einer stillschweigenden Deckung im Rahmen einer gängigen Versicherung ausgehen.

Etwas mehr als die Hälfte der Befragten (52%) befürwortet eine Risikodeckung zumindest zu einem Teil durch den Bund bei einem gravierenden, schweizweiten Cybereingriff.

1.6 Fazit

Unter Berücksichtigung der hohen Zahl an Betroffenen von Cyberangriffen und dem eher tiefen Fachwissen sowie den noch wenig umgesetzten Sicherheitsmassnahmen, halten es die Studienautoren für empfehlenswert, die Sensibilität der Geschäftsführenden und Mitarbeitenden zu stärken.

Ob eine erhöhte Sensibilität bereits dazu führt, dass der Cyberschutz in den KMUs tatsächlich verbessert wird, ist fraglich. Wie diese Studie zeigt, steigt mit der Risiko-Einschätzung auch die Bereitschaft zu einem besseren Cyberschutz, aber das bedeutet noch nicht, dass auch effektiv Massnahmen umgesetzt werden. Deshalb kann die Einführung von bedarfsgerechten Mindeststandards durchaus sinnvoll sein.

Die allfällige Einführung von gesetzlichen Mindeststandards müsste an den in dieser Studie aufgezeigten Gegebenheiten in den KMUs ausgerichtet werden bzw. müssten vor einer konkreten Einführung noch weitere Abklärungen getroffen werden, um die Umsetzungsmöglichkeit und -fähigkeit in den KMUs zu überprüfen.

Die Umsetzung einer gesetzlichen Meldepflicht, die über kritische Infrastrukturen hinausgeht, ist im Hinblick auf den aktuellen Wissensstand und die vorhandenen Ressourcen (z.B. Systeme zur Erkennung von Cyber-Vorfällen) in den Schweizer KMUs komplex. Voraussetzungen wären eine einfache Durchführung, Anonymität und v.a. auch ein glaubwürdiger Mehrwert für die KMUs im Sinne einer höheren Sicherheit durch ein Warnsystem, welches durch die vollständigere Erfassung der Angriffe möglich würde.

2 Ausgangslage und Ziele

2.1 Mandat und Fragestellung

Aufgrund der Aktualität des Themas haben sich verschiedene Stakeholder aus Wirtschaft und Verbänden zusammengetan, um zu erheben, inwieweit Cyberrisiken von Schweizer KMU-Verantwortlichen erkannt und als Bedrohung wahrgenommen werden und welche Massnahmen dagegen bereits getroffen oder geplant sind. Zusätzlich wurde die Akzeptanz von allfälligen gesetzlichen Mindeststandards und einer Meldepflicht erhoben.

Ziel der Befragungsstudie war ein repräsentatives Abbild der Schweizer KMU-Landschaft bezüglich Cyberrisk (Stellenwert, Awareness, Einstellung), die als Grundlage für weitere Entscheidungen dienen soll.

2.2 Konzept und Fragebogen

Es war ausdrücklich das Ziel dieser Studie, das Wissen und die (subjektive) Meinung der KMU-GeschäftsführerInnen und nicht dasjenige der IT-Fachpersonen zu erheben, da die Geschäftsführenden die massgeblichen EntscheiderInnen über die Priorität und das Budget von Sicherheitsmassnahmen sind.

Die Komplexität der Daten- und Kommunikationssicherheit wächst kontinuierlich aufgrund der fortschreitenden Digitalisierung, dabei ist es für Geschäftsführende kaum möglich, mit dem nötigen Fachwissen aktuell zu bleiben.

Aufgrund dieses Settings wurde bewusst auf Fachtermini verzichtet und der Fragebogen möglichst allgemeinverständlich gestaltet. Trotzdem waren einzelne Befragte teilweise mit der Komplexität des Themas überfordert; dies ist bei der Analyse und Interpretation zu berücksichtigen.

Der Fragebogen wurde unter Anleitung von gfs-zürich von einem interdisziplinären Fach-Team aus der ICT-, Versicherungs- und Zertifizierungsbranche sowie der Informatiksteuerung des Bundes entwickelt und in die fünf Themenbereiche Awareness, Massnahmen, Mindeststandards, Meldepflicht und Cyber-Versicherung unterteilt. Die durchschnittliche Interviewdauer lag bei 14 Minuten.

2.3 Befragung und Stichprobe

Die Befragung wurde vom 13. bis 27. September 2017 mit GeschäftsführerInnen von KMUs (1 bis 249 Mitarbeitende) in der deutsch-, französisch- und italienischsprachigen Schweiz durchgeführt. Es handelt sich um eine disproportionale Stichprobe, d.h. die Firmengrössen wurden nicht gemäss ihrem effektiven Anteil an der gesamten Schweizer KMU-Landschaft befragt, sondern über- bzw. unterproportional. Mit dieser Vorgehensweise wurde sichergestellt, dass auch mit den kleinen (10-49 Mitarbeitende) und mittleren KMUs (50-249 Mitarbeitende) genügend Interviews durchgeführt wurden, um über sie eine statistisch abgesicherte Aussage machen zu können. Folgende Tabelle zeigt die disproportionale Verteilung der Interviews sowie die effektive Verteilung in der Schweizer KMU-Landschaft:

Grössenklasse (Anzahl Beschäftigte)	Anzahl Interviews in der Stichprobe	%-Anteil in der Stichprobe	Anzahl Unternehmen in der Schweiz	%-Anteil in der Schweiz
Mikrounternehmen (1-9 Mitarbeitende)	100	33.3%	522'380	90%
Kleine Unternehmen (10-49 Mitarbeitende)	100	33.3%	49'130	8.5%
Mittlere Unternehmen (50-249 Mitarbeitende)	100	33.3%	8'881	1.5%
Total	**300**	**100%**	**580'391**	**100%**

Quelle: BFS, Statistik der Unternehmensstruktur (STATENT), provisorische Zahlen für 2015
https://www.kmu.admin.ch/kmu/de/home/kmu-politik/kmu-politik-zahlen-und-fakten/kmu-in-zahlen/firmen-und-beschaeftigte.html

Für Aussagen über die gesamten Schweizer KMUs wurde die Stichprobe entsprechend der effektiven KMU-Verteilung pro Schweizer Grossregion (Espace Mittelland, Genferseeregion, Ost-/NW-/Zentral-Schweiz, Zürich, Tessin) gewichtet.

Die Adressen stammen von einem Schweizer Adressbroker aus einem Potential von über 100'000 Adressen. Sie wurden nach Sprachregion und Firmengrösse vorgeschichtet, die Quotierung erfolgte gemäss den am Telefon erhobenen Antworten (Region und Firmengrösse). Die Ausschöpfung lag bei 13%, was für die Zielgruppe „GeschäftsführerInnen" ein üblicher Wert ist.

3 Ergebnisse

3.1 Stellenwert der IT und IT-Sicherheit in den KMUs

Zum Einstieg in die Befragung wurde mit verschiedenen Fragen der Stellenwert der IT und der IT-Sicherheit sowie der gefühlte Informationsstand der GeschäftsführerInnen abgefragt.

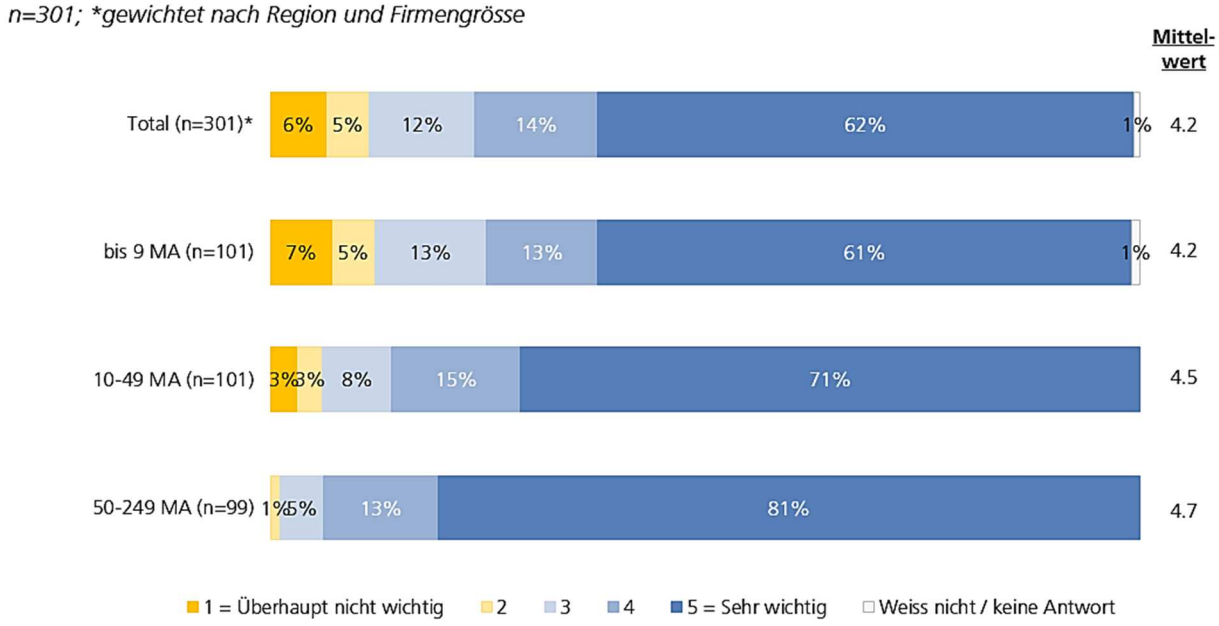
Eine vollständige Erhebung der Risk Exposure („Risiko-Ausgesetztheit“) ist im Rahmen einer telefonischen Befragung nicht möglich, sondern würde einen Expertenbesuch vor Ort bedingen. In der hier vorliegenden Studie wurde eine Auswahl von Faktoren, welche sich auf die Risk Exposure auswirken, abgefragt. Bei der Interpretation der Resultate ist zu berücksichtigen, dass es sich bei den Antworten um die subjektive Einschätzung der GeschäftsführerInnen handelt.

3.1.1 Wichtigkeit der IT

Je nach Tätigkeitsbereich, Grösse und Organisation einer Firma sind die Risiken und Auswirkungen eines Cyberangriffs von unterschiedlicher Tragweite. Ein Velomechaniker mit drei Angestellten, der mit einem einzigen Computer gelegentlich Ersatzteile bestellt, hat verständlicherweise eine andere Einstellung zu Cyberrisiken als ein Software-Entwickler mit ebenfalls drei Angestellten, der über diverse sensible (Kunden-)Daten verfügt. Die Firmengrösse allein ist deshalb noch kein Indikator für die Risk Exposure. Auch die Branchenzugehörigkeit gibt noch zu wenig Auskunft, gibt es doch beispielsweise innerhalb der Industriebranche diverse unterschiedliche Szenarien, die zu einer höheren oder tieferen Risk Exposure führen. Deshalb wurde in der Befragung zuerst einmal die Wichtigkeit einer funktionierenden IT abgefragt, um eine entsprechende Unterteilung vornehmen zu können. Unternehmen, welche das Funktionieren ihrer IT als wichtig bis sehr wichtig bezeichnen (Skalenwerte 4-5 auf einer 5er Skala), müssten theoretisch auch eine höhere Sensibilität gegenüber dem Thema Cybersicherheit haben.

Rund zwei Drittel der Befragten (62%) bewerten das kontinuierliche Funktionieren ihrer IT als sehr wichtig. Je grösser das Unternehmen, desto wichtiger ist dieser Aspekt für die Befragten – trotzdem gibt es auch bei den Firmen mit 10-49 Mitarbeitenden noch einen kleinen Anteil (3%) welche eine funktionierende IT als „überhaupt nicht wichtig“ bezeichnen.

