carmasec

security. done. right.

“Unterstützen Cybersicherheit und Datenschutz Unternehmen bei der Digitalisierung?”

Auswertung der Studienergebnisse

Inhaltsverzeichnis

Einleitung

Die Digitalisierung ist eine der zentralen Herausforderungen, die Unternehmen gegenwärtig bewältigen müssen, um auf dem (nationalen und internationalen) Markt wettbewerbsfähig zu bleiben. Eine wichtige Aufgabe dabei: Cybersicherheit. Insbesondere in den vergangenen 20 Jahren wurde das Aktionsfeld der klassischen IT-Sicherheit auf das Internet bzw. den Cyber-Raum ausgeweitet. Die wachsende Bedeutung von Cloud-Diensten, die zunehmende Verbreitung und Nutzung von mobilen Endgeräten und die damit einhergehenden Auswirkungen auf die Arbeitsorganisation (Remote-Working, Homeoffice usw.) haben die IT-Sicherheit immer wieder vor neuen Herausforderungen gestellt.
Daher hat der Gesetzgeber auf diese Entwicklungen mit Regulierungsmaßnahmen reagiert, die in der Öffentlichkeit oftmals kontrovers diskutiert werden. Die Datenschutz-Grundverordnung, auch bekannt geworden als DS-GVO, ist ein entsprechendes Beispiel.

Forschungsfragen

In der vorliegenden Studie wurde die Meinung der betroffenen Zielgruppen zu folgenden Fragestellungen erhoben:

Welche Bedeutung hat Digitalisierung auf das Unternehmen? Verfügen Unternehmen über eine Digitalisierungsstrategie?

Welchen Einfluss hat Cybersicherheit auf die digitale Transformation von Unternehmen? Wird sie eher als eine Chance oder ein Hindernis durch die Professionals wahrgenommen?

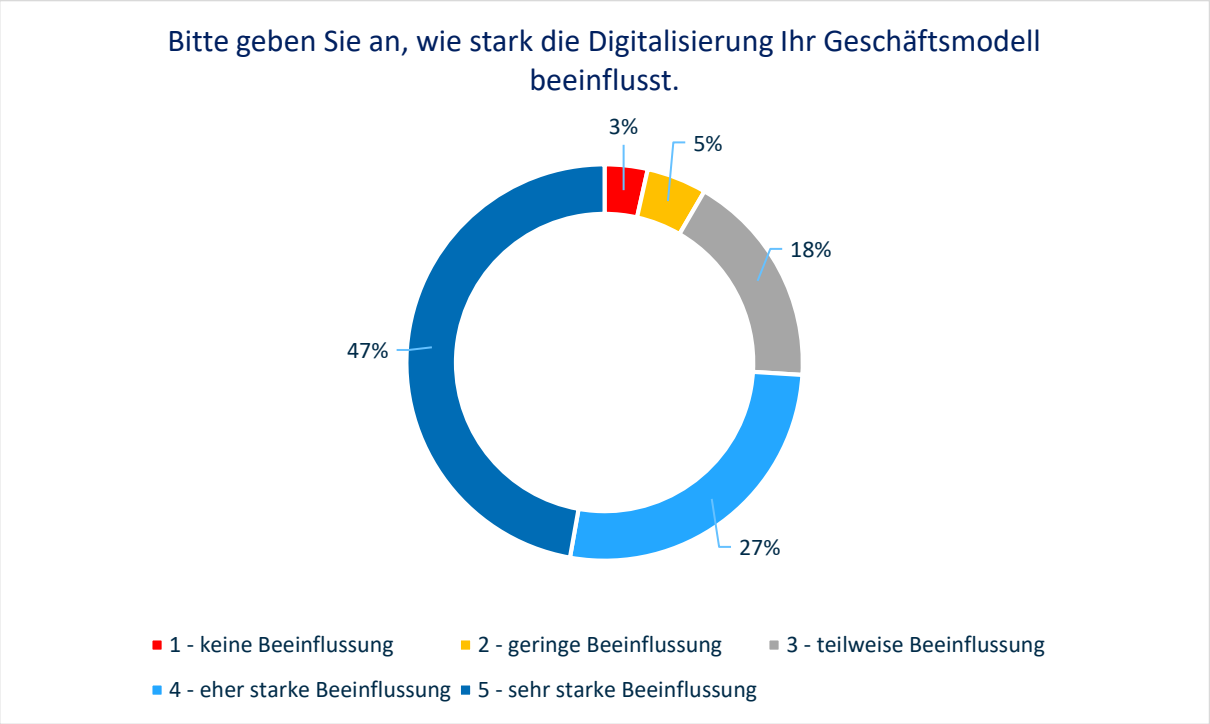
Wie gut sind die Unternehmen in Hinblick auf die Anforderungen der Cybersicherheit ausgestattet?

Adressaten der Studie bildeten dabei Geschäftsführer, Chief (Security) Information Officer, Chief Digital Officer, Riskmanager oder IT-Leiter. Entsprechend ist das vorliegende Forschungsvorhaben eine Meinungsumfrage, die das Stimmungsbild betroffener bzw. an Cybersicherheit beteiligter Träger von Expertenwissen erhoben hat.

Vorstellung der Ergebnisse

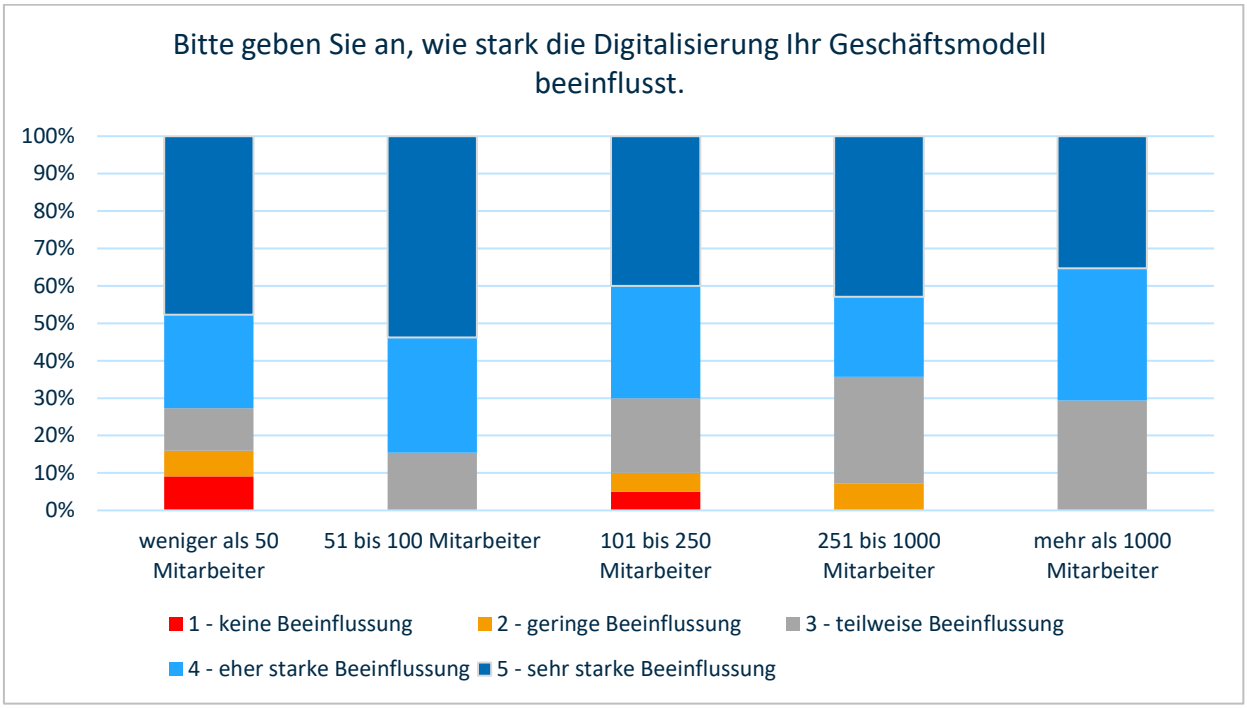
Frage 1: Bitte geben Sie an, wie stark die Digitalisierung Ihr Geschäftsmodell beeinflusst.

Betrachtung aller Befragten



Der Einfluss der Digitalisierung wird von einer großen Mehrzahl der Probanden als sehr stark oder eher stark angesehen. Weniger als einer von zehn Befragten sieht in der digitalen Transformation keinen oder nur einen geringen Einfluss auf sein Geschäftsmodell.

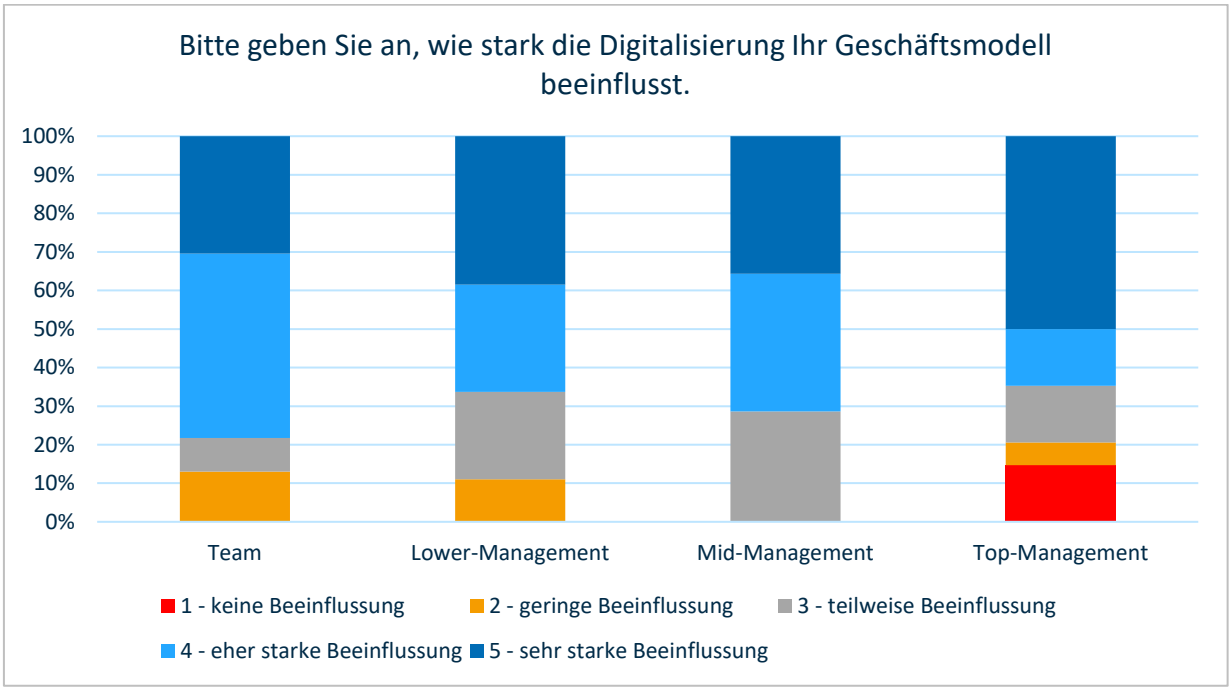
Ergebnisse nach Unternehmensgröße



Vor allem in kleineren Unternehmen mit 51 bis 100 Mitarbeitern wird der Einfluss der Digitalisierung auf das Geschäftsmodell von den meisten Befragten als sehr stark oder eher stark bewertet (gesamt 84,6%).

