

POTENZIALANALYSE DIGITAL SECURITY

2017

Delivering Transformation. Together.

sopra  steria
CONSULTING

POTENZIALANALYSE DIGITAL SECURITY

Datum: Mai 2017

Impressum

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt.

Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen schriftlichen Zustimmung der Sopra Steria GmbH, nachfolgend auch Sopra Steria Consulting.

Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen und die Einspeicherung und Verarbeitung in elektronischer Form. Eine Weitergabe an Dritte ist nicht gestattet.

Realisierung: Faktenkontor GmbH
Ludwig-Erhard-Straße 37
D-20459 Hamburg
Tel.: +49 40 253185-111
Fax: +49 40 253185-311

Sopra Steria GmbH
Hans-Henny-Jahnn-Weg 29, 22085 Hamburg
Telefon: +49 40 22703-0
E-Mail: info.de@soprasteria.com

Vorsitzender des Aufsichtsrates: Vincent Paris
Geschäftsführer: Urs Michael Krämer
Gesellschaftssitz: Hamburg - HRB 130 165 Amtsgericht Hamburg - USt-ID-Nr.: DE118671351



AGENDA

1 Untersuchungsansatz	Seite 4
2 Management Summary	Seite 5
3 Ergebnisse Digital Security	Seite 9
Process Digitisation and Automation	Seite 10
IT Architecture Transformation	Seite 14
Data-driven Agility	Seite 16
Business Model Innovation	Seite 18
Digital Empowerment	Seite 21
Digital Platform Management	Seite 31
Customer and Partner Engagement	Seite 33
Digital Compliance	Seite 39
Digital Leadership	Seite 42
Statistik	Seite 43



UNTERSUCHUNGSANSATZ

Thema der Studie

Der Berichtsband stellt die Ergebnisse einer Online-Befragung zum Thema „Digital Security“ dar, die im Auftrag von Sopra Steria Consulting durchgeführt wurde.

Befragungszeitraum

Die Daten sind im April 2017 erhoben worden. Die Befragung wurde über ein Online-Panel durchgeführt. Die Ergebnisse sind auf ganze Zahlen gerundet.

Zielgruppe

205 IT-Entscheider aus Unternehmen ab 500 Mitarbeitern der Branchen Banken, Versicherungen, sonstige Finanzdienstleister, Energieversorger, Automotive, sonstiges Verarbeitendes Gewerbe, Telekommunikation und Medien, Öffentliche Verwaltung. Explizit ausgeschlossen wurden Beratungsunternehmen und Anbieter von IT-Lösungen.

Zeitvergleich

Die Daten werden mit den Ergebnissen der Studie „Digital Security 2015“ verglichen. Für die Studie im Jahr 2015 wurden 110 IT-Entscheider befragt.



AGENDA

1 | Untersuchungsansatz

2 | Management Summary

3 | Ergebnisse Digital Security

- Process Digitisation and Automation
- IT Architecture Transformation
- Data-driven Agility
- Business Model Innovation
- Digital Empowerment
- Digital Platform Management
- Customer and Partner Engagement
- Digital Compliance
- Digital Leadership
- Statistik



MANAGEMENT SUMMARY

- Mit der fortlaufenden Digitalisierung der Wirtschaft gehen umfangreiche neue Herausforderungen für die digitale Sicherheit der Unternehmen einher. IT-Sicherheitsvorfälle mit millionenfachen Identitätsdiebstählen zeigen, dass die Cyber-Angriffe auf IT-Infrastrukturen weiterhin komplexer und professioneller werden. Die Entscheider-Befragung „Digital Security 2017“ orientiert sich an zentralen Disziplinen der digitalen Exzellenz aus der gleichnamigen Studie von Sopra Steria Consulting.
- **Digital Leadership:** Die Statistiken und die nahezu täglichen Pressemeldungen über Cyber-Angriffe rufen die deutsche Unternehmenslandschaft weiterhin zum Handeln auf. Demgegenüber wird die mangelnde Initiative vieler Unternehmen beim Schutz gegen Cyber-Angriffe als „Digitale Sorglosigkeit“ bewertet.
- 73 Prozent der IT-Entscheider schließen sich in der aktuellen Befragung dieser Meinung an. Vor allem Vorstand und Geschäftsführer verharmlosen aus Sicht von knapp 40 Prozent der IT-Entscheider die Gefahr von Cyber-Angriffen. Ein Viertel der IT-Entscheider beklagt eine zu hohe Risikobereitschaft seitens der Unternehmensleiter, ein weiteres Viertel fühlt sich zu wenig über die konkreten Gefahren, z. B. durch staatliche Institutionen oder durch die Presse, informiert. Interessant ist, dass im Vergleich zur letzten Befragung rund 30 Prozent der IT-Entscheider sagen, dass deutsche Unternehmen nicht sorglos mit dem Thema umgehen. Vor zwei Jahren waren es nur 15 Prozent (S. 42).
- **Digital Compliance:** Im Juli 2015 wurde im deutschen Bundestag das IT-Sicherheitsgesetz verabschiedet. Es fordert von Betreibern besonders gefährdeter und kritischer Infrastrukturen ein Mindestsicherheitsniveau sowie die Meldung von Sicherheitsvorfällen. Sieben von zehn IT-Entscheidern beurteilen den Umfang der staatlichen Regulierung im Hinblick auf die IT-Sicherheit als angemessen. Nur 12 Prozent sehen hier Lücken und bewerten die staatliche Regulierung als zu gering. Zum Vergleich: Vor zwei Jahren war es rund ein Fünftel (S. 39).



MANAGEMENT SUMMARY

- **Digital Platform Management:** Ein wichtiger Bestandteil der Digitalen Exzellenz ist die Nutzung von Social Media zur Kommunikation und Interaktion mit Kunden. 86 Prozent der befragten Unternehmen nutzen bereits Social Media (2015: 80%). Beschränkungen der Social-Media-Kommunikation aus Gründen der IT-Sicherheit erscheinen im Hinblick auf die Aktualität und Kreativität eher als Hürde. Dennoch sind Maßnahmen zur Verhinderung eines ungewollten Datenabflusses wichtig. Zur Absicherung setzen die Entscheider hauptsächlich Schulungen und Awareness-Kampagnen (70%) sowie technische Data Leakage Prevention Maßnahmen ein (64%; S. 31). Diese waren in der Befragung aus dem Jahr 2015 ebenfalls die Top-Maßnahmen.
- **Customer & Partner Engagement:** Eine weitere externe Anbindung nutzen bereits 83 Prozent der befragten Unternehmen (2015: 61%). Knapp 70 Prozent sind über digitale Plattformen oder Softwarelösungen mit Lieferanten oder Dienstleistern vernetzt, 57 Prozent mit ihren Kunden (S. 33). Nahezu alle Unternehmen, die mit ihren Dienstleistern und Lieferanten verbunden sind, verfolgen dabei IT-Sicherheitsmaßnahmen: Vor allem schützen sie sich durch vertraglich vereinbarte Mindestsicherheitsmaßnahmen vor Datenmissbrauch, Datenabfluss und Cyber-Attacken (69%). Auch in der Befragung 2015 war das die meistumgesetzte Maßnahme (75%; S. 36).
- **Digital Empowerment:** Über die Nutzung von mobilen Endgeräten können immense Mengen von Unternehmensdaten durch Unachtsamkeit in falsche Hände gelangen. Darüber hinaus produziert die Sensorik mobiler Geräte (Kamera, Mikrofon, GPS, NFC) Daten, die als sensibel eingestuft werden müssen. Die damit verbundenen möglichen Gefahren sind den Unternehmen bewusst: 95 Prozent führen IT-Sicherheitsmaßnahmen für mobile Endgeräte durch (2015: 90%). Vor allem Mobile Device Management (65%), regelmäßige Sicherheitsüberprüfungen (65%), oder eine Mobile Security Policy (54%) werden zum Schutz eingesetzt (S. 27).
- Das Thema Informationssicherheit erfordert generell von jedem Mitarbeiter ein Mindestmaß an Mitwirkung und „Security Awareness“ – also ein Bewusstsein für Informationssicherheitsaspekte. Diese Mitwirkung kann je nach Rolle unterschiedliche Aufgaben und Verpflichtungen umfassen. Nahezu alle befragten Unternehmen führen Maßnahmen zur Security Awareness durch. Knapp die Hälfte davon regelmäßige Maßnahmen für alle Mitarbeiter. Bei knapp der Hälfte der Unternehmen sind die Maßnahmen für alle angesprochenen Mitarbeiter dieselben (S. 21).



MANAGEMENT SUMMARY

- **Data-driven Agility:** Wenn Unternehmen Daten sammeln, dann steht dabei nicht immer der Zweck der Datennutzung fest. Dies steht oft im Widerspruch zur Zweckbindung insbesondere von personenbezogenen Daten. Knapp 30 Prozent der IT-Entscheider meinen, dass die Zweckbindung von personengebundenen Daten gelockert werden sollte (2015: 35%). Dafür wären sie im Gegenzug auch bereit, mehr in Prozesse und Tools zu investieren, um die Daten flexibel auswerten zu können und gleichermaßen, die IT-Sicherheits- und Datenschutzerfordernungen zu erfüllen. 44 Prozent der IT-Experten sprechen sich allerdings gegen so eine Lockerung aus. Dass dann die eine oder andere Auswertung nicht gemacht werden kann, nehmen sie dafür in Kauf (2015: 48%; S. 16).
- **IT Architecture Transformation:** Viele Unternehmen haben eine IT-Strategie, die beschreibt wie sich die Transformation ihrer IT-Architektur vollziehen soll. Seltener ist eine IT-Sicherheitsstrategie, die die IT-Strategie unterstützt. Sie soll sowohl Ziele der Informationssicherheit und Prinzipien zur Umsetzung formulieren als auch zu Trends im Markt und neuen Technologien Stellung beziehen. Sechs von zehn der befragten Unternehmen folgen einer solchen IT-Sicherheitsstrategie (2015: 65%). Ein Drittel der befragten Unternehmen arbeitet daran (2015: 25%; S. 14).
- **Process Digitisation and Automation:** In Bezug auf die Einführung einer neuen Technologie vertreten rund zwei Drittel der IT-Entscheider die Meinung, dass vorab alle IT-Risiken geklärt sein müssen (2015: 65%). Knapp ein Drittel der IT-Entscheider gibt neuen Technologien hingegen auch eine Chance, wenn noch nicht alle IT-Risiken bekannt sind (2015: 35%; S. 10). Auch beim Vorantreiben der Digitalisierung und Automation von Prozessen gehen die Unternehmen eher auf Nummer sicher: In knapp 40 Prozent Unternehmen dürfen IT-Projekte erst starten, wenn ein Sicherheitskonzept der IT vorliegt, in 49 Prozent muss vor Produktivnahme einer Anwendung oder eines IT-Systems ein Sicherheitskonzept vorliegen. Nur in zwei Prozent der Unternehmen ist ein IT-Sicherheitskonzept nicht zwingend vorgeschrieben (2015: 10%; S. 12).
- **Business Model Innovation:** Um eine exzellente IT-Versorgung im Unternehmen sicherzustellen, ist eine schnelle Reaktionsfähigkeit der IT notwendig. Das stellt auch die IT-Sicherheit vor spezielle Herausforderungen: Die Anpassung der IT-Architektur, Datensicherheit oder der Einsatz von Cloud-basierten Lösungen sind dafür nur einige Beispiele, die Mitarbeiter in IT-Abteilungen fordern. Knapp zwei Drittel der Unternehmen wollen in den nächsten zwölf Monaten in erster Linie eigene IT-Mitarbeiter für die speziellen Aufgaben der IT-Sicherheit ausbilden (2015: 54%; S. 18).