C5: Wie wichtig ist das kontinuierliche Funktionieren der IT für Ihr Unternehmen?
*n=301; *gewichtet nach Region und Firmengrösse*

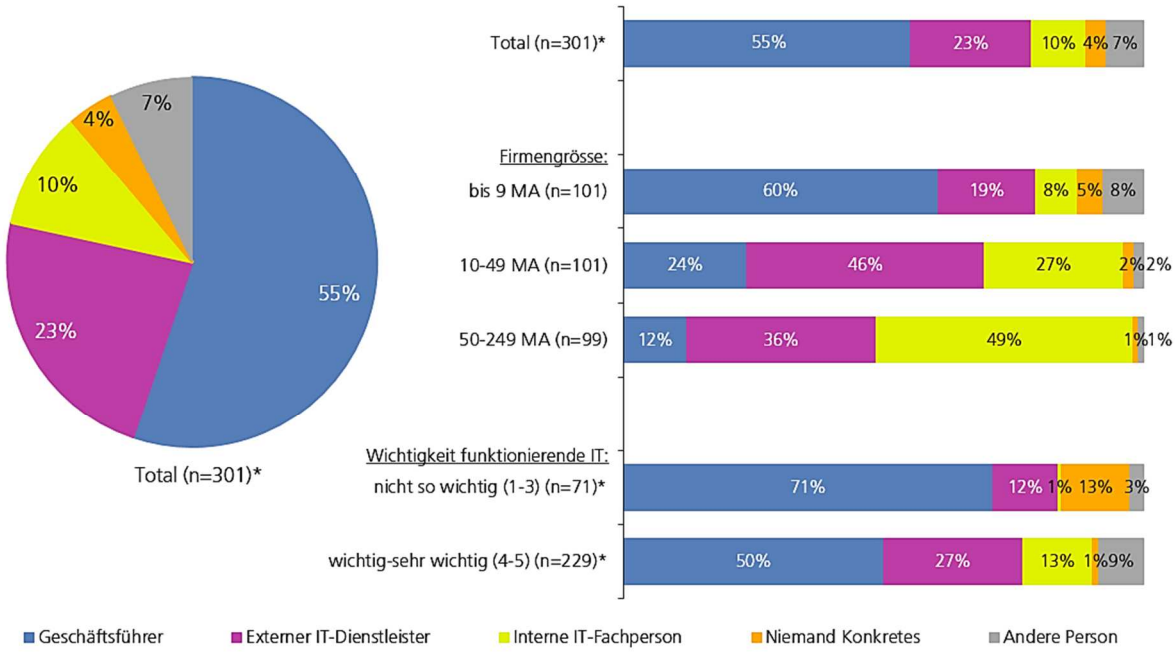


3.1.2 Verantwortlichkeit für IT-Sicherheit

Bei über der Hälfte der Unternehmen (55%) ist der/die GeschäftsführerIn selber für die IT-Sicherheit verantwortlich. Je grösser die Firma ist und je wichtiger das Funktionieren der IT eingeschätzt wird, desto eher wird eine interne oder externe Fachperson für die Sicherheit eingesetzt.

Bei den Firmen, die „niemand konkretes" in der Verantwortung für die IT-Sicherheit angeben, handelt es sich vorwiegend um Firmen, die das Funktionieren der IT als eher unwichtig bezeichnen und die weniger als 10 Mitarbeitende haben.

C6: Wer ist bei Ihnen für die IT-Sicherheit verantwortlich?
*n=301; *gewichtet nach Region und Firmengrösse*



3.1.3 Informationsgrad

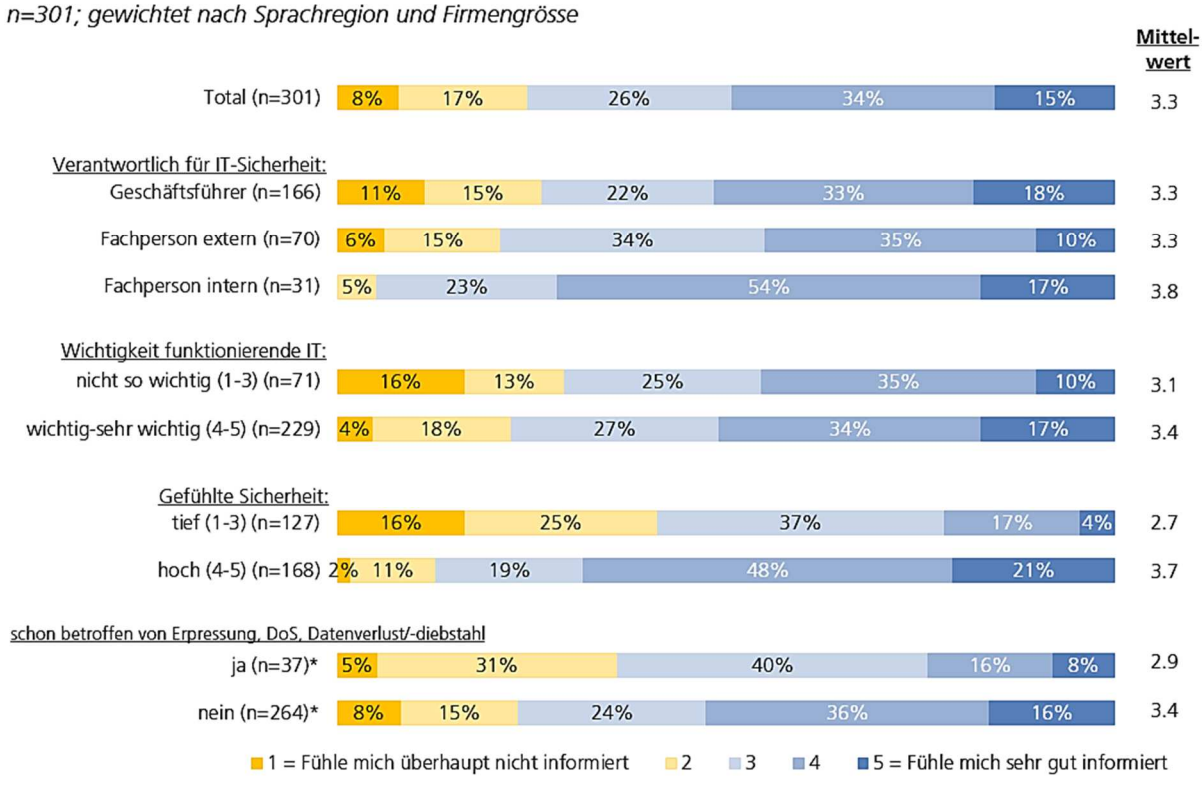
Knapp die Hälfte der befragten GeschäftsführerInnen (49%) fühlt sich gut bis sehr gut, ein Viertel fühlt sich eher nicht bis überhaupt nicht über die Cyberrisk-Thematik informiert (25%).

In Unternehmen, in denen eine funktionierende IT wichtig bis sehr wichtig ist, fühlen sich die Befragten signifikant besser informiert (Mittelwert 3.4) als wenn die IT nicht so wichtig ist (Mittelwert 3.1). Gleiches gilt für die gefühlte Sicherheit: Fühlen sich die Befragten eher bis sehr sicher, schätzen sie auch ihren Informationsgrad höher ein (Mittelwert 3.7) als wenn sie sich weniger sicher fühlen (Mittelwert 2.7).

Dass der gefühlte hohe Informationsgrad mit dem Sicherheitsgefühl positiv korreliert, bedeutet nicht zwingend, dass das Sicherheitsgefühl vom hohen Informationsgrad herrührt; ein kausaler Zusammenhang kann mit dieser Studie nicht nachgewiesen werden. Es kann durchaus auch gerade umgekehrt der Fall sein, dass die Befragten sich in falscher Sicherheit wiegen, weil ihr Informationsgrad nur gefühlt hoch, in Wirklichkeit aber eher zu tief ist. Hinweise auf einen zu tiefen Informationsgrad finden sich z.B. im Kapitel 3.2.2, wo die tiefe Risiko-Einschätzung trotz der hohen Betroffenheitszahlen von Cyberangriffen besprochen wird, und im Kapitel 3.3.2, wo sich die umgesetzten Sicherheits-Massnahmen als eher tief erweisen.

Ausserdem zeigt sich auch, dass Befragte, welche bereits einmal von einem Cyberangriff betroffen waren, sich signifikant schlechter informiert fühlen (Mittelwert 2.9) als Befragte, welche keine Angriffserfahrungen haben (Mittelwert 3.4). Dies obwohl sie wahrscheinlich durch den Lernprozess nach dem Angriff in Wirklichkeit über ein höheres Fachwissen verfügen. Es scheint deshalb, dass mit steigendem Wissen auch die Unsicherheit steigt bzw. der gefühlte Informationsgrad sinkt.

F1: Ganz allgemein: Wie gut fühlen Sie sich persönlich in der Cyberrisk-Thematik informiert?
n=301; gewichtet nach Sprachregion und Firmengrösse

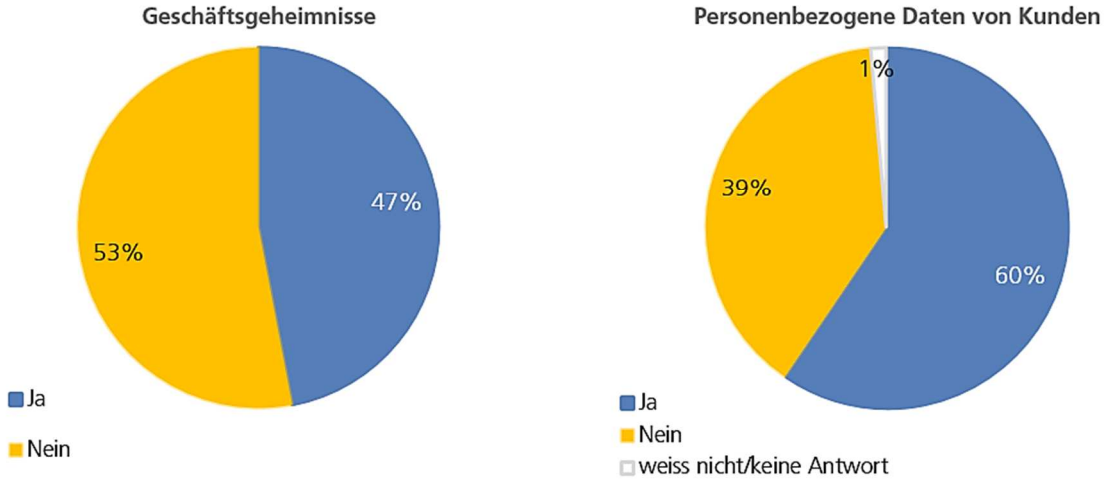


3.1.4 Sensitive Daten

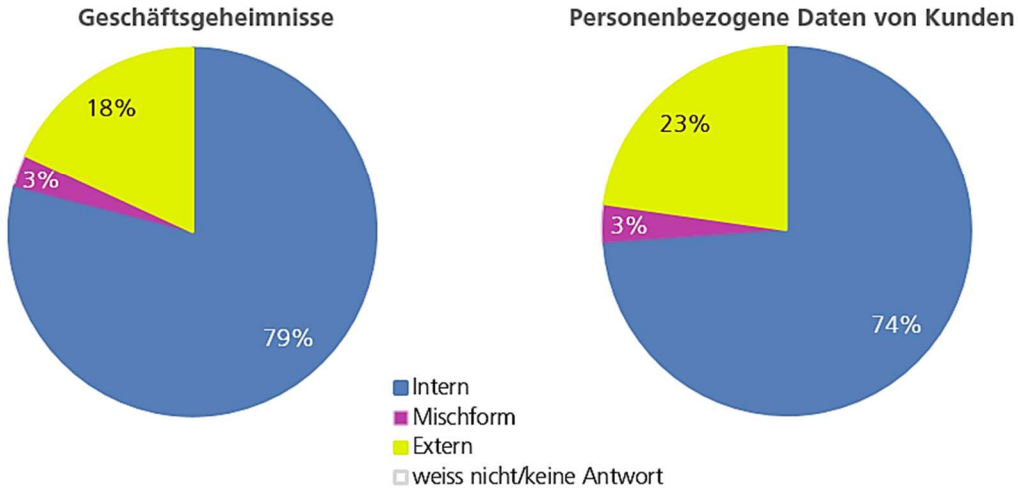
Um die Betroffenheit der befragten Unternehmen bezüglich sensitiver Daten abschätzen zu können, wurden explizit die Bewirtschaftung von Geschäftsgeheimnissen und personenbezogenen Daten von Kunden abgefragt. In beiden Fällen ist eine erhöhte Wachsamkeit vor Cyberangriffen angebracht.

Knapp die Hälfte der befragten Firmen bewirtschaftet Geschäftsgeheimnisse (47%) und drei von fünf Firmen verwalten personenbezogene Kundendaten (60%).