Bei kleinen Unternehmen mit weniger als 50 Mitarbeiter hingegen sieht mehr als jeder vierte Befragte keinen bis einen mittleren Einfluss der Digitalisierung auf das eigene Geschäftsmodell („Keine Beeinflussung“: 9,1%; „Eher keine Beeinflussung“: 6,8%; „Eine mittlere Beeinflussung“: 11,4%).

Ergebnisse nach Hierarchieebene

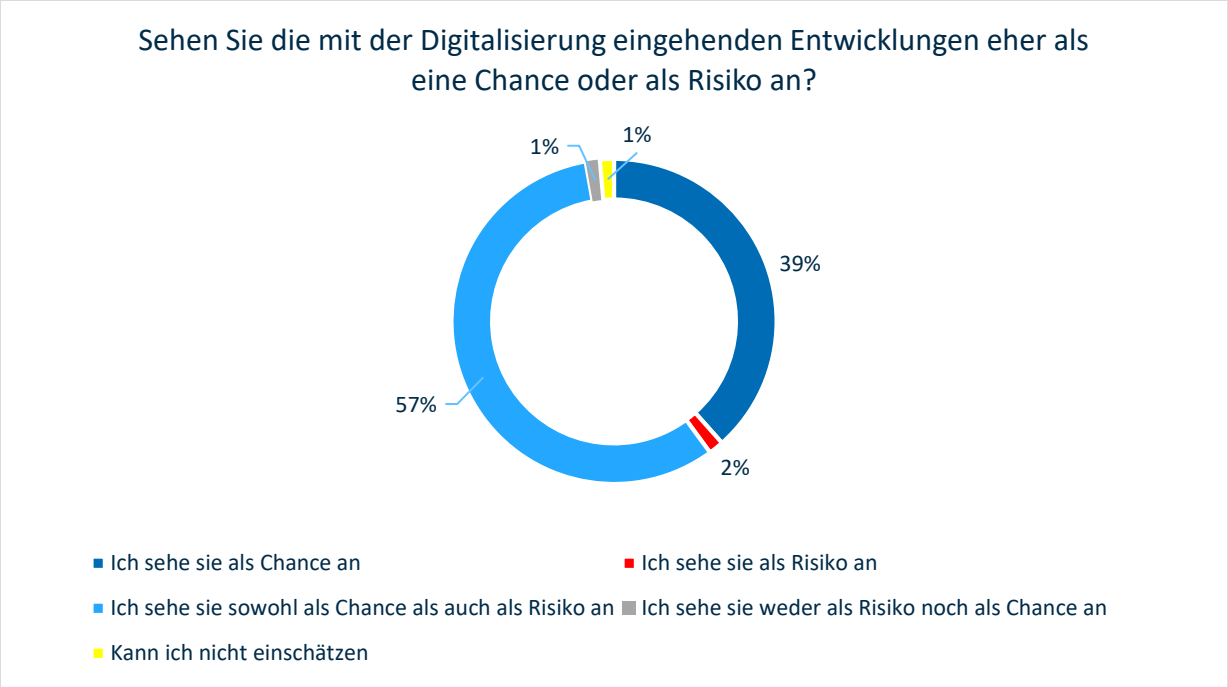


Es ist festzustellen, dass mit steigendem Hierarchiegrad des Probanden der wahrgenommene Einfluss der Digitalisierung auf das Geschäftsmodell abnimmt. Nur jeder achte Befragte, der der Hierarchieebene Team angehört, sieht keinen oder einen geringen Einfluss der Digitalisierung auf das Geschäftsmodell.

Nur jeder fünfte Top-Manager sieht keinen oder nur einen geringen Einfluss auf das Geschäftsmodell.

Frage 2: Sehen Sie die mit der Digitalisierung eingehenden Entwicklungen eher als eine Chance oder als Risiko an?

Betrachtung aller Befragten



Fast alle Probanden sehen in der Digitalisierung Chancen (insg. 95,7%).

Eine Mehrzahl der Probanden nimmt allerdings auch die Risiken, die mit der Digitalisierung einhergehen, wahr. (Sehe die Digitalisierung sowohl als Chance als auch als Risiko: 57,2%).

Ergebnisse nach Unternehmensgröße

Sehen Sie die mit der Digitalisierung eingehenden Entwicklungen eher als eine Chance oder als Risiko an?	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ich sehe sie als Chance an	52,3%	61,5%	20%	35,7%	29,4%
Ich sehe sie als Risiko an	2,3%	0%	0%	0%	0%
Ich sehe sie sowohl als Chance als auch als Risiko an	45,5%	38,5%	80%	64,3%	64,7%
Kann ich nicht einschätzen	0%	0%	0%	0%	5,9%

In diesem Punkt ist eine unterschiedliche Wahrnehmung abhängig von der Unternehmensgröße festzustellen:

Große Unternehmen mit mehr als 1000 Beschäftigten fokussieren stärker neben den Chancen auch die Risiken (für 64,7% bedeutet Digitalisierung sowohl Chance als auch Risiko, nur 29,4% sehen die Digitalisierung als reine Chance).In kleinen Unternehmen mit weniger als 50 Mitarbeitern hingegen sehen 52,3 % der Befragten die Digitalisierung als Chance nur 45,5% der Befragten sowohl als Chance als auch als Risiko. Die skeptischste Einstellung zu Digitalisierung haben allerdings Mitarbeiter in Unternehmen mit 101 – 250 Angestellten. Hier sehen sogar 80% die digitale Transformation sowohl als Chance als auch als Risiko.

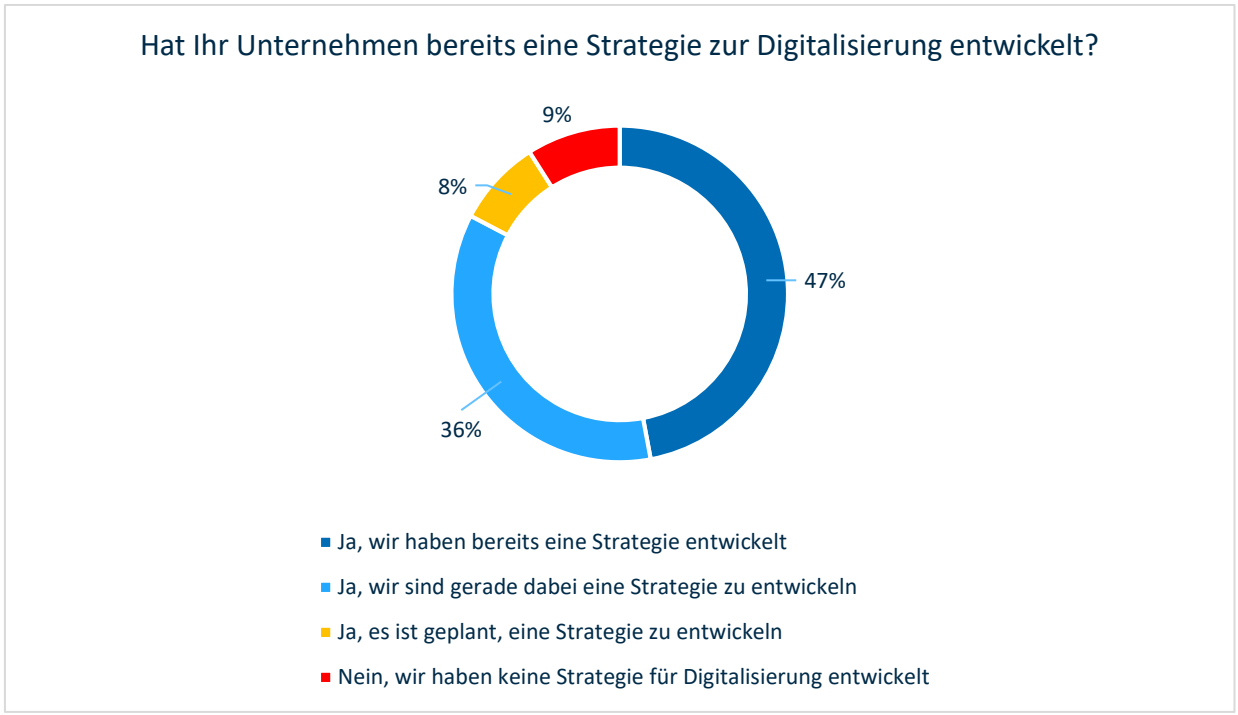
Ergebnisse nach Hierarchieebene

Sehen Sie die mit der Digitalisierung eingehenden Entwicklungen eher als eine Chance oder als Risiko an?	Team	Lower-Management	Mid-Management	Top-Management
Ich sehe sie als Chance an	43,5%	22,7%	35,7%	58,8%
Ich sehe sie als Risiko an	0%	0%	0%	2,9%
Ich sehe sie sowohl als Chance als auch als Risiko an	52,2%	77,3%	64,3%	38,2%
Ich sehe weder als Risiko noch als Chance an	0%	0%	0%	0%
Kann ich nicht einschätzen	4,3%	0%	0%	0%

Hier ist interessant, dass tatsächlich das Lower Management, also die Teamleiter, am ehesten neben den Chancen der Digitalisierung auch die Risiken sehen (77,3%). Am optimistischsten sind die Top-Manager (58,8%: Digitalisierung ist eine Chance, 38,2%: Sowohl Chance als auch Risiko).

Frage 3: Hat Ihr Unternehmen bereits eine Strategie zur Digitalisierung entwickelt?

Betrachtung aller Befragten



Die Mehrzahl der Unternehmen der Befragten hat bereits eine Digitalstrategie entwickelt oder ist gerade dabei (82,6%). Nur einer von zehn Befragten gibt an, dass sein Unternehmen keine Digitalstrategie besitzt oder plant.