AGENDA

1 | Untersuchungsansatz

2 | Management Summary

3 | Ergebnisse Digital Security

Process Digitisation and Automation

IT Architecture Transformation

Data-driven Agility

Business Model Innovation

Digital Empowerment

Digital Platform Management

Customer and Partner Engagement

Digital Compliance

Digital Leadership

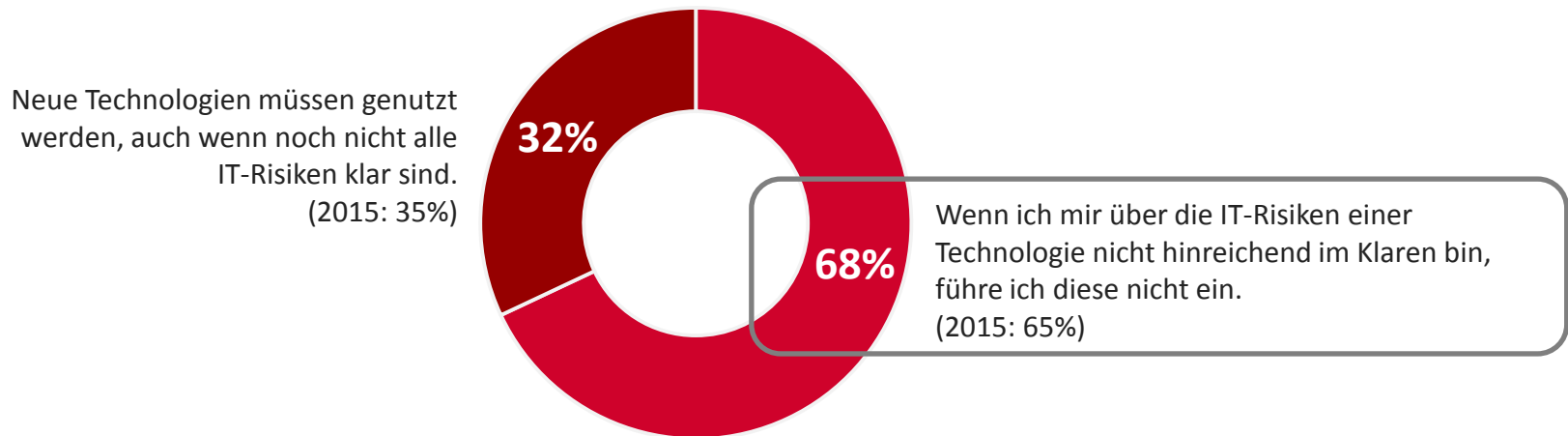
Statistik



ERGEBNISSE

PROCESS DIGITISATION AND AUTOMATION

- Einführung einer neuen Technologie: Für 68 Prozent der IT-Entscheider nur, wenn die IT-Risiken vorab geklärt sind.



Frage 1: Die Digitalisierung und Automation von Prozessen dringt in Bereiche vor, die bisher ohne Vernetzung, manuell oder ohne IT-Unterstützung betrieben wurden (z.B. IT-Service-Management-Automatisierung, SmartHome, car2car Kommunikation). Nicht immer sind bei Einführung einer Technologie alle Fragestellungen der IT-Sicherheit geklärt und mithin alle IT-Risiken bekannt. Welchen Standpunkt vertreten Sie?
Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)

ERGEBNISSE

PROCESS DIGITISATION AND AUTOMATION

- Vor allem IT-Entscheider aus dem Verarbeiteten Gewerbe führen neue Technologien ein, wenn die Risiken noch nicht bekannt sind.

Einführung einer neuen Technologie	Total	Branche					
		Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	205	75	62	23	19	13	13
Wenn ich mir über die IT-Risiken einer Technologie nicht hinreichend im Klaren bin, führe ich diese nicht ein.	68%	65%	61%	74%	95%	77%	62%
Neue Technologien müssen genutzt werden, auch wenn noch nicht alle IT-Risiken klar sind.	32%	35%	39%	26%	5%	23%	38%

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 1: Die Digitalisierung und Automation von Prozessen dringt in Bereiche vor, die bisher ohne Vernetzung, manuell oder ohne IT-Unterstützung betrieben wurden (z.B. IT-Service-Management-Automatisierung, SmartHome, car2car Kommunikation). Nicht immer sind bei Einführung einer Technologie alle Fragestellungen der IT-Sicherheit geklärt und mithin alle IT-Risiken bekannt. Welchen Standpunkt vertreten Sie?

Basis: Alle Befragten, N = 205 (Einfachnennung)

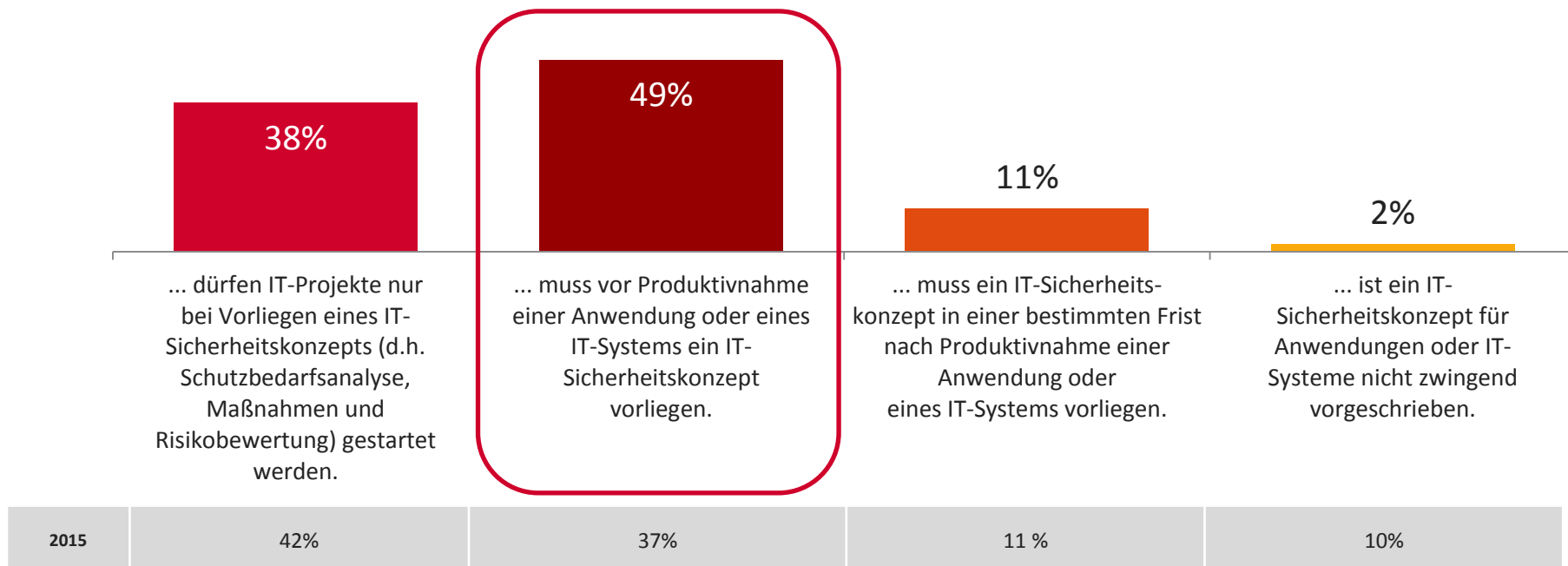


ERGEBNISSE

PROCESS DIGITISATION AND AUTOMATION

- In jedem zweiten Unternehmen muss vor Produktivnahme ein IT-Sicherheitskonzept vorliegen.

In meinem Unternehmen ...



Frage 2: Das Vorantreiben der Digitalisierung und Automation von Prozessen fordert spezielle IT-Sicherheitsmaßnahmen. Wie ist die Situation in Ihrem Unternehmen?
Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)



ERGEBNISSE

PROCESS DIGITISATION AND AUTOMATION

- Vor allem bei Finanzdienstleistern und im Verarbeitenden Gewerbe muss vor Produktivnahme ein IT-Sicherheitskonzept vorhanden sein.

In meinem Unternehmen...	Total	Branche					
		Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	205	75	62	23	19	13	13
...dürfen IT-Projekte nur bei Vorliegen eines IT-Sicherheitskonzepts (d.h. Schutzbedarfsanalyse, Maßnahmen und Risikobewertung) gestartet werden.	38%	32%	27%	65%	48%	62%	39%
...muss vor Produktivnahme einer Anwendung oder eines IT-Systems ein IT-Sicherheitskonzept vorliegen.	49%	53%	56%	31%	42%	31%	46%
...muss ein IT-Sicherheitskonzept in einer bestimmten Frist nach Produktivnahme einer Anwendung oder eines IT-Systems vorliegen.	11%	12%	15%	4%	5%	7%	15%
...ist ein IT-Sicherheitskonzept für Anwendungen oder IT-Systeme nicht zwingend vorgeschrieben.	2%	3%	2%	0%	5%	0%	0%

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

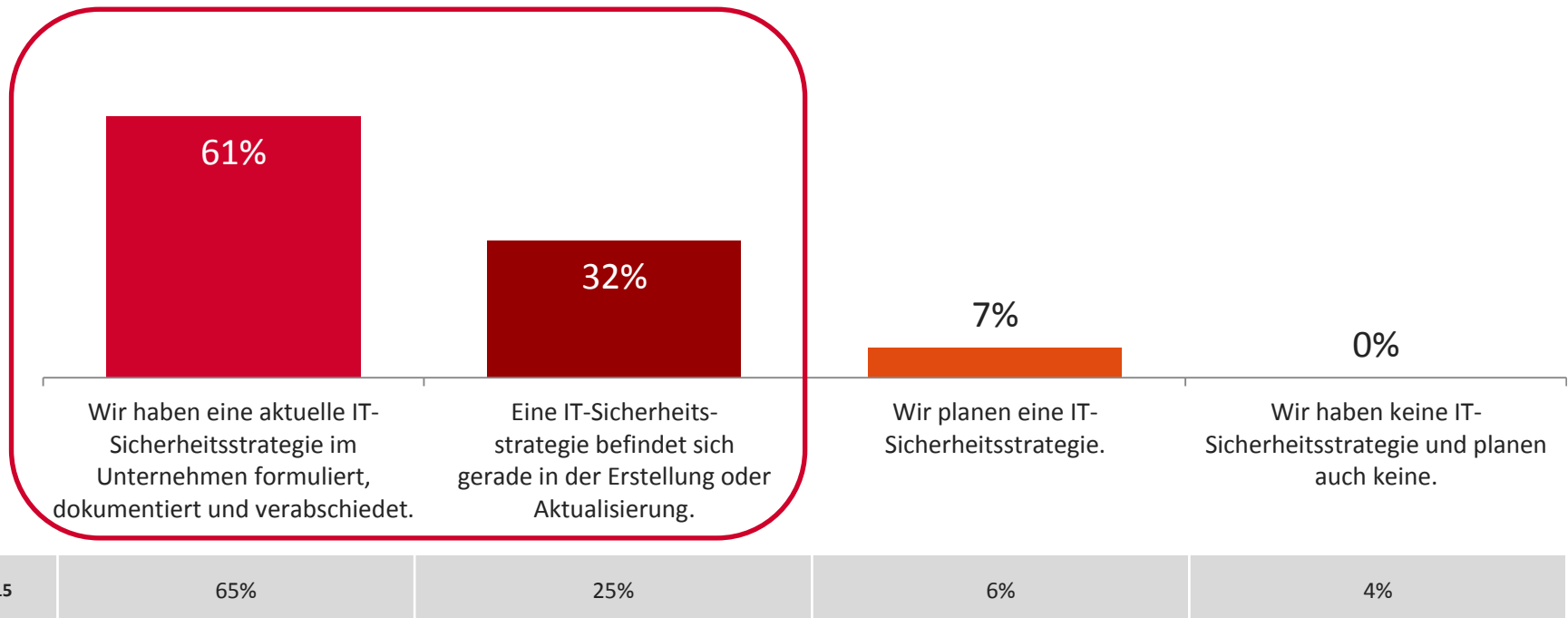
Frage 2: Das Vorantreiben der Digitalisierung und Automation von Prozessen fordert spezielle IT-Sicherheitsmaßnahmen. Wie ist die Situation in Ihrem Unternehmen?
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

IT ARCHITECTURE TRANSFORMATION

- Sechs von zehn der Unternehmen folgen bereits einer aktuellen IT-Sicherheitsstrategie. Knapp ein Drittel arbeitet daran.



