POTENZIALANALYSE DIGITAL SECURITY

2015

Delivering Transformation. Together.

sopra steria
CONSULTING

POTENZIALANALYSE DIGITAL SECURITY

Datum: August 2015

Impressum

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

erstellt von / am	geprüft von / am	freigegeben von / am
KS / 16.7.2015	TH / 16.7.2015	JF / tt.mm.jjjj

Sopra Steria GmbH
Hans-Henny-Jahnn-Weg 29, 22085 Hamburg
Telefon: +49 40 22703-0
Fax: +49 40 22703-7999
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

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.
Befra-gungs-zeitraum	Die Daten sind im Juni und Juli 2015 erhoben worden. Die Befragung wurde über ein Online-Panel durchgeführt. Die Ergebnisse sind auf ganze Zahlen gerundet.
Zielgruppe	110 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.

AGENDA

1 | Untersuchungsansatz

2 | Management Summary

3 | Ergebnisse Digital Security

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

Statistik

MANAGEMENT SUMMARY

- Mit der Digitalisierung der Wirtschaft gehen umfangreiche neue Herausforderungen für die digitale Sicherheit der Unternehmen einher. IT-Sicherheitsvorfälle mit millionenfachen Identitätsdiebstählen und die Enthüllungen Edward Snowdens haben gezeigt, dass die Cyber-Angriffe auf IT-Infrastrukturen immer komplexer und professioneller werden. Die Entscheider-Befragung „Digital Security 2015“ orientiert sich an zentralen Disziplinen der digitalen Exzellenz aus der Studie von Sopra Steria Consulting.

- Die Statistiken 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. 85 Prozent der IT-Entscheider schließen sich dieser Meinung an. Vor allem Vorstand und Geschäftsführer verharmlosen aus Sicht von mehr als der Hälfte der IT-Entscheider die Gefahr von Cyber-Angriffen (S. 48).

- Dabei scheinen die Unternehmen mögliche Schwachstellen durchaus zu kennen: Acht von zehn Unternehmen haben nach den Erkenntnissen aus den Snowden-Enthüllungen ihre IT-Sicherheitsmaßnahmen angepasst. In 43 Prozent der Unternehmen wurden deswegen umfangreiche IT-Sicherheitsmaßnahmen initiiert, 38 Prozent haben zumindest einzelne Maßnahmen auf den Weg gebracht (S. 45). Trotzdem herrscht Unsicherheit unter den IT-Entscheidern: Knapp 40 Prozent fühlen sich zu wenig über die konkreten Gefahren, z. B. durch staatliche Institutionen oder durch die Presse, informiert (S. 48).

- **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. Zwei Drittel der IT-Entscheider beurteilen den Umfang der staatlichen Regulierung im Hinblick auf die IT-Sicherheit als angemessen. Allerdings: Ein Fünftel der IT-Entscheider sieht hier Lücken und bewertet die staatliche Regulierung als zu gering (S. 42).

MANAGEMENT SUMMARY

- **Digital Platform Management:** Ein wichtiger Bestandteil der Digitalen Exzellenz ist die Nutzung von Social Media und die Präsenz auf Plattformen zur Kommunikation und Interaktion mit Kunden. 80 Prozent der befragten Unternehmen nutzen bereits Social Media. 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 rund 70 Prozent der Entscheider Schulungen und Awareness-Kampagnen sowie technische Data Leakage Prevention Maßnahmen ein (S. 33).

- **Customer & Partner Engagement**: Eine weitere externe Anbindung nutzen bereits sechs von zehn der befragten Unternehmen. Sie sind über digitale Plattformen oder Softwarelösungen mit Lieferanten bzw. Dienstleistern oder Kunden vernetzt. Mehr als die Hälfte ist so mit seinen Dienstleistern oder Lieferanten verbunden (S. 36). 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 (75%, S. 39).

- **Digital Empowerment:** Auch 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 verbunden möglichen Gefahren sind den Unternehmen bewusst: 90 Prozent führen IT-Sicherheitsmaßnahmen für mobile Endgeräte durch. Vor allem regelmäßige Sicherheitsüberprüfungen (66%), eine Mobile Security Policy (65%) oder Mobile Device Management (60%) werden zum Schutz eingesetzt (S. 29).