Ergebnisse nach Unternehmensgröße

Hat Ihr Unternehmen bereits eine Strategie zur Digitalisierung entwickelt?	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja, wir haben bereits eine Strategie entwickelt	54,5%	53,8%	30%	42,9%	41,2%
Ja, wir sind gerade dabei eine Strategie zu entwickeln	27,3%	30,8%	60%	50%	41,2%
Ja, es ist geplant, eine Strategie zu entwickeln	4,5%	0%	10%	7,1%	11,8%
Nein, wir haben keine Strategie für Digitalisierung entwickelt	13,6%	15,4%	0%	0%	5,9%

Vor allem sehr kleine Unternehmen bis 50 bzw. 100 Mitarbeitern verfügen bereits über eine Digitalstrategie (54,5%/53,8%). Vor allem mittelgroße Unternehmen mit 101 bis 250 MA befinden sich noch in der Entwicklung einer Digitalstrategie. (60%). Nur 30% der Mitarbeiter dieser Unternehmen geben an, bereits über eine Digitalstrategie zu verfügen. Größere Unternehmen bis 1000 MA und über 1000 MA sind wieder besser aufgestellt: 42,9% bzw. 41,2% verfügen bereits über eine Digitalstrategie

Ergebnisse nach Hierarchieebene

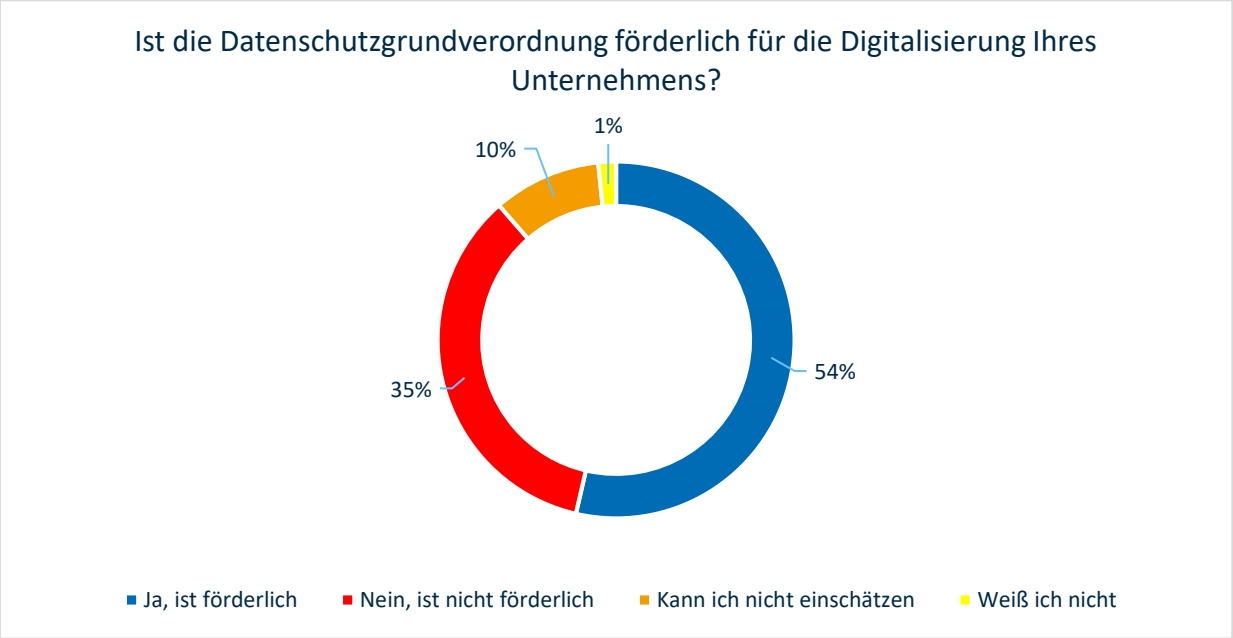
Hat Ihr Unternehmen bereits eine Strategie zur Digitalisierung entwickelt?	Team	Lower-Management	Mid-Management	Top-Management
Ja, wir haben bereits eine Strategie entwickelt	26,1%	45,5%	39,3%	64,7%
Ja, wir sind gerade dabei eine Strategie zu entwickeln	52,2%	50%	50%	14,7%
Ja, es ist geplant, eine Strategie zu entwickeln	4,3%	4,5%	10,7%	5,9%
Nein, wir haben keine Strategie für Digitalisierung entwickelt	17,4%	0%	0%	14,7%

In der Hierarchieebene Team haben die Unternehmen von lediglich 26,1% der Befragten bereits eine Digitalstrategie entwickelt. Hingegen 64,7% der Top-Manager geben an, bereits eine Digitalstrategie entwickelt zu haben. Jeder zweite Befragte, der den Hierarchieebenen Team, Lower-Management oder Mit-Management angehört, gibt allerdings an, dass sein Unternehmen gerade an der Entwicklung einer Digitalisierungsstrategie arbeitet.

Frage 4: Bitte geben Sie an, welche der folgenden Gesetze förderlich für die Digitalisierung eines Unternehmens sind.

4.1 Datenschutzgrundverordnung (DS-GVO)

Betrachtung aller Befragten



Mehr als die Hälfte der Probanden sieht die DS-GVO als förderlich für die Digitalisierung ihres Unternehmens an(53,65%).

Immerhin mehr als ein Drittel der Befragten empfindet die DS-GVO nicht als förderlich für die Digitalisierung des Unternehmens.

Festzustellen ist, dass die DS-GVO über eine große Bekanntheit verfügt, nur 10 % der Probanden geben an, die Förderlichkeit der DS-GVO auf die Digitalisierung ihres Unternehmens nicht einschätzen zu können. Nur 1.6% der Befragten geben an “weiß ich nicht”.

Ergebnisse nach Unternehmensgröße

Datenschutzgrundverordnung (DS-GVO)	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja, ist förderlich	52,3%	76,9%	50%	50%	41,2%
Nein, ist nicht förderlich	40,9%	15,4%	40%	35,7%	47,1%
Kann ich nicht einschätzen	6,8%	0%	10%	14,3%	11,8%
Weiß ich nicht	0%	7,7%	0%	0%	0%

Bemerkenswert ist, dass vor allem kleine Unternehmen die DS-GVO bei der Digitalisierung mehrheitlich als förderlich empfinden.

Es kann festgestellt werden: Je kleiner das Unternehmen, desto größer die positive Einstellung zur DS-GVO.

Ergebnisse nach Hierarchieebene

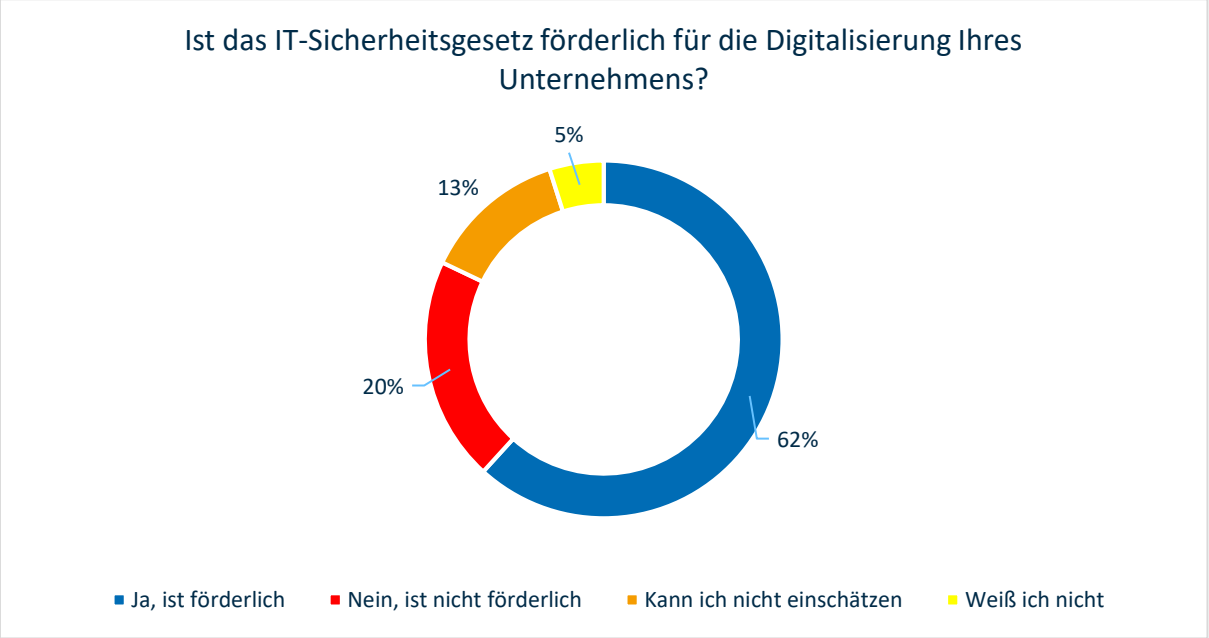
Datenschutzgrundverordnung (DS-GVO)	Team	Lower-Management	Mid-Management	Top-Management
Ja, ist förderlich	60,9%	59,1%	50%	47%
Nein, ist nicht förderlich	26,1%	36,4%	39,3%	47%
Kann ich nicht einschätzen	13%	4,5%	10,7%	6%
Weiß ich nicht	0%	0%	0%	0%

In Bezug auf die Job-Positionen kann festgestellt werden: Je höher der Befragte in der Hierarchie angesiedelt ist, desto weniger spricht er sich für die Förderlichkeit der DS-GVO auf die Digitalisierung des Unternehmens aus (förderlich: Team: 60,9%, Top-Manager: 47%). Im Umkehrschluss empfinden Teammitglieder die DS-GVO am seltensten als nichtförderlich (26,1%), Top-Manager sie am häufigsten als nichtförderlich (47%).

Festzustellen ist außerdem, dass etwa jeder achte der Hierarchieebene Team aussagt, dass er die Förderlichkeit der DS-GVO nicht einschätzen kann (13%), im Top-Management ist nur etwa jeder 17. (6%).

4.2 IT-Sicherheitsgesetz

Betrachtung aller Befragten



Das IT-Sicherheitsgesetz wird von fast zwei Dritteln der Probanden als förderlich für die Digitalisierung ihres Unternehmens wahrgenommen (61,7%). Nur jeder fünfte empfindet die Vorschrift als nicht förderlich (20,3%) Festzustellen ist aber auch, dass 17,9% der Probanden diese Einschätzung nicht vornehmen konnten („Kann ich nicht einschätzen“: 13%, „weiß ich nicht“: 4,9%).

Ergebnisse nach Unternehmensgröße

IT-Sicherheitsgesetz	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja, ist förderlich	63,6%	69,2%	65%	64,3%	47,1%
Nein, ist nicht förderlich	20,5%	15,4%	15%	28,6%	35,3%

Es ist festzustellen, dass sowohl Mitarbeiter kleiner Unternehmen als auch Mitarbeiter mittelgroßer Unternehmen bis zu 1000 Mitarbeiter mehrheitlich das IT-Sicherheitsgesetz als förderlich betrachten. Lediglich Probanden großer Unternehmen mit mehr als 1001 Mitarbeitern schätzten mitregulatorische Vorgabe als förderlich, mehr als jeder Dritte sogar als nicht förderlich ein.

Ergebnisse nach Hierarchieebene

IT-Sicherheitsgesetz	Team	Lower-Management	Mid-Management	Top-Management
Ja, ist förderlich	73,9%	63,6%	67,9%	50%
Nein, ist nicht förderlich	4,3%	36,4%	17,9%	26,5%
Kann ich nicht einschätzen	13%	0%	14,3%	17,6%
Weiß ich nicht	8,7%	0%	0%	5,9%

In der hierarchischen Clusterung stechen vor allem die Team-Mitglieder als Befürworter des IT-Sicherheitsgesetzes hervor (förderlich: 73,9%). In dieser Ebene herrscht auch das größte Wissen um das Gesetz, lediglich 3,4% der Befragten konnten die Förderlichkeit für ihr Unternehmen nicht einschätzen, keiner antwortete mit “Weiß ich nicht”. Am skeptischsten ist die Gruppe der Top-Manager. Nur jeder zweite (50%) gibt an, das Gesetz als förderlich für das Unternehmen wahrzunehmen. Allerdings herrscht in dieser Gruppe auch die höchste Unwissenheit - 17,6% der Top-Manager gaben an, die Förderlichkeit der Richtlinie nicht einschätzen zu können, 5,9 % antworteten mit “Weiß ich nicht”.