Frage 3: Viele Unternehmen besitzen eine IT-Strategie, die beschreibt wie sich eine Transformation ihrer IT-Architektur vollziehen soll. Deutlich seltener anzutreffen ist eine IT-Sicherheitsstrategie, die die IT-Strategie stützt und z.B. sowohl Ziele der Informationssicherheit und Prinzipien zur Umsetzung formuliert als auch zu Trends im Markt sowie Technologien Stellung bezieht. Wie ist die Situation in Ihrem Unternehmen?

Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)



ERGEBNISSE

IT ARCHITECTURE TRANSFORMATION

- Vor allem große Unternehmen arbeiten mit einer aktuellen IT-Sicherheitsstrategie.

IT-Sicherheitsstrategie	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	205	71	95	39
Wir haben eine aktuelle IT-Sicherheitsstrategie im Unternehmen formuliert, dokumentiert und verabschiedet.	61%	62%	51%	82%
Eine IT-Sicherheitsstrategie befindet sich gerade in der Erstellung oder Aktualisierung.	32%	28%	43%	13%
Wir planen eine IT-Sicherheitsstrategie.	7%	10%	6%	5%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 3: Viele Unternehmen besitzen eine IT-Strategie, die beschreibt wie sich eine Transformation ihrer IT-Architektur vollziehen soll. Deutlich seltener anzutreffen ist eine IT-Sicherheitsstrategie, die die IT-Strategie stützt und z.B. sowohl Ziele der Informationssicherheit und Prinzipien zur Umsetzung formuliert als auch zu Trends im Markt sowie Technologien Stellung bezieht. Wie ist die Situation in Ihrem Unternehmen?

Basis: Alle Befragten, N = 205 (Einfachnennung)

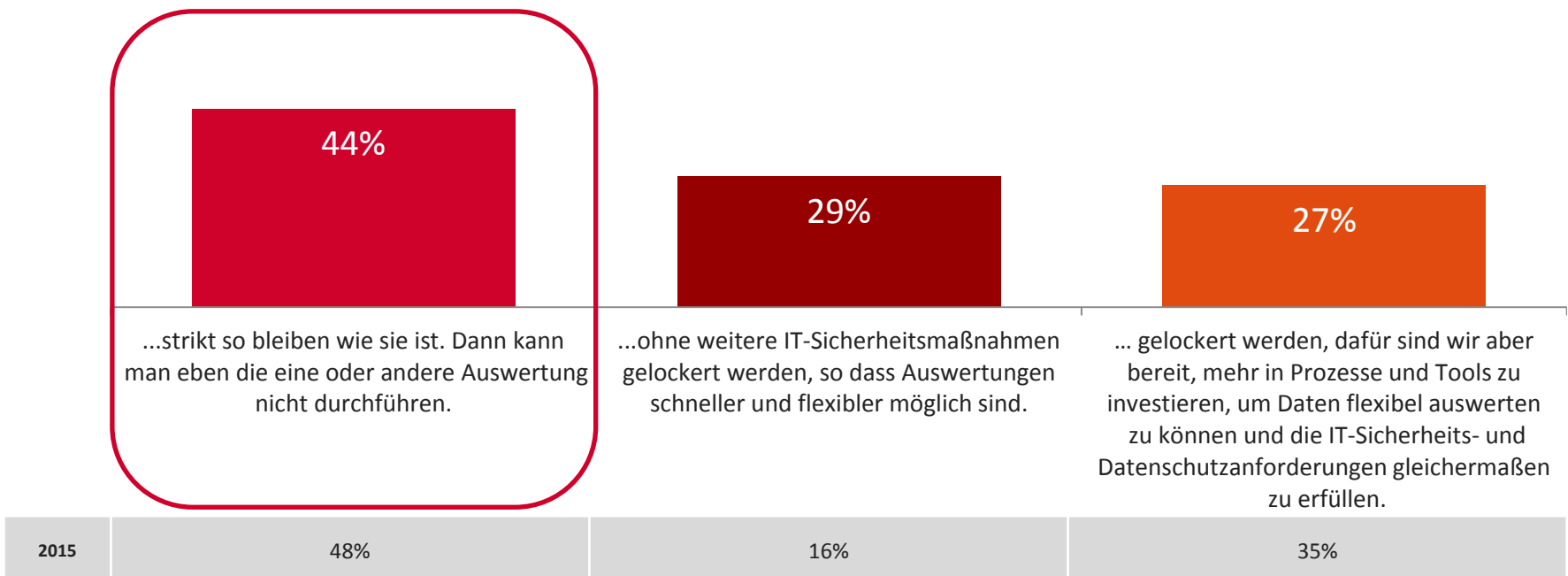


ERGEBNISSE

DATA-DRIVEN AGILITY

- Etwa die Hälfte der IT-Entscheider spricht sich gegen die Lockerung der Zweckbindung von personengebundenen Daten aus.

Die Zweckbindung von personengebundenen Daten sollte....



Frage 4: Wenn datengetriebene Entscheidungen getroffen werden sollen, steht bei der Sammlung von Daten nicht immer bereits der Zweck der Datennutzung fest. Dies steht oft im Widerspruch zur Zweckbindung insbesondere von personenbezogenen Daten. Welcher der folgenden Aussagen stimmen Sie zu? Die Zweckbindung von personengebundenen Daten sollte....
Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)

ERGEBNISSE

DATA-DRIVEN AGILITY

- IT-Entscheider des mittleren Managements sind mehrheitlich gegen eine Lockerung der Zweckbindung von personengebundenen Daten.

Die Zweckbindung von personengebundenen Daten sollte....	Total	Position		
		Leitender Angestellter erste Führungsebene	Leitender Angestellter zweite Führungsebene	Mittleres Management/Führungskraft Fachabteilung/Spezialist
Basis	205	96	53	56
...strikt so bleiben wie sie ist. Dann kann man eben die eine oder andere Auswertung nicht durchführen.	44%	37%	38%	62%
...ohne weitere IT-Sicherheitsmaßnahmen gelockert werden, so dass Auswertungen schneller und flexibler möglich sind.	29%	32%	36%	18%
...gelockert werden, dafür sind wir aber bereit, mehr in Prozesse und Tools zu investieren, um Daten flexibel auswerten zu können und die IT-Sicherheits- und Datenschutzerfordernungen gleichermaßen zu erfüllen.	27%	31%	26%	20%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

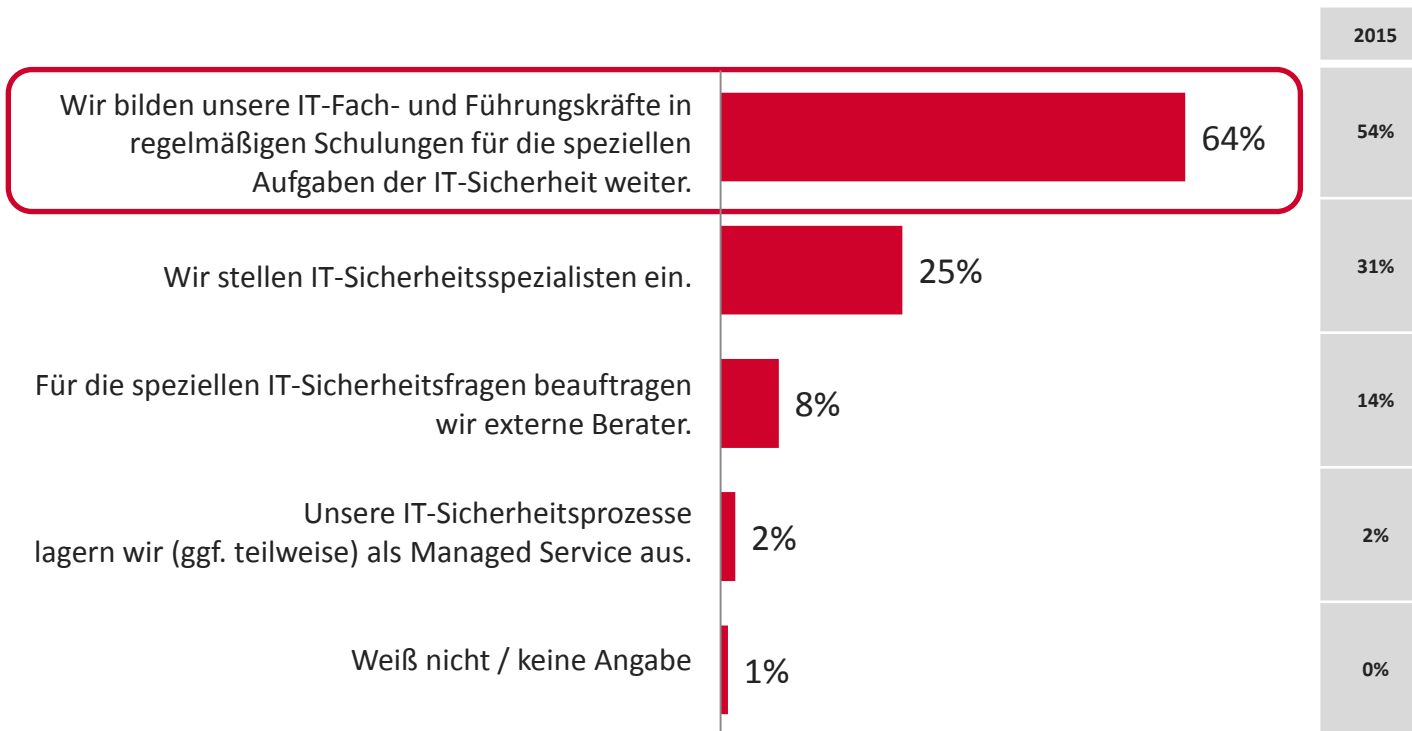
Frage 4: Wenn datengetriebene Entscheidungen getroffen werden sollen, steht bei der Sammlung von Daten nicht immer bereits der Zweck der Datennutzung fest. Dies steht oft im Widerspruch zur Zweckbindung insbesondere von personenbezogenen Daten. Welcher der folgenden Aussagen stimmen Sie zu? Die Zweckbindung von personengebundenen Daten sollte....
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

BUSINESS MODEL INNOVATION

- Personalstrategie: Die Mehrheit der Unternehmen bildet in erster Linie eigene IT-Mitarbeiter für spezielle Aufgaben der IT-Sicherheit aus.



Frage 5: Um eine exzellente IT-Versorgung im Unternehmen sicherzustellen, ist eine schnelle Reaktionsfähigkeit der IT notwendig. Das stellt auch die IT-Sicherheit vor spezielle Herausforderungen: Die Anpassung der IT-Architektur, Datensicherheit oder der Einsatz von Cloud-basierten Lösungen sind dafür nur einige Beispiele, die Mitarbeiter in IT-Abteilungen fordern. Welche Personalstrategie verfolgt Ihr Unternehmen für die nächsten 12 Monate in erster Linie, wenn es um die speziellen Herausforderungen in der IT-Sicherheit geht?
Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)



ERGEBNISSE

BUSINESS MODEL INNOVATION

- Spezielle IT-Sicherheitsanforderungen: Besonders das Verarbeitende Gewerbe bevorzugt die Weiterbildung eigener IT-Experten.