- 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. Neun von zehn Unternehmen führen Maßnahmen zur Security Awareness durch. Knapp 70 Prozent führen regelmäßige Maßnahmen durch, ein Fünftel bietet sporadisch Maßnahmen an. Sie sind dabei in mehr als der Hälfte der Unternehmen auf die unterschiedlichen Rollen oder Aufgaben der Mitarbeiter zugeschnitten (S. 23).

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. Etwa ein Drittel der IT-Entscheider spricht sich dafür aus, dass die Zweckbindung von personengebundenen Daten gelockert werden sollte. 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 Datenschutzanforderungen zu erfüllen. Knapp die Hälfte der IT-Experten, spricht sich allerdings gegen so eine Lockerung aus. Dass dann die eine oder andere Auswertung nicht gemacht werden kann, nehmen sie dafür in Kauf (S. 17).

- **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. Überraschende 65 Prozent der befragten Unternehmen folgen einer solchen IT-Sicherheitsstrategie (S. 14).

- **Process Digitisation and Automation:** In Bezug auf die Einführung einer neuen Technologie vertreten knapp zwei Drittel der IT-Entscheider die Meinung, dass vorab alle IT-Risiken geklärt sein müssen. Rund ein Drittel der IT-Entscheider gibt neuen Technologien hingegen auch eine Chance, wenn noch nicht alle IT-Risiken bekannt sind (S. 10). Auch beim Vorantreiben der Digitalisierung und Automation von Prozessen gehen die Unternehmen eher auf Nummer sicher: In vier von zehn Unternehmen dürfen IT-Projekte erst starten, wenn ein Sicherheitskonzept der IT vorliegt, in 37 Prozent muss vor Produktivnahme einer Anwendung oder eines IT-Systems ein Sicherheitskonzept vorliegen. Nur in 10 Prozent der Unternehmen ist ein IT-Sicherheitskonzept nicht zwingend vorgeschrieben (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. Mehr als die Hälfte der Unternehmen will in den nächsten zwölf Monaten in erster Linie eigene IT-Mitarbeiter für die speziellen Aufgaben der IT-Sicherheit ausbilden (S. 20).

AGENDA

1 | Untersuchungsansatz

2 | Management Summary

3 | Ergebnisse Digital Security

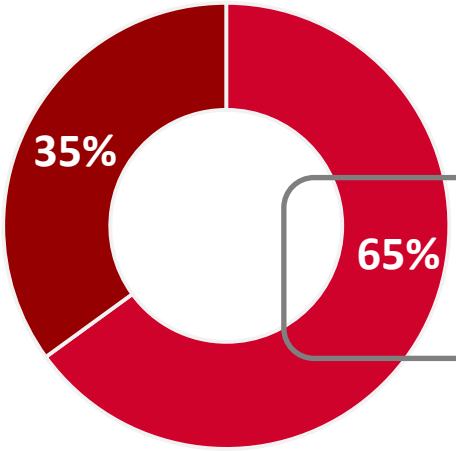
- Process Digitisation and Automation
- IT Architecture Transformation
- Data-driven Agility
- Business Modell Innovation
- Digital Empowerment
- Digital Platform Management
- Customer and Partner Engagement
- Digital Compliance
- Digital Leadership

Statistik

ERGEBNISSE
PROCESS DIGITISATION AND AUTOMATION

- Einführung einer neuen Technologie: Für 65 Prozent der IT-Entscheider nur, wenn die IT-Risiken vorab geklärt sind.

Neue Technologien müssen genutzt werden, auch wenn noch nicht alle IT-Risiken klar sind.



Wenn ich mir über die IT-Risiken einer Technologie nicht hinreichend im Klaren bin, führe ich diese nicht ein.

Einführung einer neuen Technologie	Total	Position		
		Leitender Angestellter erste Führungsebene	Leitender Angestellter zweite Führungsebene	Mittleres Management/Führungskraft Fachabteilung/Spezialist
Basis	110	66	29	15
Wenn ich mir über die IT-Risiken einer Technologie nicht hinreichend im Klaren bin, führe ich diese nicht ein.	**65%**	**73%**	**52%**	**60%**
Neue Technologien müssen genutzt werden, auch wenn noch nicht alle IT-Risiken klar sind.	**35%**	**27%**	**48%**	**40%**

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. SmartHome, car2car Kommunikation). Nicht immer sind bei Einführung einer Technologie alle Fragestellungen der IT-Sicherheit geklärt. Welchen Standpunkt vertreten Sie?
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
PROCESS DIGITISATION AND AUTOMATION

- Vor allem IT-Entscheider aus der Finanzdienstleistungsbranche führen neue Technologien nur ein, wenn die Risiken bekannt sind.