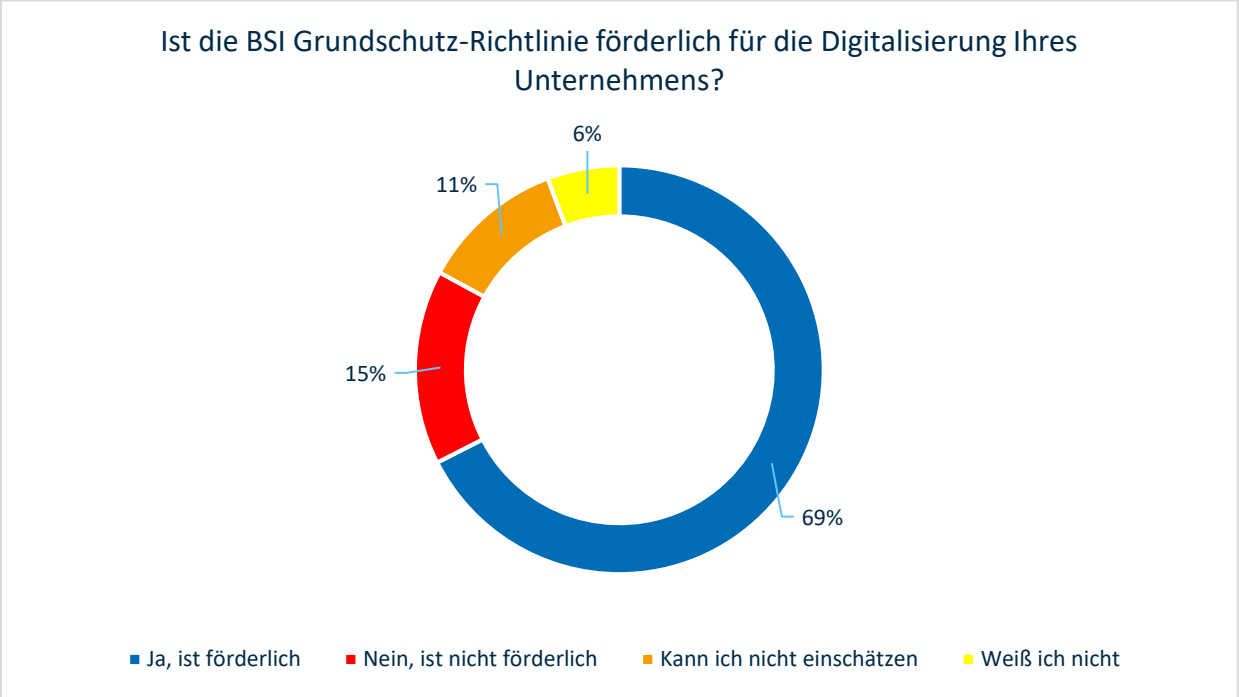
Vergleich mit der DS-GVO

Interessant an den Ergebnissen zur Einstellung zum IT-Sicherheitsgesetz ist vor allem der Vergleich mit den Einstellungen der Probanden zur DS-GVO:

Es wird von einer größeren Mehrheit als förderlich empfunden als die DS-GVO. (61,1% zu 53,56%) und auch deutlich weniger nicht als förderlich wahrgenommen (20,3% zu 35%). Es herrscht aber auch eine größere Unkenntnis über das IT-Sicherheitsgesetz als über die DS-GVO („kann ich nicht einschätzen“: 13% zu 9,8%; „weiß ich nicht“: 4,9% zu 1,6%). Hier könnte geschlussfolgert werden, dass das IT-Sicherheitsgesetz aufgrund der enthaltenen Regelungen für die Digitalisierung von Unternehmen förderlicher ist als die DS-GVO. Oder es kann angenommen werden, dass aufgrund der negativ eingefärbten Berichterstattung über die DS-GVO die Einstellung dazu negativer ist.

4.3 ISO-27001/BSI Grundschutz

Betrachtung aller Befragten



Die ISO-27001/BSI Grundschutz-Richtlinie wird von allem Probanden im Vergleich mit allen anderen regulatorischen Vorgaben als am förderlichsten für die Digitalisierung des Unternehmens empfunden (67,5%). Die Befragten sind mit dem Grundschutz ebenfalls gut vertraut, lediglich 11,4% antworteten “kann ich nicht einschätzen”, 5,7% mit “weiß ich nicht”.

Dies kann mit der Tatsache, dass ISO-Normen in Deutschland zertifiziert werden müssen und damit für hohe Qualität und Glaubwürdigkeit stehen. Eine solche Zertifizierung erzeugt eine positive Wahrnehmung auf Seiten der Unternehmen und ihrer Kunden. Zudem ist das System der ISO-Zertifizierung etabliert und damit im Vergleich zur DS-GVO weniger mit fachlichen und rechtlichen Unsicherheiten besetzt.

Ergebnisse nach Unternehmensgröße

BSI Grundschutz-Richtlinie	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja, ist förderlich	65,9%	61,54%	60%	85,7%	76,5%
Nein, ist nicht förderlich	13,6%	15,4%	25%	14,3%	17,6%
Kann ich nicht einschätzen	13,6%	7,7%	15%	0%	5,9%
Weiß ich nicht	6,8%	15,4%	0%	0%	0%

Die Wahrnehmung der BSI Grundschutz Richtlinie innerhalb der unterschiedlichen Unternehmensgrößen ist durchgehend sehr positiv. Lediglich Befragte mittelgroße Unternehmen mit 101 bis 250 Mitarbeiter sehen nur zu 60% die Förderlichkeit der Vorgabe für die Digitalisierung. Jeder vierte sieht dagegen keine Förderlichkeit. Auffällig ist, dass im Fall der BSI Grundschutz-Richtlinie nicht das fehlende Wissen der Grund für die Einschätzung sein kann. Insbesondere in kleinen Unternehmen bis zu 50 MA sprechen sich fast zwei Drittel der Befragten für eine Förderlichkeit aus, aber fast jeder vierte Befragte antwortete mit “Kann ich nicht einschätzen” (13,6%) oder “weiß ich nicht” (6,8%). Hingehen in mittelgroßen Unternehmen mit 101 bis zu 250 MA sagten lediglich 15% der Befragten “kann ich nicht einschätzen”, keiner antwortete mit “weiß ich nicht”.

Ergebnisse nach Hierarchieebene

ISO-27001/BSI Grundschutz	Team	Lower-Management	Mid-Management	Top-Management
Ja, ist förderlich	78,3%	72,7%	75%	52,9%
Nein, ist nicht förderlich	4,3%	22,8%	14,3%	23,5%
Kann ich nicht einschätzen	13%	0%	10,7%	14,7%
Weiß ich nicht	4,3%	4,5%	0%	8,8%

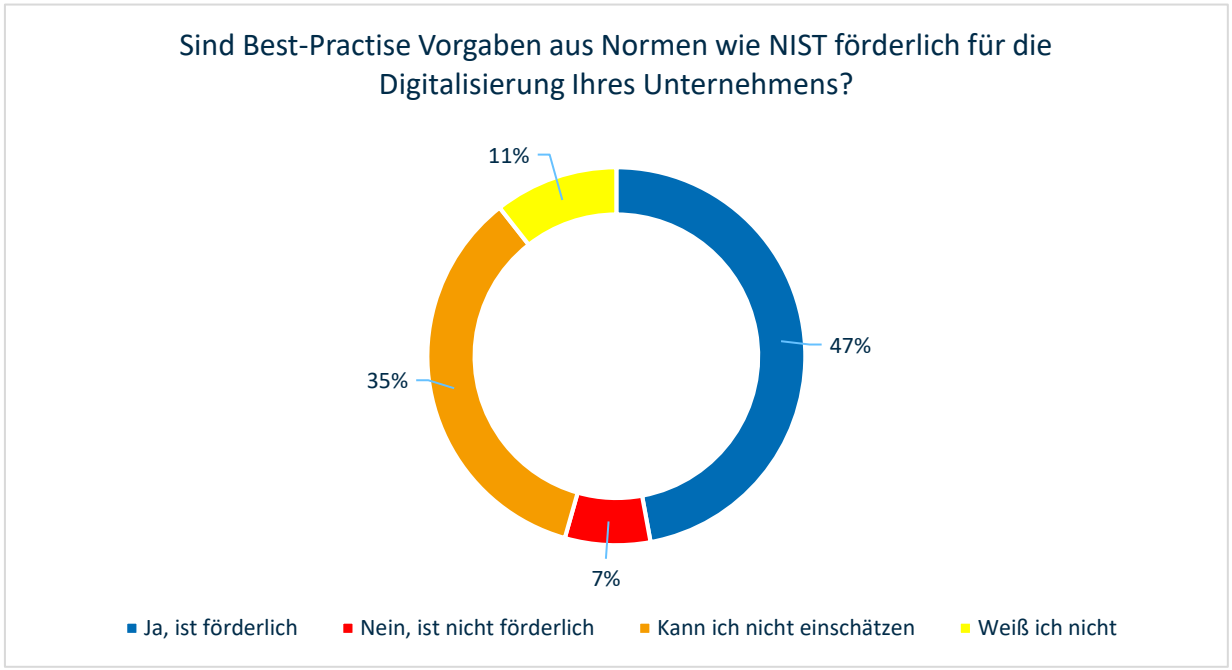
Äquivalent zu den Ergebnissen der Einstellungen zu DS-GVO, IT-Sicherheitsgesetz und NIST kann festgestellt werden, dass das Top-Management die skeptischste Einstellung zur BSI Grundschutz-Richtlinie aufzeigt (förderlich: 52,9%, nicht förderlich: 23,5%). Dagegen sind Team-Angehörige zu 78,3% von der Förderlichkeit des Gesetzes überzeugt, lediglich jeder 20. (4,3%) hält die Förderlichkeit für nicht gegeben.

Hinsichtlich des Wissens über die IT Grundschutz-Richtlinie kann festgestellt werden, dass fast jeder 4. Top-Manager sich nicht ausreichend informiert fühlt, um die Förderlichkeit des BSI IT-Grundschutzes einordnen zu können („Kann ich nicht einschätzen": 14,7 %, „Weiß ich nicht": 8,8%)

Im Vergleich fühlt die Hierarchieebene des Lower Managements zu einem sehr großen Teil ausreichend informiert: Lediglich 4,5% der Befragten antworteten mit "weiß ich nicht".

4.4 Best-Practise Vorgaben aus Normen wie NIST

Betrachtung aller Befragten



Normen des National Institute of Standards werden auch in Deutschland oft in Form von "Best Practice"-Vorgaben empfohlen. Die Befragten aus unserer Studie äußerten sich bezüglich der Förderlichkeit von Digitalisierung im Unternehmen eher positiv. Fast jeder Zweite sieht NIST-Normen als förderlich an (47,1%). Fast genauso viele Befragte können die Förderlichkeit jedoch nicht einschätzen. 35% äußerten sich mit "kann ich nicht einschätzen", 10,6% wählten "weiß ich nicht". Nur 7,3% sehen keinen Vorteil in NIST-Normen für die Digitalisierung ihres Unternehmens.