Personalstrategie für die nächsten 12 Monate	Branche						
	Total	Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	205	75	62	23	19	13	13
Wir bilden unsere IT-Fach- und Führungskräfte in regelmäßigen Schulungen für die speziellen Aufgaben der IT-Sicherheit weiter.	64%	55%	74%	48%	80%	77%	69%
Wir stellen IT-Sicherheitspezialisten ein.	25%	36%	16%	34%	5%	23%	23%
Für die speziellen IT-Sicherheitsfragen beauftragen wir externe Berater.	8%	9%	10%	9%	5%	0%	8%
Unsere IT-Sicherheitsprozesse lagern wir (ggf. teilweise) als Managed Service aus.	2%	0%	0%	9%	5%	0%	0%
Weiß nicht / keine Angabe	1%	0%	0%	0%	5%	0%	0%

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 5: Um eine exzellente IT-Versorgung im Unternehmen sicherzustellen, ist eine schnelle Reaktionsfähigkeit der IT notwendig. Das stellt auch die IT-Sicherheit vor spezielle Herausforderungen: Die Anpassung der IT-Architektur, Datensicherheit oder der Einsatz von Cloud-basierten Lösungen sind dafür nur einige Beispiele, die Mitarbeiter in IT-Abteilungen fordern. Welche Personalstrategie verfolgt Ihr Unternehmen für die nächsten 12 Monate in erster Linie, wenn es um die speziellen Herausforderungen in der IT-Sicherheit geht?
Basis: Alle Befragten, N = 205 (Einfachnennung)



Geringe Fallzahl



ERGEBNISSE

BUSINESS MODEL INNOVATION

- IT-Sicherheitsexperten: Vor allem Unternehmen mit 1.000 bis unter 5.000 Mitarbeitern setzen auf interne Weiterbildung.

Personalstrategie für die nächsten 12 Monate	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	205	71	95	39
Wir bilden unsere IT-Fach- und Führungskräfte in regelmäßigen Schulungen für die speziellen Aufgaben der IT-Sicherheit weiter.	64%	55%	74%	59%
Wir stellen IT-Sicherheitsspezialisten ein.	25%	31%	19%	31%
Für die speziellen IT-Sicherheitsfragen beauftragen wir externe Berater.	8%	14%	3%	10%
Unsere IT-Sicherheitsprozesse lagern wir (ggf. teilweise) als Managed Service aus.	2%	0%	3%	0%
Weiß nicht / keine Angabe	1%	0%	1%	0%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

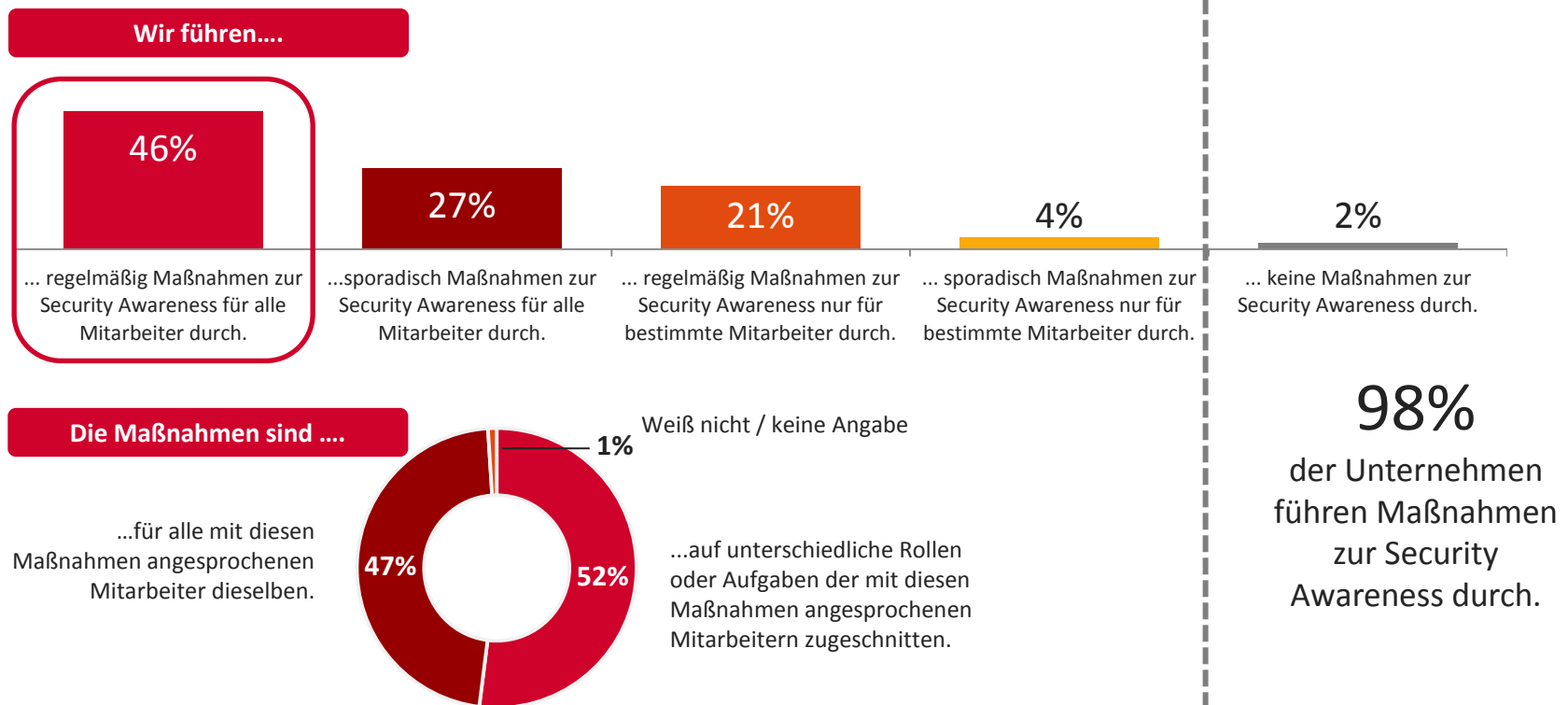
Frage 5: Um eine exzellente IT-Versorgung im Unternehmen sicherzustellen, ist eine schnelle Reaktionsfähigkeit der IT notwendig. Das stellt auch die IT-Sicherheit vor spezielle Herausforderungen: Die Anpassung der IT-Architektur, Datensicherheit oder der Einsatz von Cloud-basierten Lösungen sind dafür nur einige Beispiele, die Mitarbeiter in IT-Abteilungen fordern. Welche Personalstrategie verfolgt Ihr Unternehmen für die nächsten 12 Monate in erster Linie, wenn es um die speziellen Herausforderungen in der IT-Sicherheit geht?
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

DIGITAL EMPOWERMENT

- Informationssicherheit: Knapp die Hälfte der Unternehmen führt regelmäßig Maßnahmen zur Security Awareness für alle Mitarbeiter durch.






Frage 6: Informationssicherheit erfordert bei jedem Mitarbeiter eines Unternehmens ein Mindestmaß an Mitwirkung und Security Awareness - also Bewusstsein für Informationssicherheitsaspekte. Diese Mitwirkung kann je nach Rolle unterschiedliche Aufgaben und Verpflichtungen umfassen. Wie gehen Sie im Unternehmen mit Security Awareness um?
 Basis: Alle Befragten, N = 205 (Einfachnennung) / Frage 7: Welcher Art sind diese Maßnahmen? Die Maßnahmen sind...
 Basis: Befragte, deren Unternehmen Maßnahmen zur Security Awareness durchführen, N = 201 (Einfachnennung)





ERGEBNISSE

DIGITAL EMPOWERMENT

- Mehr als die Hälfte der Finanzdienstleister führt regelmäßig Maßnahmen zur Security Awareness für alle Mitarbeiter durch.

Wir führen...	Total	Branche					
		Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	205	75	62	23	19 	13 	13 
...regelmäßig Maßnahmen zur Security Awareness für alle Mitarbeiter durch.	46%	58%	45%	48%	16%	46%	31%
...sporadisch Maßnahmen zur Security Awareness für alle Mitarbeiter durch.	27%	24%	26%	30%	37%	39%	23%
...regelmäßig Maßnahmen zur Security Awareness nur für bestimmte Mitarbeiter durch.	21%	17%	21%	9%	42%	15%	38%
...sporadisch Maßnahmen zur Security Awareness nur für bestimmte Mitarbeiter durch.	4%	1%	5%	9%	0%	0%	8%
...keine Maßnahmen zur Security Awareness durch.	2%	0%	3%	4%	5%	0%	0%

 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 6: Informationssicherheit erfordert bei jedem Mitarbeiter eines Unternehmens ein Mindestmaß an Mitwirkung und Security Awareness - also Bewusstsein für Informationssicherheitsaspekte. Diese Mitwirkung kann je nach Rolle unterschiedliche Aufgaben und Verpflichtungen umfassen. Wie gehen Sie im Unternehmen mit Security Awareness um?
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

DIGITAL EMPOWERMENT

- Jedes zweite Unternehmen ab 5.000 Mitarbeitern führt regelmäßig Maßnahmen zur Security Awareness für alle Mitarbeiter durch.

Wir führen...	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	205	71	95	39
...regelmäßig Maßnahmen zur Security Awareness für alle Mitarbeiter durch.	46%	54%	37%	56%
...sporadisch Maßnahmen zur Security Awareness für alle Mitarbeiter durch.	27%	15%	38%	23%
...regelmäßig Maßnahmen zur Security Awareness nur für bestimmte Mitarbeiter durch.	21%	27%	19%	15%
...sporadisch Maßnahmen zur Security Awareness nur für bestimmte Mitarbeiter durch.	4%	1%	5%	3%
...keine Maßnahmen zur Security Awareness durch.	2%	3%	1%	3%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 6: Informationssicherheit erfordert bei jedem Mitarbeiter eines Unternehmens ein Mindestmaß an Mitwirkung und Security Awareness - also Bewusstsein für Informationssicherheitsaspekte. Diese Mitwirkung kann je nach Rolle unterschiedliche Aufgaben und Verpflichtungen umfassen. Wie gehen Sie im Unternehmen mit Security Awareness um?
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

DIGITAL EMPOWERMENT

- Security Awareness: Unternehmen mit 1.000 bis unter 5.000 Mitarbeitern schneiden Maßnahmen eher auf die Rollen und Aufgaben der Mitarbeiter zu.

Die Maßnahmen sind...	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	201	69	94	38
...für alle mit diesen Maßnahmen angesprochenen Mitarbeiter dieselben.	47%	55%	40%	50%
...auf unterschiedliche Rollen oder Aufgaben der mit diesen Maßnahmen angesprochenen Mitarbeitern zugeschnitten.	52%	45%	60%	47%
Weiß nicht / keine Angabe	1%	0%	0%	3%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 7: Welcher Art sind diese Maßnahmen? Die Maßnahmen sind...