Einführung einer neuen Technologie	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasser-versorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
Wenn ich mir über die IT-Risiken einer Technologie nicht hinreichend im Klaren bin, führe ich diese nicht ein.	**65%**	**76%**	**53%**	**38%**	**86%**	**67%**	**33%**
Neue Technologien müssen genutzt werden, auch wenn noch nicht alle IT-Risiken klar sind.	**35%**	**24%**	**47%**	**63%**	**14%**	**33%**	**67%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

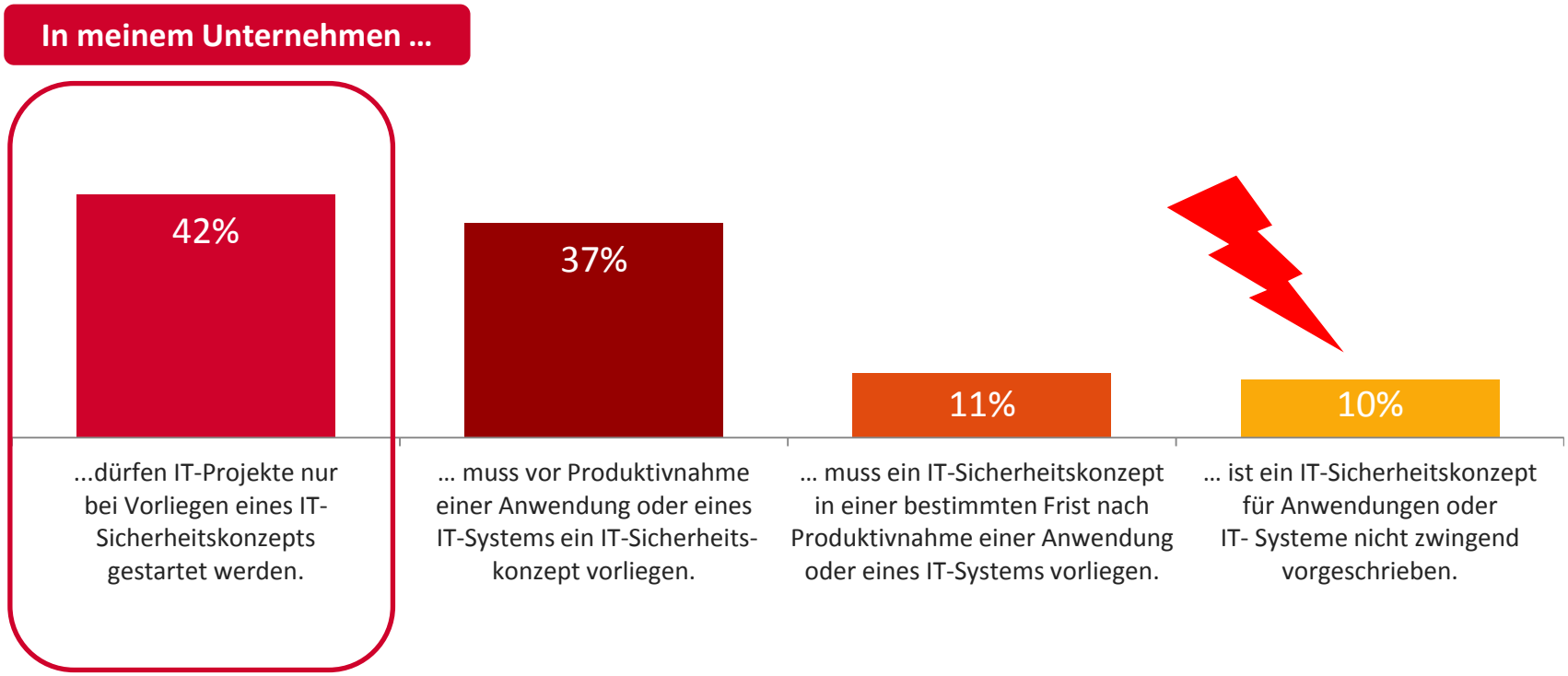
5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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. SmartHome, car2car Kommunikation). Nicht immer sind bei Einführung einer Technologie alle Fragestellungen der IT-Sicherheit geklärt. Welchen Standpunkt vertreten Sie?
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
PROCESS DIGITISATION AND AUTOMATION