Ergebnisse nach Unternehmensgröße

Best-Practise Vorgaben aus Normen wie NIST	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja, ist förderlich	47,7%	53,8%	30%	64,3%	52,9%
Nein, ist nicht förderlich	9,1%	15,4%	5%	0%	11,8%
Kann ich nicht einschätzen	29,5%	15,4%	55%	28,6%	35,3%
Weiß ich nicht	13,6%	15,4%	10%	7,1%	0%

Hinsichtlich der Clusterung in Unternehmensgrößen zeigt sich, dass vor allem in mittelgroßen Unternehmen mit 101-250 Mitarbeitern NIST-Normen als wenig förderlich angesehen werden (ist förderlich: 30%). Dies kann mit geringer Kenntnis der NIST-Normen erklärt werden: Fast zwei von drei Befragten dieser Unternehmensgröße antworteten mit “kann ich nicht einschätzen” (55%) oder “weiß nicht” (10%). Eine große Akzeptanz erfahren die Best Practice-Vorgaben nach NIST in größeren Unternehmen mit 251 bis zu 1000 Mitarbeitern. Hier sprechen sich 64,3% der Befragten für die Förderlichkeit aus.

Die restlichen Befragten können die Förderlichkeit entweder nicht einschätzen (28,6%) oder antworteten mit “weiß ich nicht” (7,1%). Hier setzt sich der oben beschriebene Trend, dass NIST-Normen bei vorhandenem Wissen als förderlich wahrgenommen werden, weiter fort.

Ergebnisse nach Hierarchieebene

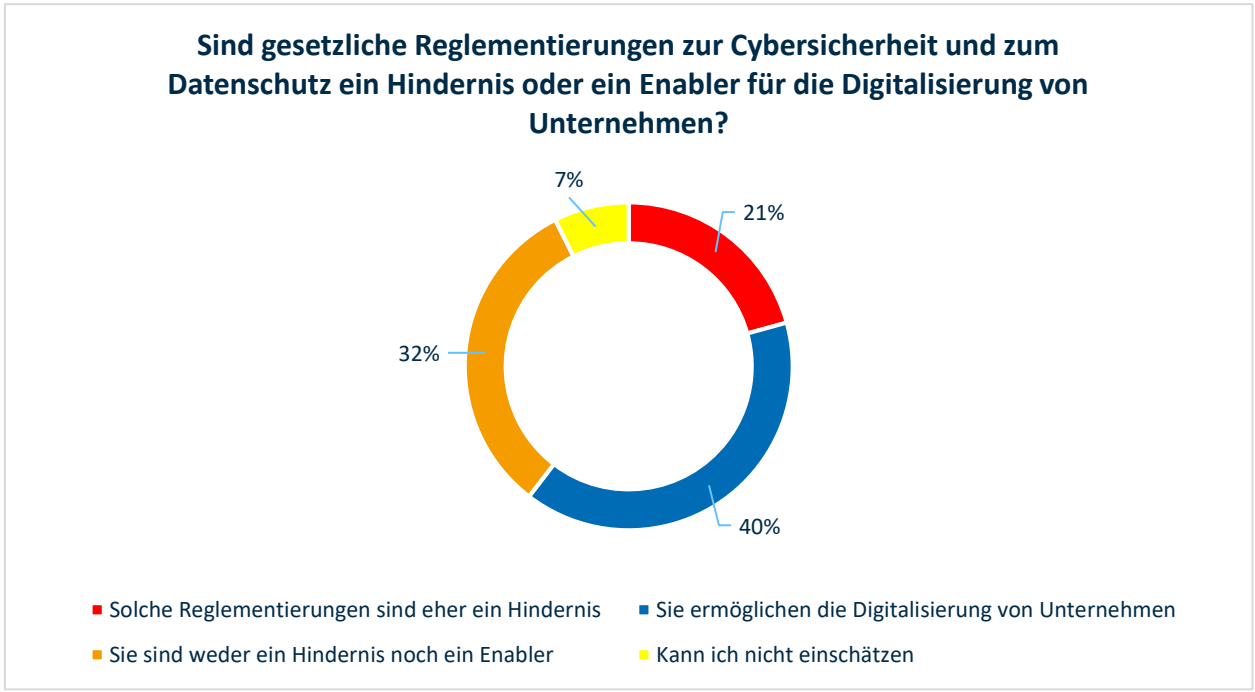
Best-Practise Vorgaben aus Normen wie NIST	Team	Lower-Management	Mid-Management	Top-Management
Ja, ist förderlich	52,2%	63,6%	42,9%	38,2%
Nein, ist nicht förderlich	0%	18,2%	3,6%	11,8%
Kann ich nicht einschätzen	43,5%	18,2%	39,3%	32,4%
Weiß ich nicht	4,3%	0%	14,3%	17,5%

Wieder kann festgestellt werden, dass das Top-Management hinsichtlich der Förderlichkeit von NIST-Normen für die Digitalisierung ihres Unternehmens am skeptischsten ist. Lediglich 38,2% sprechen sich für die Förderlichkeit aus. Damit sind Best Practice-Vorgaben aus NIST die vom Top-Management klar als am wenigsten für förderlich gehaltene Vorgabe. Die Ursache ist im fehlenden Wissen zu suchen. Fast jeder zweite Top-Manager gibt an, die Förderlichkeit von NIST-Normen nicht bewerten zu können („kann ich nicht einschätzen”: 32,4%; „weiß ich nicht”: 17,5%).

Die den Best Practice-Vorgaben aus NIST gegenüber am ehesten positiv eingestellte Hierarchieebene ist die des Lower-Managements. Hier sprechen sich 63,6% für eine Förderlichkeit aus, nur 18,2% sehen die regulatorische Vorgabe als nicht förderlich für die Digitalisierung ihres Unternehmens an. Ebenfalls ist diese Gruppe die am ehesten informierte: Nur 18,2% der befragten Teamleiter geben an, die Förderlichkeit von NIST-Normen nicht einschätzen zu können.

Frage 5: Sind gesetzliche Reglementierungen zur Cybersicherheit und zum Datenschutz ein Hindernis oder ein Enabler für die Digitalisierung von Unternehmen?

Betrachtung aller Befragten



Einzelnen regulatorischen Vorschriften stehen die Befragten mehrheitlich positiv gegenüber. Bei der Frage nach einer grundsätzlichen Ansicht hinsichtlich der Förderlichkeit von regulatorischen Vorschriften in Bezug auf die Digitalisierung äußern sich die Probanden verhaltener. Lediglich 39,7% aller Befragten sind der Meinung, dass gesetzliche Vorgaben zu Cybersicherheit und Datenschutz die Digitalisierung von Unternehmen ermöglichen. 32,2% äußern sich neutral (“sind weder Hindernis noch Enabler”). Jeder fünfte Befragte sieht Reglementierungen eher als Hindernis (20,7%).

Ergebnisse nach Unternehmensgröße

Größe des Unternehmens	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Solche Reglementierungen sind eher ein Hindernis	29,5%	7,7%	25%	21,4%	17,6%
Sie ermöglichen die Digitalisierung von Unternehmen	43,2%	38,5%	40%	14,3%	41,2%
Sie sind weder ein Hindernis noch ein Enabler	22,7%	46,2%	25%	57,1%	35,3%

Am ehesten sind Mitarbeiter kleiner Unternehmen skeptisch in Bezug auf regulatorische Vorschriften in der Rolle als Business-Enabler. 29,5% der Befragten betrachten Reglementierungen eher als Hindernis. Über alle Unternehmensgrößen hinweg werden Vorschriften von einer Mehrzahl der Befragten als Enabler oder weder als Enabler noch als Hindernis angesehen.

Dabei fällt allerdings auf, dass Unternehmen mit 251 bis 1000 Mitarbeitern regulatorische Vorgaben in der Mehrzahl weder als Hindernis noch als Enabler wahrnehmen (57,3%). Dies weicht von den Ergebnissen der Befragten anderer Unternehmensgrößen ab.

Ergebnisse nach Hierarchieebene

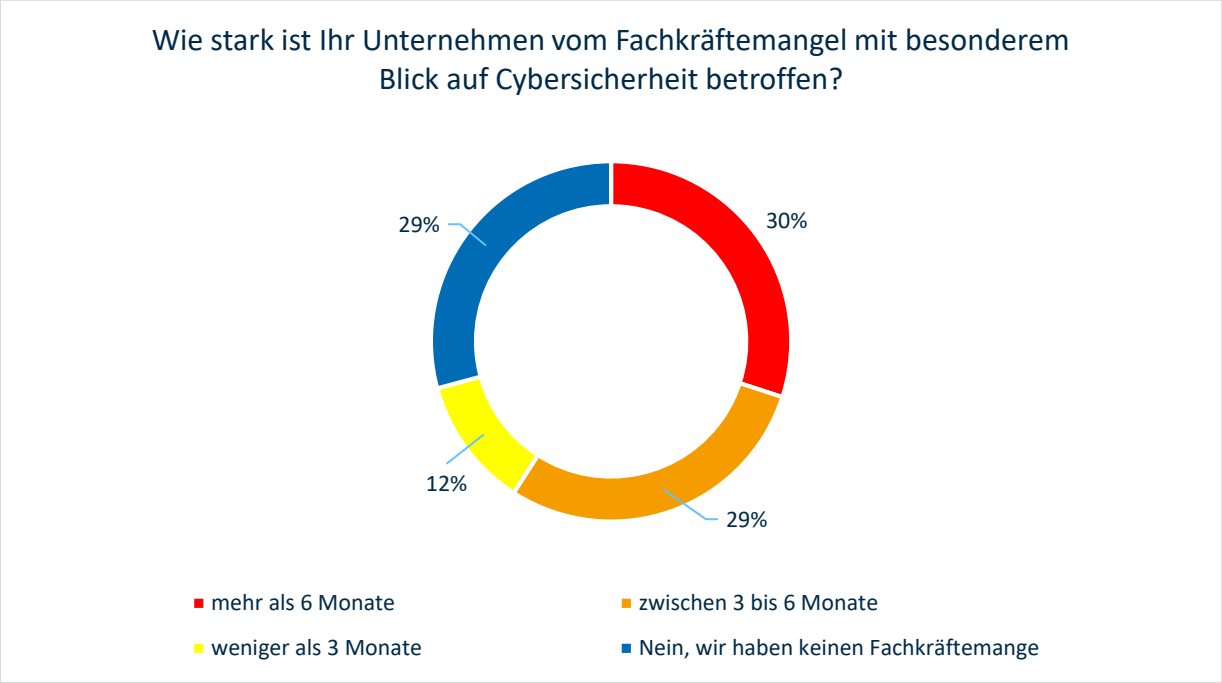
Sind gesetzliche Reglementierungen ein Hindernis oder ein Enabler für die Digitalisierung von Unternehmen?	Team	Lower-Management	Mid-Management	Top-Management
Solche Reglementierungen sind eher ein Hindernis	21,7%	18,2%	21,4%	35,4%
Sie ermöglichen die Digitalisierung von Unternehmen	34,8%	50%	25%	44,1%
Sie sind weder ein Hindernis noch ein Enabler	34,8%	31,8%	50%	17,6%

In der Betrachtung der Ergebnisse der Clusterung nach Hierarchieebenen kann vor allem bei den Top-Managern eine entschiedene Aussage festgestellt werden. So empfinden 35,4 % der Top-Manager Reglementierungen als Hindernis und sogar 44,1 % der Top-Manager Reglementierungen als Business-Enabler. Lediglich 17,6% sehen keinen Einfluss von regulatorischen Vorgaben auf die Digitalisierung.