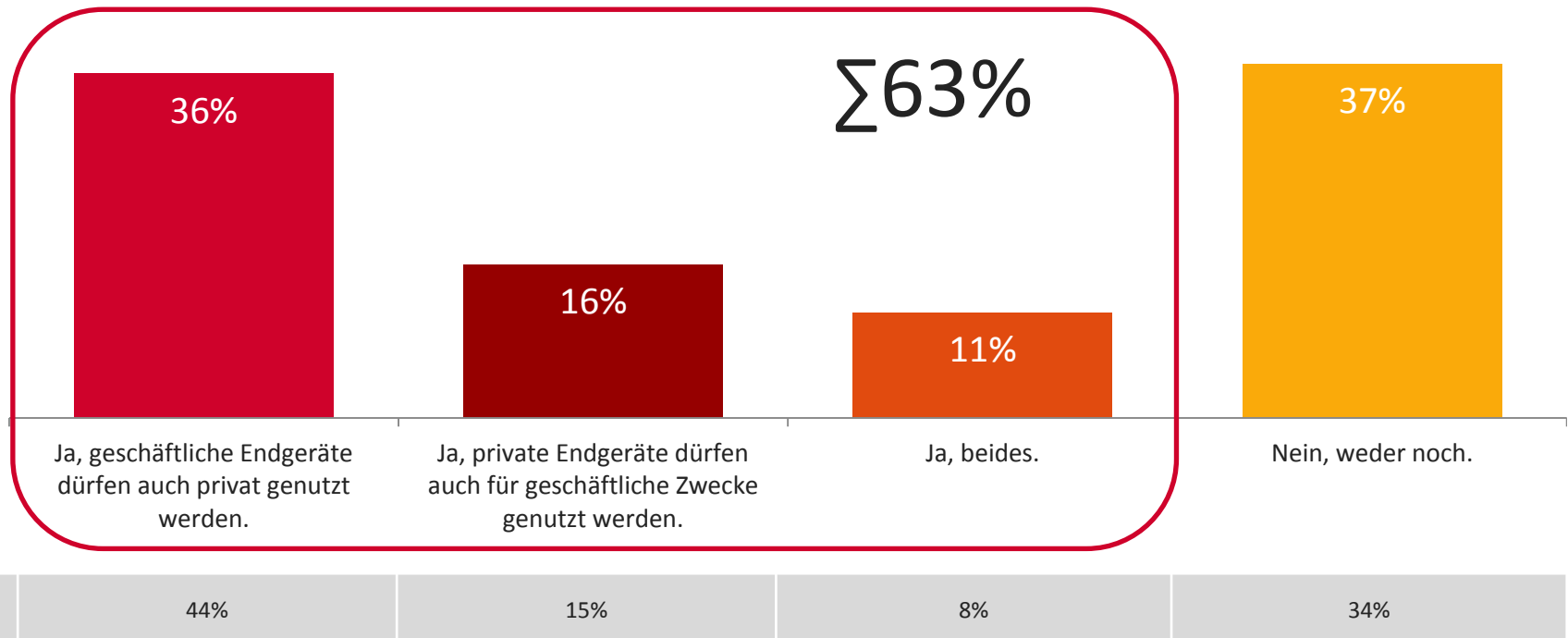
Basis: Befragte, deren Unternehmen Maßnahmen zur Security Awareness durchführen, N = 201 (Einfachnennung)



ERGEBNISSE

DIGITAL EMPOWERMENT

- Mobile Devices: In sechs von zehn Unternehmen werden Geschäftliches und Privates auf mobilen Endgeräten vermischt.



Frage 9: Kommen wir zum Thema Mobile Devices. Ist es in Ihrem Unternehmen erlaubt, geschäftliche Endgeräte (Smartphones, Tablets) auch privat zu nutzen oder private Endgeräte auch für geschäftliche Zwecke zu verwenden?

Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)



ERGEBNISSE

DIGITAL EMPOWERMENT

- Mobile Endgeräte: Mehr als die Hälfte der Unternehmen ab 5.000 Mitarbeitern verbietet eine Mischung von Geschäftlichem und Privatem.

Mobile Endgeräte	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	205	71	95	39
Ja, geschäftliche Endgeräte dürfen auch privat genutzt werden.	36%	45%	34%	26%
Ja, private Endgeräte dürfen auch für geschäftliche Zwecke genutzt werden.	16%	13%	22%	8%
Ja, beides.	11%	11%	11%	10%
Nein, weder noch.	37%	31%	33%	56%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 9: Kommen wir zum Thema Mobile Devices. Ist es in Ihrem Unternehmen erlaubt, geschäftliche Endgeräte (Smartphones, Tablets) auch privat zu nutzen oder private Endgeräte auch für geschäftliche Zwecke zu verwenden?

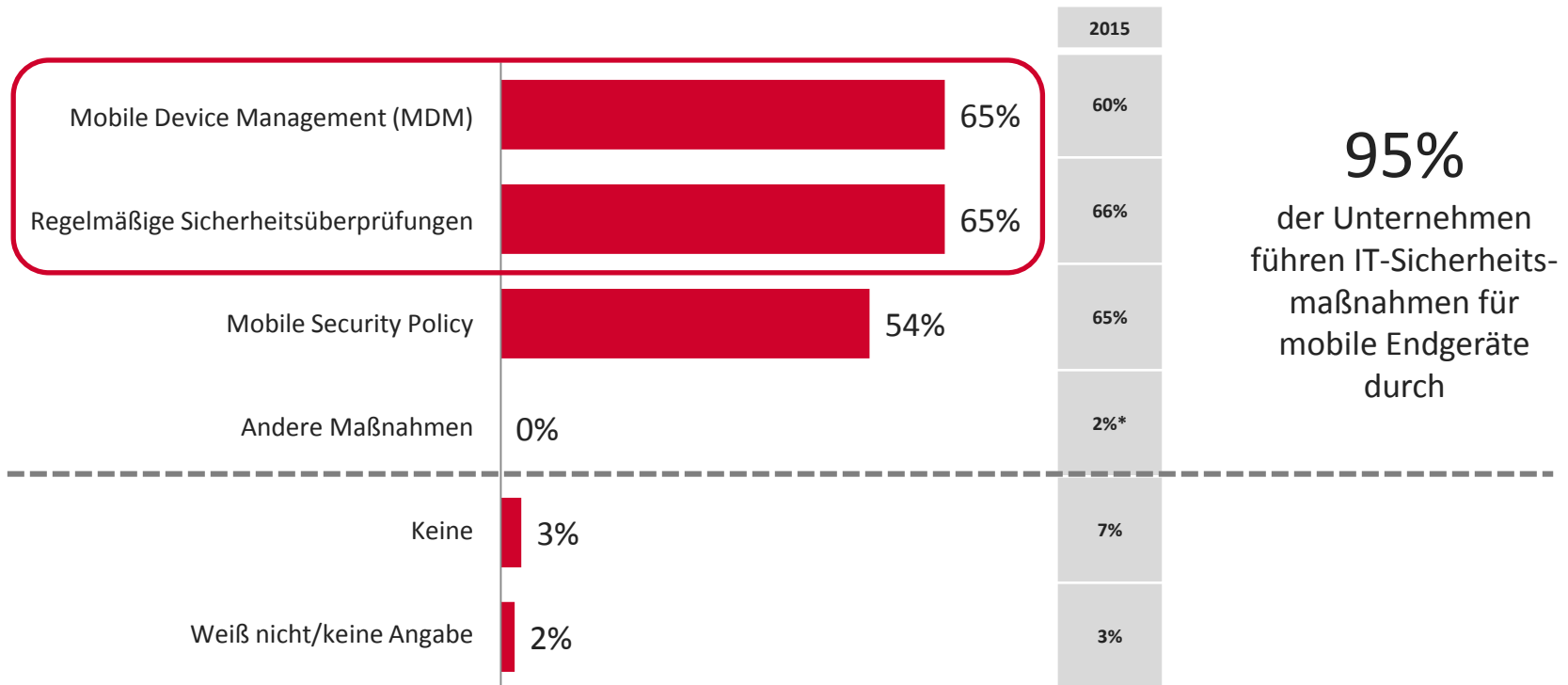
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

DIGITAL EMPOWERMENT

- Die Mehrheit der Unternehmen arbeitet mit einem Mobile Device Management und führt Sicherheitsüberprüfungen durch.



Frage 10: Über mobile Geräte können heute immense Mengen von Unternehmensdaten durch Unachtsamkeit in falsche Hände gelangen. Auch die Sensorik mobiler Geräte (Kamera, Mikrofon, GPS, NFC) produziert Daten, die als sensibel eingestuft werden müssen. Mobile Geräte erfordern eine eigene Qualität von IT-Sicherheitsmaßnahmen.

Welche sind in Ihrem Unternehmen umgesetzt?

Basis: Alle Befragten, N = 205 (2015: N = 110) (Mehrfachnennungen) *Eigenes VPN-System/angepasste Software.



ERGEBNISSE

DIGITAL EMPOWERMENT

- Vor allem Unternehmen aus dem Verarbeitenden Gewerbe haben ein Mobile Device Management.

IT-Sicherheitsmaßnahmen für mobile Geräte	Total	Branche					
		Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	205	75	62	23	19	13	13
Mobile Device Management (MDM)	65%	59%	77%	52%	74%	54%	69%
Regelmäßige Sicherheitsüberprüfungen	65%	60%	69%	65%	63%	92%	54%
Mobile Security Policy	54%	52%	58%	39%	63%	77%	38%
Keine	3%	4%	2%	4%	0%	0%	8%
Weiß nicht/keine Angabe	2%	4%	0%	0%	5%	0%	0%

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 10: Über mobile Geräte können heute immense Mengen von Unternehmensdaten durch Unachtsamkeit in falsche Hände gelangen. Auch die Sensorik mobiler Geräte (Kamera, Mikrofon, GPS, NFC) produziert Daten, die als sensibel eingestuft werden müssen. Mobile Geräte erfordern eine eigene Qualität von IT-Sicherheitsmaßnahmen.

Welche sind in Ihrem Unternehmen umgesetzt?

Basis: Alle Befragten, N = 205 (Mehrfachnennungen)



Geringe Fallzahl



ERGEBNISSE

DIGITAL EMPOWERMENT

- Vor allem Unternehmen mit 1.000 bis unter 5.000 Mitarbeitern arbeiten mit einer Mobile Security Policy.

IT-Sicherheitsmaßnahmen für mobile Geräte	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	205	71	95	39
Mobile Device Management (MDM)	65%	68%	64%	64%
Regelmäßige Sicherheitsüberprüfungen	65%	62%	71%	59%
Mobile Security Policy	54%	45%	64%	46%
Keine	3%	7%	1%	0%
Weiß nicht/keine Angabe	2%	0%	1%	8%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 10: Über mobile Geräte können heute immense Mengen von Unternehmensdaten durch Unachtsamkeit in falsche Hände gelangen. Auch die Sensorik mobiler Geräte (Kamera, Mikrofon, GPS, NFC) produziert Daten, die als sensibel eingestuft werden müssen. Mobile Geräte erfordern eine eigene Qualität von IT-Sicherheitsmaßnahmen.

Welche sind in Ihrem Unternehmen umgesetzt?

Basis: Alle Befragten, N = 205 (Mehrfachnennungen)



ERGEBNISSE

DIGITAL EMPOWERMENT

- Mobile Endgeräte: In Unternehmen, in denen Geschäftliches und Privates vermischelt werden darf, gibt es eher eine Mobile Security Policy.

IT-Sicherheitsmaßnahmen für mobile Geräte	Nutzung mobiler Endgeräte		
	Total	Private / geschäftliche Endgeräte dürfen geschäftlich / privat genutzt werden	Weder noch
Basis	205	130	75
Mobile Device Management (MDM)	65%	68%	60%
Regelmäßige Sicherheitsüberprüfungen	65%	61%	73%
Mobile Security Policy	54%	60%	44%
Keine	3%	2%	5%
Weiß nicht/keine Angabe	2%	1%	4%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 10: Über mobile Geräte können heute immense Mengen von Unternehmensdaten durch Unachtsamkeit in falsche Hände gelangen. Auch die Sensorik mobiler Geräte (Kamera, Mikrofon, GPS, NFC) produziert Daten, die als sensibel eingestuft werden müssen. Mobile Geräte erfordern eine eigene Qualität von IT-Sicherheitsmaßnahmen.

Welche sind in Ihrem Unternehmen umgesetzt?