- Überraschend: In vier von zehn Unternehmen dürfen IT-Projekte erst starten, wenn ein IT-Sicherheitskonzept vorliegt.



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 = 110 (Einfachnennung)

ERGEBNISSE
PROCESS DIGITISATION AND AUTOMATION

- Vor allem Finanzdienstleister sichern ihre IT-Projekte vorab durch ein IT-Sicherheitskonzept ab.

In meinem Unternehmen…	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasserversorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
…dürfen IT-Projekte nur bei Vorliegen eines IT-Sicherheitskonzepts gestartet werden.	**42%**	**57%**	**31%**	**13%**	**57%**	**0%**	**0%**
… muss vor Produktivnahme einer Anwendung oder eines IT-Systems ein IT-Sicherheitskonzept vorliegen.	**37%**	**30%**	**47%**	**50%**	**29%**	**33%**	**67%**
…muss ein IT-Sicherheitskonzept in einer bestimmten Frist nach Produktivnahme einer Anwendung oder eines IT-Systems vorliegen.	**11%**	**11%**	**13%**	**25%**	**0%**	**0%**	**0%**
… ist ein IT-Sicherheitskonzept für Anwendungen oder IT-Systeme nicht zwingend vorgeschrieben.	**10%**	**2%**	**9%**	**13%**	**14%**	**67%**	**33%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

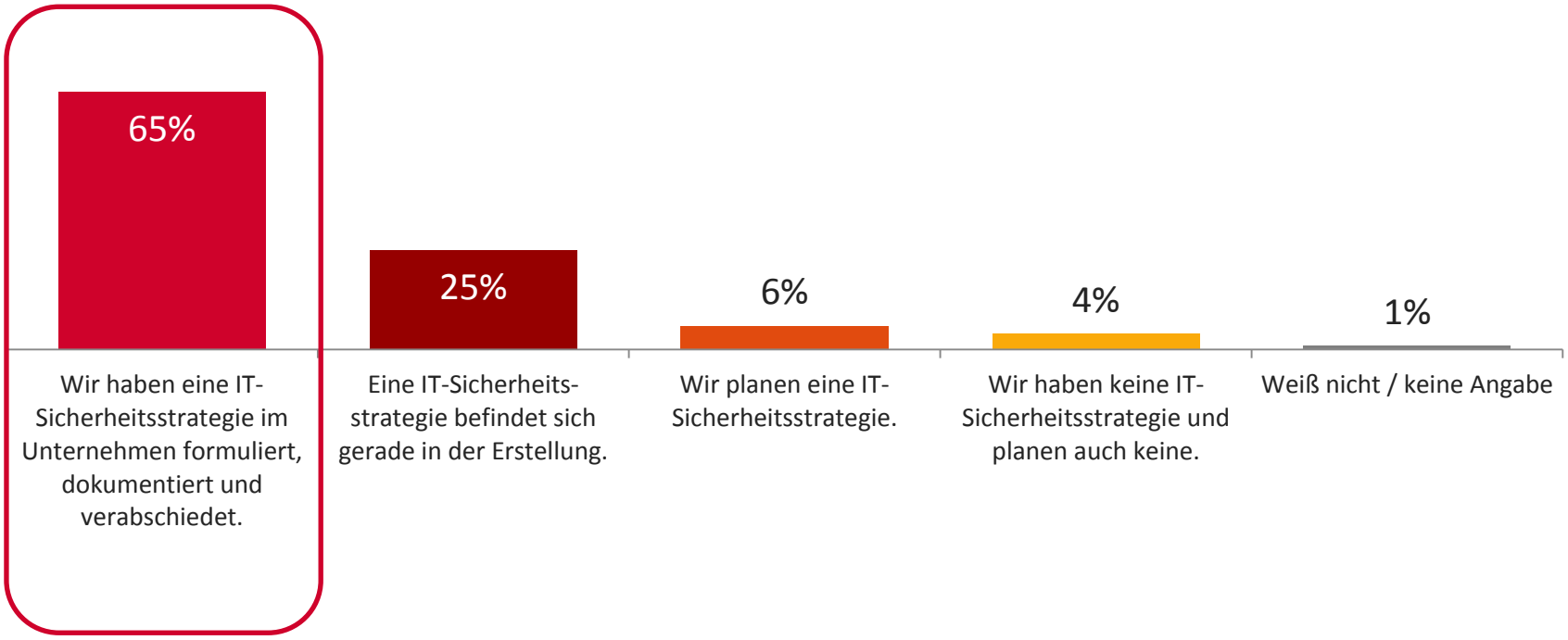
5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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 = 110 (Einfachnennung)