Damit äußert sich die Gruppe der Top-Manager auch insgesamt am skeptischsten. In allen anderen Hierarchie-Gruppen sieht lediglich jeder fünfte Befragte gesetzliche Reglementierungen als Hindernis für die Digitalisierung.

Frage 6: Wie stark ist Ihr Unternehmen vom Fachkräftemangel mit besonderem Blick auf Cybersicherheit betroffen? Geben Sie uns dazu an, wie lange Vakanzen - schätzungsweise - unbesetzt bleiben

Betrachtung aller Befragten



Es ist allgemein festzustellen, dass in Bezug auf die Besetzung von Vakanzen in der Cybersicherheit die Mehrzahl der Probanden einen Fachkräftemangel beklagen muss. So suchen 29,1% zwischen 3 bis 6 Monaten nach einem entsprechenden Experten. Weitere 30% der Befragten suchen länger als ein halbes Jahr nach entsprechender Unterstützung. Im Gegenzug sagen 29,2% der Befragten aus, dass sie keinen Fachkräftemangel zu beklagen haben.

Ergebnisse nach Unternehmensgröße

Wie stark ist Ihr Unternehmen vom Fachkräftemangel insb. bei Cybersicherheit betroffen?	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	weniger als 50 Mitarbeiter
mehr als 6 Monate	20,5%	23,1%	25%	50%	29,4%
zwischen 3 bis 6 Monate	11,4%	46,2%	45%	35,7%	41,2%
weniger als 3 Monate	11,4%	15,4%	15%	7,1%	11,8%
Nein, wir haben keinen Fachkräftemangel	56,8%	15,4%	15%	7,1%	17,6%

Jeder zweite Mitarbeiter eines größeren Unternehmens mit 251 bis zu 1000 Mitarbeitern gibt an, mehr als sechs Monate nach einer Fachkraft für Vakanzen im Bereich der Cybersicherheit zu suchen (50%). Damit sind diese Unternehmen am stärksten vom Fachkräftemangel betroffen. In kleineren Unternehmen mit 51 bis 100 Mitarbeitern sucht nahezu jeder zweite Befragte (46,2%) zumindest 3 bis 6 Monate nach einem entsprechend qualifizierten Mitarbeiter.

Am wenigsten betroffen von der langen Suche nach Cybersicherheits-Experten sind scheinbar kleine Unternehmen mit weniger als 50 Mitarbeitern. Hier gibt mehr als jeder Zweite an, nicht vom Fachkräftemangel betroffen zu sein. (56,8%) Es ist allerdings zu vermuten, dass insbesondere kleine Unternehmen Cybersicherheits-Expertise nicht intern verorten, sondern hierzu externe Beratungsleistungen einkaufen.

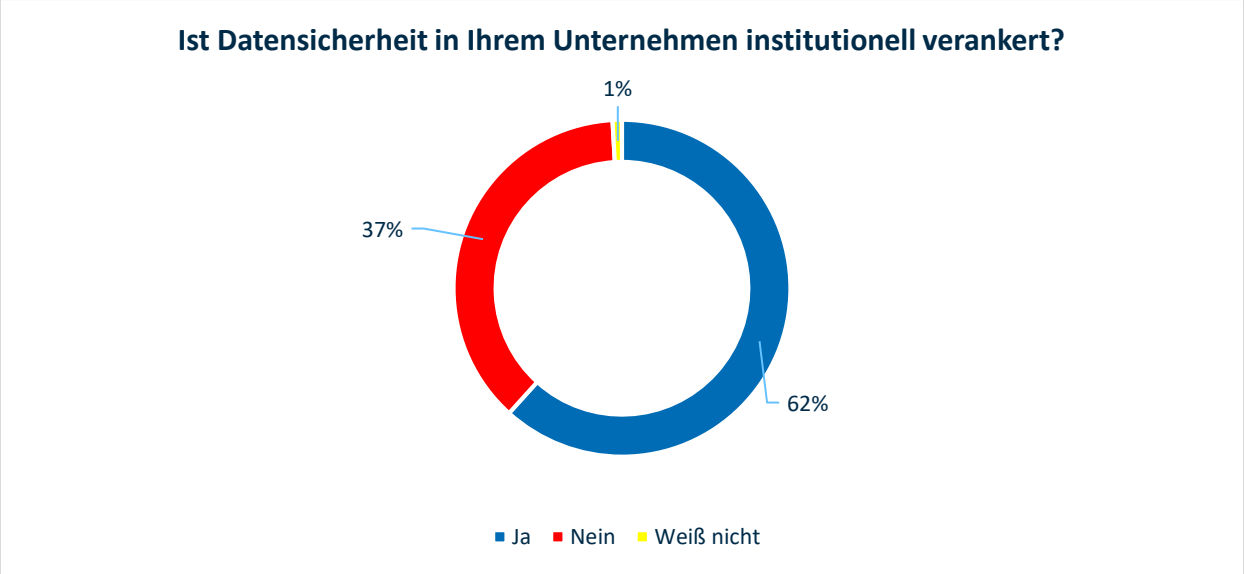
Ergebnisse nach Hierarchieebene

Wie stark ist Ihr Unternehmen vom Fachkräftemangel insb. bei Cybersicherheit betroffen?	Team	Lower-Management	Mid-Management	Top-Management
mehr als 6 Monate	34,8%	22,7%	35,7%	17,6%
zwischen 3 bis 6 Monate	26,1%	50%	35,7%	14,7%
weniger als 3 Monate	21,7%	13,6%	14,3%	2,9%
Nein, wir haben keinen Fachkräftemangel	17,4%	13,6%	14,3%	64,7%

Insbesondere die Ebene der Top-Manager gibt an, vom Fachkräftemangel nicht betroffen zu sein (64,7%) Nur jeder dritte Top-Manager sucht länger als drei Monate nach einem Experten für Cybersicherheit. Die Befragten aller anderen Hierarchie-Ebenen sind mehrheitlich vom Fachkräftemangel betroffen und benötigen 3 Monate, um eine entsprechende Vakanz zu besetzen.

Frage 7: Ist Datensicherheit in Ihrem Unternehmen institutionell verankert, z.B. durch Einrichtung eines Chief Information Security Officers (CISO)?

Betrachtung aller Befragten



Nahezu zwei von drei Befragten (61,7%) geben an, dass in ihrem Unternehmen Datensicherheit institutionell verankert sei, nahezu alle anderen Befragten (37,4%) antworteten mit „nein". Nur 0,9% der Probanden konnte die Frage nicht beantworten. Dies lässt auf ein großes Bewusstsein für die Notwendigkeit eines institutionell verankerten Datenschutzes in den Unternehmen schließen.

Ergebnisse nach Unternehmensgröße

Ist Datensicherheit in Ihrem Unternehmen institutionell verankert?	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	weniger als 50 Mitarbeiter
Ja	50%	61,5%	60%	71,4%	88,2%
Nein	47,7%	38,5%	40%	28,6%	11,8%

Es kann festgestellt werden, dass je größer ein Unternehmen ist, desto wahrscheinlicher es Datenschutz institutionell verankert hat. So hat nur jedes zweite kleine Unternehmen eine solche Struktur (50%), hingegen aber fast neun von zehn großen Unternehmen mit mehr als 1001 Mitarbeitern (88,2%).

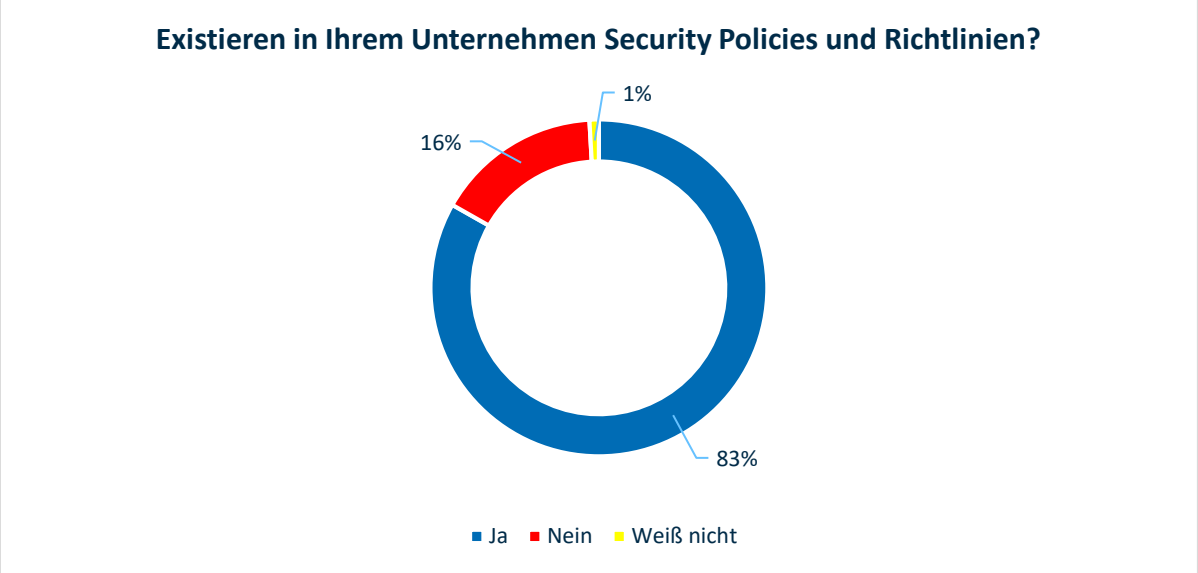
Ergebnisse nach Hierarchieebene

Ist Datensicherheit in Ihrem Unternehmen institutionell verankert?	Team	Lower-Management	Mid-Management	Top-Management
Ja	60,9%	77,3%	67,9%	47,1%
Nein	34,8%	22,7%	28,6%	52,9%

Auch bei dieser Betrachtung kann eine Abweichung der Antworten vom Top-Management im Vergleich zu den anderen Befragten festgestellt werden. So gibt die Mehrheit der Top-Manager an, über keine institutionelle Verankerung von Datensicherheit in ihren Unternehmen zu verfügen (52,9%). Die Befragten aller anderen Hierarchieebenen beantworten die Frage mehrheitlich mit „Ja".

Frage 8: Existieren in Ihrem Unternehmen Security Policies und Richtlinien?

