

## Cybercrime im Mittelstand

Patrick Ulrich, Vanessa Frank, Alice Timmermann

Suggested citation:

Ulrich, P., Frank, V. and Timmermann, A. (2020), *Cybercrime im Mittelstand*.

### Abstract

Die Bedrohung durch Cyber-Kriminalität entwickelt sich ständig weiter. Auch die Studie des Aalener Instituts für Unternehmensführung (AAUF) zeigt, dass Cyber-Security ein durchaus Ernst zunehmendes Thema ist, dessen sich die Geschäftsleitung zwingend annehmen sollte, gehören Cyber-Angriffe doch mittlerweile schon zum Alltag vieler Unternehmen.

STAKEHOLDER  
MODELLE  
SYSTEME  
TRANSPARENZ  
VERHALTEN  
ENTSCHEIDUNGEN  
FAMILY BUSINESS  
VERANTWORTUNG  
INTEGRITÄT

**WERTORIENTIERUNG  
GOVERNANCE**

VERANTWORTUNG  
TRANSPARENZ  
RISK MANAGEMENT  
SYSTEME  
MODELLE  
INTERESSEN  
STAKEHOLDER  
TRANSFER  
FORSCHUNG

## **Cybercrime im Mittelstand**

**Studienserie „Erfolgsfaktoren der  
Unternehmensführung“**

**Band 5, ISBN 978-3-947393-04-6**

## Impressum

*Direktorium* Professor Dr. habil. Patrick Ulrich  
Professor Dr. Ingo Scheuermann

*Wissenschaftlicher Projektleiter* Professor Dr. habil. Patrick Ulrich

*Weitere beteiligte Personen* Vanessa Frank  
Alice Timmermann

*Herausgeber* Professor Dr. habil. Patrick Ulrich  
Professor Dr. Ingo Scheuermann

Hochschule Aalen  
Aalener Institut für Unternehmensführung (AAUF)  
Beethovenstr. 1  
D-73430 Aalen

*Copyright* © 2020 by Aalener Institut für Unternehmensführung (AAUF)

*Druck* Aalen 2020  
Printed in Germany

# Inhaltsverzeichnis

<b>Executive Summary .....</b>	<b>6</b>
<b>1 Einleitung.....</b>	<b>8</b>
1.1 Zielsetzung und Aufbau der Studie .....	8
1.2 Methodik .....	9
<b>2 Allgemeine Angaben zum Unternehmen .....</b>	<b>11</b>
2.1 Rechtsform .....	11
2.2 Verteilung nach Branche .....	12
2.3 Unternehmensbereich der befragten Person .....	13
2.4 Gesamtumsatz im letzten Geschäftsjahr.....	14
2.5 Anzahl der Mitarbeiter/innen .....	15
2.6 Familienunternehmen.....	16
<b>3 Menschliche Risiken versus technische Risiken .....</b>	<b>17</b>
3.1 Priorität von Cyber-Security .....	17
3.2 Häufigkeit von Cyber-Attacken .....	18
3.3 Einschätzung der größten Herausforderungen bei Cyber-Attacken .....	18
3.4 Identifizierung der Angreifer bei Cyber-Attacken .....	19
3.5 Priorität von Cyber-Risiken.....	20
3.6 Bewertung von Cyber-Risiken .....	21
3.7 Herausforderungen in der Abwehr aktueller Cyber-Risiken .....	22
3.8 Regelmäßigkeit in der Identifizierung und Überwachung von Cyber-Risiken.....	23
3.9 Sicherheitslücken im Unternehmen.....	24
3.10 Entdeckung von Sicherheitslücken.....	25
3.11 Dauer der Entdeckung von Sicherheitslücken.....	26
3.12 Dauer der Entdeckung bei Verstößen gegen Sicherheitsbestimmungen .....	28
<b>4 Mögliche Verlustszenarien .....</b>	<b>29</b>
4.1 Schadenspotenzial verschiedener Cyber-Attacken .....	29
4.2 Vorhandensein eines Notfall-Reaktionsplans .....	30
4.3 Verbesserungspotenziale im Reaktionsplan .....	31
4.4 Finanzielle Mittel zur Abwehr eines Cyber-Angriffs.....	32
<b>5 Organisatorische Fragestellungen .....</b>	<b>33</b>
5.1 Cyber-Security als Teil der Unternehmensstrategie .....	33
5.2 Nutzung eines Information Security Management Systems (ISMS) .....	34
5.3 Funktionsfähigkeit bestimmter Prozesse innerhalb der eigenen Organisation im Hinblick auf Cyber-Attacken.....	34
5.4 Verantwortungsträger für Informationssicherheit .....	35

5.5	Einschätzung der Kompetenzen von Führungskräften .....	36
5.6	Schulungs- und Weiterbildungsangebote für Mitarbeiter und Führungskräfte .....	37
5.7	Sensibilisierung von Mitarbeitern in verschiedenen Bereichen der Informationssicherheit	38
5.8	Durchführung von Cyber-Sicherheitsinitiativen .....	40
<b>6</b>	<b>Cyberversicherung .....</b>	<b>41</b>
6.1	Jährliche Ausgaben für Cyber-Security.....	41
6.2	Zuordnung der Kosten für Cyber-Security.....	42
6.3	Geplante Investitionskosten für 2020 im Vergleich zum Vorjahr .....	43
6.4	Anteil der Unternehmen mit Cyber-Versicherung .....	44
6.5	Durch die Cyber-Versicherung abgedeckte Risiken .....	45
<b>7</b>	<b>Erfolgseinschätzung.....</b>	<b>47</b>
7.1	Prozessuale Verbesserungspotenziale .....	47
7.2	Aktuelle und zukünftige Relevanz von Cyber-Security im Unternehmen .....	49
	<b>Literatur .....</b>	<b>51</b>

# Abbildungsverzeichnis

ABBILDUNG 1: TEILNAHME-, AUSSCHÖPFUNGS- UND RÜCKLAUFQUOTE .....	10
ABBILDUNG 2: RECHTSFORM.....	11
ABBILDUNG 3: VERTEILUNG NACH BRANCHE.....	12
ABBILDUNG 4: UNTERNEHMENSBEREICH .....	13
ABBILDUNG 5: UMSATZ IN MIO. EUR .....	14
ABBILDUNG 6: ANZAHL DER MITARBEITER/INNEN .....	15
ABBILDUNG 7: FAMILIENUNTERNEHMEN.....	16
ABBILDUNG 8: PRIORITÄT CYBER-SECURITY .....	17
ABBILDUNG 9: ANZAHL DER CYBER-ATTACKEN.....	18
ABBILDUNG 10: HERAUSFORDERUNGEN BEI CYBER-ATTACKEN .....	19
ABBILDUNG 11: ANGREIFER .....	20
ABBILDUNG 12: PRIORITÄT VON CYBER-RISIKEN .....	21
ABBILDUNG 13: BEWERTUNG VON CYBER-RISIKEN .....	22
ABBILDUNG 14: HERAUSFORDERUNGEN IN DER ABWEHR VON CYBER-RISIKEN.....	23
ABBILDUNG 15: IDENTIFIZIERUNG UND ÜBERWACHUNG VON CYBER-RISIKEN .....	24
ABBILDUNG 16: SICHERHEITSLÜCKEN .....	25
ABBILDUNG 17: ENTDECKUNG VON SICHERHEITSLÜCKEN .....	26
ABBILDUNG 18: DAUER DER ENTDECKUNG VON SICHERHEITSLÜCKEN .....	27
ABBILDUNG 19: DAUER DER ENTDECKUNG BEI SICHERHEITSVERSTÖßEN.....	28
ABBILDUNG 20: SCHADENSPOTENZIAL VON CYBER-ATTACKEN .....	29
ABBILDUNG 21: REAKTIONSPLAN FÜR DEN FALL EINES CYBER-ANGRIFFS .....	30
ABBILDUNG 22: VERBESSERUNGSPOTENZIAL .....	31
ABBILDUNG 23: VORHANDENSEIN FINANZIELLER MITTEL FÜR ABWEHR .....	32
ABBILDUNG 24: CYBER-SECURITY TEIL DER UNTERNEHMENSSTRATEGIE.....	33
ABBILDUNG 25: NUTZUNG EINES ISMS.....	34
ABBILDUNG 26: FUNKTIONSFÄHIGKEIT VON PROZESSEN.....	35
ABBILDUNG 27: VERANTWORTUNGSTRÄGER INFORMATIONSSICHERHEIT.....	36
ABBILDUNG 28: KOMPETENZ FÜHRUNGSKRÄFTE.....	37
ABBILDUNG 29: INTERNE UND EXTERNE WEITERBILDUNGSMAßNAHMEN .....	38
ABBILDUNG 30: SENSIBILISIERUNG DER MITARBEITER TEIL 1 .....	39
ABBILDUNG 31: SENSIBILISIERUNG DER MITARBEITER TEIL 2 .....	39
ABBILDUNG 32: HÄUFIGKEIT VON CYBERSICHERHEITSINITIATIVEN TEIL 1 .....	40
ABBILDUNG 33: HÄUFIGKEIT VON CYBERSICHERHEITSINITIATIVEN TEIL 2 .....	41
ABBILDUNG 34: AUSGABEN FÜR CYBER-SECURITY .....	42
ABBILDUNG 35: CYBER-SECURITY KOSTEN .....	43
ABBILDUNG 36: GEPLANTE INVESTITIONSKOSTEN FÜR CYBER-SECURITY .....	44
ABBILDUNG 37: VORHANDENSEIN EINER CYBER-SECURITY .....	45
ABBILDUNG 38: ABGEDECKTE RISIKEN.....	46
ABBILDUNG 39: VERBESSERUNGSPOTENZIAL IN PROZESSEN .....	48
ABBILDUNG 40: RELEVANZ VON CYBER-SECURITY TEIL 1.....	49
ABBILDUNG 41: RELEVANZ VON CYBER-SECURITY TEIL 2.....	50

## Executive Summary

Die Bedrohung durch Cyber-Kriminalität entwickelt sich ständig weiter. Auch die Studie des Aalener Instituts für Unternehmensführung (AAUF) zeigt, dass Cyber-Security ein durchaus Ernst zunehmendes Thema ist, dessen sich die Geschäftsleitung zwingend annehmen sollte, gehören Cyber-Angriffe doch mittlerweile schon zum Alltag vieler Unternehmen.

Knapp die Hälfte der Studienteilnehmer wird täglich von bis zu 10 internen Cyber-Attacken ausspioniert oder geschädigt (externe Cyber-Attacken 38 Prozent). Die Bedrohung ist den Unternehmen durchaus bekannt, daher setzen sie auch stark auf konventionelle Sicherheitsvorkehrungen. 89 Prozent der Probanden setzen häufig einen Virenschanner oder 84 Prozent eine Firewall ein. Mehr als die Hälfte der befragten Unternehmen legt die Anwendung von Zugriffsrechten fest und nutzt einen Passwortschutz.

Einige Unternehmen sind somit schon gut vorbereitet, allerdings zeigt sich noch Nachholbedarf hinsichtlich der organisatorischen Umsetzung. Bei fast 40 Prozent der Studienteilnehmer ist Cyber-Security kein Teil der Unternehmensstrategie. Auch nur 43 Prozent haben einen Notfall-Reaktionsplan ausgearbeitet. Zwar geben 23 Prozent an, einen in Planung zu haben aber auch 34 Prozent verfügen über keinen solchen Reaktionsplan. Des Weiteren lässt sich der Umfrage entnehmen, dass nur 26 Prozent der Befragten ein Information Security Management System (ISMS) nutzen, welches das Ziel hat die Informationssicherheit dauerhaft festzuschreiben, zu steuern, zu kontrollieren und fortlaufend aufrechtzuerhalten.

Zwar sind 70 Prozent der Probanden im Falle eines Cyber-Angriffs ausreichend über die erforderlichen finanziellen Mittel abgesichert, jedoch treffen die Unternehmen auf einige große Herausforderungen, die die Abwehr eines Angriffs erschweren. Das fehlende Security Bewusstsein der Mitarbeiter, aber auch das frühzeitige Erkennen der relevanten Angriffe entpuppen sich als die beiden größten Herausforderungen. Über die Hälfte schätzt aber auch das Umsetzen der Sicherheitsstandards im Unternehmen als sehr große Herausforderung ein. Des Weiteren mangelt es den Unternehmen an der regelmäßigen Identifizierung und Überwachung der Cyber-Risiken, denn nur 15 Prozent der Probanden geben an, Cyber-Risiken sehr regelmäßig zu überwachen.

Weitere organisatorische Gründe, wie die innerbetriebliche Reaktionsgeschwindigkeit auf Cyber-Attacken wird von 57 Prozent als große Herausforderung wahrgenommen. Auch die mangelnde Vorbereitung der Mitarbeiter auf solche Angriffe, die ungeschulten Mitarbeiter und zunehmende Nutzung mobiler Endgeräte sowie die Identifikation eines tatsächlichen Cyber-Angriffs stellen weitere Herausforderungen und somit Sicherheitslücken im Unternehmen dar.

Insbesondere ist eine zuständige Fachabteilung bezüglich des Themas Cyber-Security gefragt passende Strategien zu entwickeln, die Bewertung von Cyber-Risiken zu veranlassen und geeignete Schutzmaßnahmen umzusetzen. In genau der Hälfte der Unternehmen ist eine zuständige Fachabteilung Verantwortungsträger der Informationssicherheit. Ein Datenschutzbeauftragter ist in 30 Prozent und der Geschäftsführer in nur 23 Prozent der Fälle dafür zuständig. Die Kompetenzen der Führungskräfte im Bereich Cyber-Security werden von knapp der Hälfte als stark ausgeprägt eingeschätzt. Mit der Sozialkompetenz sind die Führungskräfte mit 48 Prozent, der Fachkompetenz mit 43 Prozent und der Methodenkompetenz mit 39 Prozent stark ausgestattet.

Hinsichtlich der Sensibilisierung der Mitarbeiter ist knapp die Hälfte der Unternehmen der Ansicht, dass insbesondere die Sensibilisierung in den Bereichen Cloud Security zu 45 Prozent, Sicherheit mobiler Endgeräte zu 44 Prozent und Datenträger sowie im Bereich Informationsklassifizierung jeweils zu 42 Prozent gering ausfällt.

# 1 Einleitung

## 1.1 Zielsetzung und Aufbau der Studie

Eine zunehmende Vernetzung und Digitalisierung von Geschäftsprozessen, vom Einkauf beim Lieferanten bis hin zum Vertrieb beim Kunden, stellt Unternehmen vor neue, sicherheitstechnische Herausforderungen. Trotz dieser eindeutigen Entwicklung werden Cyber-Risiken, noch immer, häufig unterschätzt. Sie werden als etwas Abstraktes wahrgenommen. Das Schadenspotenzial ist den Unternehmen oftmals nicht bewusst. Häufig sind immaterielle Werte durch Cyber-Risiken in Gefahr, welche sich nur schwer eindeutig beziffern lassen. Ein einziger Cyber-Angriff, besonders für kleine und mittlere Unternehmen, kann schnell zu einer ernstzunehmenden Bedrohung für den Unternehmenserfolg werden oder gar existenzbedrohende Ausmaße annehmen. Wie real die Bedrohung durch Cyber-Kriminelle wirklich ist, zeigt eine Cyber-Sicherheitsumfrage<sup>1</sup>, die das BSI im Rahmen der Allianz für Cyber-Sicherheit 2019 deutschlandweit mit 1.039 Unternehmen und anderen Institutionen durchführte. Danach hatten deutschlandweit ein Drittel (33 Prozent) aller befragten Betriebe Cyber-Sicherheitsvorfälle zu verzeichnen; 26 Prozent der kleinen und mittelständischen Unternehmen gaben an, 2018 von Cyber-Attacken betroffen gewesen zu sein.<sup>2</sup> Bei einem Großteil hatten die Cyber-Sicherheitsvorfälle Betriebsstörungen oder -ausfälle (87 Prozent) sowie erhebliche Kosten (65 Prozent) für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme zur Folge.<sup>3</sup>

Da aufgrund des voranschreitenden technologischen Fortschritts das Thema Cyber-Security zukünftig noch stärker an Bedeutung gewinnen wird, hat das Aalener Institut für Unternehmensführung (AAUF) eine Studie zu Cyber-Security im deutschen Mittelstand durchgeführt.

Ziel der Studie ist es, den aktuellen Stand zu Cyber-Kriminalität, Cyber-Risiken und Cyber-Sicherheit im deutschen Mittelstand darzulegen. Hierbei stehen insbesondere

---

<sup>1</sup> Bundesamt für Sicherheit in der Informationstechnik (2019): Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen – Fassung vom 18.04.2019.

<sup>2</sup> Bundesamt für Sicherheit in der Informationstechnik (2019): Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen – Fassung vom 18.04.2019, S. 11 u. 25.

<sup>3</sup> Bundesamt für Sicherheit in der Informationstechnik (2019): Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen, Fassung vom 18.04.2019, S. 12.

die Ausgestaltung des Cyber-Sicherheits-Managements sowie aktuelle Herausforderungen im Mittelpunkt.

## 1.2 Methodik

Die Datenerhebung erfolgte mit Hilfe eines standardisierten Online-Fragebogens, der offene und geschlossene Fragen enthielt. Zur Überprüfung des Fragebogens wurde zunächst ein Pre-Test mit mehreren Probanden durchgeführt. Im Anschluss erfolgte die tatsächliche Befragung im Zeitraum vom 23.10.2019 bis zum 31.12.2019. Hierfür wurden vorab mit Hilfe der Datenbank Nexis per Zufallsprinzip E-Mail-Adressen von deutschen Unternehmen generiert.

Insgesamt wurden 14.495 Unternehmen per E-Mail kontaktiert, wobei 1.612 E-Mails nicht zugestellt werden konnten. Somit erhielten 12.883 Unternehmen den Link zur Onlineumfrage. Der Onlinefragebogen wurde im Befragungszeitraum 415-mal aufgerufen, was einer Teilnahmequote von 3,22 Prozent entspricht. 372 Unternehmen beantworteten die gestellten Fragen, wobei 188 Unternehmen die Umfrage vorzeitig abgebrochen haben (Ausschöpfungsquote: 89,64 Prozent). Die Stichprobengröße beläuft sich somit auf 184 Unternehmen und die Rücklaufquote auf 1,43 Prozent.

In diesem Zusammenhang ist anzumerken, dass es bei einzelnen Fragestellungen dennoch zu unterschiedlichen Nennungen kommen kann, da der partielle Antwortausfall (Item-Non-Response) im vorliegenden Ergebnisbericht nicht berücksichtigt wurde. Dies liegt daran, dass bei der Gestaltung des Fragebogens bewusst auf das Festlegen von Pflichtfragen verzichtet wurde, da teilweise sehr themenspezifische und sensible Daten abgefragt wurden. Die Auswertung der Daten erfolgte mittels Microsoft Excel.

Abbildung 1 veranschaulicht die Berechnung der Teilnahme-, Ausschöpfungs- und Rücklaufquote.