ERGEBNISSE
IT ARCHITECTURE TRANSFORMATION

- Überraschend: Knapp zwei Drittel der Unternehmen folgen einer IT-Sicherheitsstrategie.



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 = 110 (Einfachnennung)

ERGEBNISSE
IT ARCHITECTURE TRANSFORMATION

- Finanzdienstleister sind in puncto IT-Sicherheitsstrategie am besten aufgestellt.

IT-Sicherheitsstrategie	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasser-versorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
Wir haben eine IT-Sicherheitsstrategie im Unternehmen formuliert, dokumentiert und verabschiedet.	**65%**	**74%**	**63%**	**25%**	**57%**	**50%**	**67%**
Eine IT-Sicherheitsstrategie befindet sich gerade in der Erstellung.	**25%**	**26%**	**19%**	**63%**	**14%**	**17%**	**0%**
Wir planen eine IT-Sicherheitsstrategie.	**6%**	**0%**	**9%**	**13%**	**0%**	**33%**	**33%**
Wir haben keine IT-Sicherheitsstrategie und planen auch keine.	**4%**	**0%**	**6%**	**0%**	**29%**	**0%**	**0%**
Weiß nicht / keine Angabe	**1%**	**0%**	**3%**	**0%**	**0%**	**0%**	**0%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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 = 110 (Einfachnennung)

ERGEBNISSE
IT ARCHITECTURE TRANSFORMATION

- Je größer das Unternehmen, desto eher existiert dort eine 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	110	41	50	19
Wir haben eine IT-Sicherheitsstrategie im Unternehmen formuliert, dokumentiert und verabschiedet.	**65%**	**59%**	**66%**	**74%**
Eine IT-Sicherheitsstrategie befindet sich gerade in der Erstellung.	**25%**	**22%**	**28%**	**21%**
Wir planen eine IT-Sicherheitsstrategie.	**6%**	**10%**	**4%**	**5%**
Wir haben keine IT-Sicherheitsstrategie und planen auch keine.	**4%**	**7%**	**2%**	**0%**
Weiß nicht / keine Angabe	**1%**	**2%**	**0%**	**0%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