F3A: Bewirtschaften Sie sensitive Daten wie…
n=301; gewichtet nach Region und Firmengrösse



F3B: Sind diese Daten intern oder extern gespeichert, oder besteht eine Mischform?
Filter 1: Falls sensitive Daten (Geschäftsgeheimnisse) bewirtschaftet werden (n=142)
Filter 2: Falls sensitive Daten (Personenbezogene Daten von Kunden) bewirtschaftet werden (n=179)
gewichtet nach Region und Firmengrösse



Von sensitiven Daten betroffene KMUs bevorzugen in rund drei Vierteln der Fälle (79% bzw. 74%) interne Speicherlösungen. Rund ein Fünftel (18%) respektive rund ein Viertel (23%) der Befragten speichern ihre sensitiven Daten extern, bei 3 Prozent besteht eine Mischform von interner und externer Speicherung.

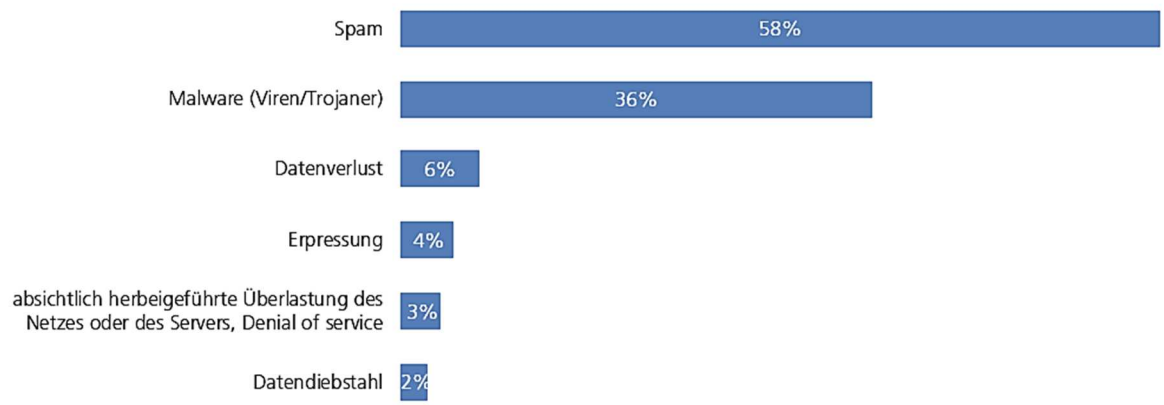
3.2 Erfahrung und Awareness Cyberrisiken

3.2.1 Erfahrung mit Cyberangriffen

Rund drei von fünf Unternehmen (58%) waren schon von Spam betroffen. Es ist davon auszugehen, dass die übrigen Befragten wohl ebenfalls Spam-Mails erhalten, diese aber durch einen Spamfilter oder dank gut geschulten Mitarbeitenden nicht als Gefahr oder „Angriff" wahrgenommen werden.

Damit ist Spam der am häufigsten genannte Cyberangriff, gefolgt von Malware wie Viren oder Trojanern, welche von rund jedem dritten Unternehmen (36%) genannt wird.

F4: War Ihre KMU schon betroffen von den folgenden Cyberangriffen?
n=301; gewichtet nach Region und Firmengrösse



Die weiteren Angriffsarten wie Datenverlust (6%), Erpressung (4%), DoS (absichtlich herbeigeführte Überlastung des Netzes oder Servers, „Denial of Service") (3%) oder Datendiebstahl (2%) sind im Vergleich dazu selten. Trotzdem dürfen sie keinesfalls verharmlost werden, denn die Folgen eines entsprechenden Angriffs können gross sein. Eine Hochrechnung auf Basis der hier erhobenen Daten auf alle Schweizer KMUs (580'391 KMUs, Stand 2015) ergibt folgende Schätzung:

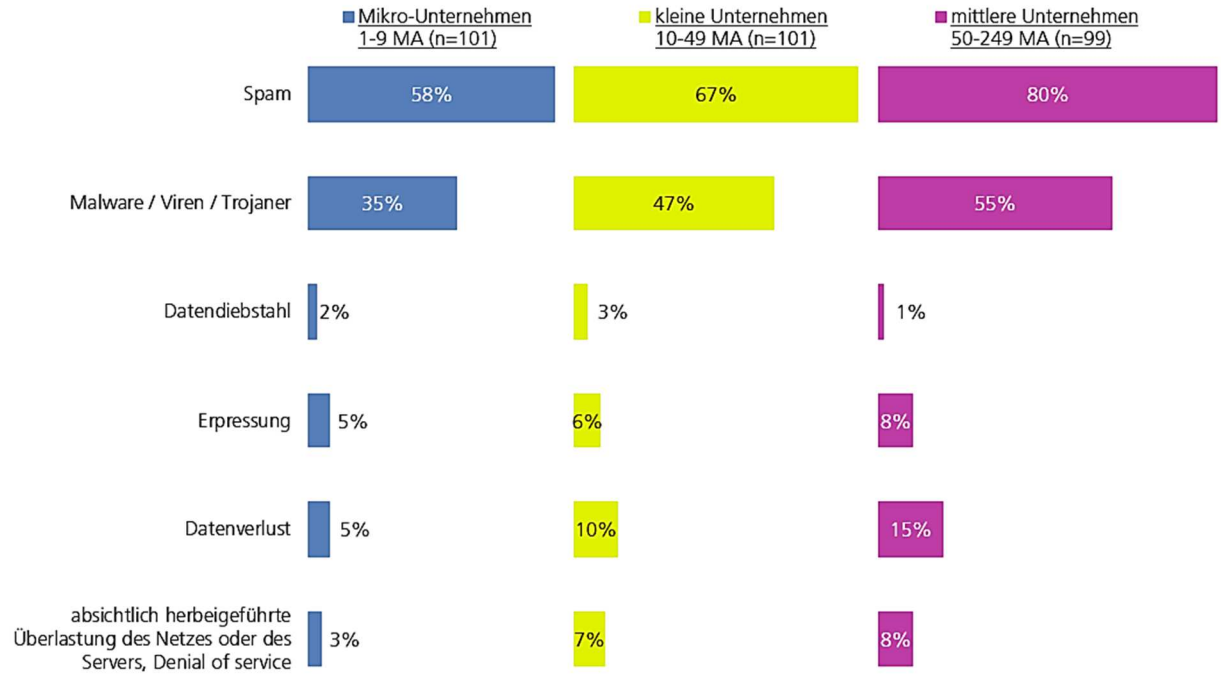
	Geschätzte Anzahl betroffener KMUs	**Spannbreite unter Berücksichtigung des Vertrauensintervalls** (bei einem Sicherheitsmass von 95% bzw. einer Fehlerwahrscheinlichkeit von 5%)
Spam (58%)	337'000	303'600 - 370'000
Malware wie Viren oder Trojaner (36%)	209'000	176'800 - 241'100
Datenverlust (6%)	35'000	18'900 - 50'700
Erpressungsfälle (4%)	23'000	10'100 - 36'300
DoS (3%)	17'000	6'000 - 28'800
Datendiebstahl (2%)	12'000	2'200 - 21'000

Die Höhe dieser Zahlen hat die Studienautoren überrascht; eine zukünftige Verminderung der Angriffsfälle dürfte im Interesse der Volkswirtschaft und der allgemeinen Sicherheit anzustreben sein.

Je grösser eine Firma ist, desto eher war sie schon von einem Cyberangriff betroffen. Dennoch werden nicht nur mittlere KMUs angegriffen. Auch Mikro- und kleine Unternehmen nennen Cyberangriffe. So waren zum Beispiel knapp drei von fünf Mikro-Unternehmen schon von Spam betroffen (58%), rund zwei Drittel von den kleinen Unternehmen (67%) und vier von fünf mittleren Unternehmen (80%).

Jedes zwanzigste Mikro-Unternehmen war schon von Erpressung oder Datenverlust (je 5%) betroffen. Zieht man in Betracht, dass die Mikro-Unternehmen rund 90 Prozent von allen Schweizer KMUs ausmachen, ist dies eine beachtliche Zahl.

4: War Ihre KMU schon betroffen von den folgenden Cyberangriffen?
n=301



3.2.2 Risiko-Einschätzung

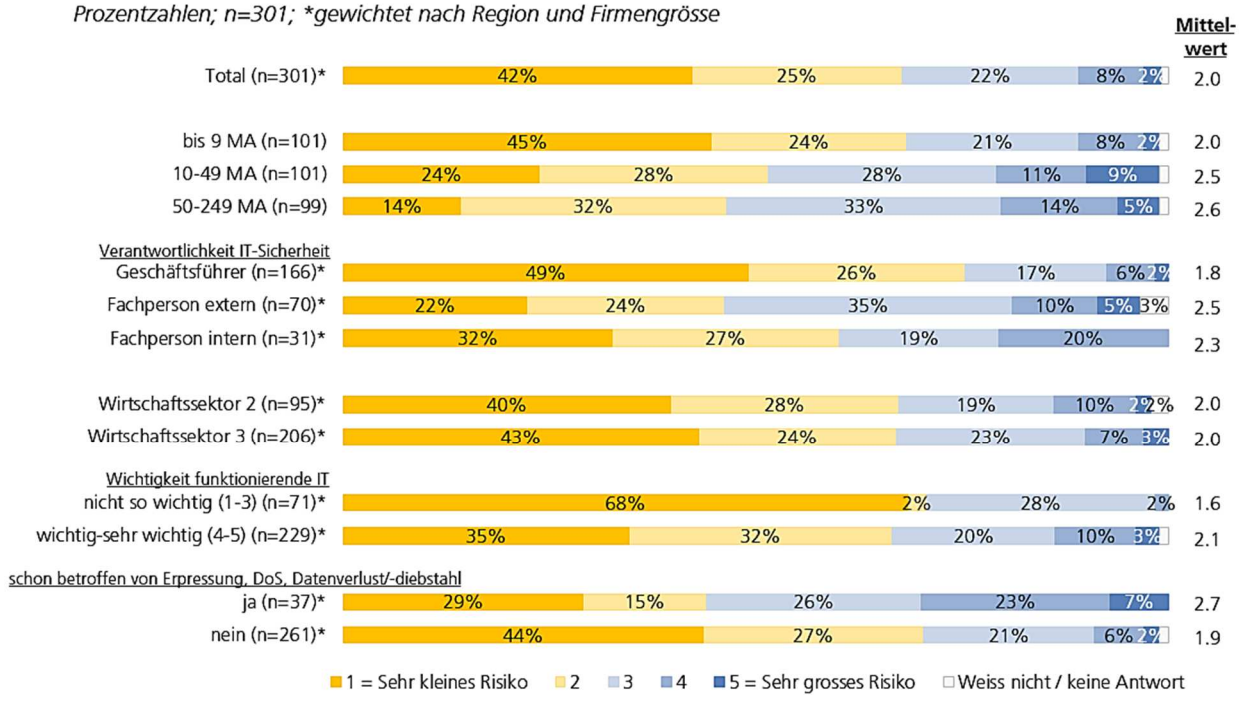
Um die befürchteten Auswirkungen eines Angriffs quantifizieren zu können, wurden die Befragten nach zwei verschiedenen Risiko-Einschätzungen gefragt: Zuerst nach dem Risiko, durch einen Angriff einen Tag lang „ausser Gefecht" zu sein, dann nach einem existenzgefährdenden Risiko.

Nur jedes zehnte Unternehmen (10%) schätzt das Risiko, durch einen Cyberangriff einen Tag ausser Kraft gesetzt zu werden, als gross bis sehr gross (Skalenwerte 4-5 auf 5er Skala) ein. Die Risiko-Einschätzung steigt mit zunehmender Grösse des Unternehmens.

Diejenigen GeschäftsführerInnen, die selbst für die IT-Sicherheit verantwortlich sind, bezeichnen das Risiko, einen Tag lang ausser Kraft gesetzt zu werden, als besonders tief (49% „sehr kleines Risiko"). Bei denjenigen Firmen, die ihre IT-Sicherheit an eine interne oder externe Fachperson delegiert haben, ist die Risiko-Einschätzung höher: Die Kausalität wird in diesem Falle so herum zu interpretieren sein, dass eine höhere Risiko-Einschätzung dazu führt, dass eine interne oder externe Fachperson eingesetzt wird.