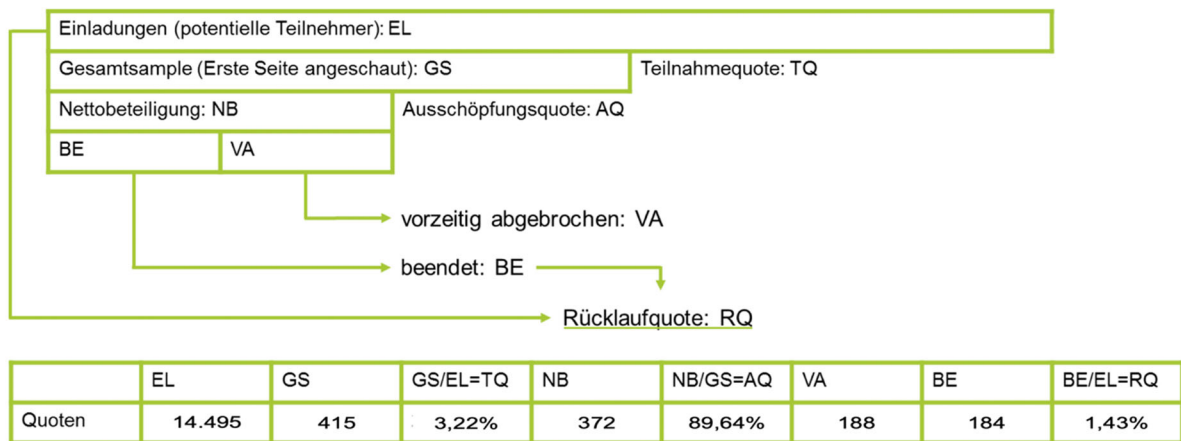


ABBILDUNG 1: TEILNAHME-, AUSSCHÖPFUNGS- UND RÜCKLAUFQUOTE

Der Fragebogen enthielt 36 Fragen, welche in sechs Abschnitte unterteilt waren. Zunächst wurden Angaben zum Unternehmen sowie zum Bearbeiter abgefragt, gefolgt von der Abfrage des Verständnisses und dem Bewusstsein für Cyber-Risiken und deren Schadenspotenzial. Im darauffolgenden Abschnitt wurden präventive Sicherheitsmaßnahmen thematisiert, während anschließend die Beurteilung des Cyber-Risk-Management und Cyber-Security-Managements erfolgte.

## 2 Allgemeine Angaben zum Unternehmen

In diesem Kapitel sind Details zu den teilnehmenden Unternehmen enthalten wie bspw. Rechtsform, Umsatz und Mitarbeiteranzahl.

### 2.1 Rechtsform

Gemäß den Angaben der Probanden haben 55 Prozent der Unternehmen die Rechtsform einer GmbH inne. 24 Prozent der Teilnehmer tragen das Rechtskleid einer GmbH & Co. KG. 11 Prozent geben an, eine andere Rechtsform zu haben, und 6 Prozent der Probanden teilen mit, dass es sich bei der Rechtsform ihres Unternehmens um eine AG handelt. Nur 2 Prozent führen an, dass ihr Unternehmen eine KG ist, 1 Prozent der Probanden ist als OHG und weitere 1 Prozent als GbR firmiert.

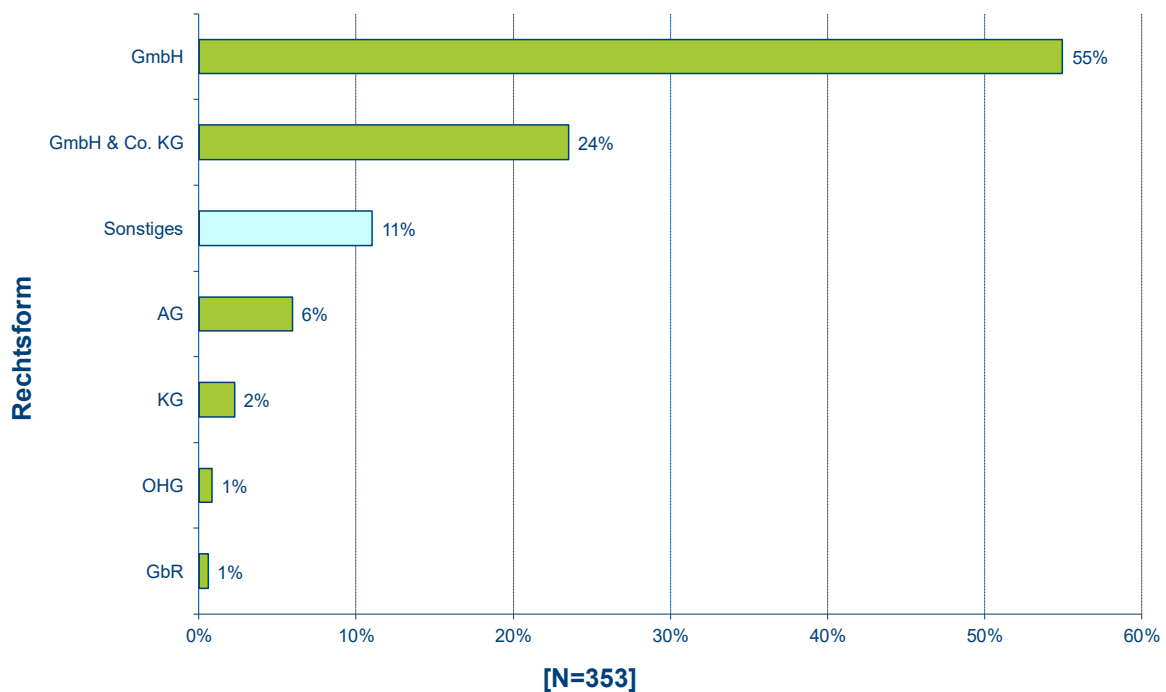


ABBILDUNG 2: RECHTSFORM

## 2.2 Verteilung nach Branche

Die Branchenzugehörigkeit der Unternehmen gestaltet sich wie folgt: 24 Prozent der Unternehmen sind im Dienstleistungsbereich tätig, 17 Prozent im Maschinen- und Anlagenbau und 9 Prozent in der Automobilindustrie. 6 Prozent der Probanden sind Logistikunternehmen und 3 Prozent im Bereich Medizintechnik tätig. Die verbleibenden 41 Prozent fallen unter „Sonstige/Keine Angaben“.

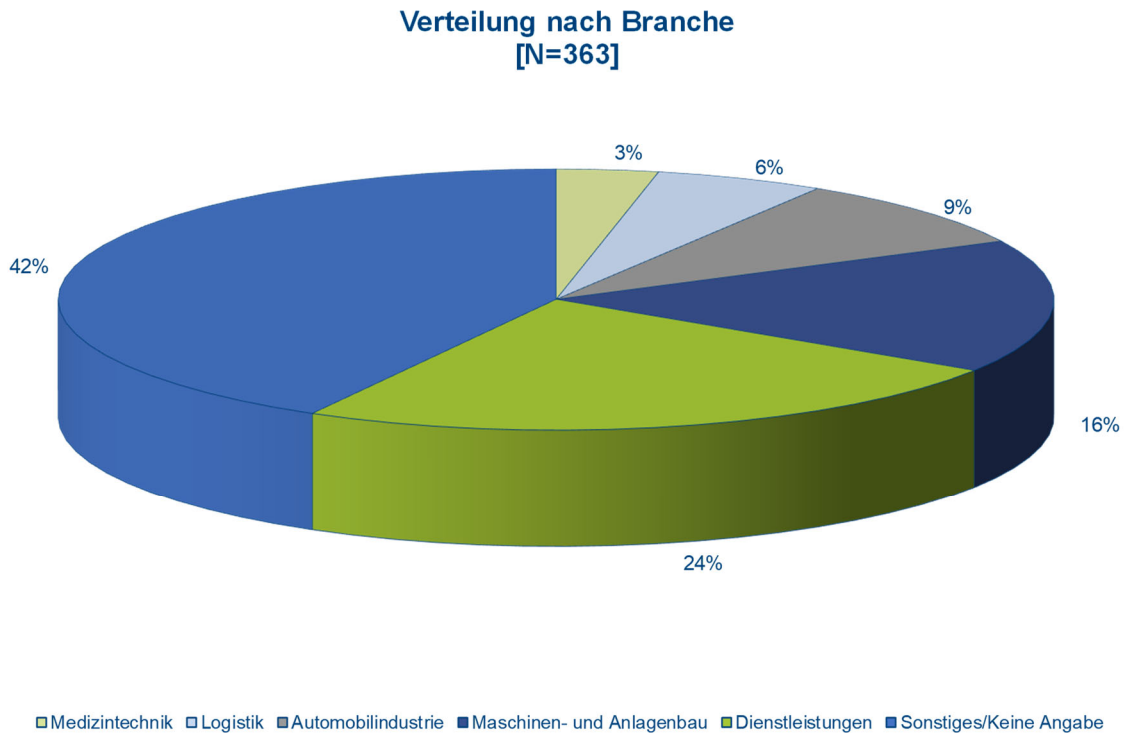


ABBILDUNG 3: VERTEILUNG NACH BRANCHE

## 2.3 Unternehmensbereich der befragten Person

Von den befragten Probanden sind 54 Prozent in der IT beschäftigt. 28 Prozent geben an der Geschäftsführung zugehörig zu sein. Des Weiteren sind 4 Prozent im Controlling tätig, 2 Prozent im Bereich HR und weitere 2 Prozent arbeiten in der Produktion. 10 Prozent fallen auf „Sonstige/Keine Angaben“.

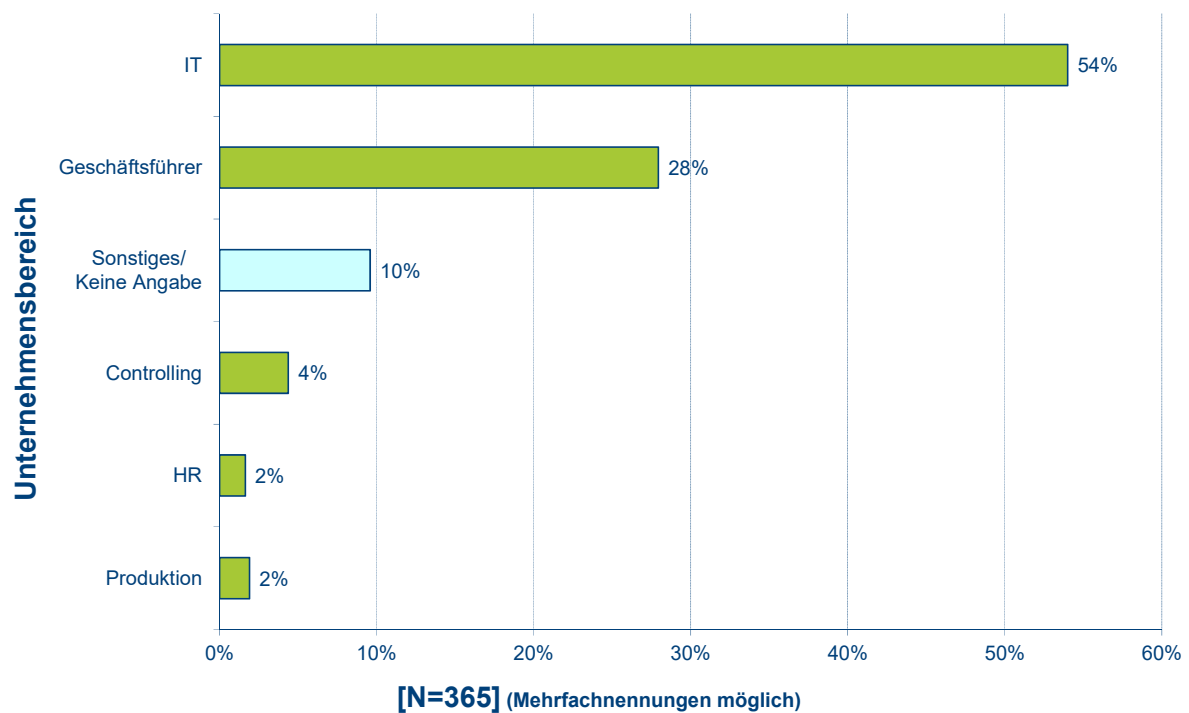


ABBILDUNG 4: UNTERNEHMENSBEREICH

## 2.4 Gesamtumsatz im letzten Geschäftsjahr

Der jährliche Gesamtumsatz der befragten Unternehmen variiert stark. 79 Prozent der befragten Unternehmen erwirtschafteten einen Umsatz bis zu 100 Mio. Euro, 13 Prozent liegen bei einem Umsatz zwischen 100 und 1.000 Mio. Euro. Weitere 5 Prozent erzielten einen Umsatz zwischen 1.000 Mio. und 10.000 Mio. Euro. Lediglich 3 Prozent der befragten Unternehmen geben an einen Umsatz von über 10.000 Mio. Euro erwirtschaftet zu haben. Das arithmetische Mittel des von allen Probanden angegebenen Jahresumsatzes liegt bei 714 Mio. Euro.

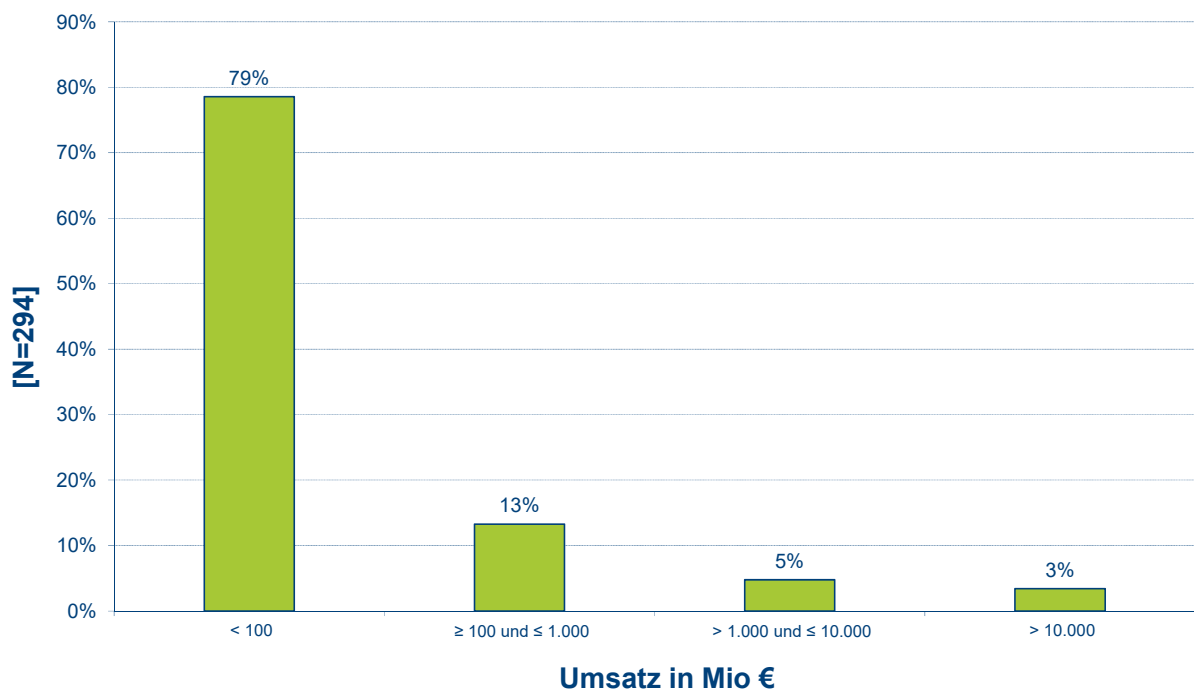


ABBILDUNG 5: UMSATZ IN MIO. EUR

## 2.5 Anzahl der Mitarbeiter/innen

Weniger als 100 Mitarbeiter/innen beschäftigen 18 Prozent der befragten Unternehmen. Die Mehrheit mit 73 Prozent machen Unternehmen mit 100 bis 1.000 Mitarbeiter/innen aus. Zwischen 1.000 und 10.000 Mitarbeiter/innen haben 8 Prozent der Unternehmen und bei 1 Prozent der Unternehmen arbeiten über 10.000 Mitarbeiter/innen. Das arithmetische Mittel aller Angaben beläuft sich auf 974 Mitarbeiter/innen.

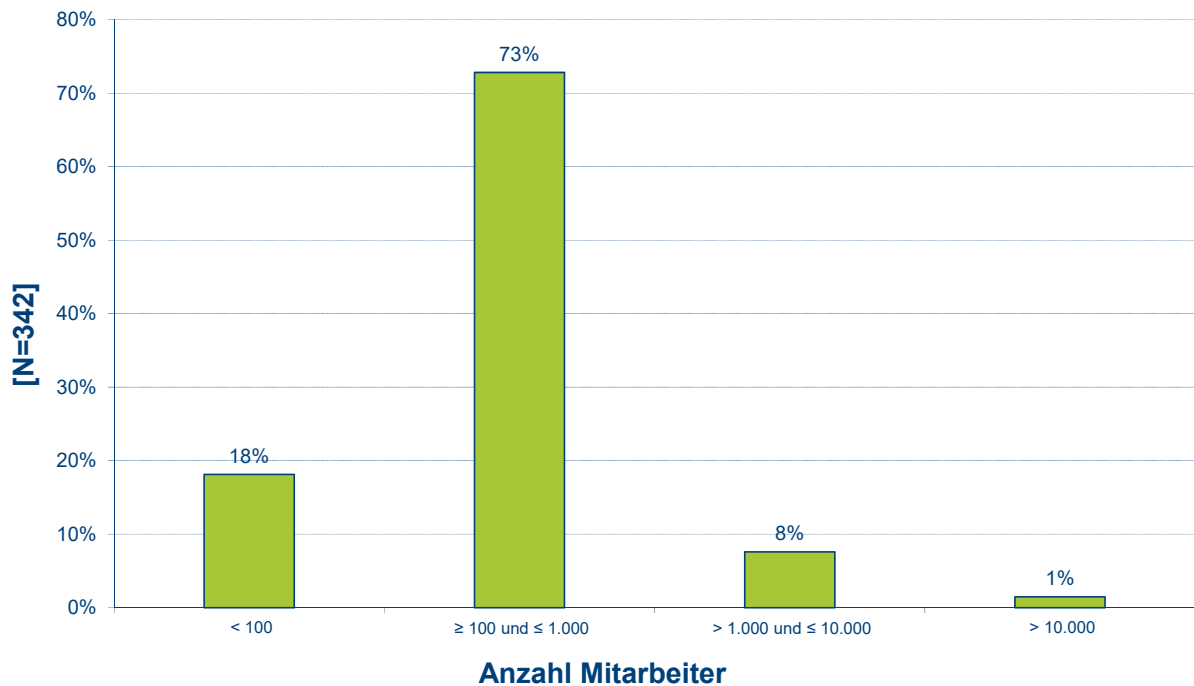


ABBILDUNG 6: ANZAHL DER MITARBEITER/INNEN

## 2.6 Familienunternehmen

Die Frage, ob es sich bei dem Unternehmen um ein Familienunternehmen handelt, beantworteten 54 Prozent der befragten Unternehmen mit „Ja“. Entsprechend sind 46 Prozent der Teilnehmer keine Familienunternehmen.

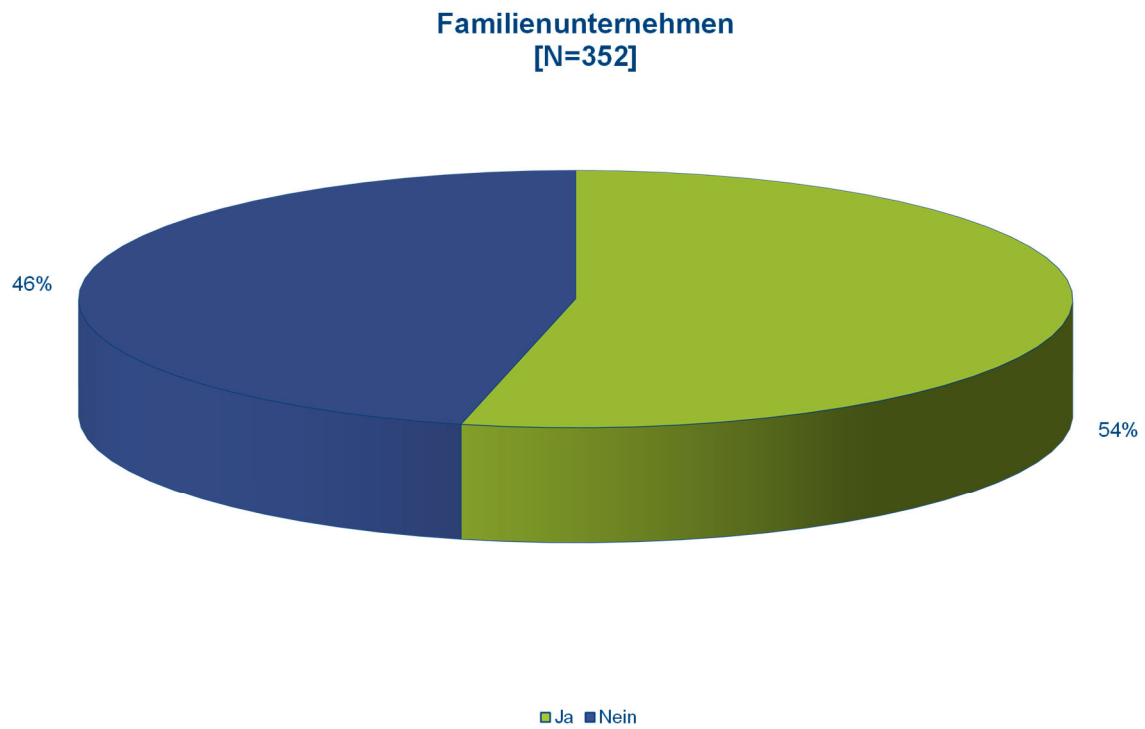


ABBILDUNG 7: FAMILIENUNTERNEHMEN

### 3 Menschliche Risiken versus technische Risiken

Das nachfolgende Kapitel thematisiert die Bedeutung von Cyber-Angriffen in Unternehmen.