Betrachtung aller Befragten



Vier von fünf Befragten antworteten mit „Ja" auf die Frage, ob in ihren Unternehmen Security Policies existieren. Nur 15,9% der Probanden befanden, dass es in ihrem Unternehmen keine solchen Policies und Richtlinien gibt. Da auch ein Großteil der Unternehmen der Befragten bereits eine Digitalstrategie entwickelt hat oder sich in der Entwicklung einer solchen Strategie befindet, kann festgestellt werden, dass Security Aspekte ein fester Bestandteil einer Digitalstrategie sind.

Ergebnisse nach Unternehmensgröße

Existieren in Ihrem Unternehmen Security Policies und Richtlinien?	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja	70,5%	84,6%	85%	100%	100%
Nein	27,3%	15,4%	15%	0%	0%

Es kann festgestellt werden, dass je größer das Unternehmen ist, desto eher existieren Security Policies und Richtlinien. Beantwortet noch jeder vierte Befragte, der einem kleinen Unternehmen mit bis zu 50 Mitarbeitern angehört, die Frage mit “Nein” (27,3%), sagen 100% der Mitarbeiter größerer und großer Unternehmen, dass sie über solche Richtlinien verfügen.

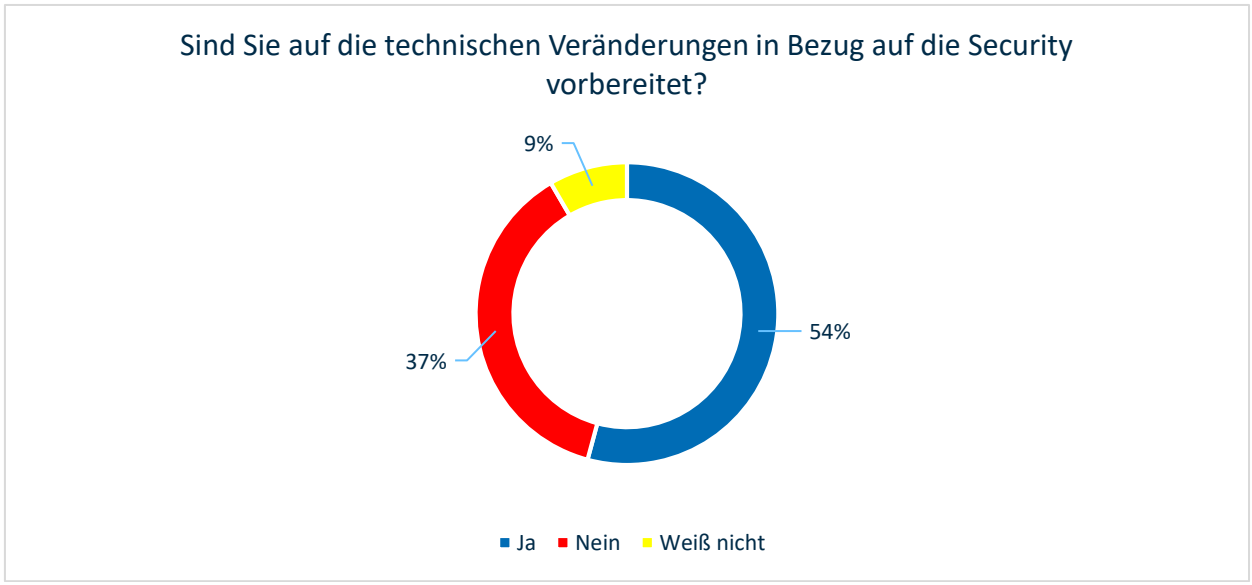
Ergebnisse nach Hierarchieebene

Existieren in Ihrem Unternehmen Security Policies und Richtlinien?	Team	Lower-Management	Mid-Management	Top-Management
Ja	87%	86,4%	89,3%	73,5%
Nein	13%	13,6%	7,1%	26,5%

Jeder vierte Angehörige des Top-Managements gibt an, dass in seinem Unternehmen Security Policies und Richtlinien nicht vorhanden sind. Angehörige aller anderen Hierarchie-Gruppen sagen mit großer Mehrheit aus, dass ihre Unternehmen über Security Policies und Richtlinien verfügt.

Frage 9: Sind Sie auf die technischen Veränderungen in Bezug auf die Security vorbereitet, z.B. durch DevSecOps, Cloud Services oder Security Automation?

Betrachtung aller Befragten



Die Mehrheit der Befragten ist sich sicher, ausreichend auf die technischen Veränderungen in Bezug auf die Security vorbereitet zu sein. Insgesamt antworteten 54,2 % mit ja. Nur etwa jeder dritte Befragte glaubt, dass sein Unternehmen noch Nachholbedarf hat (37,4%). Jeder zwölfte Befragte gibt an, diese Frage nicht beantworten zu können (8,4%).

Ergebnisse nach Unternehmensgröße

Sind Sie auf die technischen Veränderungen in Bezug auf die Security vorbereitet?	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja	63,6%	76,9%	35%	42,9%	47,1%
Nein	27,3%	15,4%	65%	50%	35,3%
Weiß nicht	9,1%	7,7%	0%	7,1%	17,6%

Insbesondere Befragte kleinerer Unternehmen mit bis zu 50 Mitarbeitern (63,6%) und 51 bis 100 Mitarbeitern (76,9%) sagen aus, dass sie gut auf die technischen Veränderungen in Bezug auf die Security vorbereitet sind. Hingegen Befragte mittelgroßer und großer Unternehmen fühlen sich eher nicht gut aufgestellt. Es ist anzunehmen, dass kleinere Unternehmen, die häufig das Thema Cybersicherheit outsourcen, sich aufgrund der eingekauften Expertise gut aufgestellt fühlen.

Auffällig ist, dass sogar fast jeder 5. Befragter, der Mitarbeiter eines großen Unternehmens ist, die Frage mit „weiß nicht" beantwortet hat (17,6%). Hier könnte die Ursache in der größeren Herausforderung der internen Kommunikation in großen Unternehmen vermutet werden.

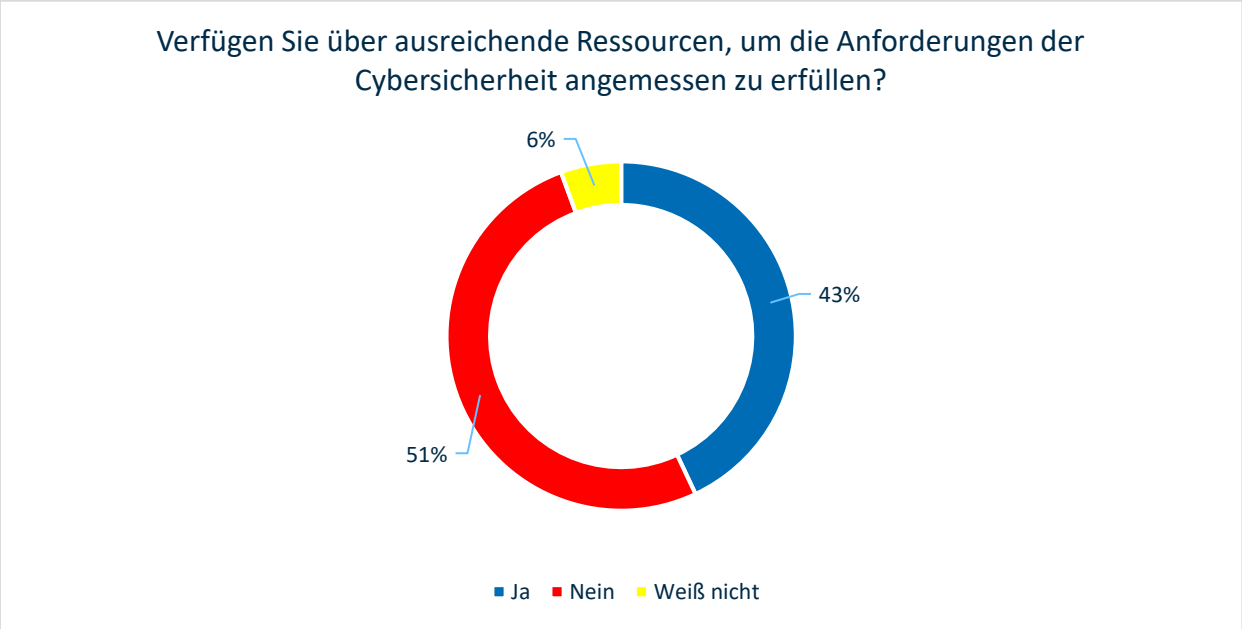
Ergebnisse nach Hierarchieebene

Sind Sie auf die technischen Veränderungen in Bezug auf die Security vorbereitet	**Team**	**Lower-Management**	**Mid-Management**	**Top-Management**
Ja	43,5%	59,1%	50%	61,8%
Nein	39,1%	40,9%	39,3%	32,4%
Weiß nicht	17,4%	0%	10,7%	5,9%

Insbesondere Top-Manager antworteten mit „Ja" auf die Frage, ob sie auf die technischen Veränderungen in Bezug auf die Security vorbereitet sind. (61,8%) Im Vergleich dazu sind nur 43,5 % der Team-Mitglieder davon überzeugt. Dies kann bedeuten, dass Security auf der Ebene der Top-Manager angesiedelt ist. Dafür spricht auch, dass mit 17,4% die meisten Angehörigen der Hierarchieebene der Team-Mitglieder „weiß nicht" auf die Frage geantwortet haben. Dagegen antworteten nur 5,9% der Top-Manager unentschieden.

Frage 10: Verfügen Sie über ausreichende Ressourcen, wie z.B. Mitarbeiter, Budget, Zugang zu neuesten Technologien usw., um die Anforderungen der Cybersicherheit angemessen zu erfüllen?

Betrachtung aller Befragten



Eine Mehrheit der Befragten (51,4%) bemängelt, dass ihre Unternehmen nicht über ausreichende Ressourcen verfügt, um die Anforderungen der Cybersicherheit angemessen zu erfüllen. 43% der Probanden beantworten die Frage mit „Ja".

Ergebnisse nach Unternehmensgröße

Verfügen Sie über ausreichende Ressourcen, um die Anforderungen der Cybersicherheit zu erfüllen?	weniger als 50 Mitarbeiter	51 bis 100 Mitarbeiter	101 bis 250 Mitarbeiter	251 bis 1000 Mitarbeiter	mehr als 1000 Mitarbeiter
Ja	54,6%	53,8%	40%	21,4%	23,5%
Nein	43,2%	38,5%	55%	71,4%	64,7%

Auch in Hinblick auf die Unternehmensgrößen ist festzustellen, dass die kleineren Unternehmen die Frage mehrheitlich positiv beantworten (<50 MA: 54,6%, 51-100 MA:53,8%). Die Angehörigen größerer und großer Unternehmen hingegen antworteten mehrheitlich mit "nein" auf die Frage nach ausreichend vorhandenen Ressourcen um die Anforderungen an Cybersicherheit angemessen zu erfüllen.