Wer schon einmal betroffen war von einem Angriff, stuft das Risiko eines erneuten Angriffs signifikant höher ein (Mittelwert 2.7) als die bisher nicht betroffenen (Mittelwert 1.9).

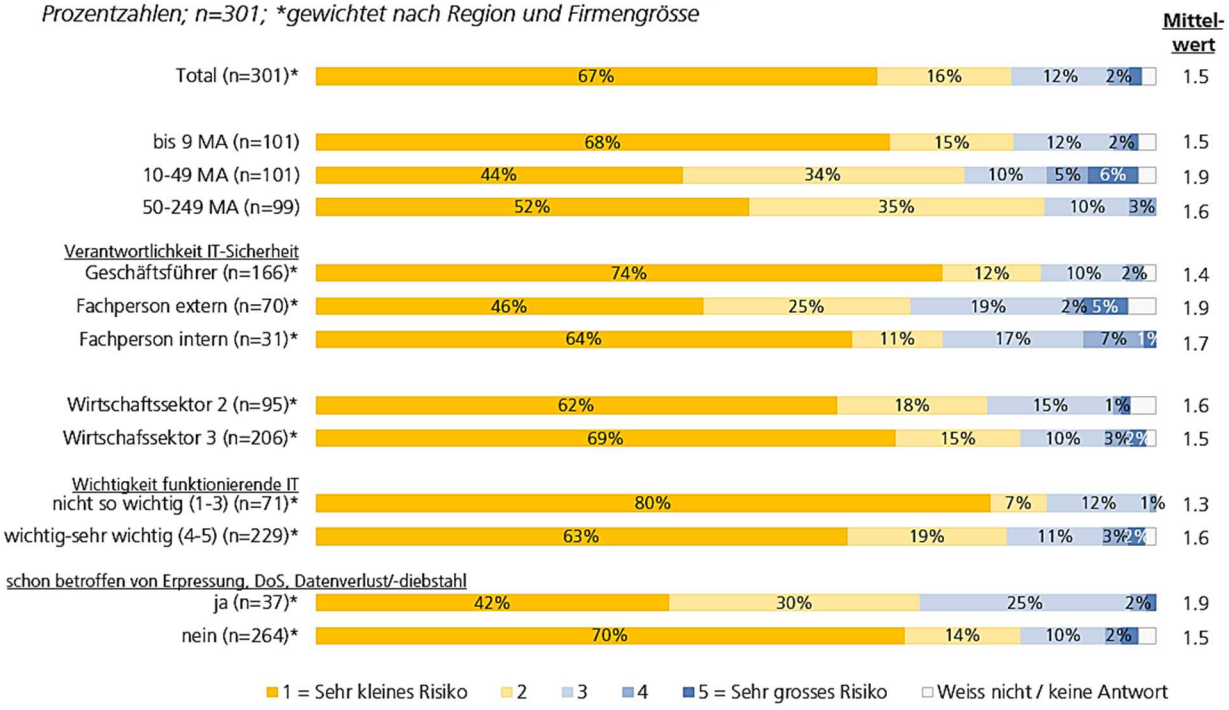
F5: Als wie hoch schätzen Sie das Risiko ein, dass Ihr KMU innerhalb von den nächsten 2-3 Jahren von einem Cyberangriff betroffen wird, welcher Ihr Geschäft mindestens einen Tag lang ausser Kraft setzt?
*Prozentzahlen; n=301; *gewichtet nach Region und Firmengrösse*



Das Risiko einer Existenzgefährdung wird von allen Befragungsgruppen als noch tiefer eingeschätzt – rund zwei Drittel (67%) von allen Befragten beurteilen das Risiko als sehr klein (Skalenwert 1 auf 5er Skala). Auch diejenigen GeschäftsführerInnen, welche ihre IT als wichtig bis sehr wichtig bezeichnen, sehen zu rund zwei Dritteln (63%) nur ein sehr kleines Risiko für ihre Existenz.

Die tiefe Einschätzung des Risikos steht im starken Widerspruch zu den Betroffenheitszahlen aus dem vorherigen Kapitel (3.2.1) und es liegt der Verdacht nahe, dass die Zahl von Angriffen und die damit verbundenen Folgen zu wenig bekannt und bewusst sind. Insofern müsste ein höherer Informationsgrad auch zu einer höheren Risiko-Einschätzung führen.

F6: Als wie hoch schätzen Sie das Risiko ein, dass Ihr KMU innerhalb von den nächsten 2-3 Jahren von einem Cyberangriff betroffen sein wird, welcher für Ihr Geschäft existenzgefährdend ist?
*Prozentzahlen; n=301; *gewichtet nach Region und Firmengrösse*



3.2.3 Gefühlter Schutz

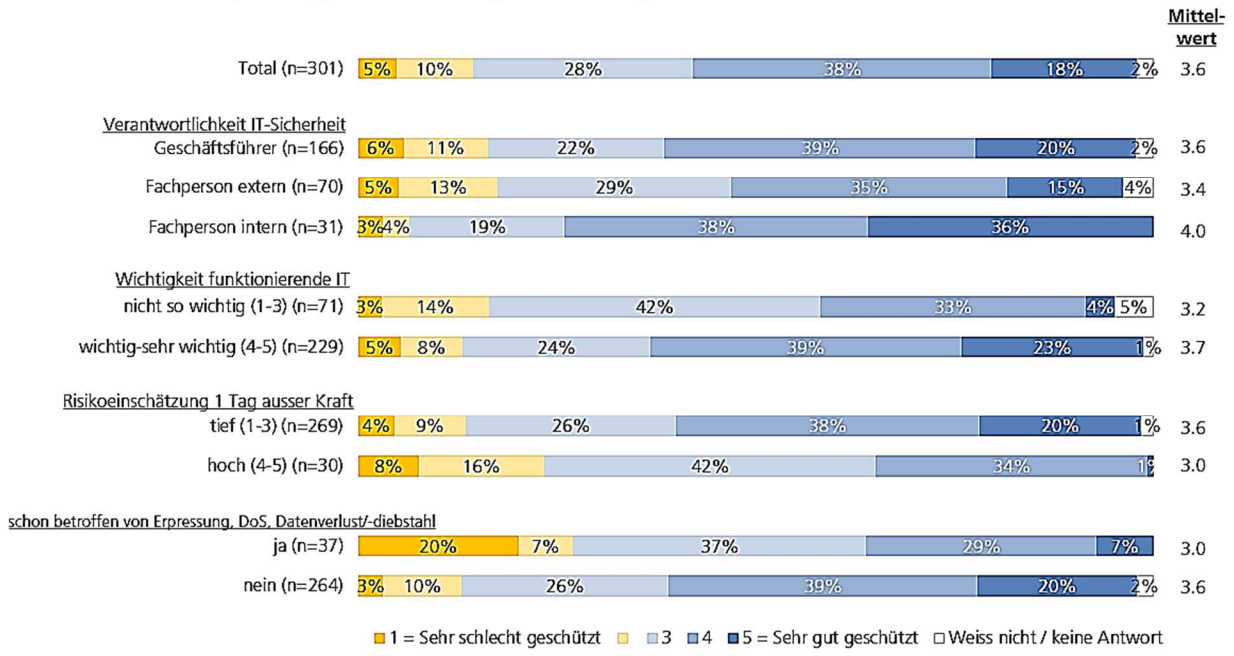
Das Sicherheitsempfinden kann durch den Informationsgrad, die Umsetzung von Schutzmassnahmen, durch das Vertrauen in zuständige Fachpersonen, aber auch durch das Risikoempfinden beeinflusst werden. Die Umsetzung von vielen Schutzmassnahmen führt aber nicht zwingend zu einem hohen Sicherheitsempfinden, sondern kann durch den steigenden Informationsgrad durchaus auch zu noch mehr Unsicherheit führen (siehe auch Kap. 3.3.2).

Bei den folgenden Zahlen handelt es sich daher wieder um die subjektive Meinung der befragten GeschäftsführerInnen und es können keine Rückschlüsse auf die effektiv umgesetzten Massnahmen gezogen werden (die Massnahmen werden im Kapitel 3.3.2 behandelt).

Mehr als die Hälfte der Befragten (56%) beurteilt den eigenen Schutz als gut bis sehr gut. Unternehmen, in denen das Funktionieren der IT wichtig bis sehr wichtig ist und Unternehmen, welche für die IT-Sicherheit eine interne Fachperson beauftragt haben, fühlen sich besser geschützt.

Wer das Angriffs-Risiko hoch einschätzt oder schon einmal betroffen war, empfindet den eigenen Schutz als signifikant tiefer als diejenigen, die das Risiko als tief einschätzen bzw. nicht von einem Cyberangriff betroffen waren. Es ist anzunehmen, dass dies zwar der subjektiven Wahrnehmung der Betroffenen entspricht, eine objektive Einschätzung jedoch zu einem anderen Ergebnis käme: Die höhere Risiko-Einschätzung bzw. die gemachten Erfahrungen aufgrund des Angriffes führen wahrscheinlich zu einem höheren Informationsgrad und zu höheren Ansprüchen an einen effektiven Cyberschutz, was wiederum zu einer tieferen Sicherheits-Einschätzung auf der Fünferskala führt.

F7: Wie gut fühlen Sie sich generell vor Cyberangriffen geschützt?
Prozentzahlen; *n=301; gewichtet nach Region und Firmengrösse*

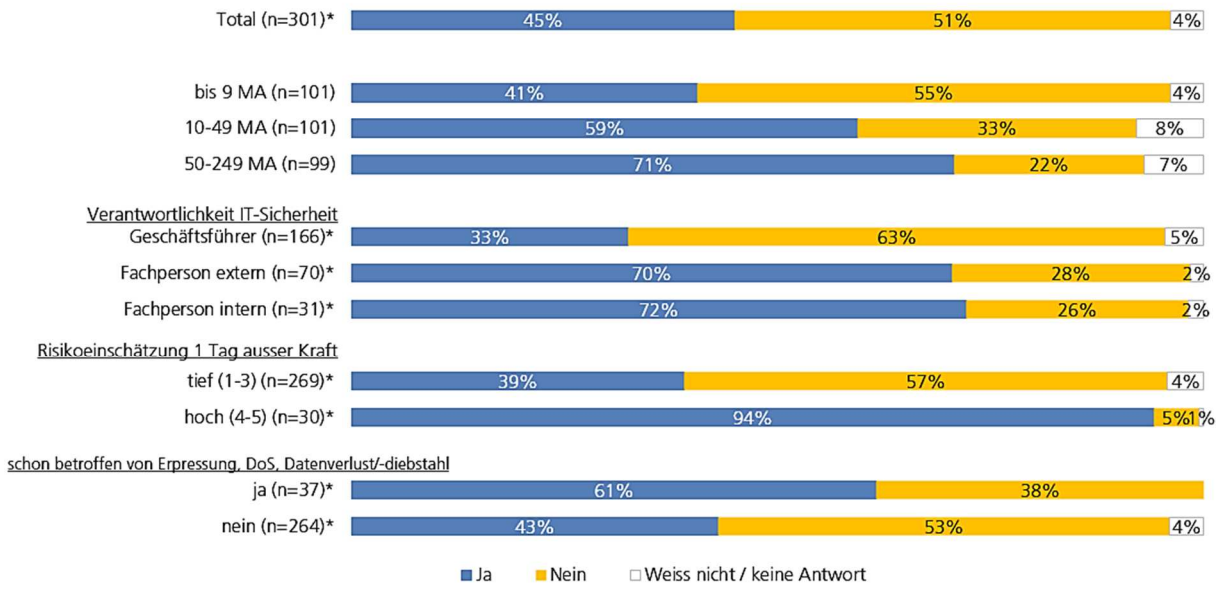


3.3 Umsetzung von Massnahmen

3.3.1 Geplante Verbesserung des Schutzes gegen Cyberangriffe

Fast die Hälfte der Befragten (45%) plant in den nächsten 2-3 Jahren ihren Schutz zu verbessern. Je grösser das Unternehmen, desto eher wird eine Verbesserung beim Cyberschutz in Angriff genommen. Besonders hoch ist die Verbesserungs-Absicht bei Unternehmen, in denen das Risiko eines Angriffs hoch eingeschätzt wird (94%). Aber auch bereits einmal von Angriffen betroffene Unternehmen beabsichtigen signifikant häufiger (61%), ihren Schutz zu verbessern, als solche die noch keine entsprechenden Erfahrungen gemacht haben (43%).