#### 3.1 Priorität von Cyber-Security

Laut der Umfrage zählt für knapp die Hälfte der befragten Unternehmen das Thema Cyber-Security nicht zu den Top-Prioritäten der Geschäftsführung. 32 Prozent geben an, der Cyber-Security eine mittlere Priorität zuzuordnen, und 9 Prozent weisen dem Thema eine geringe Priorität zu. Eine sehr geringe Priorität geben 1 Prozent der befragten Unternehmen an. Eine hohe Priorität geben 42 Prozent an und 16 Prozent der Probanden messen der Cyber-Security eine sehr hohe Bedeutung bei.

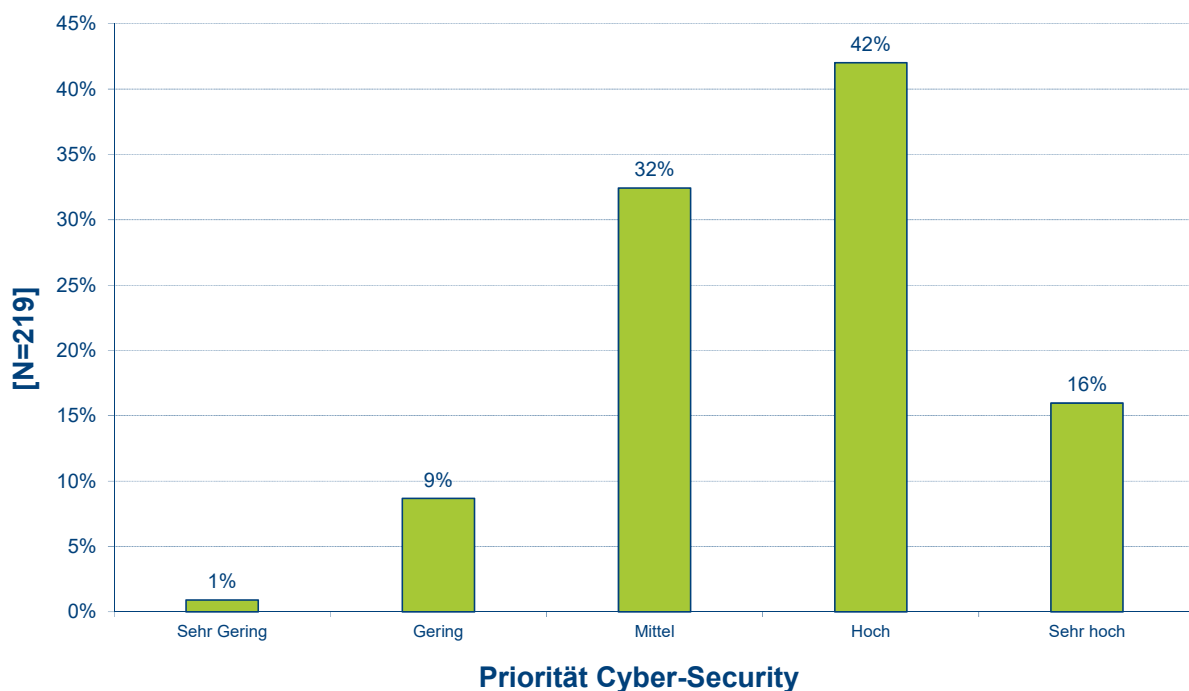


ABBILDUNG 8: PRIORITÄT CYBER-SECURITY

### 3.2 Häufigkeit von Cyber-Attacken

Im Anschluss wurden sämtliche Teilnehmer befragt, mit wie vielen (internen und externen) Cyber-Attacken das Unternehmen täglich zu kämpfen hat. Bei 45 Prozent der Befragten liegen die internen Cyber-Attacken am Tag unter 10. Bei externen Cyber-Attacken sind es 38 Prozent. Zwischen 10 und 100 internen Cyber-Attacken zu verzeichnen haben 6 Prozent, extern 34 Prozent. Bei 2 Prozent liegen die internen Attacken zwischen 100 und 1.000 täglich, 12 Prozent geben an täglich zwischen 100 und 1.000 externen Attacken ausgesetzt zu sein. Die Häufigkeit von internen Attacken zwischen 1.000 und 10.000 liegt bei 1 Prozent, extern bei 6 Prozent. Mehr als 10.000 interne Cyber-Attacken gehabt zu haben geben 1 Prozent der Befragten an. Weitere 1 Prozent der Unternehmen berichten von mehr als 10.000 externen Cyber-Attacken.

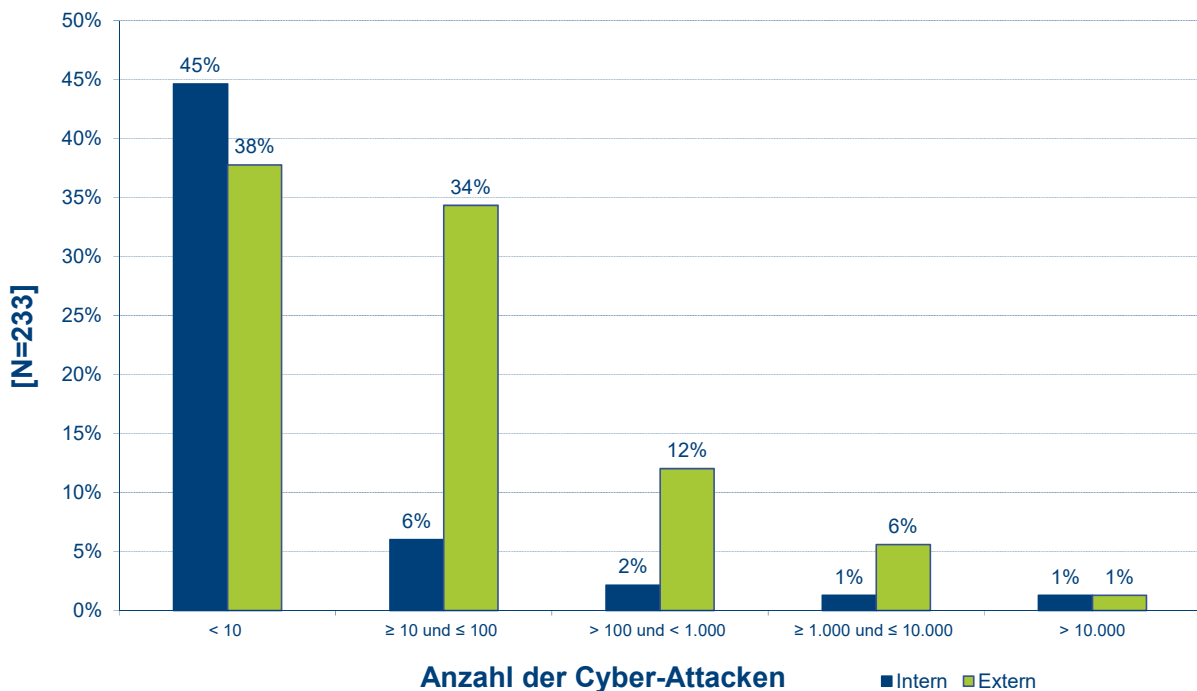


ABBILDUNG 9: ANZAHL DER CYBER-ATTACKEN

### 3.3 Einschätzung der größten Herausforderungen bei Cyber-Attacken

Über die Hälfte der Unternehmen (57 Prozent: 21 Prozent sehr groß und 36 Prozent groß) sieht besonders in der innerbetrieblichen Reaktionsgeschwindigkeit auf Cyber-Attacken eine große Herausforderung. Für die Hälfte (50 Prozent) der befragten Probanden ist die Identifikation eines tatsächlichen Cyber-Angriffs sehr

herausfordernd (18 Prozent sehr groß und 32 Prozent groß). 42 Prozent (14 Prozent sehr groß und 28 Prozent groß) der teilnehmenden Unternehmen sind der Ansicht, die mangelnde Vorbereitung der Mitarbeiter auf Cyber-Angriffe stelle eine große Herausforderung dar. Ebenfalls 42 Prozent (11 Prozent sehr groß und 31 Prozent groß) bewerten den unternehmerischen Reaktionsplan als große Herausforderung. Die mangelnde Vorbereitung von Führungskräften auf Cyber-Attacken wird von 41 Prozent (16 Prozent sehr groß und 25 Prozent groß) der Teilnehmer als große Herausforderung eingestuft. Die Unklarheit über Zuständigkeiten stellt lediglich für 20 Prozent (7 Prozent sehr groß und 13 Prozent groß) eine große Herausforderung dar.

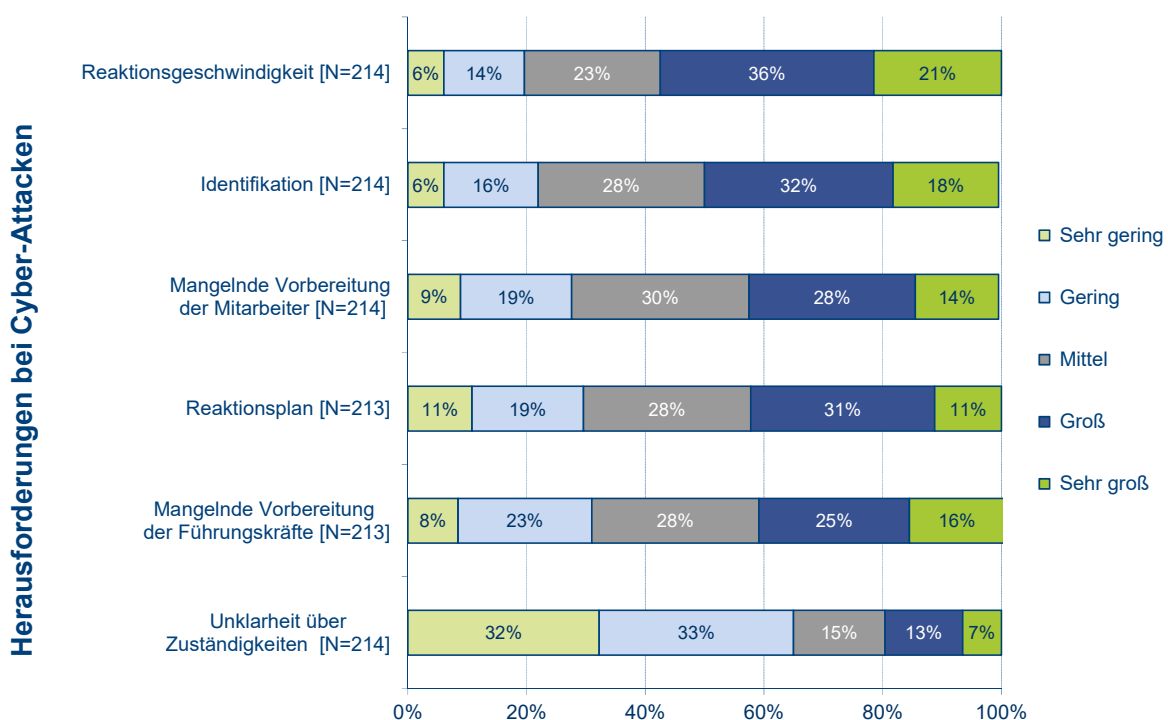


ABBILDUNG 10: HERAUSFORDERUNGEN BEI CYBER-ATTACKEN

### 3.4 Identifizierung der Angreifer bei Cyber-Attacken

Die nächste Frage hatte zum Ziel, herauszufinden, welche Art von Angreifern am häufigsten identifiziert wird. 44 Prozent der Probanden gibt an, dass keine Identifikation des Angreifers möglich war. 21 Prozent der Probanden teilen mit, dass Hacker für Cyber-Attacken verantwortlich sind. Nach Aussagen von 14 Prozent sind zudem kleinkriminelle Cracker an Angriffen beteiligt. Hacktivisten werden von 8 Prozent als Verantwortliche für Cyber-Attacken genannt. Organisiertes Verbrechen

und Geheimdienste werden von 7 Prozent für verantwortlich gehalten. Insider werden bei 6 Prozent als Angreifer identifiziert.

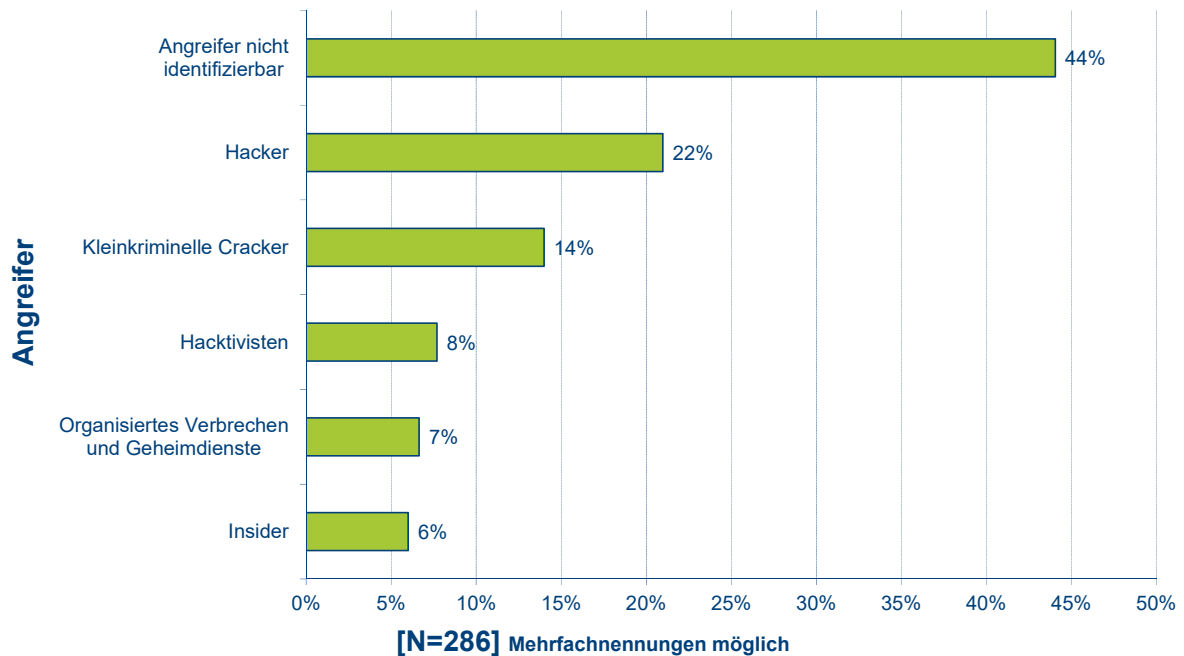


ABBILDUNG 11: ANGREIFER

### 3.5 Priorität von Cyber-Risiken

Des Weiteren wurde danach gefragt welche Priorität Cyber-Risiken, mithin die Ursachenforschung in den Unternehmen einnimmt. Die Studie zeigt: Cyber-Risiken scheinen für fast die Hälfte der Unternehmen kein zentrales Thema zu sein. 37 Prozent der befragten Unternehmen attestieren dieser Thematik eine lediglich mittlere Priorität, während 8 Prozent eine geringe und 3 Prozent eine sehr geringe Priorität angeben. Nur bei 15 Prozent der Probanden nehmen Cyber-Risiken eine sehr hohe, bei 38 Prozent eine hohe Priorität ein.

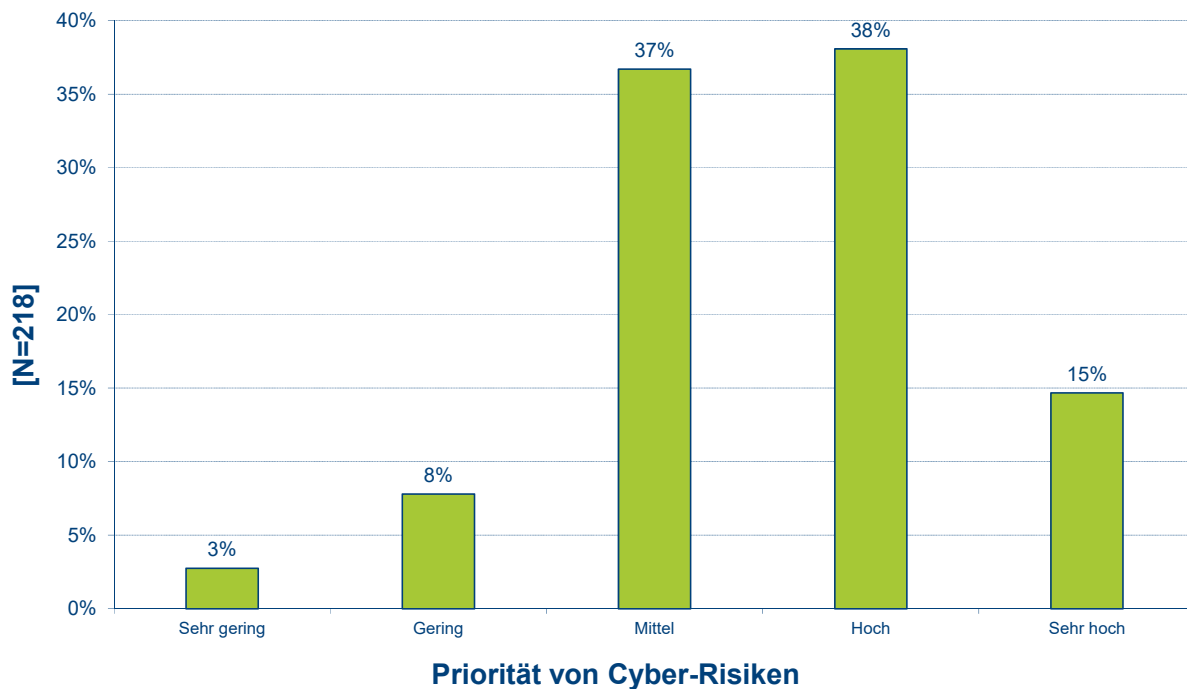


ABBILDUNG 12: PRIORITÄT VON CYBER-RISIKEN

### 3.6 Bewertung von Cyber-Risiken

Hier wurde gefragt, welche Methoden zur Bewertung von Cyber-Risiken in den Unternehmen verwendet werden. Knapp die Hälfte (49 Prozent) der teilnehmenden Unternehmen gibt an, keine Bewertungsmethoden für Cyber-Risiken zu haben. Bei 16 Prozent erfolgt die Bewertung beschreibend, ohne Verwendung von Kategorien, Zahlen oder Rankings. Eine Verwendung von Kategorien wie „hoch/mittel/niedrig“ oder Fähigkeitsmodelle wie z.B. „Reifegrade“ zum Vergleich mit anderen Organisationen kommen bei 13 Prozent der Befragten zur Anwendung. 12 Prozent der Probanden geben an, eine ökonomische Quantifizierung basierend auf geschätzten finanziellen Verlusten innerhalb eines Zeitrahmens, z.B. Value-at-Risk-Modellierung, vorzunehmen. Bei 8 Prozent werden Cyber-Risiken anhand von numerischen Scores oder Rankings innerhalb eines festen Rahmens bewertet. 2 Prozent der befragten Unternehmen geben an, ihre Bewertung anhand von Implementierungsebenen innerhalb des National Institute of Standards and Technology (NIST) Cybersecurity-Frameworks durchzuführen.