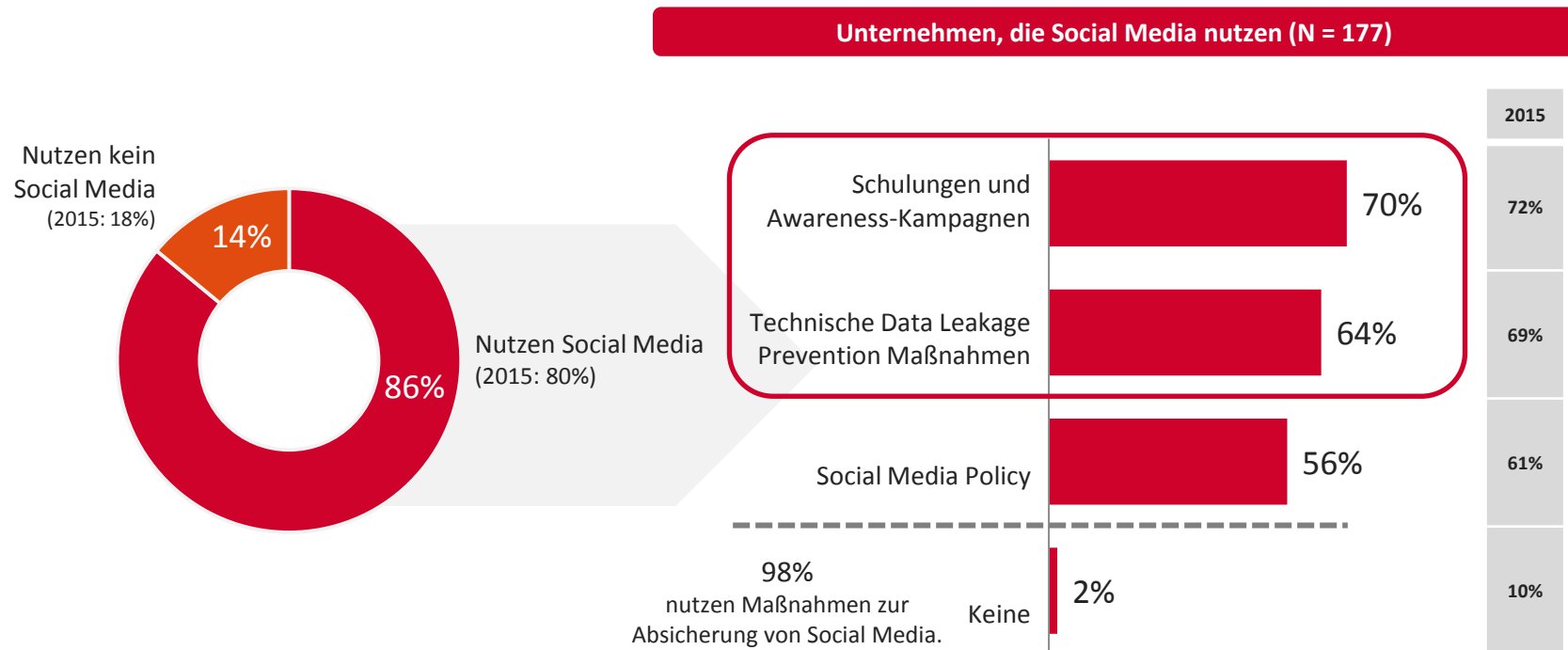
Basis: Alle Befragten, N = 205 (Mehrfachnennungen)



ERGEBNISSE

DIGITAL PLATFORM MANAGEMENT

- Top-Maßnahmen zur Absicherung von Social Media: Schulungen und Awareness-Kampagnen sowie technische Data Leakage Prevention.






Frage 8: Ein wichtiger Bestandteil der Digitalen Exzellenz ist die Nutzung von Social Media. Einschränkungen aus Gründen der IT-Sicherheit erscheinen im Hinblick auf Kreativität und Kommunikation eher hinderlich. Dennoch sind Maßnahmen zur Verhinderung des ungewollten Datenabflusses angeraten. Welche Maßnahmen hat Ihr Unternehmen zur Absicherung von Social Media umgesetzt? Basis: Alle Befragten, N = 205 (2015: N = 110) (Berechnung Nutzer/Nicht-Nutzer)
 Basis: Befragte, die Social Media nutzen, N = 177 (2015: N = 88) (Mehrfachnennungen)





ERGEBNISSE

DIGITAL PLATFORM MANAGEMENT

- Eine Social Media Policy nutzen rund zwei Drittel der Social-Media-aktiven Finanzdienstleister.

Maßnahmen	Total	Branche					
		Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	177	72	51	18	17 	11 	8 
Schulungen und Awareness-Kampagnen	70%	64%	71%	78%	82%	82%	63%
Technische Data Leakage Prevention Maßnahmen	64%	60%	75%	39%	65%	82%	63%
Social Media Policy	56%	65%	57%	33%	24%	73%	75%
Keine	2%	0%	2%	0%	12%	0%	0%

 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 8: Ein wichtiger Bestandteil der Digitalen Exzellenz ist die Nutzung von Social Media. Einschränkungen aus Gründen der IT-Sicherheit erscheinen im Hinblick auf Kreativität und Kommunikation eher hinderlich. Dennoch sind Maßnahmen zur Verhinderung des ungewollten Datenabflusses angeraten. Welche Maßnahmen hat Ihr Unternehmen zur Absicherung von Social Media umgesetzt?

Basis: Befragte, die Social Media nutzen, N = 177 (Mehrfachnennungen)

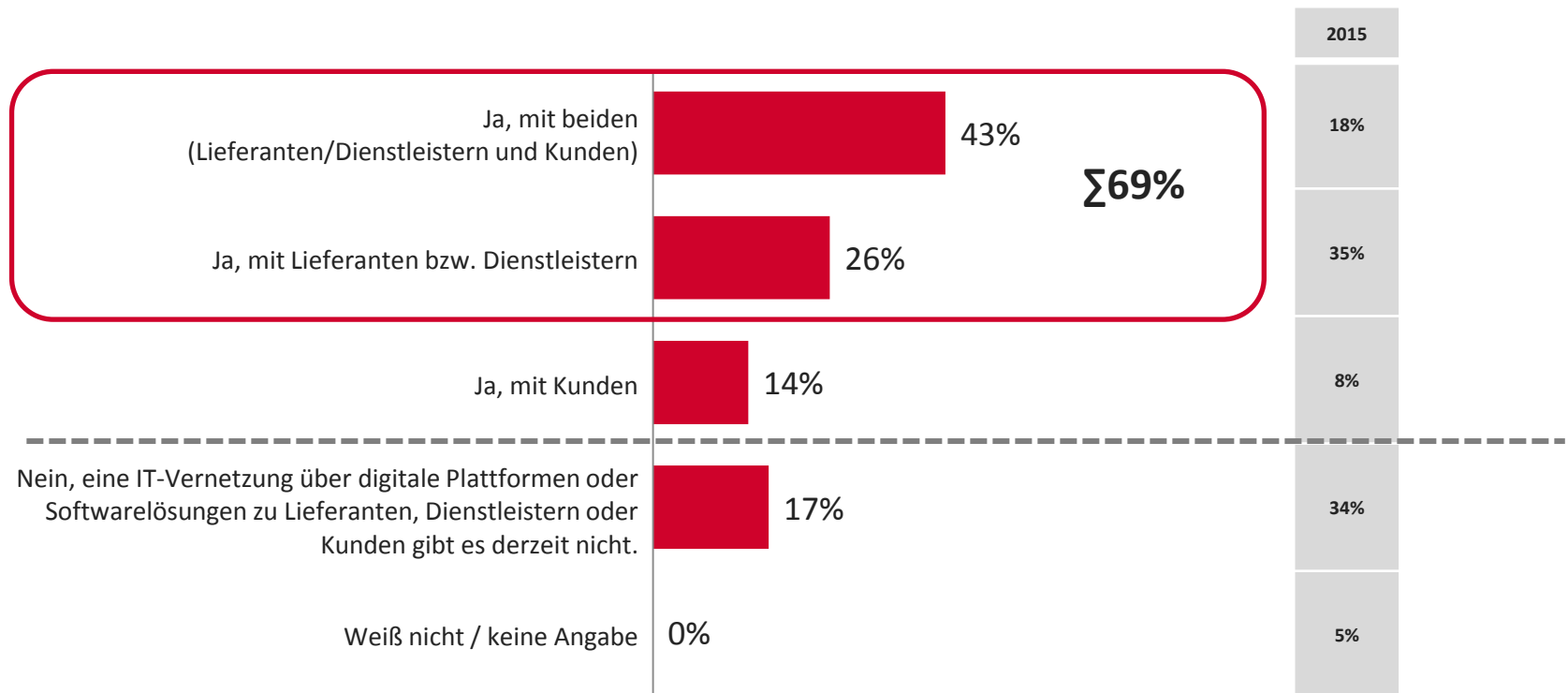

Geringe Fallzahl



ERGEBNISSE

CUSTOMER & PARTNER ENGAGEMENT

- Knapp 70 Prozent der Unternehmen sind mit Lieferanten bzw. Dienstleistern über digitale Plattformen oder Software vernetzt.



Frage 11: Kommen wir zum Thema Vernetzung von Unternehmen mit Lieferanten, Dienstleistern und Kunden über digitale Plattformen oder Softwarelösungen. Ist Ihr Unternehmen mit Lieferanten, Dienstleistern oder Kunden elektronisch vernetzt? Hinweis: Eine Kommunikation via E-Mail oder Fax ist hier nicht als Vernetzung zu verstehen.
Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)



ERGEBNISSE

CUSTOMER & PARTNER ENGAGEMENT

- Acht von zehn der befragten Finanzdienstleister setzen bereits eine IT-Vernetzung über digitale Plattformen oder Softwarelösungen ein.

IT-Vernetzung	Total	Branche					
		Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	205	75	62	23	19	13	13
Ja, mit beiden	43%	40%	47%	30%	48%	46%	46%
Ja, mit Lieferanten und / oder Dienstleistern	26%	28%	29%	30%	26%	16%	8%
Ja, mit Kunden	14%	12%	6%	18%	21%	23%	38%
Nein, eine IT-Vernetzung über digitale Plattformen oder Softwarelösungen zu Lieferanten, Dienstleistern oder Kunden gibt es derzeit nicht.	17%	20%	18%	22%	5%	15%	8%

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 11: Kommen wir zum Thema Vernetzung von Unternehmen mit Lieferanten, Dienstleistern und Kunden über digitale Plattformen oder Softwarelösungen. Ist Ihr Unternehmen mit Lieferanten, Dienstleistern oder Kunden elektronisch vernetzt? Hinweis: Eine Kommunikation via E-Mail oder Fax ist hier nicht als Vernetzung zu verstehen.
Basis: Alle Befragten, N = 205 (Einfachnennung)



Geringe Fallzahl



ERGEBNISSE

CUSTOMER & PARTNER ENGAGEMENT

- Unternehmen mit 500 bis unter 1.000 Mitarbeitern sind seltener mit Kunden, Dienstleistern und Lieferanten digital vernetzt.

IT-Vernetzung	Unternehmensgröße			
	Total	500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	205	71	95	39
Ja, mit beiden	43%	32%	50%	41%
Ja, mit Lieferanten und / oder Dienstleistern	26%	35%	15%	38%
Ja, mit Kunden	14%	6%	21%	13%
Nein, eine IT-Vernetzung über digitale Plattformen oder Softwarelösungen zu Lieferanten, Dienstleistern oder Kunden gibt es derzeit nicht.	17%	27%	14%	8%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 11: Kommen wir zum Thema Vernetzung von Unternehmen mit Lieferanten, Dienstleistern und Kunden über digitale Plattformen oder Softwarelösungen. Ist Ihr Unternehmen mit Lieferanten, Dienstleistern oder Kunden elektronisch vernetzt? Hinweis: Eine Kommunikation via E-Mail oder Fax ist hier nicht als Vernetzung zu verstehen.