F8: Beabsichtigen Sie, innerhalb der nächsten 2-3 Jahre Ihren Schutz gegen Cyberangriffe zu verbessern?
Prozentzahlen; *n=301; *gewichtet nach Region und Firmengrösse*



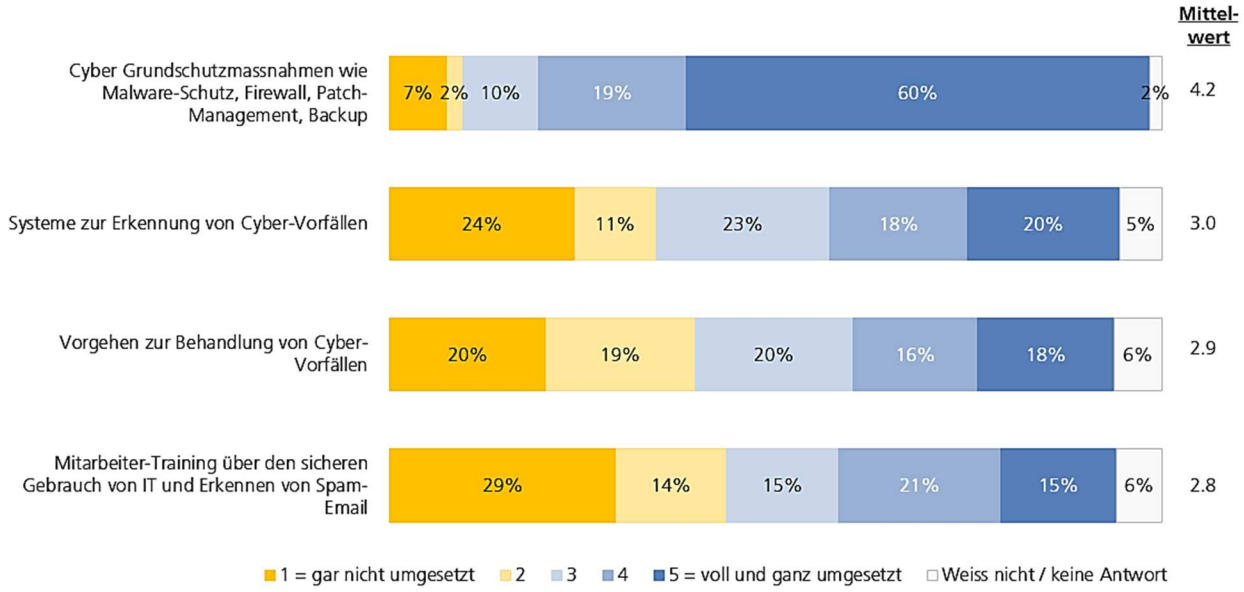
3.3.2 Umgesetzte Sicherheitsmassnahmen

Rund vier von fünf Unternehmen (79%) haben technische Grundschutzmassnahmen eher bzw. voll und ganz (Skalenwerte 4-5 auf 5er Skala) umgesetzt. Über Erkennungssysteme (38%) oder ein Kontinuitäts-Management (34%) verfügen nur noch gut ein Drittel der Unternehmen. Noch tiefer sind die Werte beim zum Governance Management gehörenden Mitarbeiter-Trainings über den sicheren Gebrauch von IT.

Auffallend: Die tiefste Umsetzungs-Einschätzung erhält der einzige nicht-technische abgefragte Sicherheitsbereich, nämlich das Training der Mitarbeitenden über den sicheren Gebrauch der IT und das Erkennen von Spam-Email. Knapp ein Drittel der Befragten (29%) beurteilt diesen Bereich als „gar nicht umgesetzt" und nur gut jeder Siebte als „voll und ganz umgesetzt" (15%). Dies obwohl die Komplexität bei der Umsetzung wohl tiefer sein dürfte als bei den anderen Massnahmen. Möglicherweise wird die Notwendigkeit oder der Nutzen von Mitarbeiter-Training als nicht sehr

hoch eingeschätzt, was in Anbetracht der hohen Betroffenheitszahlen von Cyberangriffen als Risikofaktor zählen dürfte.

F9: Welche der folgenden Sicherheitsmassnahmen sind bei Ihnen umgesetzt?
n=301; gewichtet nach Region und Firmengrösse



Ist das Funktionieren der IT in einem Unternehmen wichtig bis sehr wichtig, führt dies bei allen abgefragten Sicherheitsmassnahmen zu signifikant höheren Nennungen bezüglich der Umsetzung. Gleiches gilt für die IT-Sicherheits-Verantwortlichkeit: Ist diese an eine interne oder externe Fachperson delegiert, werden signifikant mehr Sicherheitsmassnahmen umgesetzt.

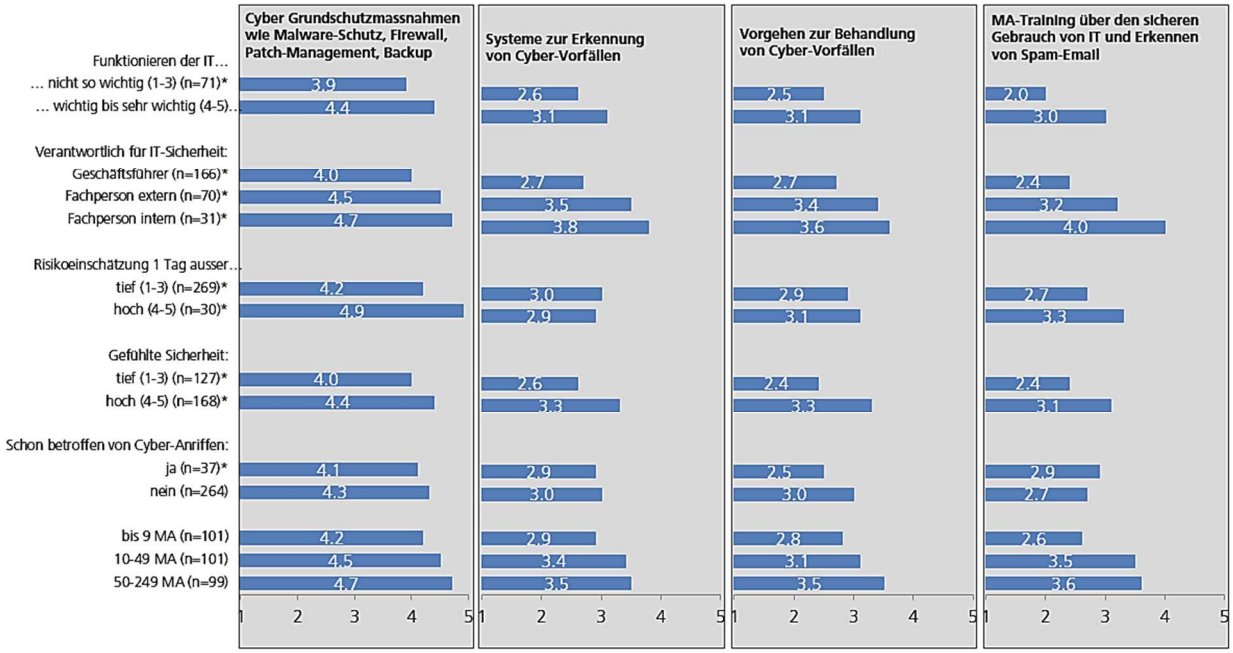
Befragte, die ein höheres Sicherheitsgefühl angeben, setzen auch sämtliche abgefragten Sicherheitsmassnahmen signifikant häufiger um als diejenigen mit einem tiefen Sicherheitsgefühl.

Ausserdem: Je grösser die Firma ist und wenn sensitive Daten vorhanden sind (hier nicht abgebildet), werden mehr Massnahmen umgesetzt.

Wird das Risiko eines Cyberangriffs als hoch bis sehr hoch eingeschätzt, wird die Umsetzung von Cyber-Grundschutzmassnahmen und von Mitarbeiter-Trainings signifikant höher eingeschätzt, nicht aber diejenige von Cyberangriffs-Erkennungssystemen und von Prozessen zur Behandlung von Cyber-Vorfällen (Kontinuitäts-Management). Cyberangriffs-Erkennungssysteme sind evt. zu wenig bekannt oder werden als nicht nötig oder zu teuer betrachtet. Die tiefe Zahl an umgesetzten Prozessen zur Behandlung von Cyber-Vorfällen (Kontinuitätsmanagement) hingegen liegt wohl eher daran, dass gerade in den vielen Mikro-Unternehmen (1-9 Mitarbeitende) wahrscheinlich generell wenige Prozesse schriftlich definiert sind.

Geschäftsführende, welche schon betroffen waren von Cyberangriffen, geben leicht tiefere Massnahmenumsetzungs-Werte an als diejenigen, die noch nicht betroffen waren. Es kann sein dass die Angriffserfahrung tatsächlich nicht zu mehr Sicherheitsmassnahmen geführt hat, es ist aber auch möglich, dass die Betroffenen ihre umgesetzten Massnahmen kritischer beurteilen.

F9: Welche der folgenden Sicherheitsmassnahmen sind bei Ihnen umgesetzt?
*Mittelwerte, n=301; *gewichtet nach Region und Firmengrösse*



3.4 Mindeststandards und Zertifizierung

3.4.1 Verwendete Standardrichtlinien

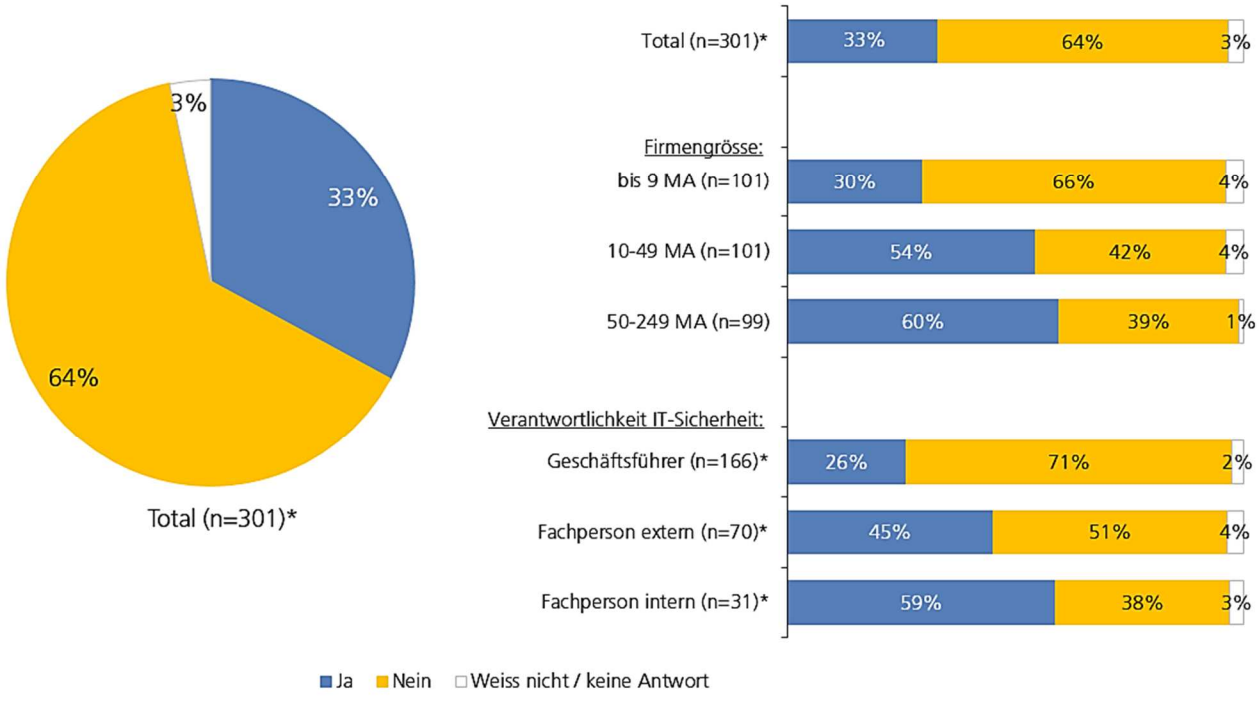
Ein Drittel der befragen GeschäftsführerInnen (33%) verwendet nach eigener Angabe Standardrichtlinien für die IT-Sicherheit. Je grösser das Unternehmen, desto eher werden Standardrichtlinien eingesetzt.