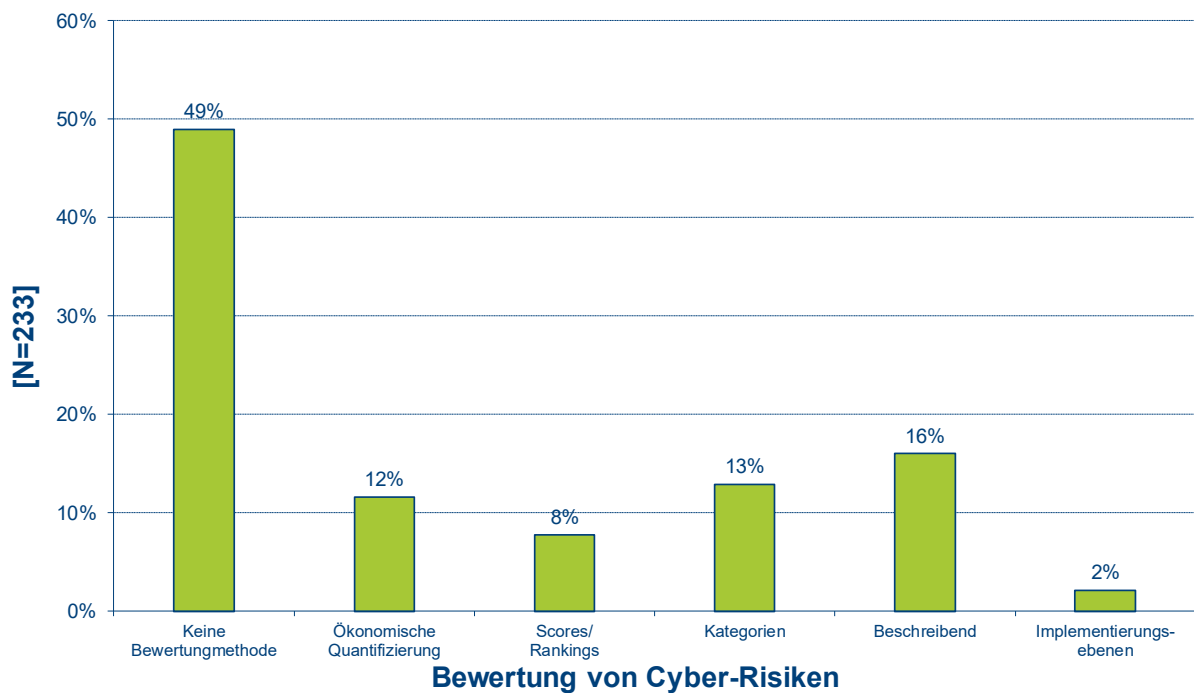


ABBILDUNG 13: BEWERTUNG VON CYBER-RISIKEN

### 3.7 Herausforderungen in der Abwehr aktueller Cyber-Risiken

Mit jeweils 61 Prozent geben die Probanden sowohl das fehlende Security Bewusstsein der Mitarbeiter als auch das frühzeitige Erkennen der relevanten Angriffe als größte Herausforderungen an. 52 Prozent schätzen das Durchsetzen von Sicherheitsstandards im Unternehmen als eine der größten Herausforderungen ein. 26 Prozent nennen zu geringe Budgets für Risk Management. Ein Fachkräftemangel ist für 24 Prozent der Unternehmen eine der größten Herausforderungen. Für 21 Prozent gehören fehlende Informationen über den Wert bedrohter Daten und Prozesse (Value at Risk) zu den größten Herausforderungen.

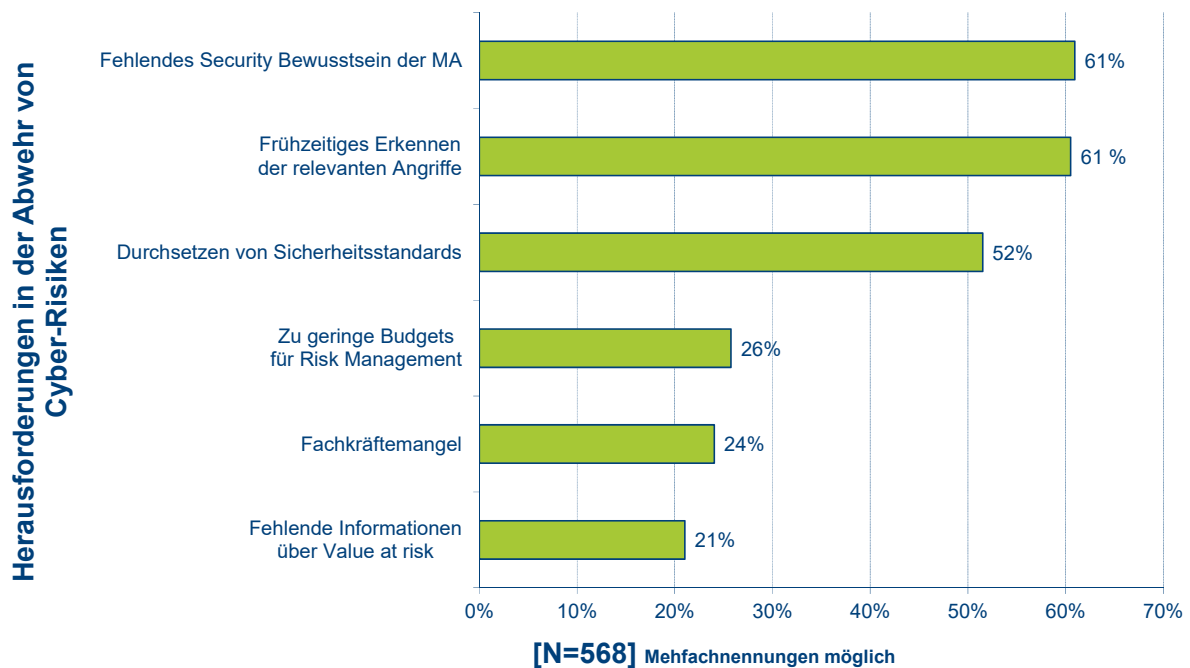


ABBILDUNG 14: HERAUSFORDERUNGEN IN DER ABWEHR VON CYBER-RISIKEN

### 3.8 Regelmäßigkeit in der Identifizierung und Überwachung von Cyber-Risiken

Bei der Regelmäßigkeit in der Identifizierung und Überwachung von Cyber-Risiken geben 15 Prozent der Probanden an, Cyber-Risiken sehr regelmäßig zu überwachen, und 36 Prozent der Probanden geben an, Cyber-Risiken regelmäßig zu überwachen. 24 Prozent der Teilnehmer stufen die Regelmäßigkeit in der Identifizierung und Überwachung als mittel ein. Bei 17 Prozent der Befragten kommt es nur unregelmäßig zu Überwachungen und eine nur sehr unregelmäßige Überwachung findet bei 8 Prozent der befragten Probanden statt.

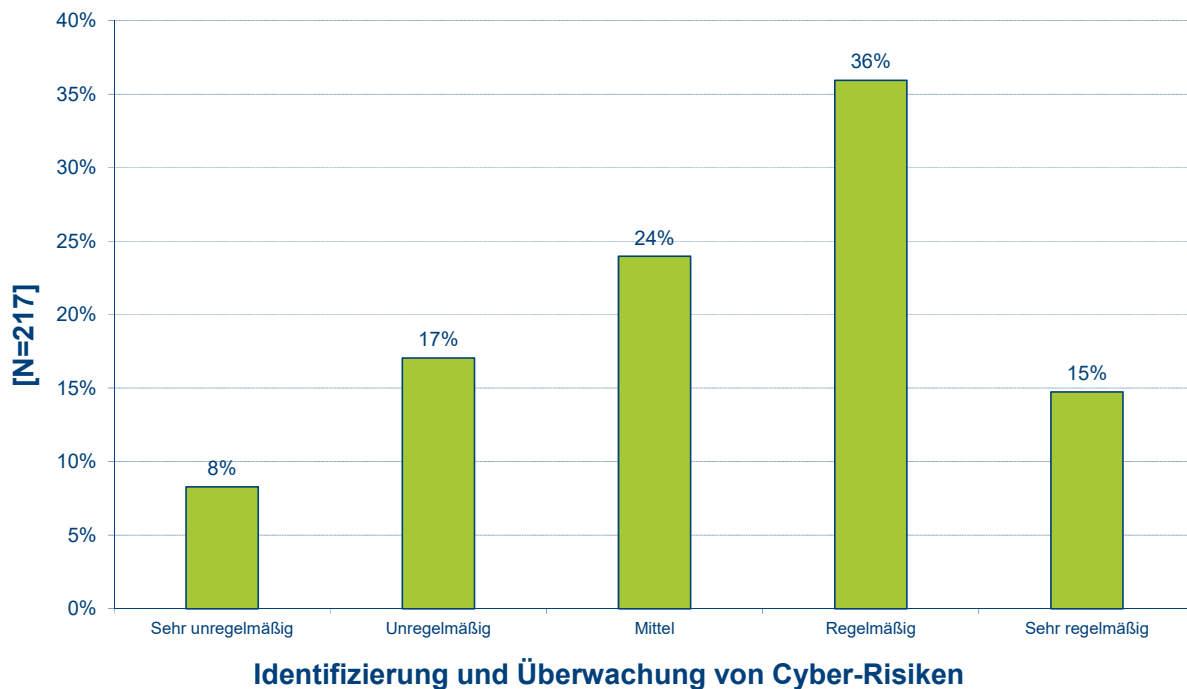


ABBILDUNG 15: IDENTIFIZIERUNG UND ÜBERWACHUNG VON CYBER-RISIKEN

### 3.9 Sicherheitslücken im Unternehmen

Als größte Sicherheitslücke innerhalb der Organisation nennt rund die Hälfte (51 Prozent: 12 Prozent sehr groß und 39 Prozent groß) der Probanden ungeschulte Mitarbeiter. Die zunehmende Nutzung mobiler Endgeräte nehmen 37 Prozent (7 Prozent sehr groß und 30 Prozent groß) der befragten Unternehmen als größte Sicherheitslücke wahr. Social Media Aktivitäten werden von 26 Prozent (8 Prozent sehr groß und 18 Prozent groß) der Umfrageteilnehmer als größte Sicherheitslücke eingeschätzt. 22 Prozent (2 Prozent sehr groß und 20 Prozent groß) geben an, interne Prozesse würden ihrer Ansicht nach die größte Sicherheitslücke darstellen. 21 Prozent (5 Prozent sehr groß und 16 Prozent groß) der Befragten sind der Meinung, Cloud Computing bilde die größte Sicherheitslücke ab.

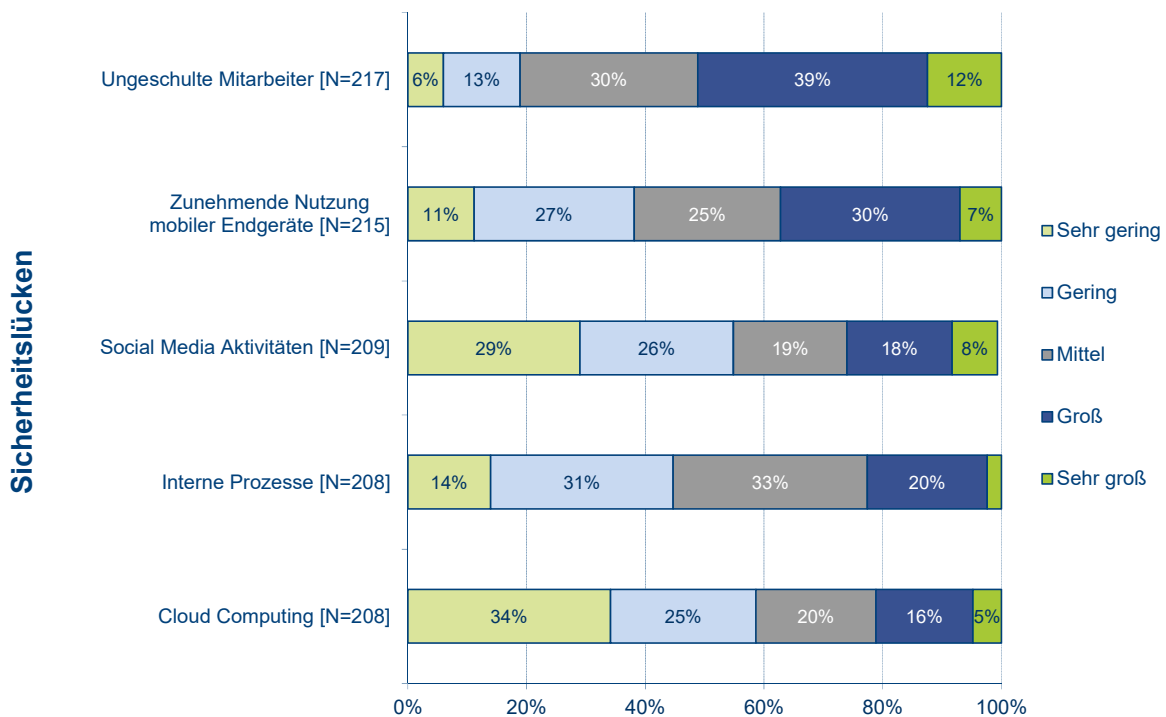


ABBILDUNG 16: SICHERHEITSLÜCKEN

### 3.10 Entdeckung von Sicherheitslücken

Hierbei geben die Probanden an, auf welche Weise bestehende Sicherheitslücken in ihrem Unternehmen entdeckt werden. 76 Prozent geben an, dass das eigene Sicherheitssystem bzw. der eigene Virenschanner die Sicherheitslücke entdeckt. Das für dieses Thema verantwortliche Team bzw. die verantwortliche Abteilung war bei 68 Prozent für das Aufdecken von Sicherheitslücken verantwortlich. Hinweise von anderen internen Personen geben 44 Prozent der Unternehmen an. Ein internes Kontrollsystem (IKS) deckt bei 27 Prozent Sicherheitslücken auf. Auch die Medien/Nachrichten haben Sicherheitslücken aufgedeckt. Dies geben 21 Prozent der befragten Unternehmen an. 9 Prozent der befragten geben, an, dass deren Lieferanten Sicherheitslücken entdecken. Von 6 bzw. 4 Prozent der Probanden werden jeweils anonyme Hinweisgeber bzw. Aufsichtsbehörden/ Strafverfolgungsbehörden als Identifikatoren genannt. 3 Prozent der befragten Unternehmen beantwortet die Frage damit, dass Wettbewerber zum Aufdecken von Sicherheitslücken beitragen.

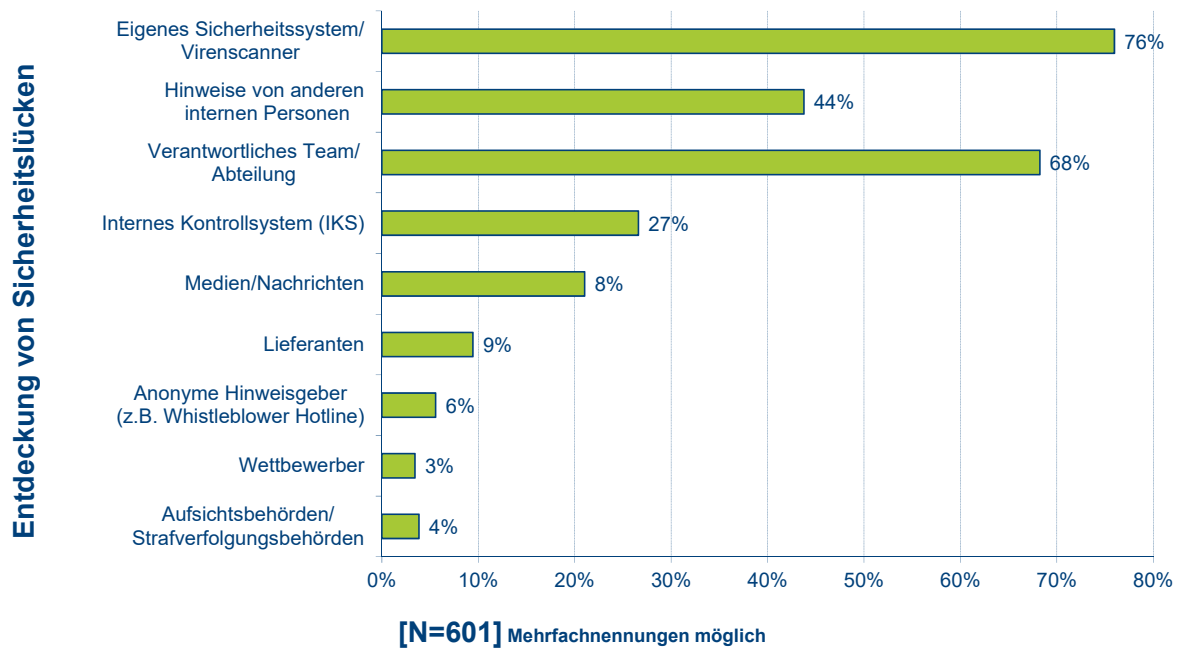


ABBILDUNG 17: ENTDECKUNG VON SICHERHEITSLÜCKEN

### 3.11 Dauer der Entdeckung von Sicherheitslücken

Hier wurde gefragt, wie lange es dauert, bis das Unternehmen eine Sicherheitslücke entdeckt. Mit 53 Prozent gibt die Mehrheit der Befragten an, eine Sicherheitslücke innerhalb von 1 bis 7 Tagen zu entdecken. Bei 30 Prozent dauert es weniger als einen Tag. 11 Prozent der Befragten geben an, hierfür zwischen 1 und 4 Wochen zu benötigen. Lediglich 6 Prozent geben an, dass Sicherheitslücken länger als einen Monat unentdeckt bleiben.

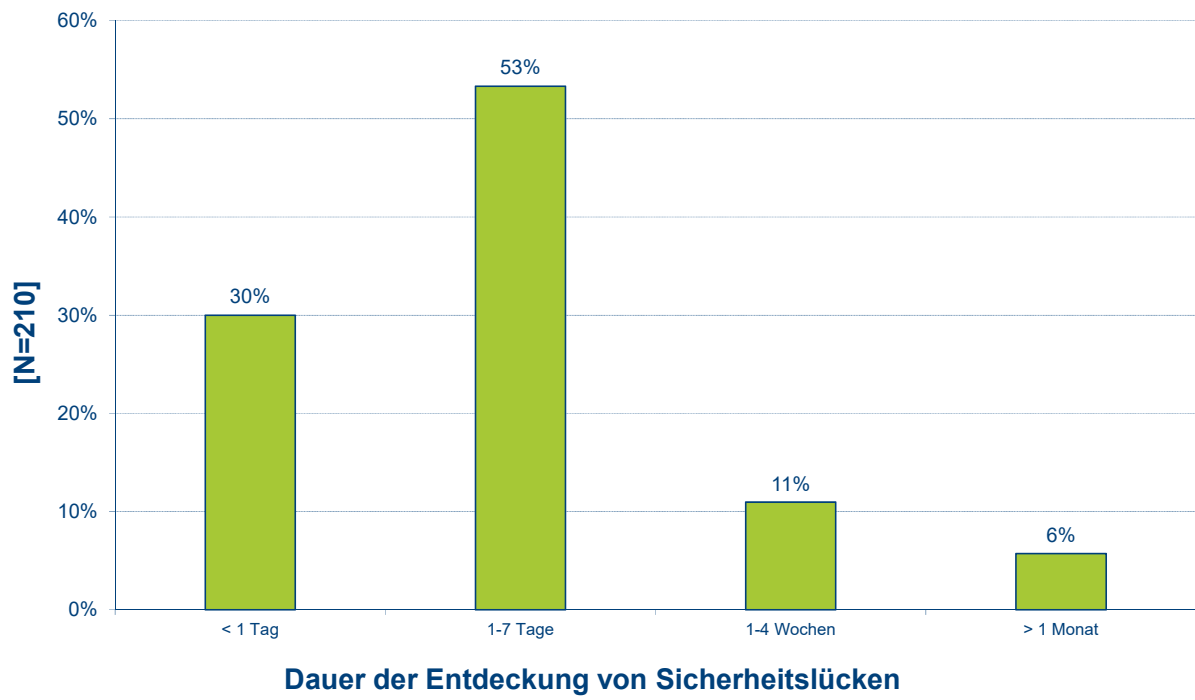


ABBILDUNG 18: DAUER DER ENTDECKUNG VON SICHERHEITSLÜCKEN

### 3.12 Dauer der Entdeckung bei Verstößen gegen Sicherheitsbestimmungen

Die Umfrageteilnehmer wurden des Weiteren gebeten, Auskunft darüber zu erteilen, wie viel Zeit die Entdeckung eines Verstoßes gegen die Sicherheitsbestimmungen in Anspruch nimmt. 7 Prozent schätzen die diesbezügliche Reaktionsgeschwindigkeit als sehr schnell ein, weitere 23 Prozent als schnell und 47 Prozent als mittel. 16 Prozent geben an, lang für die Entdeckung von Verstößen zu benötigen, 7 Prozent sehr lang.