Ergebnisse nach Hierarchieebene

Verfügen Sie über ausreichende Ressourcen, um die Anforderungen der Cybersicherheit zu erfüllen?	Team	Lower-Management	Mid-Management	Top-Management
Ja	30,4%	36,4%	32,1%	64,5%
Nein	52,2%	59,1%	64,3%	35,5%

Die nach Hierarchie-Ebenen der Probanden geclusterten Ergebnisse zeigen wieder eine deutliche Abweichung in der Haltung der Top-Manager im Vergleich zu den anderen Hierarchieebenen. So sagen fast zwei Drittel der Top-Manager, dass ihre Unternehmen über ausreichend Ressourcen verfügen, um die Anforderungen der Cybersicherheit angemessen zu erfüllen. Lediglich ein Drittel der Befragten aller anderen Hierarchieebenen äußert sich ebenfalls positiv. Es scheint also hier einen Wahrnehmungsbruch zwischen Top-Managern mit Budget-Entscheidungsbefugnis und Hierarchieebenen, die für die Umsetzung der entsprechenden Maßnahmen verantwortlich sind, zu geben.

Zusammenfassung und Fazit

Diese Studie erhebt die Einstellungen von IT-Experten sowie Managern zu der Frage, inwieweit regulatorische Vorgaben zu Datenschutz und Cybersicherheit förderlich für die Digitalisierung in Unternehmen sind.

Die Studie wurde in drei Schwerpunktthemen unterteilt. In diesem Fazit werden die Ergebnisse nochmals zusammengefasst und ein Ausblick gegeben.

1. Welche Bedeutung hat Digitalisierung auf das Unternehmen? Verfügen Unternehmen über eine Digitalisierungsstrategie?

Den Einfluss der Digitalisierung auf das Geschäftsmodell bewerten vier von fünf Teilnehmern und Teilnehmerinnen als stark oder sehr stark. Jeder zweite Top-Manager konstatiert eine starke Beeinflussung, das Thema ist also strategisch in der obersten Führungsebene zu vermuten. Zudem sehen fast alle Befragten die Digitalisierung als Chance oder zumindest sowohl als Chance als auch als Risiko an für das eigene Unternehmen an (95,7%). Daher überrascht es nicht, dass die Unternehmen von mehr als 80% der Befragten bereits über eine Digitalstrategie verfügen oder diese gerade entwickeln.

Es kann also festgestellt werden, dass die digitale Transformation den deutschen Mittelstand stark beeinflusst und daher strategisch im Top-Management angesiedelt ist.

2. Welchen Einfluss hat Cybersicherheit auf die digitale Transformation von Unternehmen? Wird sie eher als eine Chance oder ein Hindernis durch die Professionals wahrgenommen?

Als Indikator zur Messung der Einstellung von IT-Professionals und Managern wurde die Einstellung zu vier unterschiedlichen regulatorischen Vorschriften abgefragt. Bezeichnend ist, dass sowohl bei der in der öffentlichen Diskussion durchaus umstrittenen Datenschutz-Grundverordnung (DS-GVO) als auch bei eher unbekannten Regelwerken wie den Best-Practise Vorgaben aus Normen wie NIST die Einstellung der Befragten hinsichtlich der Förderlichkeit eher positiv ist.

So sehen mehr als die Hälfte der Befragten die DS-GVO als förderlich an (53,65%). Etwa jeder dritte empfindet die DS-GVO allerdings als hinderlich. Weniger medial diskutierte Vorgaben wie das IT-Sicherheitsgesetz empfinden sogar fast zwei von drei Befragten als förderlich. Die BSI Grundschutz-Richtlinie wird sogar von 67,5% der Befragten als für die Digitalisierung des eigenen Unternehmens förderlich empfunden.

Und auch die Best-Practise Vorgaben aus Normen wie NIST werden von einem Großteil der Befragten als förderlich empfunden (47,1%), obwohl auch eine große Unkenntnis bezüglich der Vorgaben herrscht („Kann ich nicht einschätzen“: 35%, „Weiß ich nicht“: 10,6%).

Insgesamt ist festzustellen, dass nur einer von fünf Befragten gesetzliche Reglementierungen als für die Digitalisierung des eigenen Unternehmens hinderlich empfindet (20,7%).

3. Wie gut sind die Unternehmen in Hinblick auf die Anforderungen der Cybersicherheit ausgestattet?

Festzustellen ist ein Fachkräftemangel im Bereich der Cybersicherheit. So suchen die Unternehmen der Befragten mehrheitlich mindestens drei bis sechs Monate (29,1%) oder länger (30%) nach einem Mitarbeiter für entsprechende Vakanzen. Betroffen sind hier vor allem größere Unternehmen. Dennoch geben die Probanden mehrheitlich an, dass Datensicherheit in ihren Unternehmen institutionell verankert ist, beispielsweise durch die Beschäftigung eines Chief Information Security Officers. (61,7%) Dass Datenschutz und Cybersicherheit eine wichtige Position in der Digitalstrategie der Unternehmen der Befragten einnehmen, kann auch den Antworten auf die Frage nach vorhandenen Security Policies und entsprechenden Richtlinien entnommen werden: So geben vier von fünf Befragten (83,2%) an, dass in ihren Unternehmen entsprechende Prozesse bereits eingeführt wurden. Immerhin mehr als jeder zweite Teilnehmer bejaht zudem die Frage, ob sein Unternehmen hinsichtlich der IT-Sicherheit auf die technischen Veränderungen, die mit der Digitalisierung einhergehen, vorbereitet ist. (54,2%)

Dennoch gibt es bei den Befragten mehrheitlich die Sorge, nicht ausreichend auf Cyberkriminalität vorbereitet zu sein. Mehr als jeder zweite negiert die Frage, ob sein Unternehmen über ausreichend Ressourcen verfügt, um Anforderungen der Cybersicherheit angemessen erfüllen zu können. (51,4%) Hier gibt es scheinbar noch den größten Informationsbedarf hinsichtlich effizienter Sicherheits-Konzepte und deren Ausgestaltung.

Ausblick

Die vorliegende Studie befasste sich mit den grundsätzlichen Einstellungen von Experten und Managern zu regulatorischen Vorgaben zu Datenschutz und Cybersicherheit und deren Förderlichkeit für die Digitalisierung von Unternehmen. Wir haben feststellen können, dass die neuen Anforderungen an Sicherheit, die die digitale Transformation mit sich bringt, in den Unternehmen teilweise auf höchster Ebene angekommen sind und bereits umgesetzt werden. Entsprechende Vorgaben des Gesetzgebers werden hierbei als förderlich empfunden. Dennoch scheint es noch Unsicherheiten hinsichtlich konkreter Maßnahmen zu geben. Außerdem kann ein großer Fachkräftemangel im Bereich der Cybersicherheit festgestellt werden.

Hier gilt es die aktuellen Problemstellungen klarer zu benennen und mittels pragmatischer Lösungsansätze anzugehen. Zudem muss den Unternehmen der Zugang zu Expertise erleichtert werden – ob über externe Beratungsangebote, interne Schulungen oder die Erhöhung der vorhandenen Fachkräfte für Cybersicherheit. Der bereits beginnende Dialog zwischen Industrie, Politik und Experten muss weiter durch Initiativen intensiviert und strukturiert werden. Dieser Aufgabe müssen sich alle Beteiligten – der Mittelstand, die Politik und die Forschung, gemeinschaftlich stellen und gemeinsame Lösungen finden.

Anhang

Untersuchungsanlage

Bei der vorliegenden Studie handelt es sich um ein **exploratives Forschungsvorhaben**, da die Forschungsfrage vergleichsweise wenig bis gar nicht erforscht ist. Die Exploration wird im Verlauf durch weitere webbasierte Erhebungen sowohl vervollständigt als auch vertieft. Um das Themenfeld „Digitalisierung und Cybersicherheit“ vollumfänglich zu erschließen, werden daher verschiedene Forschungsstrategien **trianguliert**, die sowohl mehrere Online-Umfragen umfassen, aber auch durch Sekundärdaten gestützt werden.

Die Online-Umfrage startete am **18.März und wurde am 18. Juli 2019** beendet. In dieser Zeit haben insgesamt 156 Entscheidungsträger an der Online-Umfrage teilgenommen, davon haben 107 den Online-Fragebogen vollständig ausgefüllt.

Die Zielgruppe, zu denen hauptsächlich Geschäftsführer, Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Security Officer (CSO), Chief Technology Officer (CTO), Chief Digital Officer und Leiter von IT-Abteilungen sowie Spezialisten aus Unternehmensberatungen gehören, wurden überwiegend über **digitale Business-Netzwerke** rekrutiert. Ferner haben drei Verbände im Bereich Cybersicherheit und Digitalisierung den Link zur Online-Umfrage über ihre Newsletter- und Social Media-Verteiler beworben. In diesem Rahmen konnten Teilnehmer für die weitere Forschungsvorhaben rekrutiert werden.

Soziodemographische Daten

Es wurden insgesamt 142 Datensätze erfasst. Die Probanden wurden zu ihrem Alter und Geschlecht befragt. Hier eine Übersicht der Altersstruktur und der Geschlechterverteilung:

Alter	**Angaben**
<20-30 Jahre	16,8 %
31-40 Jahre	32,7 %
41-50	28 %
>51	21,5 %

Geschlecht	Angaben
männlich	15,9 %
weiblich	83,2 %
divers	0,93 %

Auswertung der Ergebnisse - Methodik

Betrachtung der Angaben aller Probanden

In den vorherigen Kapiteln wurden die Ergebnisse der Befragung vorgestellt und diskutiert. Tabellen und Grafiken veranschaulichen die gewonnen Erkenntnisse. Hierbei werden zunächst die Ergebnisse aller Befragten betrachtet.

Unterscheidung nach Unternehmensgrößen

Es erfolgt eine Diskussion der Antworten hinsichtlich der Unternehmensgröße, bei denen die Befragten tätig sind. Die Studie clustert diese in folgende fünf Typen:

- Kleine Unternehmen bis zu 50 Mitarbeitern (MA)
- Kleinere Unternehmen mit 51 bis zu 100 MA
- Mittelgroße Unternehmen mit 101 bis zu 250 MA
- Größere Unternehmen mit 251 bis zu 1000 MA
- Große Unternehmen ab 1001 MA

Hinsichtlich der Unternehmenszugehörigkeit teilen sich die Probanden wie folgt auf:

Bitte geben Sie an, wie groß das Unternehmen ist, in dem Sie beschäftigt sind	Angaben
weniger als 50 Mitarbeiter	41,1 %
51 bis 100 Mitarbeiter	12,2 %
101 bis 250 Mitarbeiter	18,7 %
251 bis 1000 Mitarbeiter	13,1 %
mehr als 1000 Mitarbeiter	15,9 %

Unterscheidung nach Zugehörigkeit zu hierarchischen Ebenen

Zuletzt betrachten wir die Antworten der Probanden hinsichtlich ihrer hierarchischen Zugehörigkeit. Diese wird von der Studie wie folgt erhoben:

- Team-Mitglied
- Lower Management (Teamleitung)
- Middle Management (Head of/Abteilungsleitung)
- Top Management (CTO, CEO)

Hinsichtlich der Zugehörigkeit zu bestimmten Hierarchieebenen teilen sich die Befragten wie folgt auf:

Hierarchieebene	**Angaben**
Top-Management	31,8 %
Mid-Management	26,2 %
Lower-Management	20,6 %
Team	21,5 %