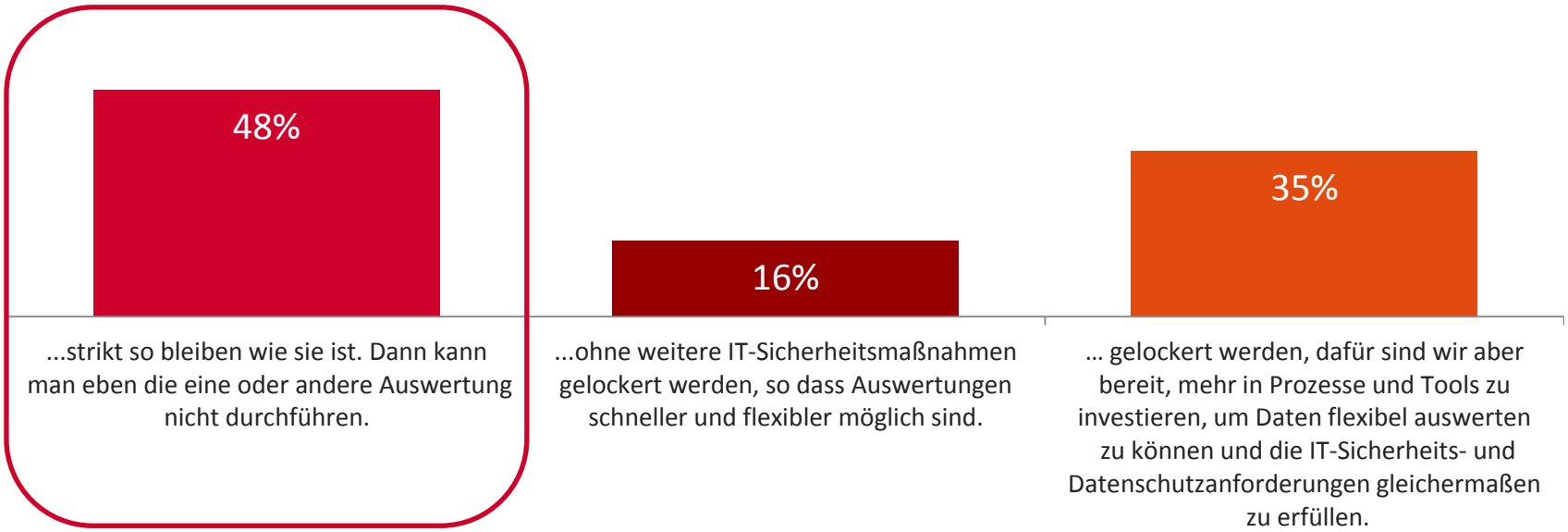
5 Prozentpunkte und mehr über Gesamtdurchschnitt

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 = 110 (Einfachnennung)

ERGEBNISSE
DATA-DRIVEN AGILITY

- Knapp 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 = 110 (Einfachnennung)

ERGEBNISSE
DATA-DRIVEN AGILITY

- Für eine Lockerung der Zweckbindung von personengebundenen Daten sprechen sich vor allem IT-Entscheider aus dem Verarbeitenden Gewerbe aus.

Die Zweckbindung von personengebundenen Daten sollte…	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasserversorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
…strikt so bleiben wie sie ist. Dann kann man eben die eine oder andere Auswertung nicht durchführen.	**48%**	**63%**	**34%**	**38%**	**43%**	**33%**	**0%**
…ohne weitere IT-Sicherheitsmaßnahmen gelockert werden, so dass Auswertungen schneller und flexibler möglich sind.	**16%**	**9%**	**19%**	**38%**	**0%**	**33%**	**67%**
… 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 Datenschutzanforderungen gleichermaßen zu erfüllen.	**35%**	**28%**	**47%**	**25%**	**57%**	**33%**	**33%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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 = 110 (Einfachnennung)

ERGEBNISSE
DATA-DRIVEN AGILITY

- IT-Entscheider der ersten Führungsebene 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	110	66	29	15
...strikt so bleiben wie sie ist. Dann kann man eben die eine oder andere Auswertung nicht durchführen.	**48%**	**61%**	**24%**	**40%**
...ohne weitere IT-Sicherheitsmaßnahmen gelockert werden, so dass Auswertungen schneller und flexibler möglich sind.	**16%**	**12%**	**21%**	**27%**
… 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 Datenschutzan-forderungen gleichermaßen zu erfüllen.	**35%**	**27%**	**55%**	**33%**