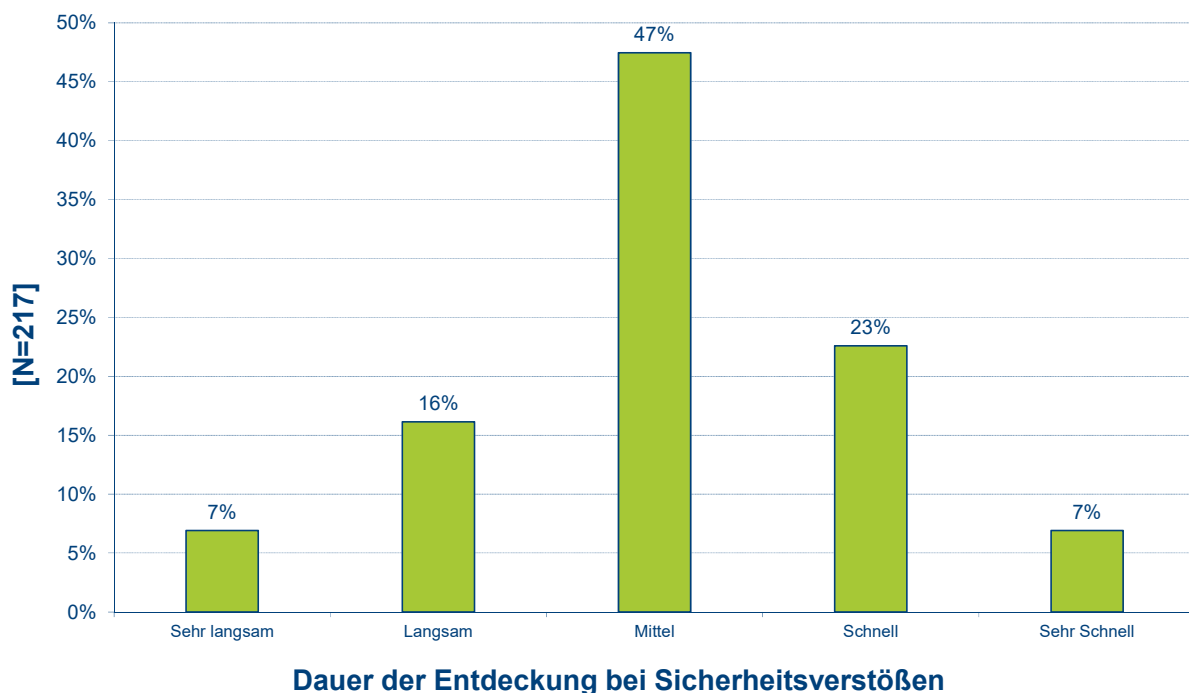


ABBILDUNG 19: DAUER DER ENTDECKUNG BEI SICHERHEITSVERSTÖßEN

## 4 Mögliche Verlustszenarien

Kapitel 4 enthält Angaben zu möglichen Verlustszenarien und deren Bewertung.

### 4.1 Schadenspotenzial verschiedener Cyber-Attacken

Zunächst sollten die Probanden das Schadenspotenzial bestimmter Cyber-Attacken einschätzen. Hierbei zeigt sich, dass die befragten Unternehmen vor allem in dem Einsatz von Schadsoftware (67 Prozent: 16 Prozent sehr hoch und 51 Prozent hoch) sowie in der Infizierung des Computers (58 Prozent: 19 Prozent sehr hoch und 39 Prozent hoch) ein hohes Schadenspotenzial sehen. Nach Ansicht von 46 Prozent der Unternehmen (13 Prozent sehr hoch und 33 Prozent hoch) birgt ebenfalls die digitale Erpressung ein beträchtliches Schadenspotenzial. 43 Prozent (8 Prozent sehr hoch und 35 Prozent hoch) sehen zudem im Identitätsdiebstahl und 37 Prozent (8 Prozent sehr hoch und 29 Prozent hoch) im Datendiebstahl durch Social Engineering ein hohes Schadenspotenzial. Der Einsatz von Schadsoftware für mobile Endgeräte kann laut 33 Prozent der Unternehmen (6 Prozent sehr hoch und 27 Prozent hoch) ebenfalls zu hohen Schäden führen. 31 Prozent der Befragten sind der Meinung, dass die massenhafte Fernsteuerung von Computern ein hohes Schadenspotenzial berge.

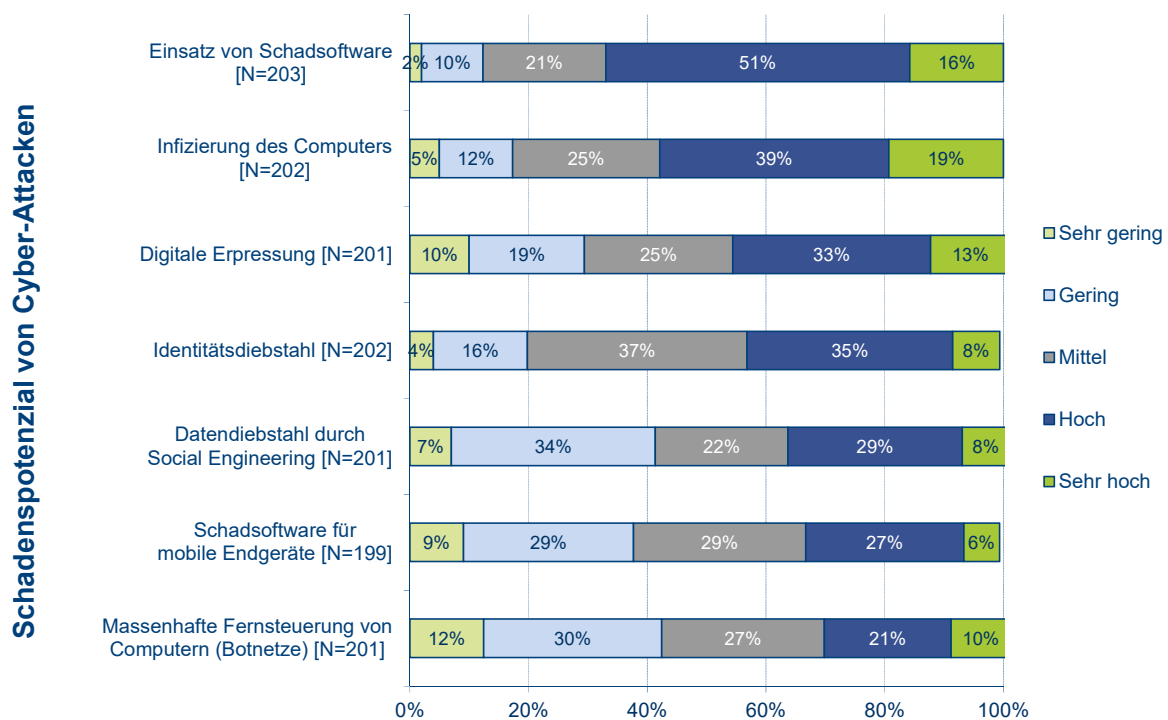


ABBILDUNG 20: SCHADENSPOTENZIAL VON CYBER-ATTAC

## 4.2 Vorhandensein eines Notfall-Reaktionsplans

43 Prozent der Unternehmen verfügen bereits über einen Notfall-Reaktionsplan im Falle eines Cyber-Angriffs. In 23 Prozent der Unternehmen ist ein solcher Reaktionsplan zumindest in Planung. Über keinen Notfall-Reaktionsplan verfügen 34 Prozent der befragten Unternehmen.

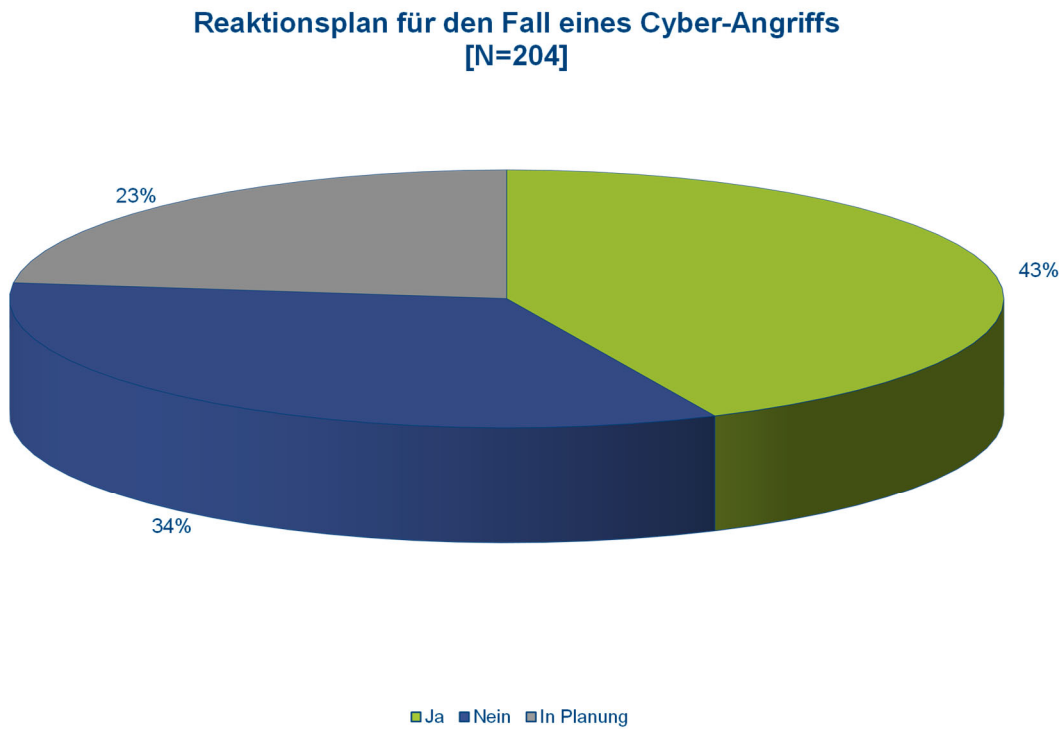


ABBILDUNG 21: REAKTIONSPLAN FÜR DEN FALL EINES CYBER-ANGRIFFS

### 4.3 Verbesserungspotenziale im Reaktionsplan

Falls die befragten Unternehmen über einen Notfall-Reaktionsplan für Cyber-Angriffe verfügen, sollten sie im Rahmen dieser Frage einschätzen, ob und wie viel Verbesserungspotenzial im aktuellen Notfall-Plan noch gesehen wird. 26 Prozent der Probanden sehen ein sehr hohes Verbesserungspotenzial in ihrem eigenen Reaktionsplan. Dahingegen schätzen 49 Prozent das Verbesserungspotenzial als mittel, 22 Prozent als gering und 3 Prozent als sehr gering ein.

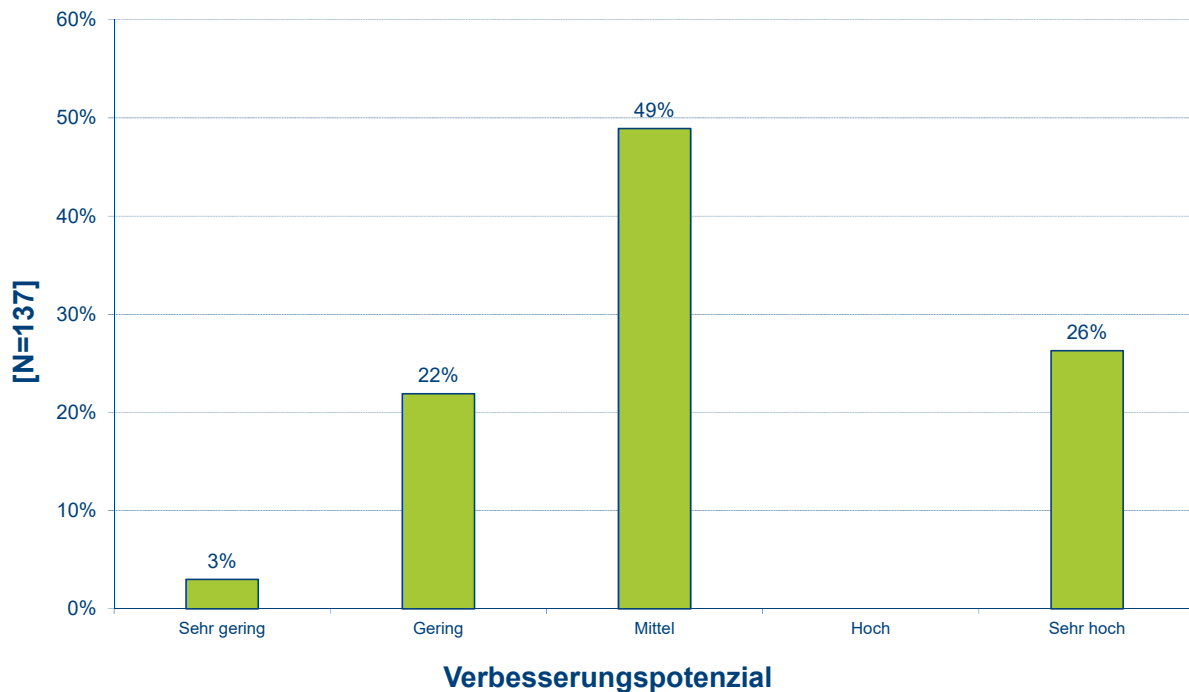


ABBILDUNG 22: VERBESSERUNGSPOTENZIAL

#### 4.4 Finanzielle Mittel zur Abwehr eines Cyber-Angriffs

Die Frage, ob das Unternehmen im Falle eines Cyber-Angriffs über die erforderlichen finanziellen Mittel verfügt, um diesen erfolgreich abzuwehren, beantworteten 70 Prozent mit „Ja“. Demnach verfügen immerhin 30 Prozent der befragten Unternehmen nicht über die nötigen finanziellen Mittel zur Abwehr eines Cyber-Angriffs.

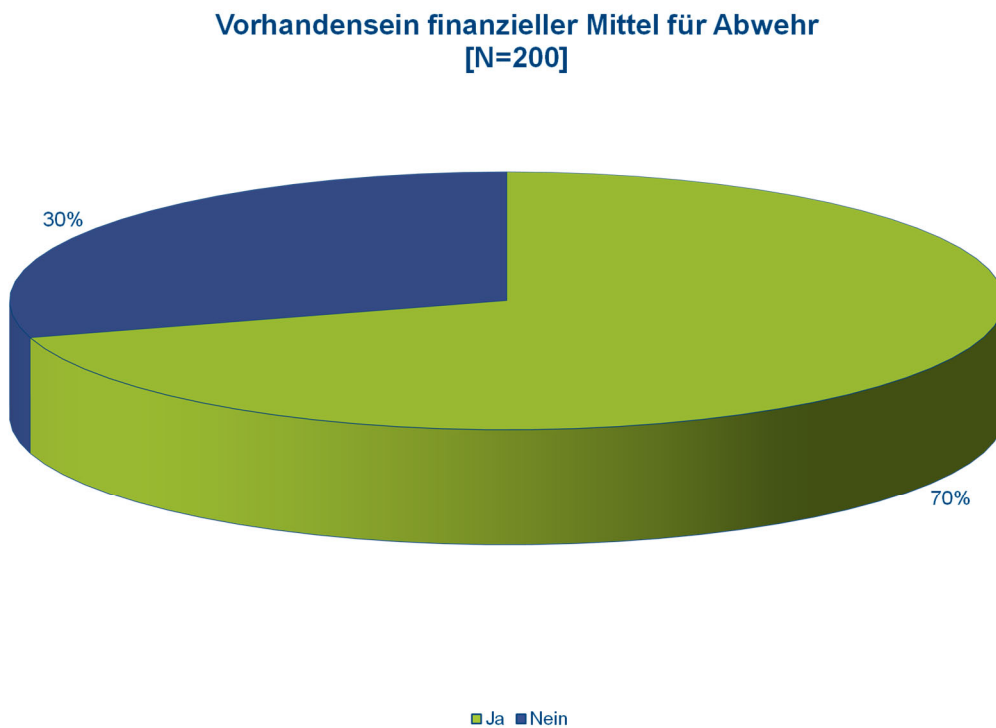


ABBILDUNG 23: VORHANDENSEIN FINANZIELLER MITTEL FÜR ABWEHR

## 5 Organisatorische Fragestellungen

In den nachfolgenden Abschnitten werden organisatorische Fragestellungen im Hinblick auf die Cyber-Sicherheit im Unternehmen näher betrachtet.

### 5.1 Cyber-Security als Teil der Unternehmensstrategie

Bei weniger als der Hälfte der Befragten (39 Prozent) ist Cyber-Security Teil der eigenen Unternehmensstrategie.

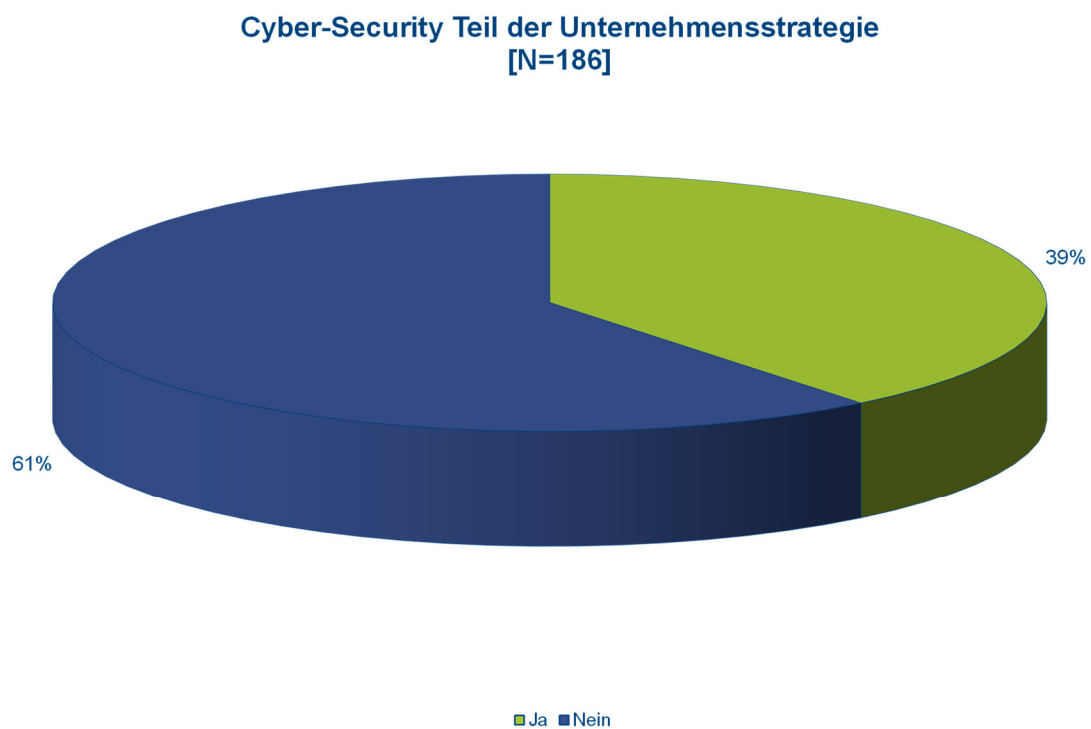


ABBILDUNG 24: CYBER-SECURITY TEIL DER UNTERNEHMENSSTRATEGIE

## 5.2 Nutzung eines Information Security Management Systems (ISMS)

Hier wurde gefragt, ob die Unternehmen ein Information Security Management System (ISMS) nutzen, um die Informationssicherheit in ihrem Unternehmen zu steuern, zu kontrollieren, sicherzustellen und zu optimieren. Die Ergebnisse zeigen, dass weniger als ein Drittel der Unternehmen (26 Prozent) ein Information Security Management System verwendet. 74 Prozent der Probanden geben an, kein ISMS zu nutzen.