Die Zahl relativiert sich allerdings etwas bei Betrachtung der Folgefrage, bei der nachgehakt wurde, um welche Standardrichtlinien es sich handelt. Von den 99 GeschäftsführerInnen, welchen diese Frage gestellt wurde (weil sie vorher angaben, sich an Standardrichtlinien zu richten), konnte rund jeder sechste die Frage nicht beantworten (16% „weiss nicht / keine Antwort").

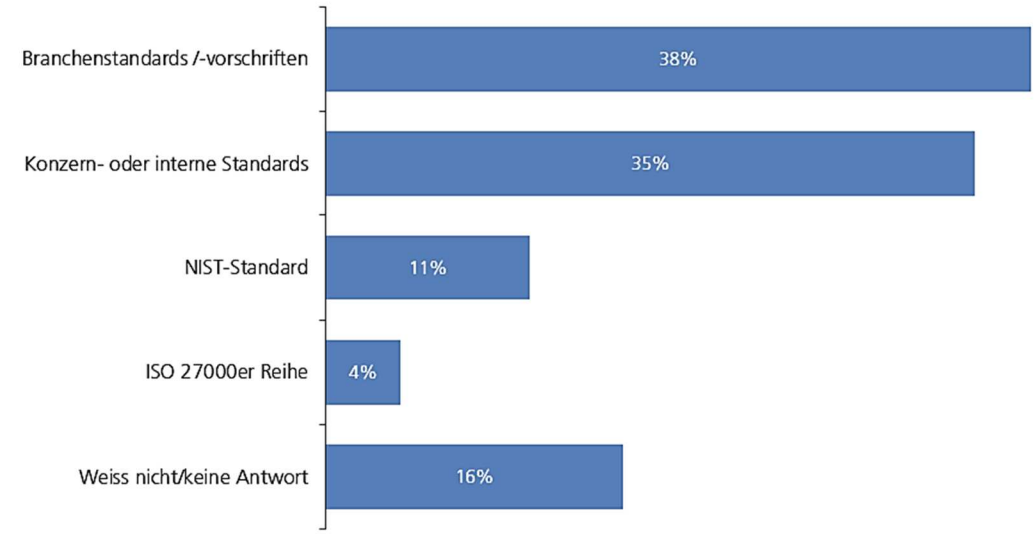
Rund zwei von fünf Unternehmen geben einen „Branchenstandard" (38%) an, knapp ein Drittel nennt Konzern- oder interne Standards (32%). In beiden Fällen kann im Rahmen dieser Studie weder Umfang noch Inhalt interpretiert werden.

Der NIST-Standard und die ISO 27000er Reihe werden von 11 bzw. 4 Prozent genannt.

F10: Gibt es Standardrichtlinien, nach denen Sie sich bei der IT-Sicherheit richten?
*n=301; *gewichtet nach Region und Firmengrösse*



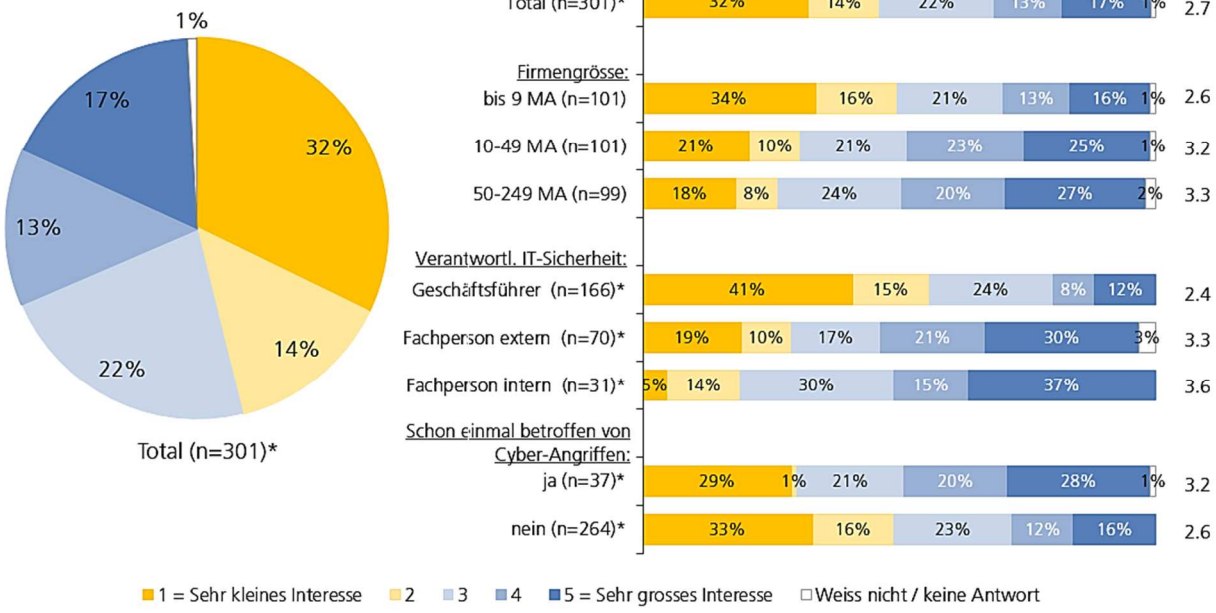
F11: Was für Standardrichtlinien sind das? *Mehrfachnennungen möglich*
Filter: Falls es im Unternehmen Standardrichtlinien für IT-Sicherheit gibt (n=99); gewichtet nach Region und Firmengrösse



3.4.2 Interesse an Sicherheitsmassnahmen-Katalog

Das Interesse an einem Massnahmenkatalog zur IT-Sicherheit ist eher tief: Rund ein Drittel (32%) äussert „sehr kleines Interesse", während am anderen Ende der Skala nur rund ein Sechstel „sehr grosses Interesse" (17%) bekundet. Ist die IT-Sicherheit an eine interne oder externe Fachperson delegiert, ist auch das Interesse an einem Massnahmenkatalog signifikant höher. Wer bereits einmal von einem Cyberangriff betroffen war, äussert ebenfalls signifikant höheres Interesse.

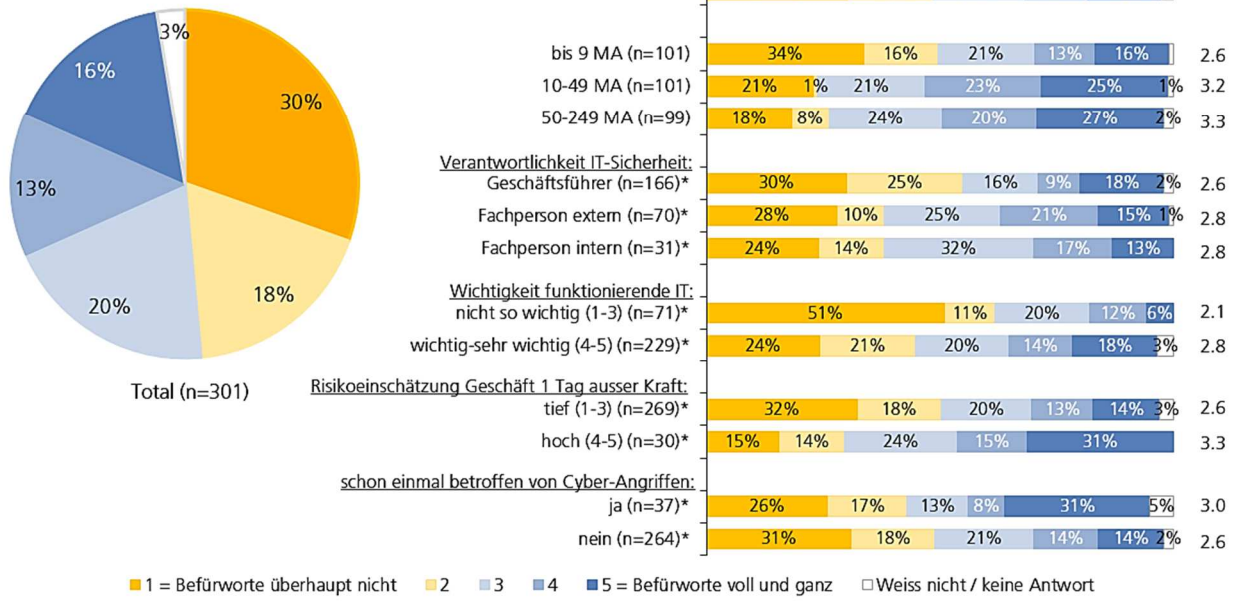
F12: Wie sehr würden Sie sich für einen Katalog von Massnahmen zur IT-Sicherheit interessieren?
*n=301; *gewichtet nach Region und Firmengrösse*



3.4.3 Verpflichtende Mindeststandards

Knapp drei von zehn Befragten (29%) befürworten verpflichtende Mindeststandards eher oder voll und ganz (Skalenwerte 4 und 5 auf 5er-Skala), knapp die Hälfte (48%) lehnt sie sehr oder eher ab (Skalenwerte 1 und 2 auf 5er-Skala). Ein Fünftel der Befragten (20%) ist unentschieden. In Firmen, in denen eine funktionierende IT wichtig bis sehr wichtig ist oder das Risiko eines Angriffs als hoch eingeschätzt wird, werden Mindeststandards signifikant häufiger befürwortet. Je grösser das Unternehmen, desto höher ist auch hier die Zustimmung.

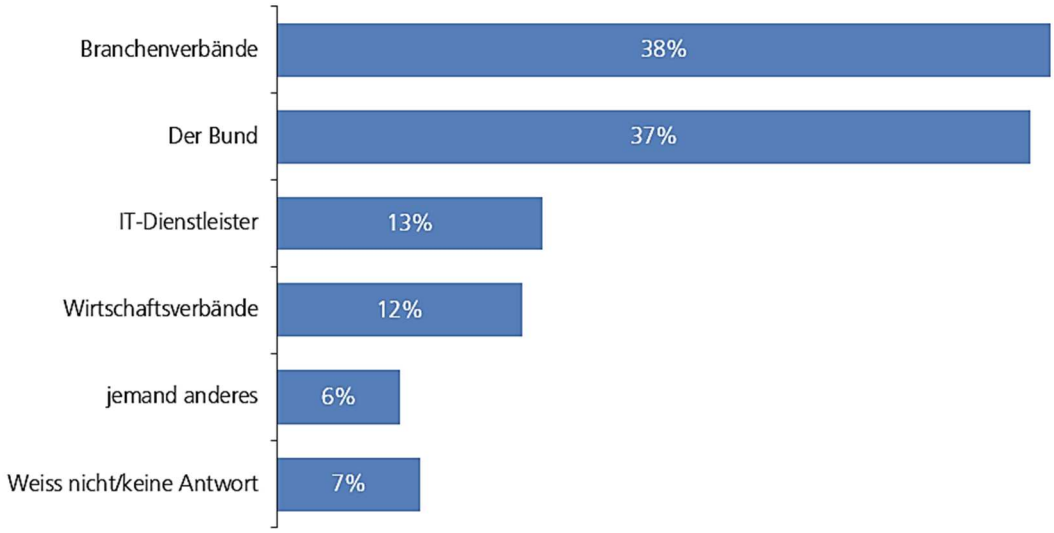
F13: Wie sehr würden Sie verpflichtende Massnahmen für Schweizer Unternehmen im Sinne von Mindeststandards befürworten? *n=301; *gewichtet nach Region und Firmengrösse*



3.4.4 Zuständigkeit für Mindeststandards

Je knapp zwei von fünf Befragten sehen die Zuständigkeit für verpflichtende Mindeststandards bei den Branchenverbänden (38%) bzw. beim Bund (37%). Nur gut jeder achte Befragte nennt IT-Dienstleister (13%) oder Wirtschaftsverbände (12%) als zuständig, wobei davon ausgegangen werden kann, dass mit „Wirtschaftsverbänden" die bekannten Dachverbände wie z.B. economiesuisse gemeint sind.