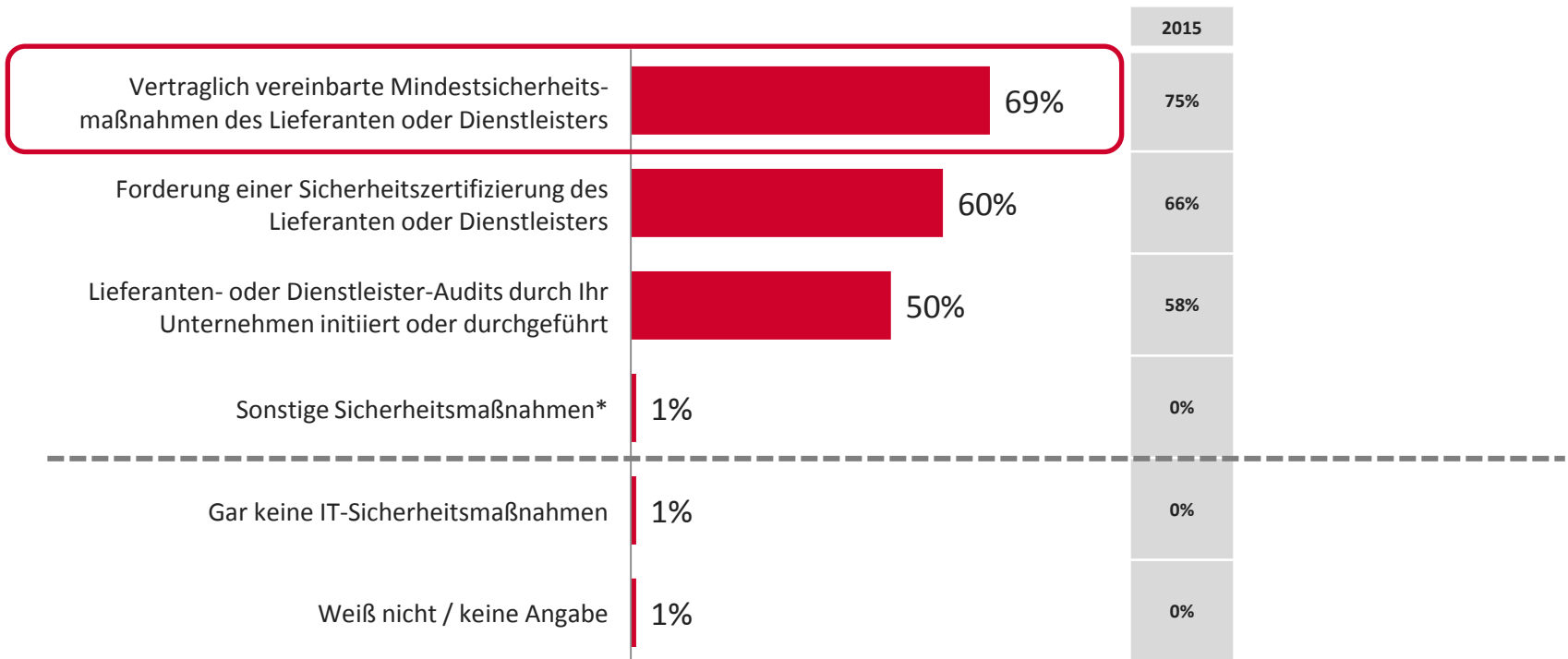
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

CUSTOMER & PARTNER ENGAGEMENT

- IT-Vernetzung: Knapp 70 Prozent der Unternehmen haben Verträge zu Mindestsicherheitsmaßnahmen mit Lieferanten oder Dienstleistern.



Frage 12: Welche IT-Sicherheitsmaßnahmen verfolgt Ihr Unternehmen im Rahmen der IT-Vernetzung zu Lieferanten, Dienstleistern?

Basis: Alle Befragten, die mit Dienstleistern/Lieferanten über digitale Plattformen oder Softwarelösungen elektronisch vernetzt sind, N = 141 (2015: N = 59) (Mehrfachnennungen)

*Hinweise auf Sicherheitslücken



ERGEBNISSE

CUSTOMER & PARTNER ENGAGEMENT

- Lieferantenaudits: Bei jedem zweiten Finanzdienstleister und Unternehmen des verarbeitenden Gewerbes eine Sicherheitsmaßnahme.

IT-Vernetzung: IT-Sicherheitsmaßnahmen	Total	Branche					
		Finanzdienstleistungen	Sonstiges Verarbeitendes Gewerbe	Öffentliche Verwaltung	Automotive	Energie- und Wasserversorgung	Telekommunikation/Medien
Basis	141	51	47	14	14	8	7
Vertraglich vereinbarte Mindestsicherheitsmaßnahmen des Lieferanten oder Dienstleisters	69%	57%	74%	86%	79%	75%	57%
Forderung einer Sicherheitszertifizierung des Lieferanten oder Dienstleisters	60%	51%	60%	57%	79%	63%	86%
Lieferanten- oder Dienstleister-Audits durch Ihr Unternehmen initiiert oder durchgeführt	50%	55%	55%	21%	71%	50%	0%
Sonstige Sicherheitsmaßnahmen	1%	0%	0%	0%	0%	0%	14%
Gar keine IT-Sicherheitsmaßnahmen	1%	0%	2%	0%	0%	0%	0%
Weiß nicht / keine Angabe	1%	0%	2%	0%	0%	0%	0%

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 12: Welche IT-Sicherheitsmaßnahmen verfolgt Ihr Unternehmen im Rahmen der IT-Vernetzung zu Lieferanten, Dienstleistern?

Basis: Alle Befragten, die mit Dienstleistern/Lieferanten über digitale Plattformen oder Softwarelösungen elektronisch vernetzt sind, N = 141 (Mehrfachnennungen)



ERGEBNISSE

CUSTOMER & PARTNER ENGAGEMENT

- Vernetzung mit Zulieferern: In größeren Unternehmen werden häufiger Verträge zu Mindestsicherheitsmaßnahmen abgeschlossen.

IT-Vernetzung: IT-Sicherheitsmaßnahmen	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	141	48	62	31
Vertraglich vereinbarte Mindestsicherheitsmaßnahmen des Lieferanten oder Dienstleisters	69%	54%	77%	74%
Forderung einer Sicherheitszertifizierung des Lieferanten oder Dienstleisters	60%	52%	65%	61%
Lieferanten oder Dienstleister-Audits durch Ihr Unternehmen initiiert oder durchgeführt	50%	52%	58%	32%
Sonstige Sicherheitsmaßnahmen	1%	2%	0%	0%
Gar keine IT-Sicherheitsmaßnahmen	1%	2%	0%	0%
Weiß nicht / keine Angabe	1%	0%	0%	3%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 12: Welche IT-Sicherheitsmaßnahmen verfolgt Ihr Unternehmen im Rahmen der IT-Vernetzung zu Lieferanten, Dienstleistern?

Basis: Alle Befragten, die mit Dienstleistern/Lieferanten über digitale Plattformen oder Softwarelösungen elektronisch vernetzt sind, N = 141 (Mehrfachnennungen)

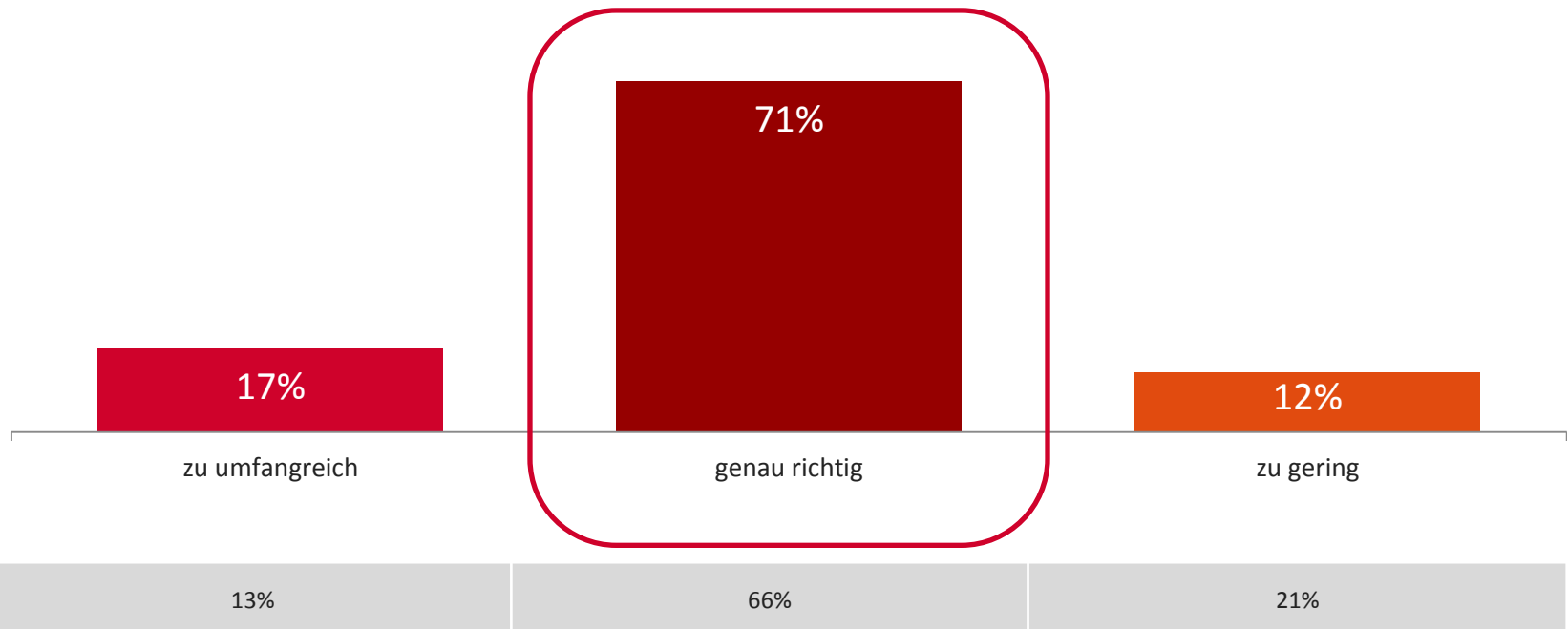


ERGEBNISSE

DIGITAL COMPLIANCE

- IT-Sicherheitsgesetz: Rund 70 Prozent der IT-Entscheider beurteilen den Umfang der staatlichen Regulierung als angemessen.

Die staatliche Regulierung im Hinblick auf die IT-Sicherheit ist...



Frage 13: Das IT-Sicherheitsgesetz wurde am 12. Juli 2015 vom deutschen Bundestag verabschiedet. Es fordert von Betreibern besonders gefährdeter und kritischer Infrastrukturen ein Mindestsicherheitsniveau sowie die Meldung von Sicherheitsvorfällen. Finden Sie die staatliche Regulierung im Hinblick auf IT-Sicherheit....
Basis: Alle Befragten, N = 205 (2015: N = 110) (Einfachnennung)



ERGEBNISSE

DIGITAL COMPLIANCE

- IT-Sicherheitsgesetz: Knapp ein Fünftel der IT-Entscheider der dritten Führungsebene bewertet die staatliche Regulierung als zu gering.

Die staatliche Regulierung im Hinblick auf die IT-Sicherheit ist....	Total	Position		
		Leitender Angestellter erste Führungsebene	Leitender Angestellter zweite Führungsebene	Mittleres Management/Führungskraft Fachabteilung/Spezialist
Basis	205	96	53	56
zu umfangreich	17%	24%	10%	12%
genau richtig	71%	66%	81%	70%
zu gering	12%	10%	9%	18%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 13: Das IT-Sicherheitsgesetz wurde am 12. Juli 2015 vom deutschen Bundestag verabschiedet. Es fordert von Betreibern besonders gefährdeter und kritischer Infrastrukturen ein Mindestsicherheitsniveau sowie die Meldung von Sicherheitsvorfällen. Finden Sie die staatliche Regulierung im Hinblick auf IT-Sicherheit...

Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

DIGITAL COMPLIANCE

- Vor allem IT-Entscheider aus kleineren Unternehmen beurteilen die staatliche Regulierung für die IT-Sicherheit als zu umfangreich.

Die staatliche Regulierung im Hinblick auf die IT-Sicherheit ist....	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	205	71	95	39
zu umfangreich	17%	28%	10%	13%
genau richtig	71%	63%	73%	79%
zu gering	12%	9%	17%	8%

■ 5 Prozentpunkte und mehr unter Gesamtdurchschnitt

■ 5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 13: Das IT-Sicherheitsgesetz wurde am 12. Juli 2015 vom deutschen Bundestag verabschiedet. Es fordert von Betreibern besonders gefährdeter und kritischer Infrastrukturen ein Mindestsicherheitsniveau sowie die Meldung von Sicherheitsvorfällen. Finden Sie die staatliche Regulierung im Hinblick auf IT-Sicherheit...