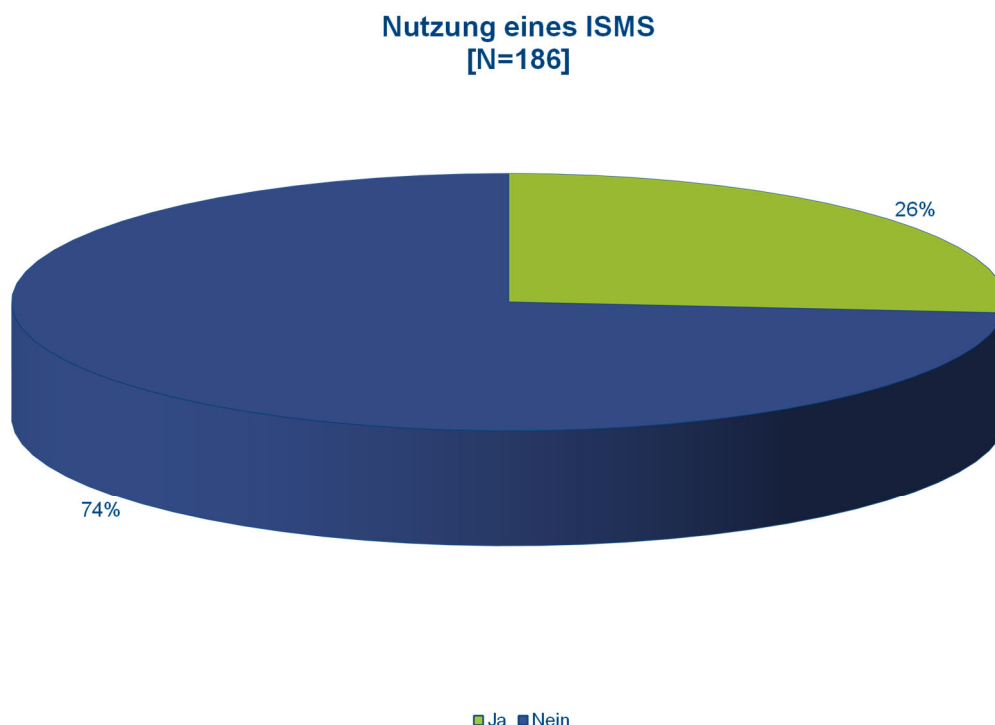


ABBILDUNG 25: NUTZUNG EINES ISMS

## 5.3 Funktionsfähigkeit bestimmter Prozesse innerhalb der eigenen Organisation im Hinblick auf Cyber-Attacks

In Bezug auf das eigene Unternehmen schätzt jeweils knapp ein Drittel die Bewertungsfähigkeit von Cyber-Attacks und die Reaktionsfähigkeit auf Cyber-Attacks als gering ein (32 Prozent: 8 Prozent sehr gering und 24 Prozent gering; 28 Prozent: 5 Prozent sehr gering und 23 Prozent gering). Auch die Identifikationsfähigkeit von Cyber-Attacks wird von 27 Prozent der Unternehmen (7 Prozent sehr gering und 20 Prozent gering) als gering eingestuft. Wohingegen beides, sowohl die Erholungs- als auch die Vermeidungsfähigkeit von Cyber-Attacks von

jeweils 38 Prozent der Probanden als hoch bewertet wird (jeweils 5 Prozent sehr hoch und 33 Prozent hoch). Jeweils 31 Prozent empfinden wiederum die Bewertungs- sowie die Identifikationsfähigkeit von Cyber-Angriffen in ihrer Organisation als hoch. Weitere 38 Prozent stufen die Reaktionsfähigkeit in ihrem Unternehmen als hoch (8 Prozent sehr hoch und 30 Prozent hoch) ein.

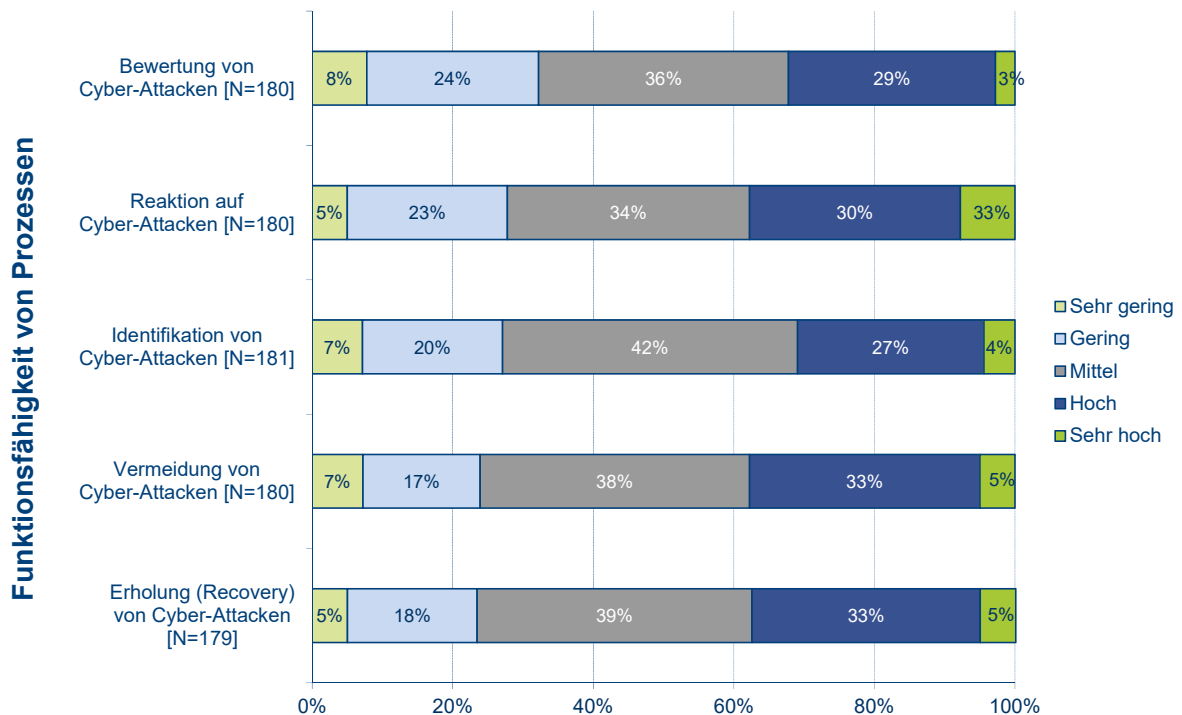


ABBILDUNG 26: FUNKTIONSFÄHIGKEIT VON PROZESSEN

## 5.4 Verantwortungsträger für Informationssicherheit

In diesem Abschnitt wurde die verantwortliche Person für Informationssicherheit innerhalb des Unternehmens erfragt. Exakt die Hälfte der Unternehmen gibt an, dass hierfür innerhalb ihrer Organisation eine zuständige Fachabteilung existiert. 30 Prozent nennen den Datenschutzbeauftragten als verantwortliche Person. 23 Prozent der Unternehmen weisen die Verantwortung für Informationssicherheit dem Chief Executive Officer (CEO) und 19 Prozent dem Chief Information Officer (CIO) zu. 15 Prozent sind der Ansicht, in ihrem Unternehmen trage der Chief Information Security Officer (CISO) die Verantwortung für Informationssicherheit. Weitere 4 Prozent nennen den Chief Technology Officer (CTO) und 3 Prozent den Chief Data Officer (CDO).

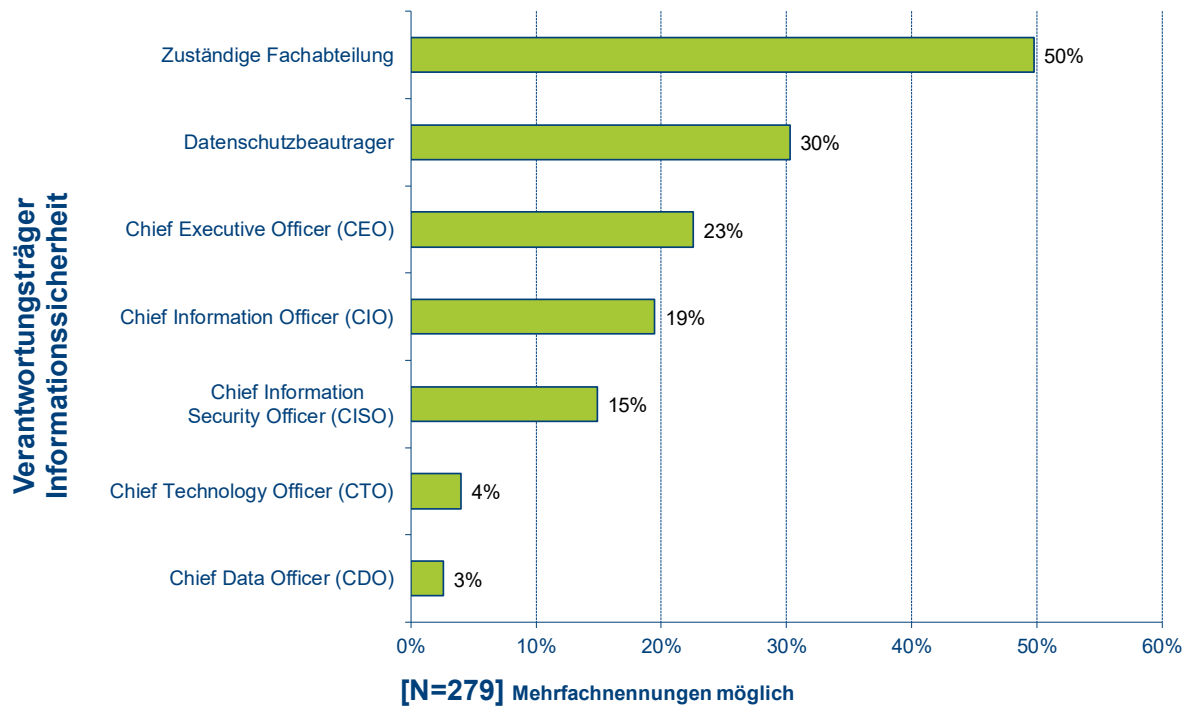


ABBILDUNG 27: VERANTWORTUNGSTRÄGER INFORMATIONSSICHERHEIT

## 5.5 Einschätzung der Kompetenzen von Führungskräften

Hier wurde um eine Beurteilung verschiedener Kompetenzen der Führungskraft im Bereich Cyber-Security gebeten. Gemäß 48 Prozent der Befragten ist insbesondere die Sozialkompetenz der Führungskraft im Unternehmen stark ausgeprägt (36 Prozent stark und 12 Prozent außerordentlich stark). 43 Prozent der Probanden geben an, die Fachkompetenz ihrer Führungskraft sei ebenfalls stark ausgeprägt (37 Prozent stark ausgeprägt und 6 Prozent außerordentlich stark ausgeprägt) und 39 Prozent sind der Ansicht, ihre Führungskraft sei mit einer starken Methodenkompetenz ausgestattet (34 Prozent stark und 5 Prozent außerordentlich stark).

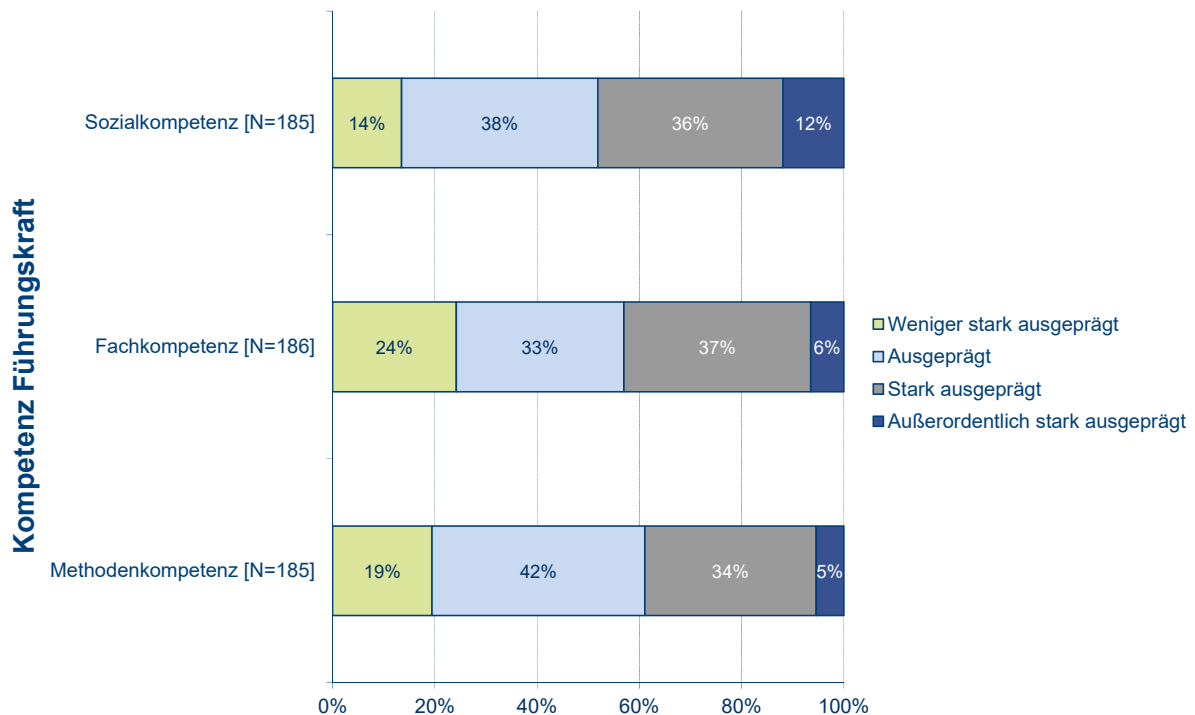


ABBILDUNG 28: KOMPETENZ FÜHRUNGSKRÄFTE

## 5.6 Schulungs- und Weiterbildungsangebote für Mitarbeiter und Führungskräfte

Im Rahmen dieser Frage wurde ermittelt, ob in den befragten Unternehmen für Mitarbeiter und Führungskräfte Schulungen und Weiterbildungen zu Cyber-Security angeboten werden. 64 Prozent der Unternehmen geben an, dass Weiterbildungsmaßnahmen im Bereich Data Security durchgeführt werden (davon 39 Prozent intern und 25 Prozent extern). 71 Prozent teilen mit, die Möglichkeit zu haben an Schulungen zum Thema Datenschutz teilzunehmen (davon 42 Prozent intern und 29 Prozent extern). Auch interne Gefahrensituationen sind bei 58 Prozent der Unternehmen Inhalt von Schulungen (45 Prozent intern und 13 Prozent extern). 18 Prozent der Unternehmen geben an, keinerlei interne und 14 Prozent keinerlei externe Weiterbildungsmaßnahmen im Bereich Cyber-Security durchzuführen.

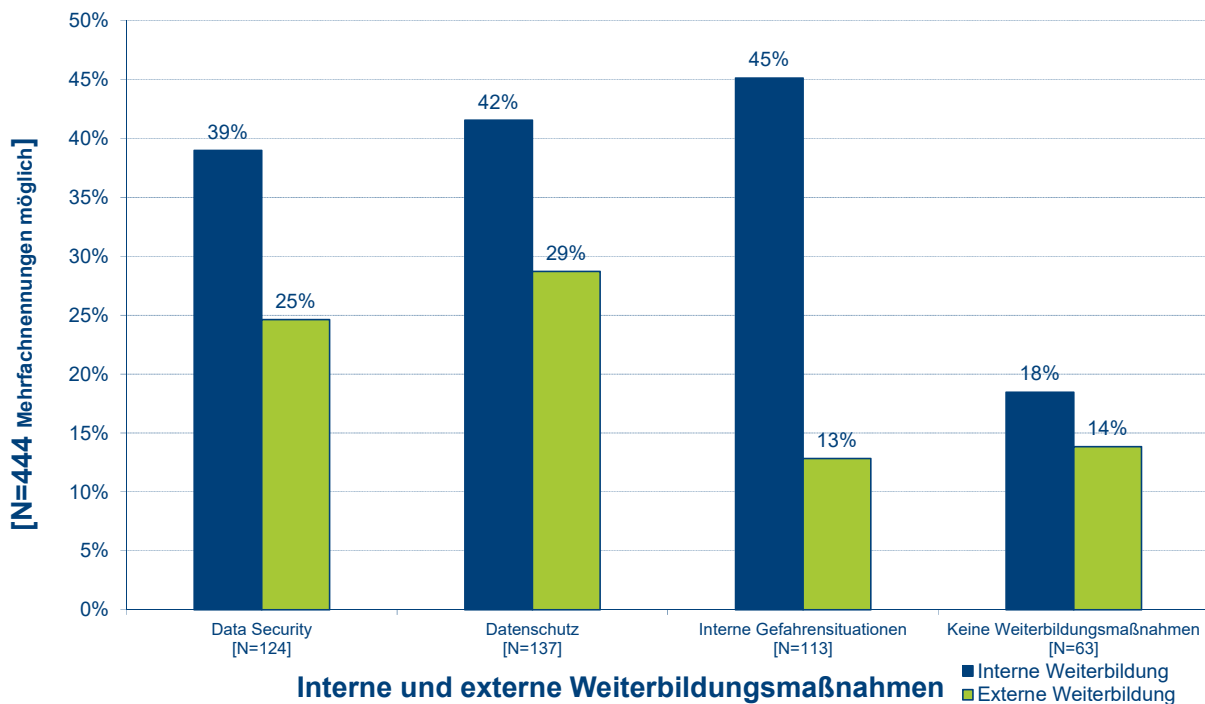


ABBILDUNG 29: INTERNE UND EXTERNE WEITERBILDUNGSMABNAHMEN

## 5.7 Sensibilisierung von Mitarbeitern in verschiedenen Bereichen der Informationssicherheit

Darüber hinaus wurden die Probanden befragt, wie sie die Sensibilisierung der Belegschaft hinsichtlich Datenschutz, Internetsicherheit, Passwortsicherheit, Richtlinie zur Informationssicherheit, Identitätsmanagement, Pishing/Social Engineering, Cloud Security, Sicherheit mobiler Datenträger, Sicherheit mobiler Endgeräte und Informationsklassifizierung einschätzen.

Knapp die Hälfte der Unternehmen ist der Ansicht, dass insbesondere die Sensibilisierung in den Bereichen Cloud Security (45 Prozent), Sicherheit mobiler Endgeräte (44 Prozent) und Datenträger (42 Prozent) sowie im Bereich Informationsklassifizierung (42 Prozent) gering bis sehr gering ausfällt. Eine hohe bis sehr hohe Sensibilität hingegen soll nach Meinung der Probanden den Datenschutz und die Internet- sowie Passwortsicherheit betreffend gegeben sein. 40 Prozent schätzen die Sensibilisierung für Datenschutz als hoch ein (34 Prozent hoch und 6 Prozent sehr hoch). 39 Prozent geben eine hohe Sensibilität hinsichtlich Internetsicherheit an (32 Prozent hoch und 7 Prozent sehr hoch). Weitere 38 Prozent

schätzen die Sensibilisierung für Passwortsicherheit als hoch ein (28 Prozent hoch und 10 Prozent sehr hoch).