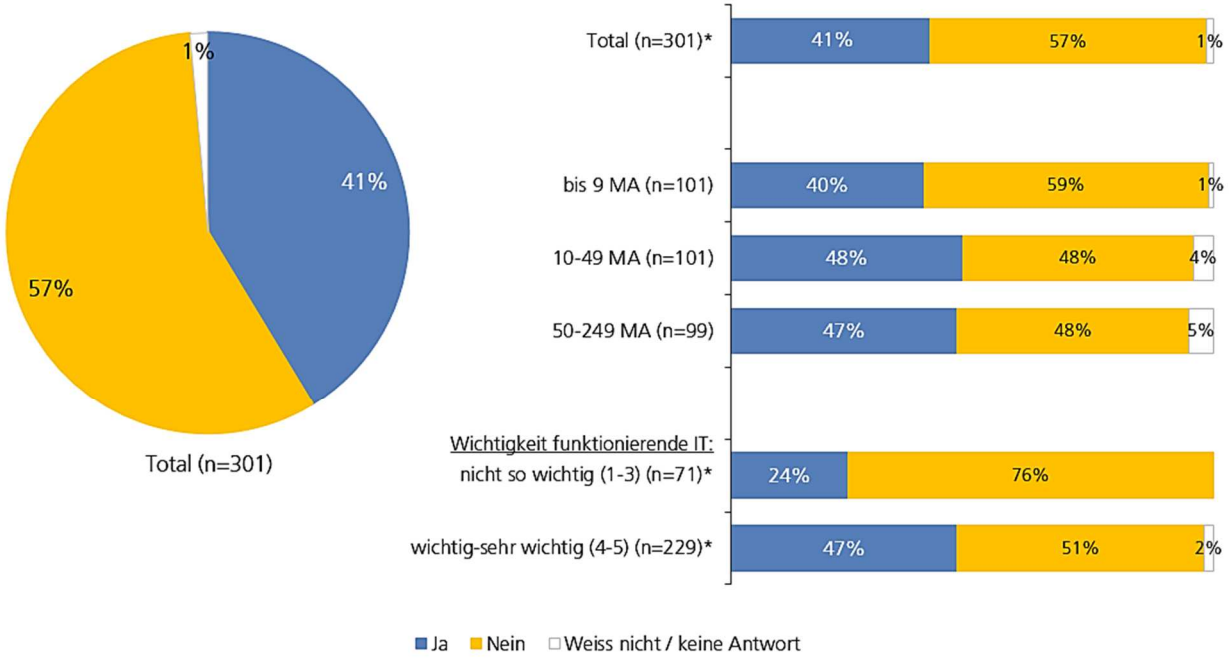
F14: Wer wäre Ihrer Meinung nach zuständig dafür, den Schweizer KMU's einen solchen verpflichtenden Katalog von Mindeststandards vorzugeben?
Mehrfachnennungen möglich; n=301; gewichtet nach Region und Firmengrösse



3.4.5 Landesweite Zertifizierung

Zwei von fünf Befragten (41%) geben an, dass eine landesweite Zertifizierung von Nutzen sein könnte. In Firmen, in denen eine funktionierende IT wichtig bis sehr wichtig ist, wird die Zertifizierung hingegen signifikant nützlicher eingestuft (47%). Tendenziell ist die Zustimmung höher, wenn sensitive Daten zumindest teilweise extern gespeichert werden (nicht abgebildet).

F15: Daten zu Geschäftsgeheimnissen oder Personen können intern oder extern bei einem Datenhoster gespeichert werden. Bitte sagen Sie mir, ob die Einführung von einer landesweiten Zertifizierung für sichere Datenspeicherung und Hosting in der Schweiz für Sie von Nutzen sein könnte.
*n=301; *gewichtet nach Region und Firmengrösse*



3.5 Meldepflicht

3.5.1 Argumente für und gegen eine Meldepflicht

Eine Meldepflicht, welche verlangen würde, dass Firmen und Verwaltungen Cyberangriffe melden müssten, wurde bei den Befragten mit je zwei Pro- und Kontra-Argumenten überprüft. Dabei haben die Pro-Argumente mehr Zustimmung erhalten als Ablehnung; bei den Kontra-Argumenten hielten sich die zustimmenden und ablehnenden Haltungen in etwa die Waage.

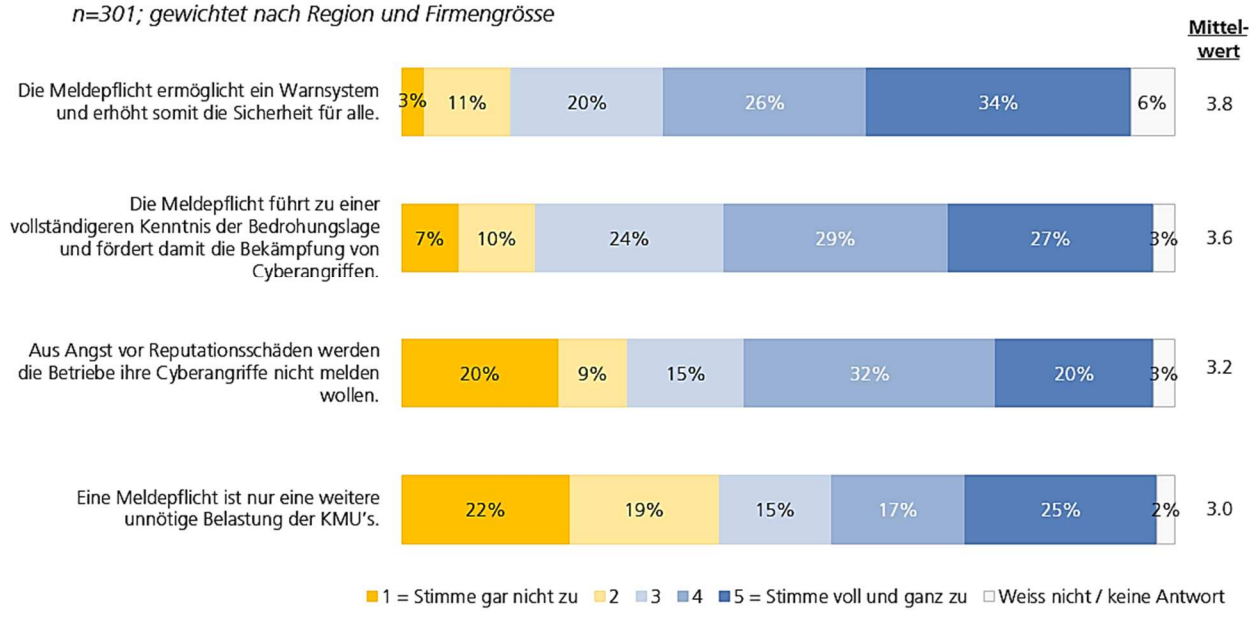
Das Wissen zum Thema Meldepflicht ist noch tief und es hat noch keine Meinungsbildung stattgefunden. Deshalb lässt sich aus der Gegenüberstellung von Pro- und Kontra-Argumenten keine allgemeingültige Zustimmung oder Ablehnung einer gesetzlichen Meldepflicht ablesen.

Die beiden Sicherheitsargumente bezüglich dem Warnsystem (60%) und der Kenntnis der Bedrohungslage (56%) erreichen die höchste Zustimmung (Skalenwerte 4 und 5 auf 5er Skala), wobei hier angemerkt werden muss, dass die Erwähnung der „erhöhten Sicherheit" und der „Förderung der Bekämpfung von Cyberangriffen" den Zustimmungswerten geholfen haben dürften.

Die Angst vor Reputationsschäden wird von einer knappen Mehrheit der Befragten (52%) bestätigt. Dieser Einwand ist ernst zu nehmen: Die Anonymität müsste bei einer gesetzlichen Meldepflicht gewährt werden können.

Unentschieden sind die Befragten beim Argument, dass eine Meldepflicht „nur eine weitere unnötige Belastung der KMUs ist". Je rund zwei von fünf Befragten stimmen dem Argument zu (42%), fast ebenso viele lehnen es ab (41%). – Wichtig wäre wohl in jedem Fall eine möglichst einfach umzusetzende Lösung für die KMUs.

F16: Ich lese Ihnen jetzt einige Argumente für und gegen eine Meldepflicht vor und bitte Sie, mir zu sagen, wie sehr Sie diesen Argumenten zustimmen.
n=301; gewichtet nach Region und Firmengrösse



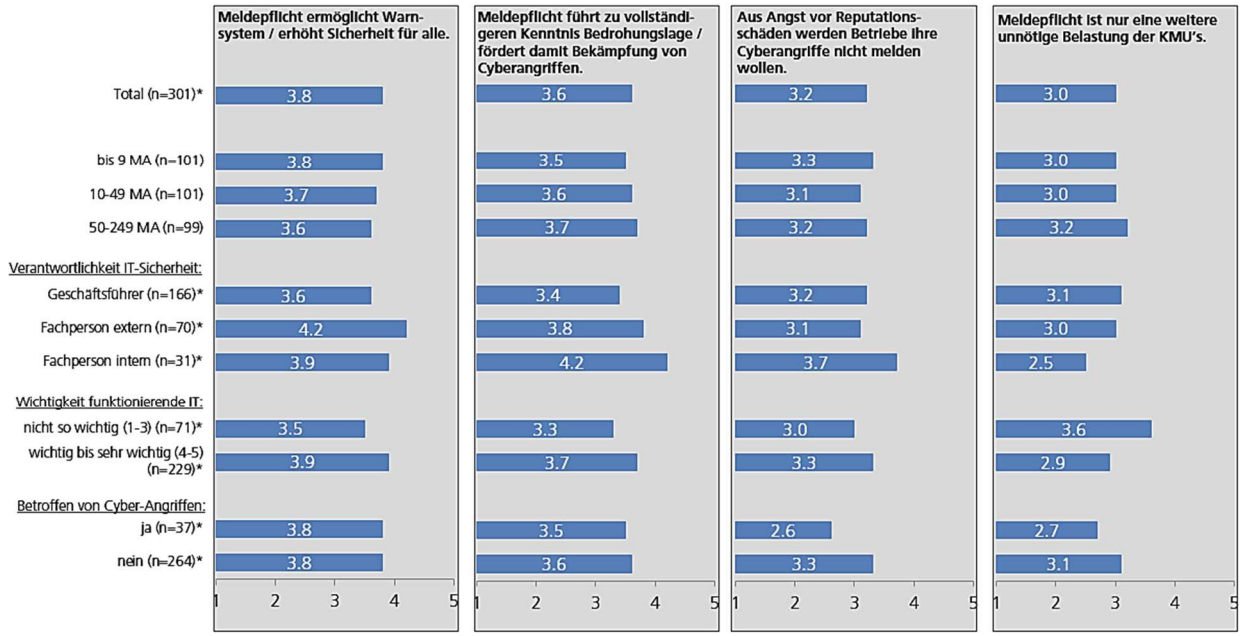
Die Argumente werden von den verschiedenen Subgruppen ähnlich beurteilt. Unterschiede ergeben sich v.a. bei der Verantwortlichkeit für die IT-Sicherheit: Firmen mit Fachpersonen (intern oder extern) stimmen den beiden Pro-Argumenten signifikant eher zu als Firmen, in welchen der/die GeschäftsführerIn zuständig ist.

Firmen, bei welchen die IT wichtig bis sehr wichtig ist, stimmen den beiden Pro-Argumenten signifikant häufiger zu (Mittelwerte 3.9 und 3.7) als diejenigen, bei denen die IT nicht wichtig ist (Mittelwerte 3.5 und 3.3).

Wer schon einmal von einem Cyberangriff betroffen war, beurteilt die Angst vor Reputationsschäden signifikant tiefer (Mittelwert 2.6) als diejenigen, die noch keine Erfahrungen mit Cyberangriffen gemacht haben (Mittelwert 3.3). Dies dürfte entweder der Fall sein, weil sie den Cyberangriff vertraulich behandeln konnten, oder aber weil sie keine negativen Erfahrungen mit einer offenen Kommunikation gemacht haben.