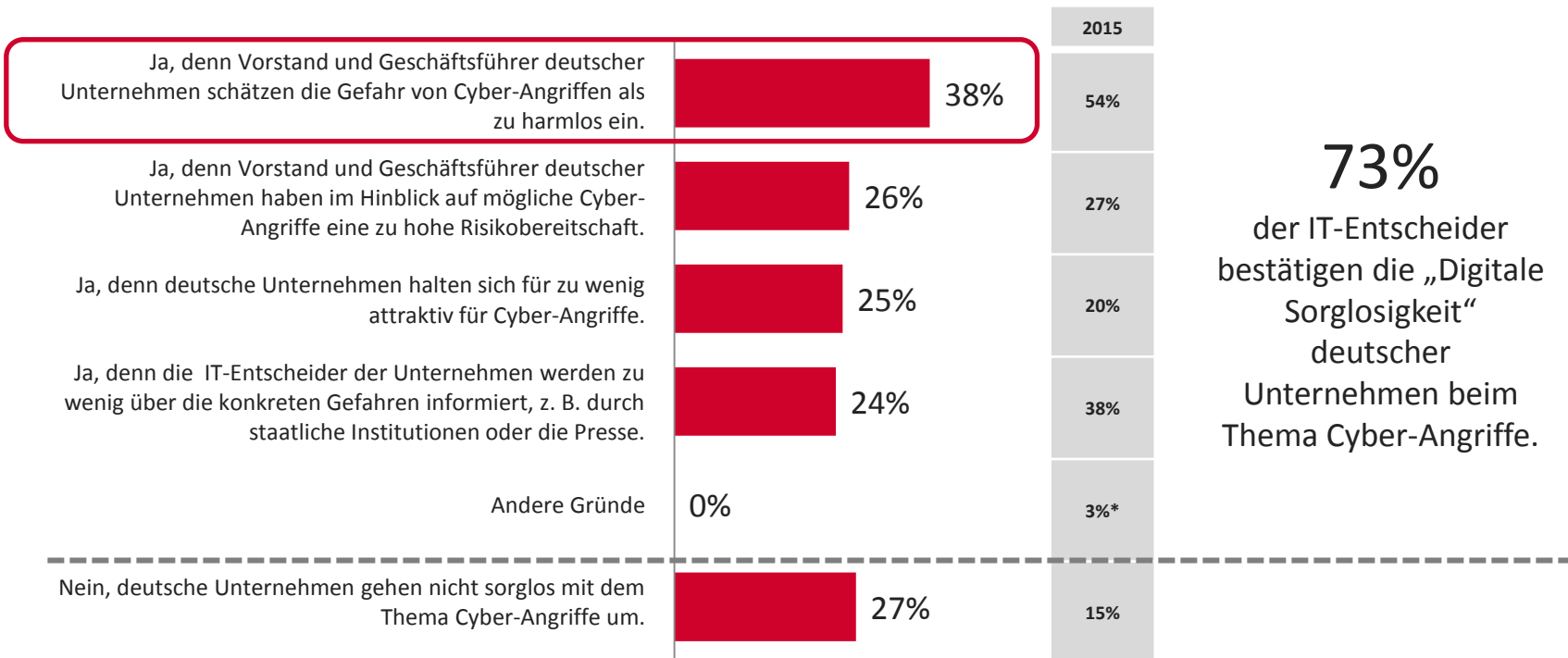
Basis: Alle Befragten, N = 205 (Einfachnennung)



ERGEBNISSE

DIGITAL LEADERSHIP

- Digitale Sorglosigkeit: Unternehmensleiter verharmlosen aus Sicht von knapp 40 Prozent der IT-Entscheider die Gefahr von Cyber-Angriffen.



Frage 14: Die Statistiken und nahezu täglichen Pressemeldungen über Cyber-Angriffe rufen die deutsche Unternehmenslandschaft unmissverständlich zum Handeln auf. Demgegenüber wird die mangelnde Initiative vieler Unternehmen beim Schutz gegen Cyber-Angriffe von der Öffentlichkeit als Digitale Sorglosigkeit bewertet. Sind Ihrer Meinung nach Unternehmen in Deutschland zu sorglos im Umgang mit dem Thema Gefahr durch Cyber-Angriffe, und wenn ja, aus welchen Gründen? Basis: Alle Befragten, N = 205 (Mehrfachnennungen)

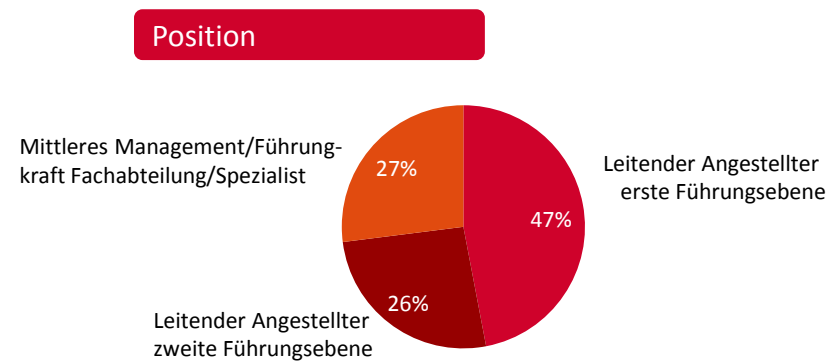
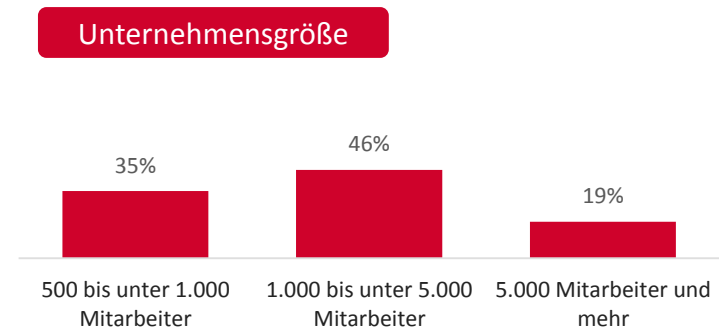
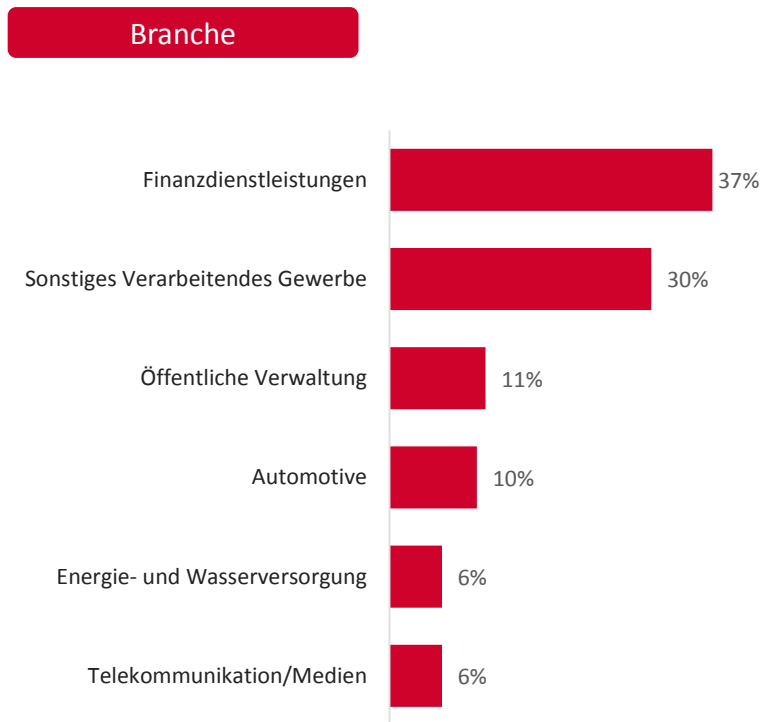
* Thema wird in den meisten Unternehmen sträflich vernachlässigt/Lücken sind bekannt, aber die IT-Entscheider werden ignoriert/Betrifft immer nur die anderen.



STATISTIK

POTENZIALANALYSE DIGITAL SECURITY

- Statistik



Statistik: Branche / Unternehmensgröße / Position
Basis: alle Befragten, N = 205

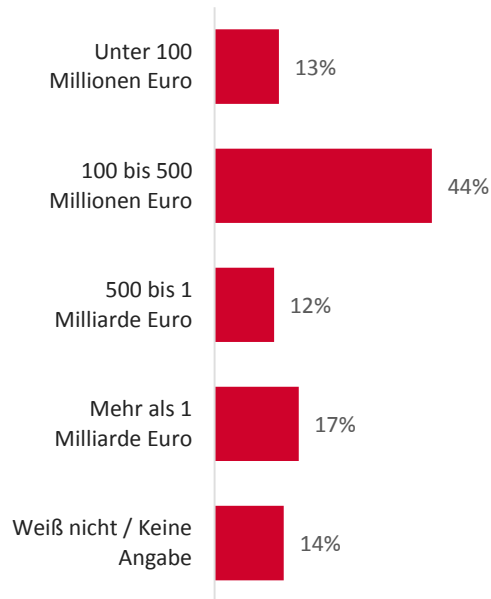


STATISTIK

POTENZIALANALYSE DIGITAL SECURITY

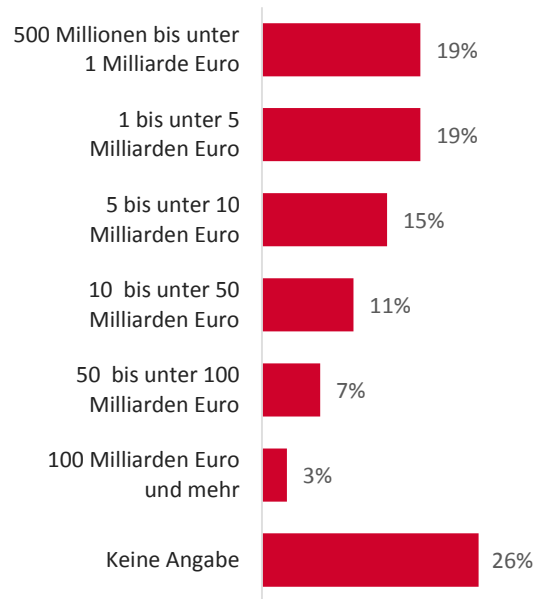
- Statistik

Jahresumsatz



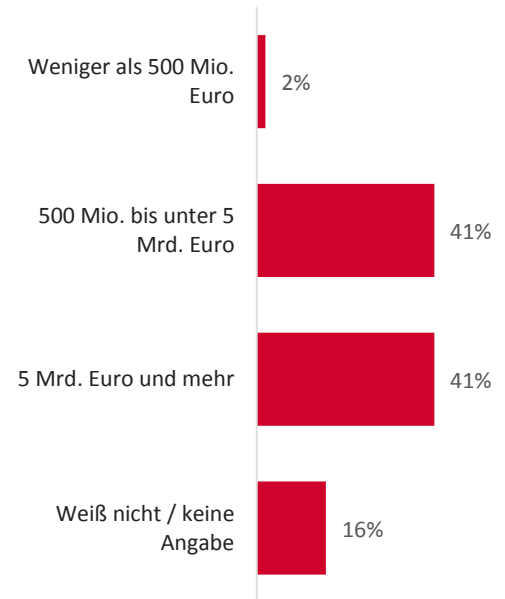
Basis: alle außer Banken und Versicherungen, N = 134

Bilanzsumme



Basis: Banken, N = 27

Bruttobeitragseinnahmen



Basis: Versicherungen, N = 44





sopra  steria
CONSULTING