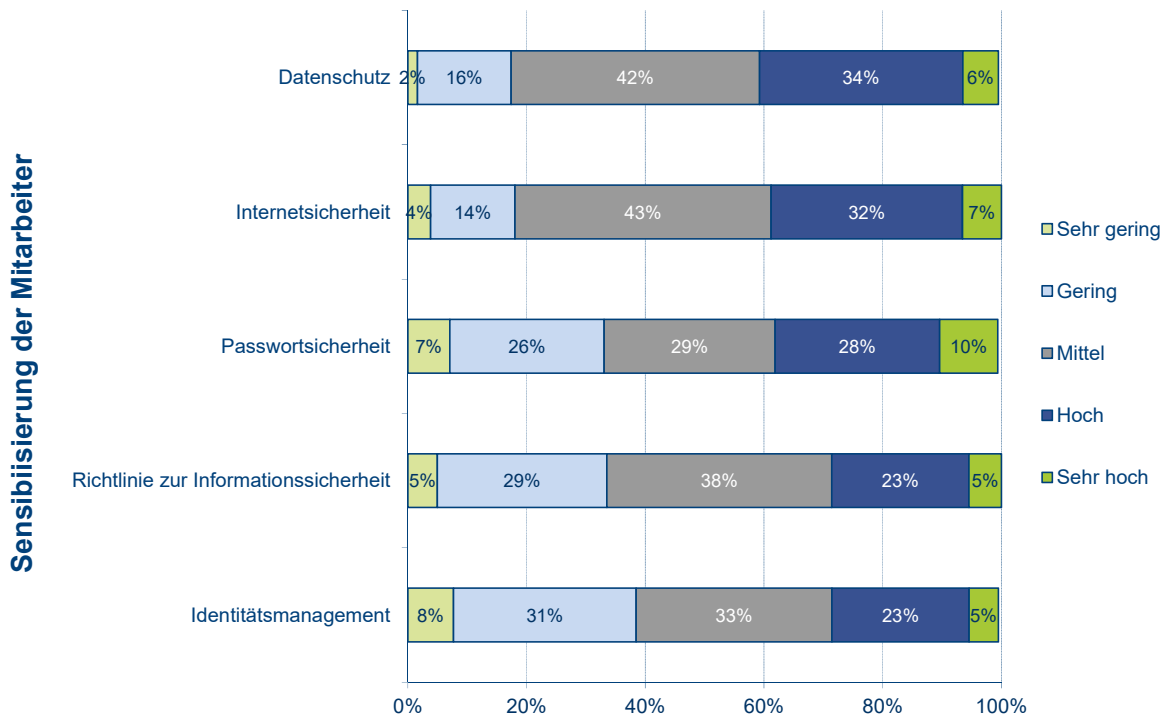


ABBILDUNG 30: SENSIBILISIERUNG DER MITARBEITER TEIL 1

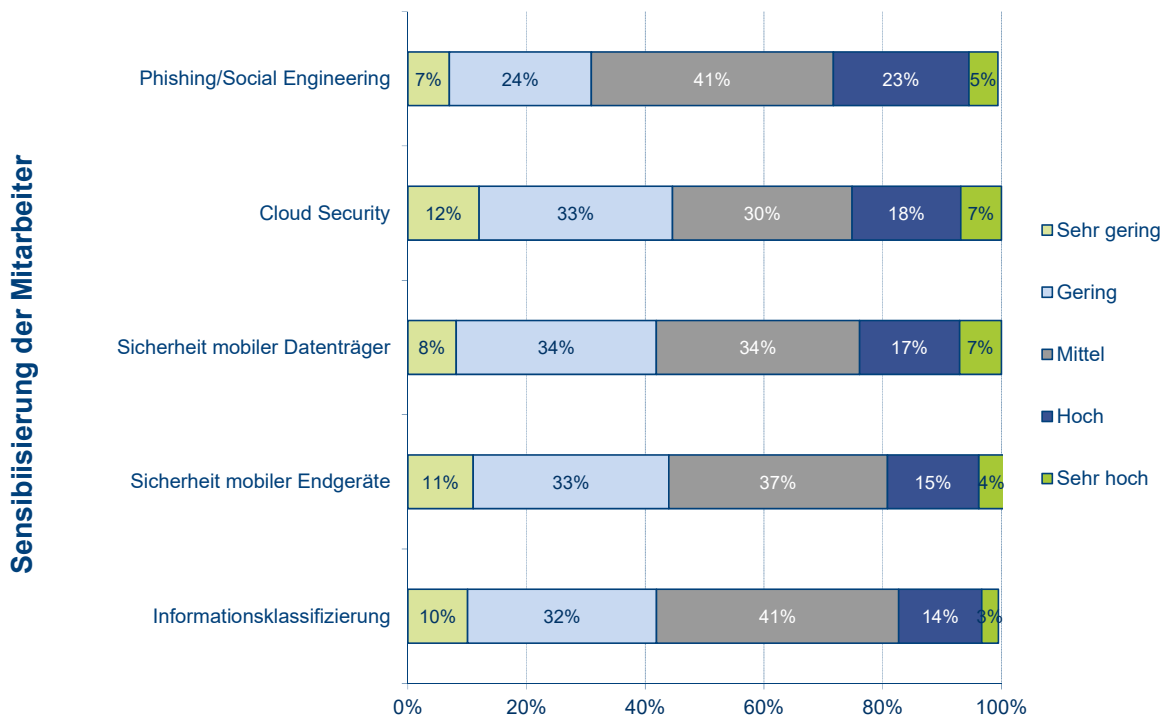


ABBILDUNG 31: SENSIBILISIERUNG DER MITARBEITER TEIL 2

## 5.8 Durchführung von Cyber-Sicherheitsinitiativen

Zudem wurden die Unternehmen gebeten, Auskunft über die Häufigkeit der Durchführung folgender Sicherheitsinitiativen zu erteilen: Virens Scanner, Passwortschutz, Firewall, Festlegung von Zugriffsrechten, Kennzeichnung von Betriebsgeheimnissen, Festlegung von Zutrittsrechten für bestimmte Räume, Sicherheits-Zertifizierung, Schulung der Mitarbeiter, Background-Checks bei sensiblen Positionen, Bestellung eines Sicherheitsverantwortlichen, Sicherheits-Audits durch externe Spezialisten und interne IT-Audits.

89 Prozent der Probanden geben an, häufig Virens Scanner einzusetzen (39 Prozent häufig und 50 Prozent sehr häufig). 84 Prozent der Befragten setzen häufig eine Firewall ein (36 Prozent häufig und 48 Prozent sehr häufig). Auch die Festlegung von Zugriffsrechten kommt laut den Angaben von 67 Prozent der Unternehmen häufig zur Anwendung (39 Prozent häufig und 28 Prozent sehr häufig). Etwas mehr als die Hälfte gibt an, häufig Schutz in Form eines Passwortes zu nutzen (52 Prozent: 35 Prozent häufig und 17 Prozent sehr häufig). In seltenen Fällen werden Background-Checks bei sensiblen Positionen (59 Prozent: 32 Prozent sehr selten und 27 Prozent selten) oder Sicherheits-Audits durch externe Spezialisten (54 Prozent: 36 Prozent sehr selten und 18 Prozent selten) durchgeführt.

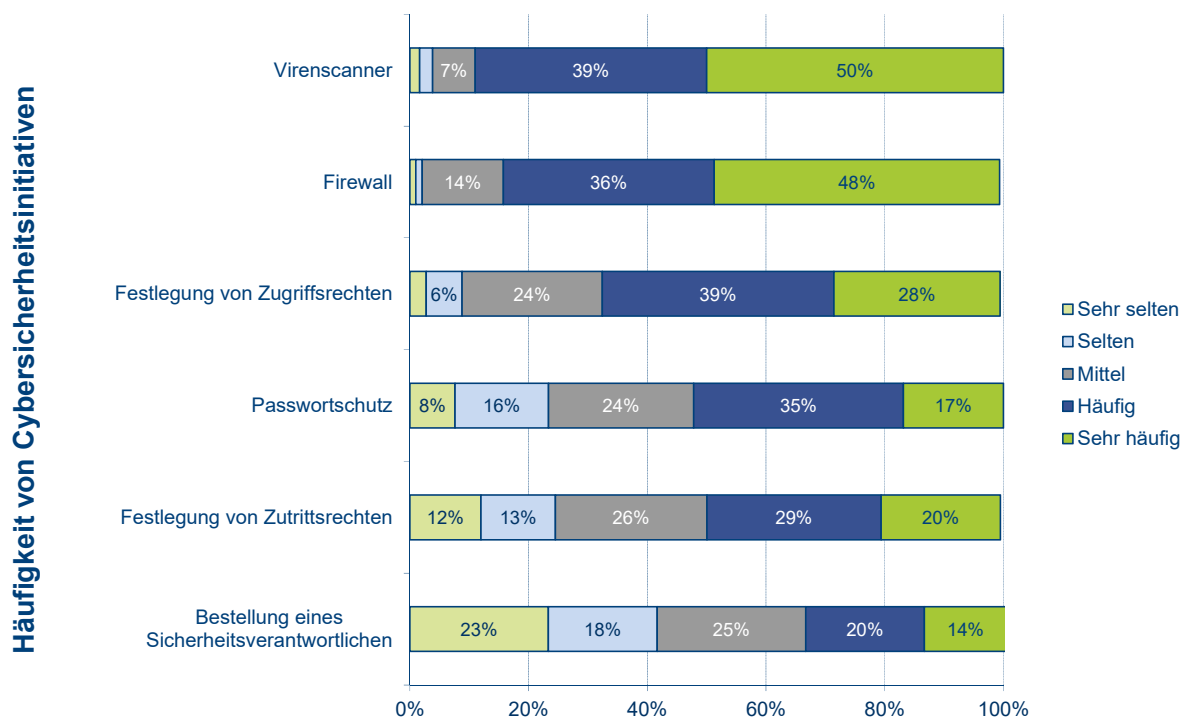


ABBILDUNG 32: HÄUFIGKEIT VON CYBERSICHERHEITSINITIATIVEN TEIL 1

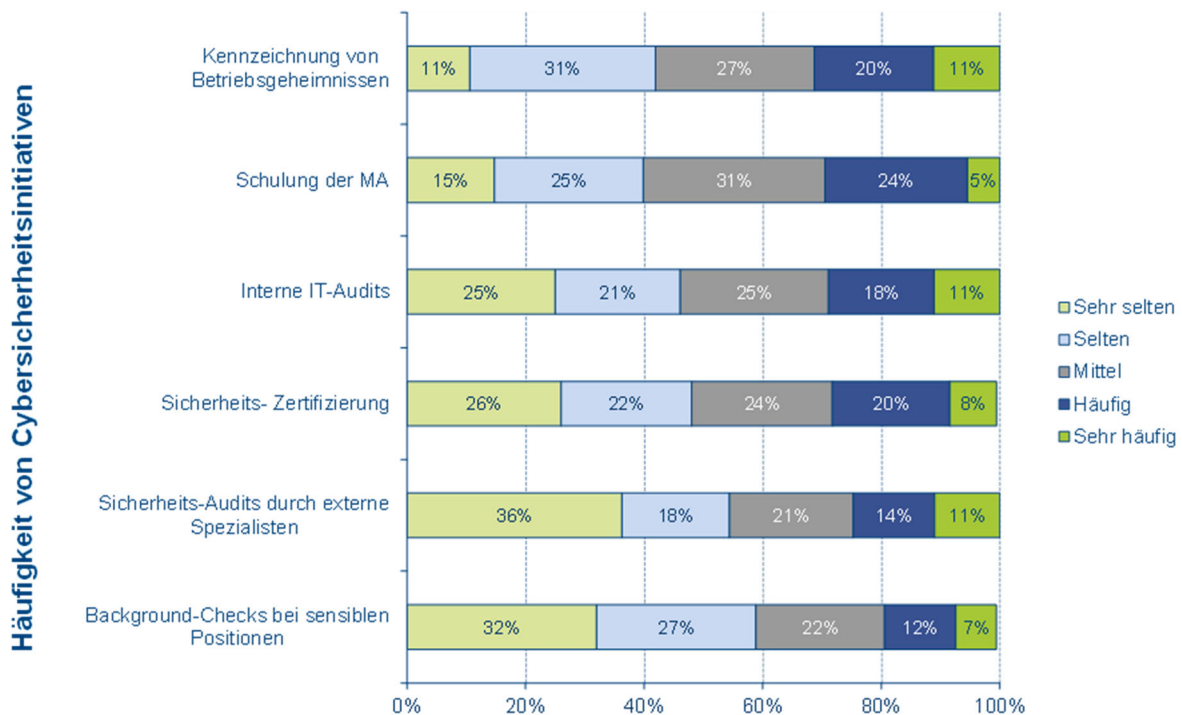


ABBILDUNG 33: HÄUFIGKEIT VON CYBERSICHERHEITSINITIATIVEN TEIL 2

## 6 Cyberversicherung

In diesem Kapitel geht es speziell um Cyberversicherungen und deren Ausgestaltung in den Unternehmen wie bspw. Kosten und Investitionen.

### 6.1 Jährliche Ausgaben für Cyber-Security

Bei der Mehrheit der befragten Unternehmen (43 Prozent) beläuft sich die Summe der jährlichen Kosten für Cyber-Security auf weniger als 10.000 Euro. 38 Prozent der Probanden geben jährlich zwischen 10.000 Euro und unter 50.000 Euro, 9 Prozent zwischen 50.000 Euro und unter 100.000 Euro, 6 Prozent zwischen 100.000 Euro und unter 500.000 Euro, 3 Prozent zwischen 500.000 Euro und unter 1 Mio. Euro und 1 Prozent mehr als 1 Mio. Euro jährlich für Cyber-Security aus.

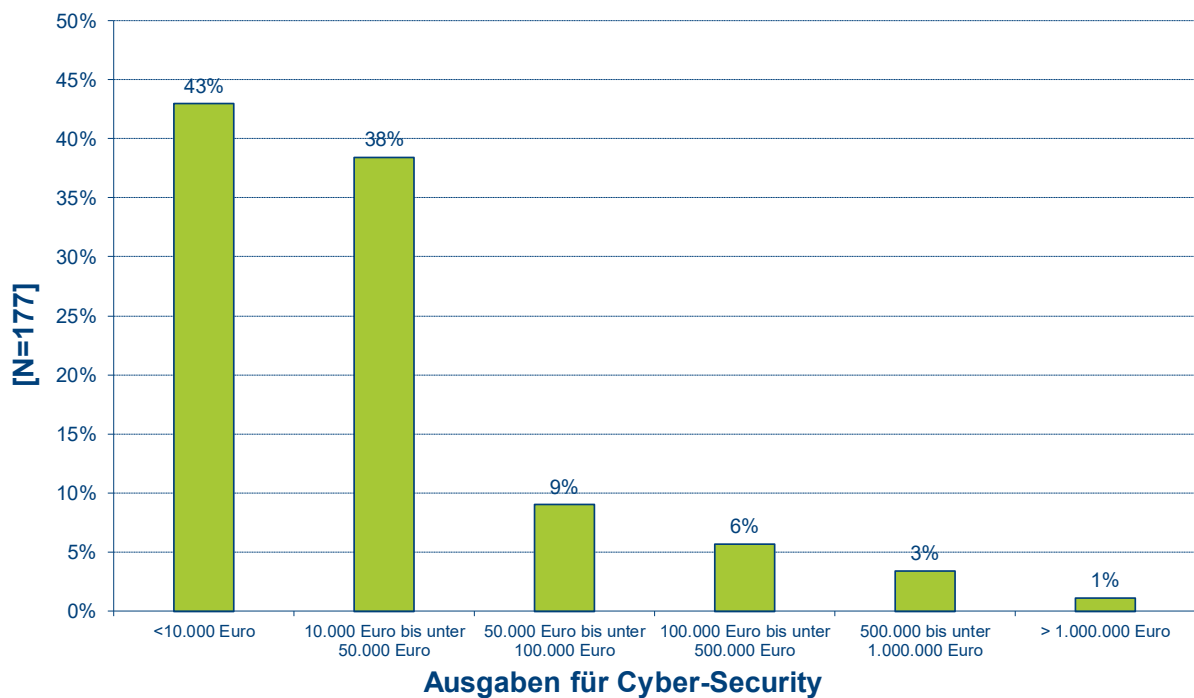


ABBILDUNG 34: AUSGABEN FÜR CYBER-SECURITY

## 6.2 Zuordnung der Kosten für Cyber-Security

Die Kosten fallen nach Angaben der Unternehmen insbesondere für Investitionen in neue Technologien oder Systeme (z.B. ISMS) an (79 Prozent: 32 Prozent hohe Kosten und 47 Prozent mittlere Kosten). Die Kosten für Schulungs- und Weiterbildungsmaßnahmen im Bereich Cyber-Security schätzen 40 Prozent als mittel und 9 Prozent als hoch ein. IT-Audits verursachen den Angaben von 38 Prozent der Probanden zufolge mittlere und nach Ansicht von 9 Prozent hohe Kosten. Die Kosten für die Identifizierung von Cyber-Risiken werden von 43 Prozent als mittel eingeschätzt und weitere 6 Prozent stufen diese Kosten als hoch ein. Im Gegensatz dazu sind 61 Prozent der Befragten der Meinung, dass für einen Reaktionsplan in ihrem Unternehmen nur geringe Kosten anfallen.

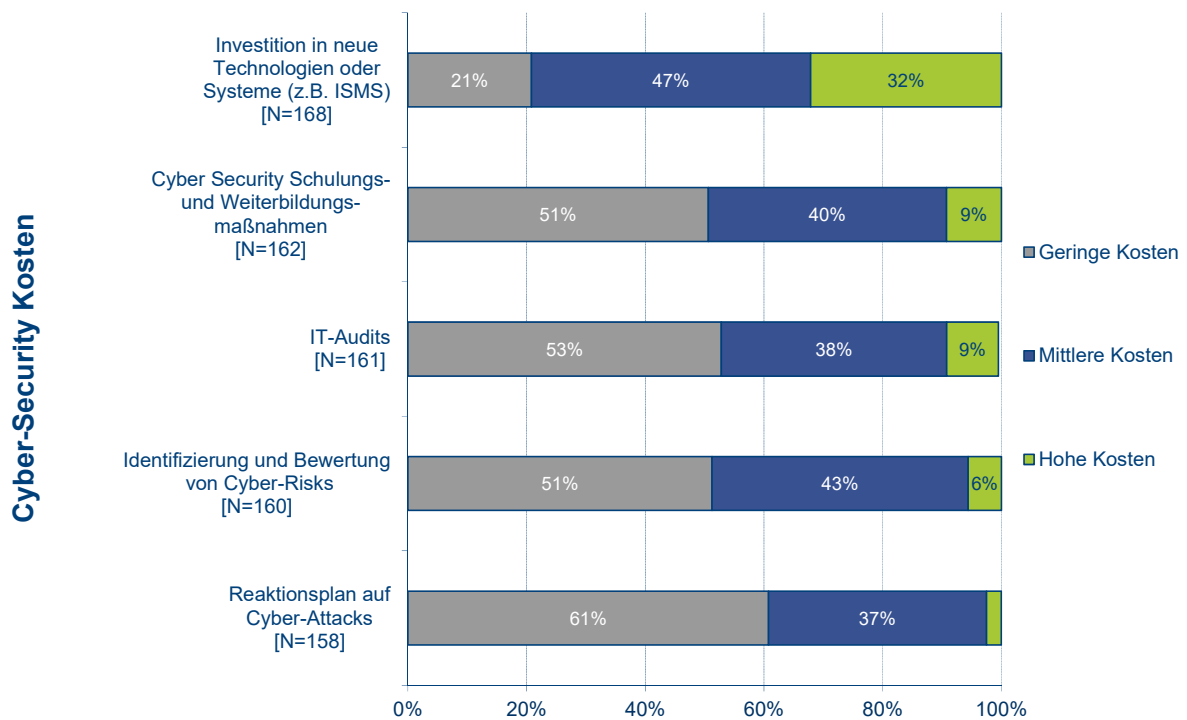


ABBILDUNG 35: CYBER-SECURITY KOSTEN

### 6.3 Geplante Investitionskosten für 2020 im Vergleich zum Vorjahr

Bei der Frage nach geplanten Investitionen im Bereich Cyber-Security gibt mit 51 Prozent der größte Teil der Probanden an, die Ausgaben für Cybersecurity im Jahr 2020 im Vergleich zum Vorjahr nicht zu erhöhen. Ein Kostenanstieg in Höhe von 10 Prozent bis 20 Prozent ist bei 31 Prozent der Unternehmen geplant. 12 Prozent geben an, die Kosten für Cyber-Security im Folgejahr um 20 Prozent bis 30 Prozent im Vergleich zu 2019 erhöhen zu wollen. Ein Kostenanstieg von 30 Prozent bis 40 Prozent bzw. von mehr als 50 Prozent ist von jeweils 3 Prozent der Unternehmen vorgesehen.