Dass eine Meldepflicht nur eine weitere unnötige Belastung der KMUs ist, empfinden diejenigen Firmen signifikant stärker, bei welchen die IT nicht so wichtig ist (Mittelwert 3.6 vs. 2.9), die das Risiko eines Cyberangriffs als tief einschätzen (Mittelwert 3.1 vs. 2.3) oder im industriellen Sektor (Sektor 2) tätig sind (Mittelwert 3.3, vs. Dienstleistungs-Sektor 3: 2.9, nicht dargestellt). Zwischen den Unternehmensgrössen gibt es aber kein unterschiedliches Antwortverhalten zu diesem Argument.

F16: Ich lese Ihnen jetzt einige Argumente für und gegen eine Meldepflicht vor und bitte Sie, mir zu sagen, wie sehr Sie diesen Argumenten zustimmen. *n=301; *gewichtet nach Region und Firmengrösse*

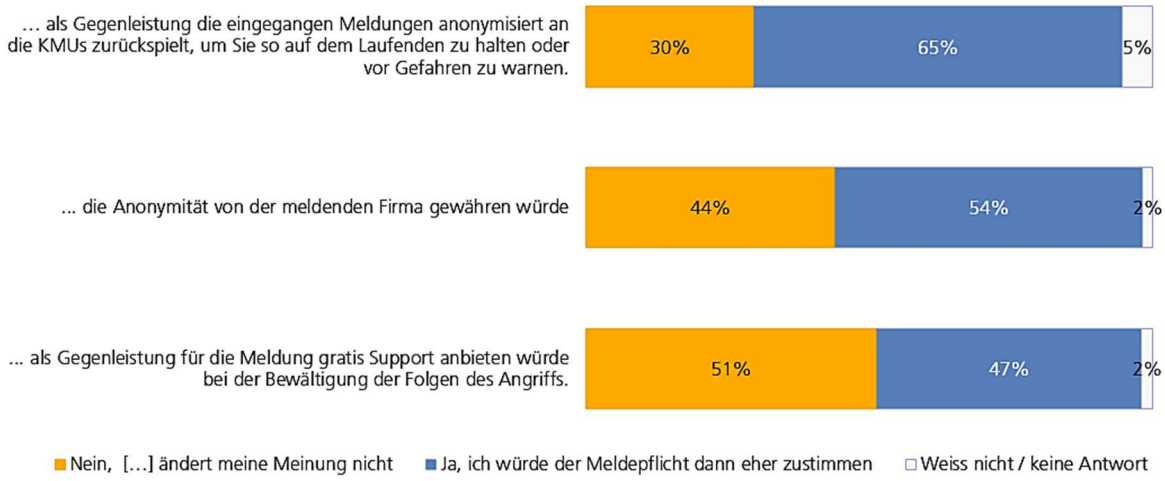


3.5.2 Ausgestaltung der Meldepflicht

Das anonymisierte Zurückspielen der eingegangenen Meldungen im Sinne einer Gegenleistung durch die Fachstelle, welche die Cyberangriffs-Meldungen entgegen nähme, würde knapp zwei Drittel der Befragten (65%) positiver einstellen gegenüber einer gesetzlichen Meldepflicht.

Rund die Hälfte der Befragten findet die Wahrung der Anonymität der meldenden Firma (54%) sowie einen gratis Support zur Bewältigung der Folgen des Angriff (47%) als wichtiger Punkt, um der Meldepflicht allenfalls zustimmen zu können.

F18-20: Würden Sie der Meldepflicht eher zustimmen, wenn die Fachstelle…?
n=301; gewichtet nach Region und Firmengrösse



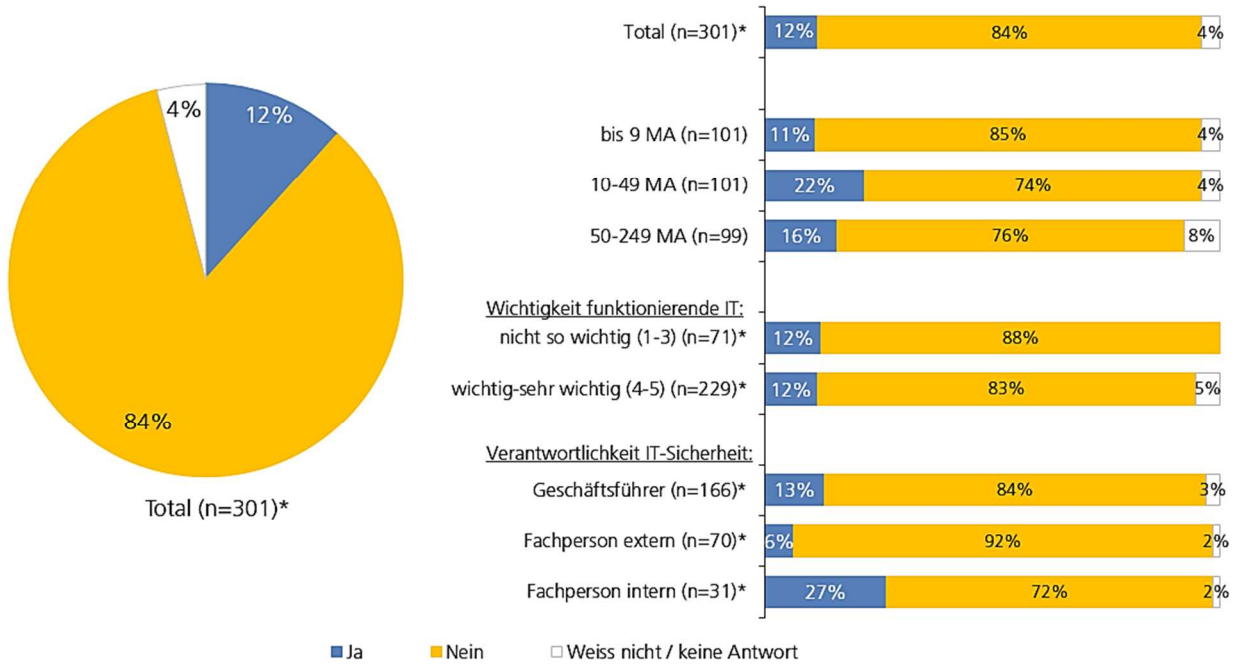
3.6 Cyber-Versicherung

3.6.1 Abschluss einer (ausdrücklichen) Cyber-Versicherung

Rund jeder achte Befragte (12%) gibt an, über eine Cyber-Versicherung zu verfügen. Bei dieser Zahl muss hinterfragt werden, ob es sich dabei um eine ausdrückliche („affirmative") Cyber-Versicherung handelt oder ob die Befragten von einer Cyber-Deckung aufgrund einer gängigen Versicherungsdeckung (stillschweigenden Deckung, „silent cover") ausgehen. Letzteres ist risikoreich, weil die Versicherungsnehmenden sich dann nicht darauf verlassen können, dass die Schäden wirklich gedeckt sind.

Unternehmen, in denen eine interne Fachperson für die IT-Sicherheit zuständig ist, haben signifikant häufiger eine Cyber-Versicherung als Unternehmen, in denen eine externe Fachperson zuständig ist. Ansonsten ergeben sich aber keine Unterschiede zwischen den Subgruppen; auch eine hohe Wichtigkeit der IT, eine hohe Risiko-Einschätzung oder eine Cyberangriffs-Erfahrung führen nicht zu einer signifikant höheren Versicherungsrate.

F21: Hat Ihre KMU eine Cyberversicherung?
*n=301; *gewichtet nach Region und Firmengrösse*

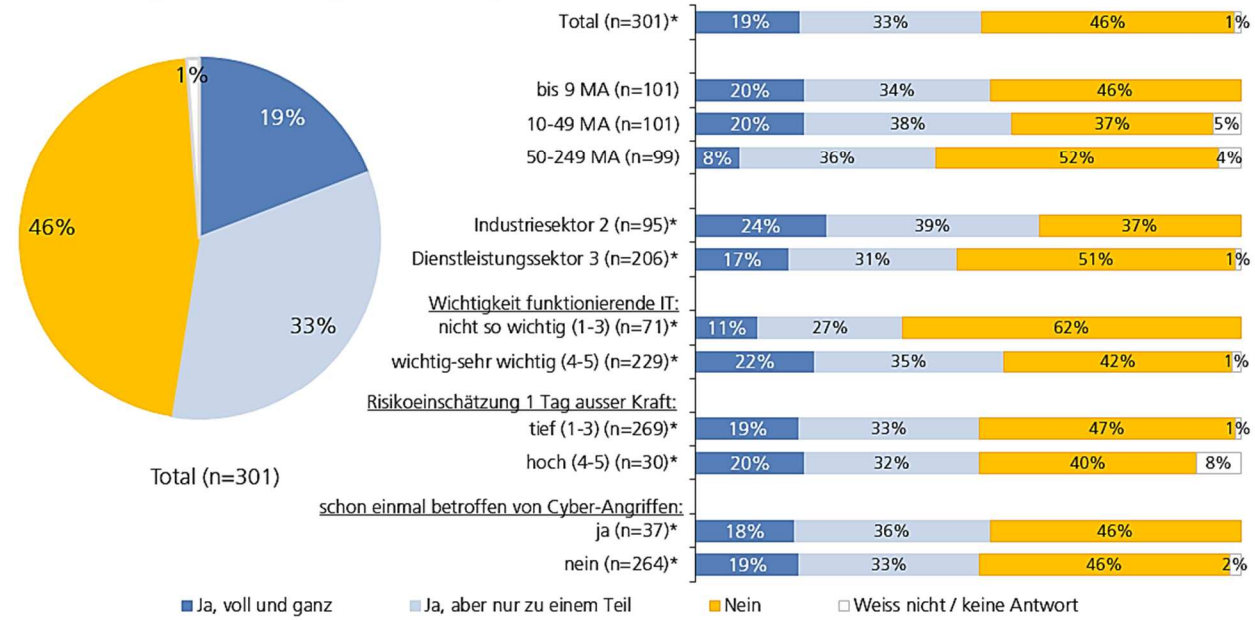


3.6.2 Risikodeckung durch den Bund bei gravierendem Angriff

Etwas mehr als die Hälfte der Befragten (52%) ist dafür, dass der Bund das finanzielle Risiko bei einem gravierenden, schweizweiten Cyberangriff zumindest zu einem Teil mittragen soll, wenn es die Versicherbarkeit übersteigt.

Die Zustimmung ist signifikant höher bei Befragten aus dem Industriesektor (63%) als bei denjenigen aus dem Dienstleistungssektor (48%). Auch Unternehmen, die ihre IT als wichtig bis sehr wichtig einstufen, stehen einer finanziellen Beteiligung des Bundes signifikant positiver gegenüber (57%) als diejenigen mit einer weniger wichtigen IT (38%). In beiden Fällen könnte die vermutete persönliche Betroffenheit eines solchen Gross-Ereignisses ein Grund für die unterschiedliche Beurteilung sein.

F22: Soll der Staat Ihrer Meinung nach das finanzielle Risiko mittragen bei einem gravierenden schweizweiten Cyberangriff, welche die Versicherbarkeit übersteigt?
*n=301; *gewichtet nach Region und Firmengrösse*



Anhang: Studiendesign in Kürze

Auftraggeber:	ICTswitzerland ISB Informatiksteuerungsorgan des Bundes ISSS Information Security Society Switzerland SQS Schweizerische Vereinigung für Qualitäts- und Managementsysteme SVV Schweizer Versicherungsverband
Inhalt:	Awareness, Kritikalität/Massnahmen, Mindeststandards, Meldepflicht und Cyber-Versicherung, soziodemografische Angaben
Grundgesamtheit:	GeschäftsführerInnen von KMUs (1-249 Mitarbeitende) in der Deutsch-, Westschweiz und im Tessin
Methode:	Telefonische Befragung (CATI)
Stichprobe:	301 durchgeführte Interviews
Gewichtung:	Disproportionale Stichprobe nach Unternehmensgrössen (1-9, 10-49, 50-249) pro Schweizer Grossregion; für die Gesamtaussagen wurden die Antworten gemäss der realen KMU-Verteilung gewichtet.
Quoten	KMU-Grösse, Region
Interviewdauer:	14 Minuten
Sprachen:	Deutsch, Französisch, Italienisch.
Auswertung:	Tabellenband Graphiken Berichterstattung
Feldphase:	13. - 27. September 2017
Projektleiter gfs-zürich:	Karin Mändli Lerch
Projektmitarbeiter:	Aleksandar Repic