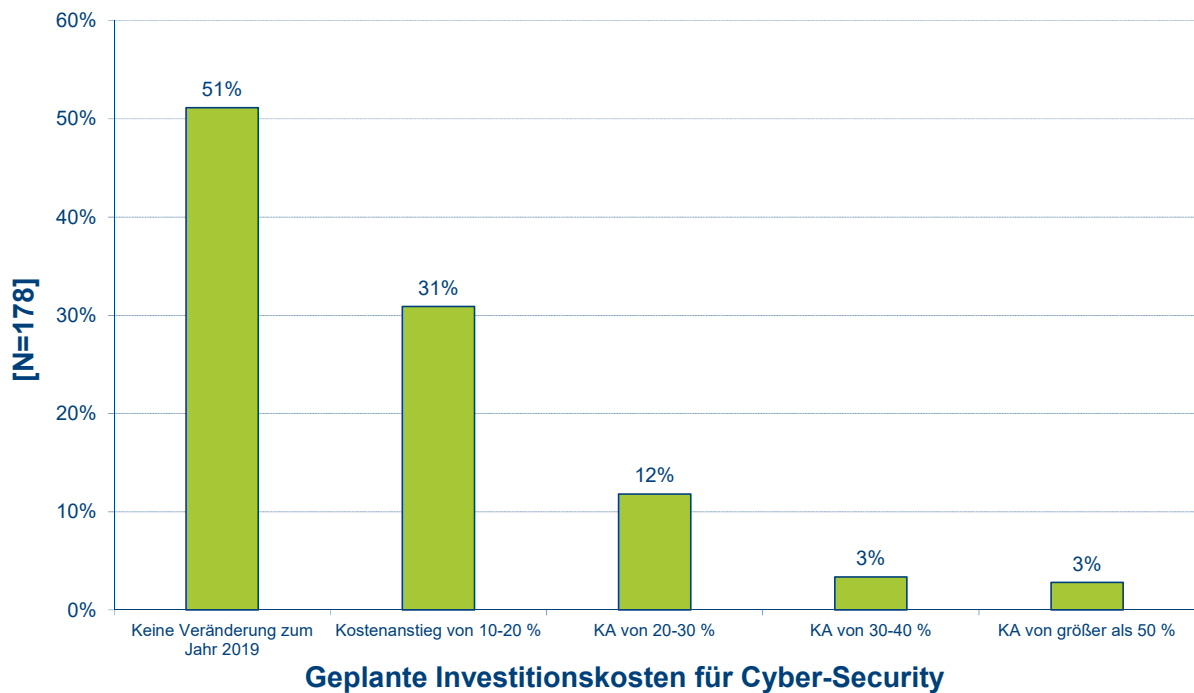


ABBILDUNG 36: GEPLANTE INVESTITIONSKOSTEN FÜR CYBER-SECURITY

## 6.4 Anteil der Unternehmen mit Cyber-Versicherung

Laut der Umfrageergebnisse hat weniger als ein Drittel (28 Prozent) der befragten Unternehmen eine Cyber-Versicherung abgeschlossen.

### Vorhandensein einer Cyber-Versicherung [N=178]

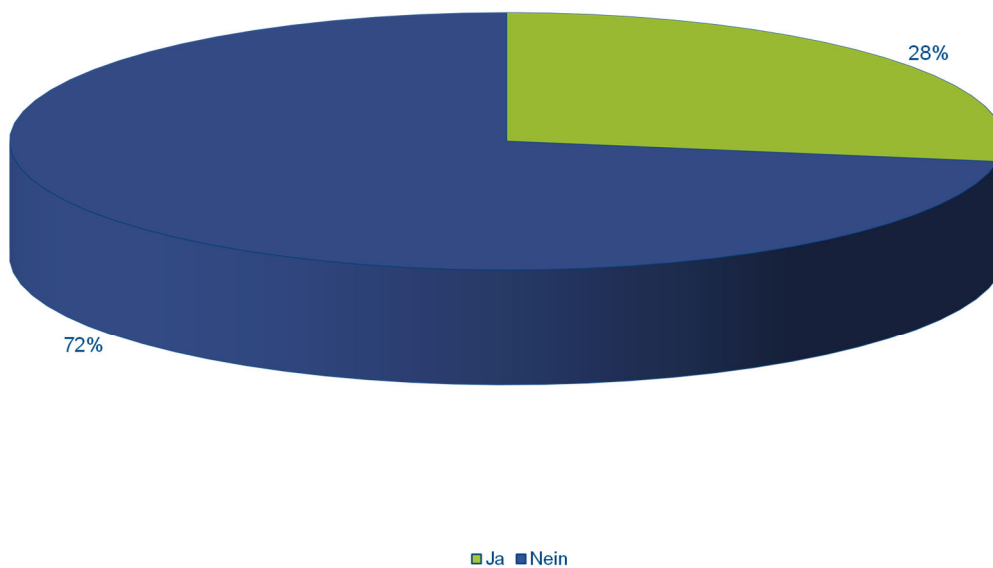


ABBILDUNG 37: VORHANDENSEIN EINER CYBER-SECURITY

## 6.5 Durch die Cyber-Versicherung abgedeckte Risiken

Bei den abgeschlossenen Cyber-Versicherungen decken 84 Prozent Eigenschäden und 82 Prozent Drittschäden aufgrund von Cyber-Crime ab. 57 Prozent der Unternehmen mit abgeschlossener Cyberversicherung geben an, dass ihre Versicherung auch das Risiko Service-Leistungen abdeckt.

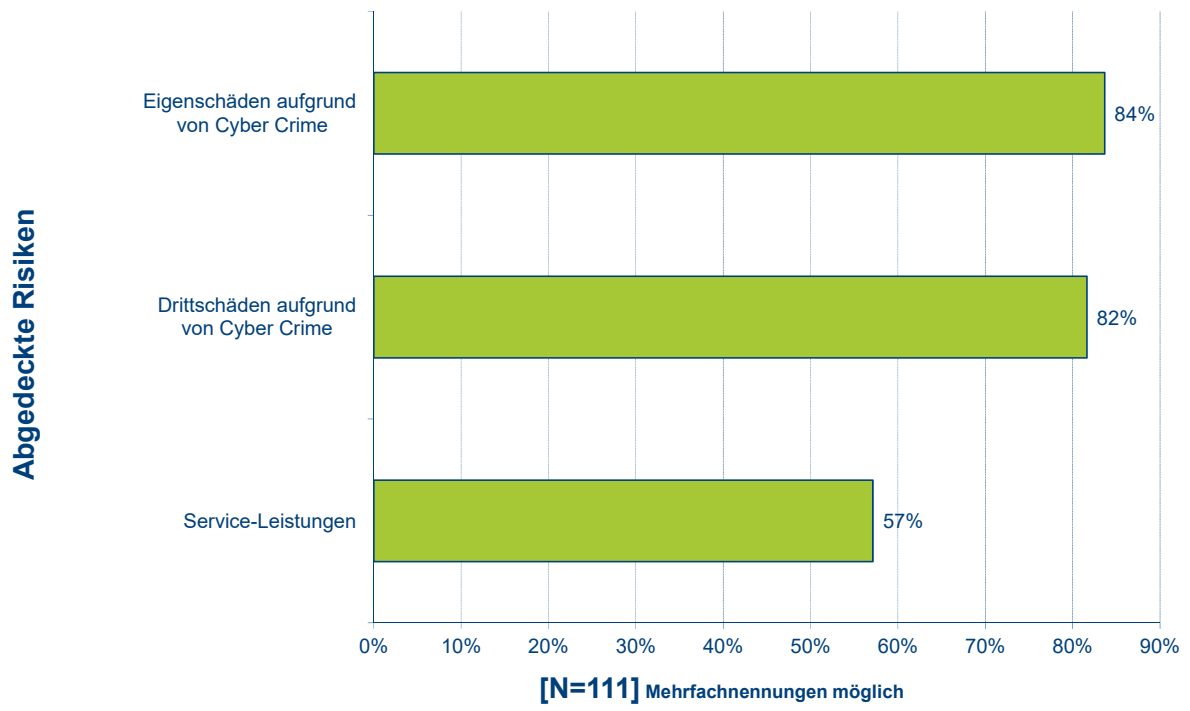


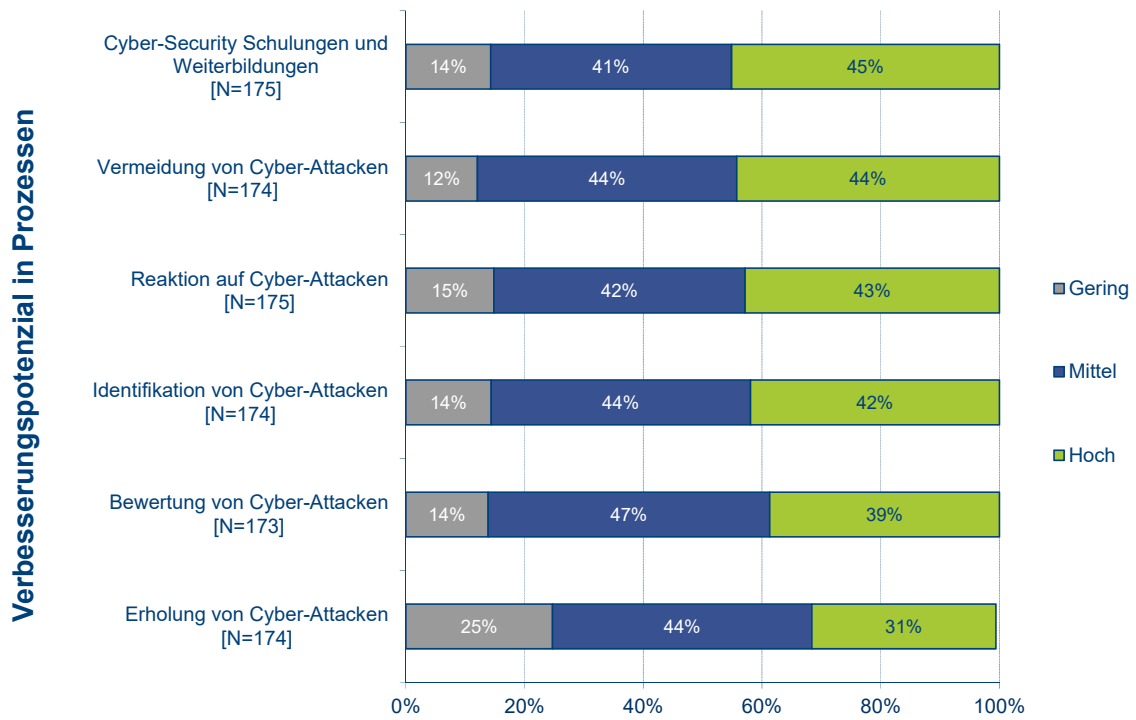
ABBILDUNG 38: ABGEDECKTE RISIKEN

## 7 Erfolgseinschätzung

In diesem Kapitel geht es um die persönliche Erfolgseinschätzung der befragten Probanden in Bezug auf prozessuale Verbesserungspotenziale und die zukünftige Relevanz von Cyber-Security im Unternehmen.

### 7.1 Prozessuale Verbesserungspotenziale

Im Rahmen dieser Frage sollten die Probanden ihre Einschätzung darüber abgeben, in welchen unternehmensinternen Prozessen mit Bezug zu Cyber-Security sie noch Verbesserungspotenzial sehen. Die Resultate ergaben, dass vor allem im Bereich Schulungs- und Weiterbildungsmaßnahmen mit Bezug zu Cyber-Security noch hohes Verbesserungspotenzial gesehen wird. 45 Prozent der Befragten sehen diesbezüglich hohes und 41 Prozent mittleres Verbesserungspotenzial. Auch bezüglich der Vermeidung von Cyber-Attacken meinen jeweils 44 Prozent der Probanden ein hohes bzw. mittleres Verbesserungspotenzial erkennen zu können. Hinsichtlich der Reaktion auf Cyber-Attacken gehen 43 Prozent von einem hohen und 42 Prozent von einem mittleren Verbesserungspotenzial aus. Die Identifikation von Cyber-Attacken betreffend sind 42 Prozent der Ansicht auch diesbezüglich bestehe hohes Verbesserungspotenzial, 44 Prozent stufen dieses als mittel ein. Bei der Bewertung von Cyber-Attacken geben 39 Prozent der Probanden an, ein hohes Verbesserungspotenzial zu sehen, 47 Prozent bewerten dieses als mittel. Der Recovery-Prozess bei stattgefundenen Cyber-Attacken weist nach Meinung von 31 Prozent hohes und nach Ansicht von 44 Prozent der Umfrageteilnehmer ein mittleres Verbesserungspotenzial auf.



**ABBILDUNG 39: VERBESSERUNGSPOTENZIAL IN PROZESSEN**

## 7.2 Aktuelle und zukünftige Relevanz von Cyber-Security im Unternehmen

Letztlich wurden die Probanden nach ihrer Einschätzung bezüglich der aktuellen und zukünftigen Relevanz von Cyber-Security befragt. Hierbei schätzen 50 Prozent der Unternehmen die aktuelle Relevanz von Cyber-Security als hoch ein (11 Prozent sehr hoch und 39 Prozent hoch). 33 Prozent attestieren dieser Thematik aktuell eine mittlere Relevanz für das Unternehmen. 12 Prozent erachten Cyber-Security im Moment als gering relevant und 5 Prozent bewerten die aktuelle Relevanz als sehr gering.

Ein anderes Bild zeigt sich bei der Frage nach der zukünftigen Relevanz von Cyber-Security im Unternehmen. 83 Prozent der Probanden sind der Meinung, dass Cyber-Security zukünftig eine wichtige Bedeutung einnehmen wird. 42 Prozent bewerten die zukünftige Relevanz als sehr hoch und 41 Prozent als hoch. 11 Prozent erachten die zukünftige Relevanz als mittel. Eine geringe Relevanz attestieren 3 Prozent der Probanden der Problematik Cyber-Security in der Zukunft, ebenfalls 3 Prozent weisen dieser eine sehr geringe Rolle zu.

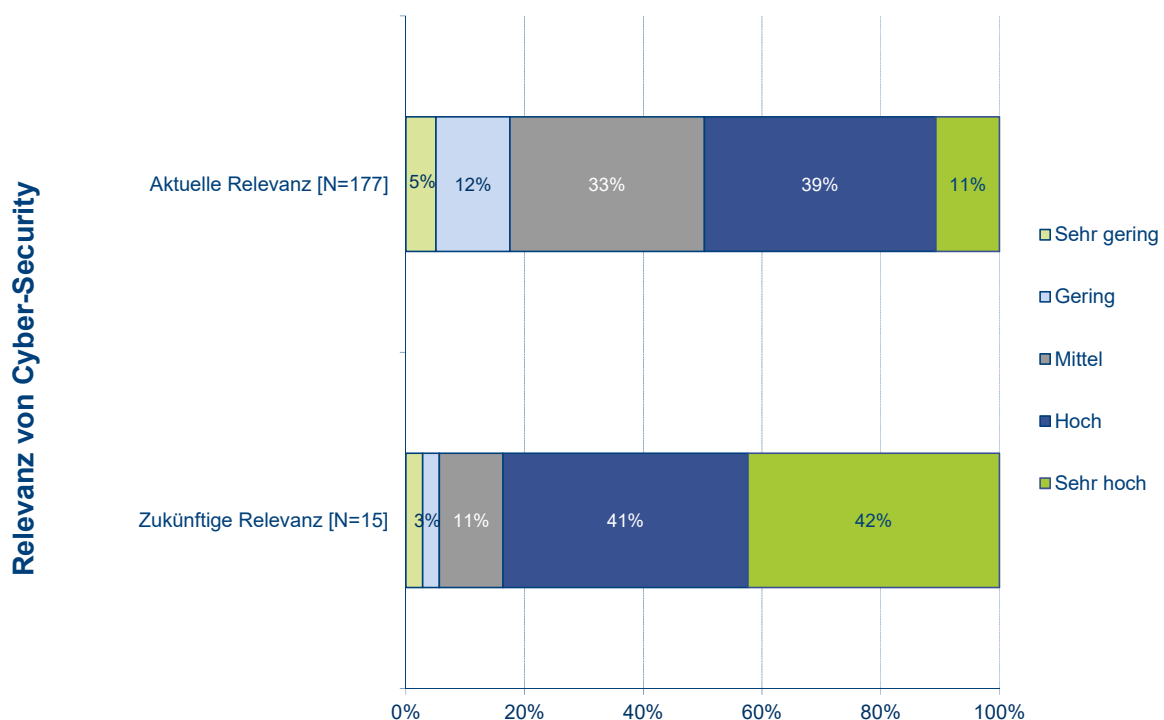


ABBILDUNG 40: RELEVANZ VON CYBER-SECURITY TEIL 1

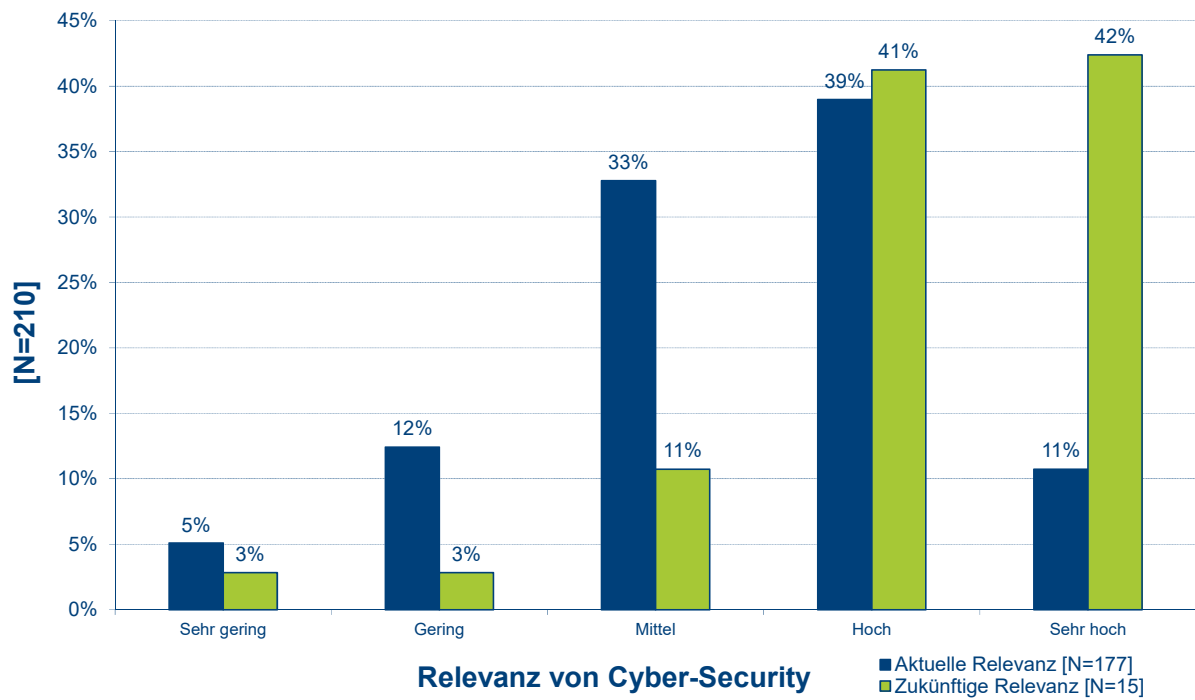


ABBILDUNG 41: RELEVANZ VON CYBER-SECURITY TEIL 2

## Literatur

Bundesamt für Sicherheit in der Informationstechnik (2019): Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen – Fassung vom 18.04.2019.