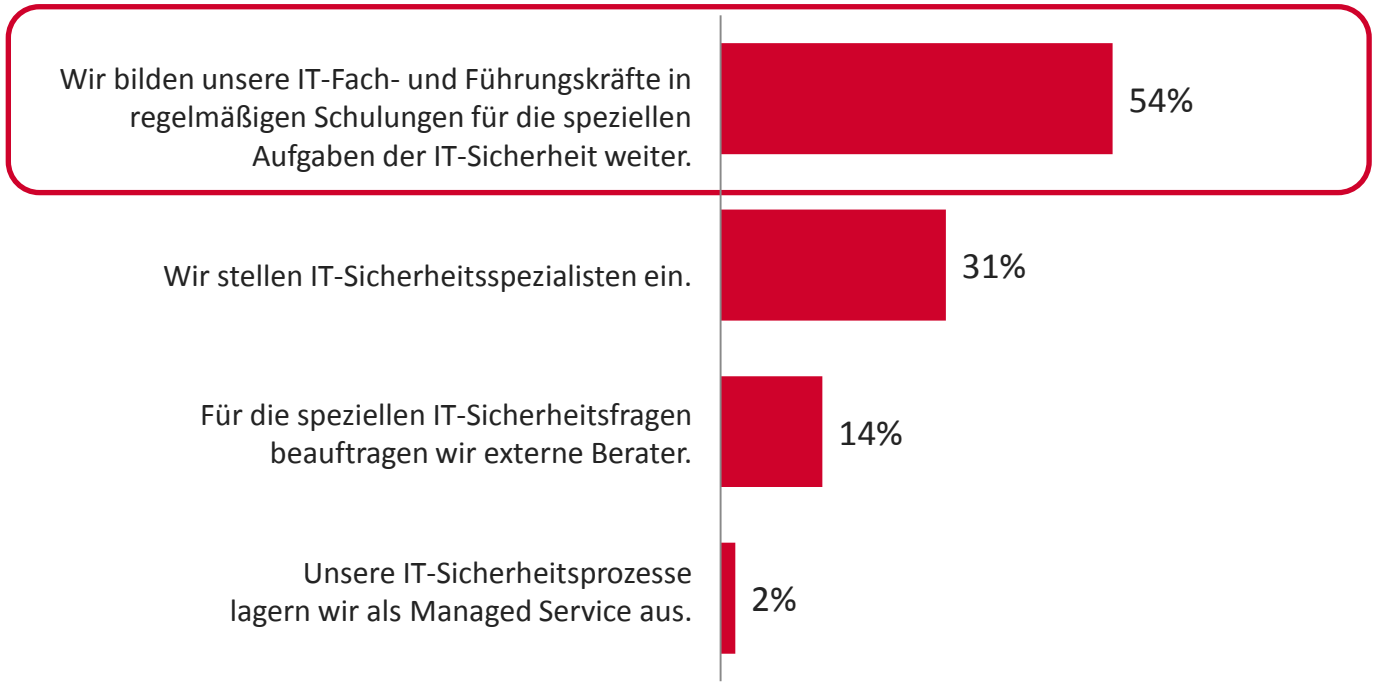
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

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 = 110 (Einfachnennung)

ERGEBNISSE
BUSINESS MODEL INNOVATION

- Personalstrategie: Mehr als die Hälfte 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 = 110 (Einfachnennung)

ERGEBNISSE
BUSINESS MODEL INNOVATION

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

Personalstrategie für die nächsten 12 Monate	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasser-versorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
Wir bilden unsere IT-Fach- und Führungskräfte in regelmäßigen Schulungen für die speziellen Aufgaben der IT-Sicherheit weiter.	**54%**	**44%**	**69%**	**75%**	**57%**	**17%**	**67%**
Wir stellen IT-Sicherheitsspezialisten ein.	**31%**	**44%**	**22%**	**25%**	**14%**	**0%**	**0%**
Für die speziellen IT-Sicherheitsfragen beauftragen wir externe Berater.	**14%**	**7%**	**9%**	**0%**	**29%**	**83%**	**33%**
Unsere IT-Sicherheitsprozesse lagern wir als Managed Service aus.	**2%**	**4%**	**0%**	**0%**	**0%**	**0%**	**0%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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 = 110 (Einfachnennung)

ERGEBNISSE
BUSINESS MODEL INNOVATION

- IT-Sicherheitsexperten: Ein Fünftel der Unternehmen ab 5.000 Mitarbeiter beauftragt externe Berater für spezielle IT-Sicherheitsfragen.

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	110	41	50	19
Wir bilden unsere IT-Fach- und Führungskräfte in regelmäßigen Schulungen für die speziellen Aufgaben der IT-Sicherheit weiter.	**54%**	**61%**	**48%**	**53%**
Wir stellen IT-Sicherheitsspezialisten ein.	**31%**	**29%**	**36%**	**21%**
Für die speziellen IT-Sicherheitsfragen beauftragen wir externe Berater.	**14%**	**7%**	**16%**	**21%**
Unsere IT-Sicherheitsprozesse lagern wir als Managed Service aus.	**2%**	**2%**	**0%**	**5%**

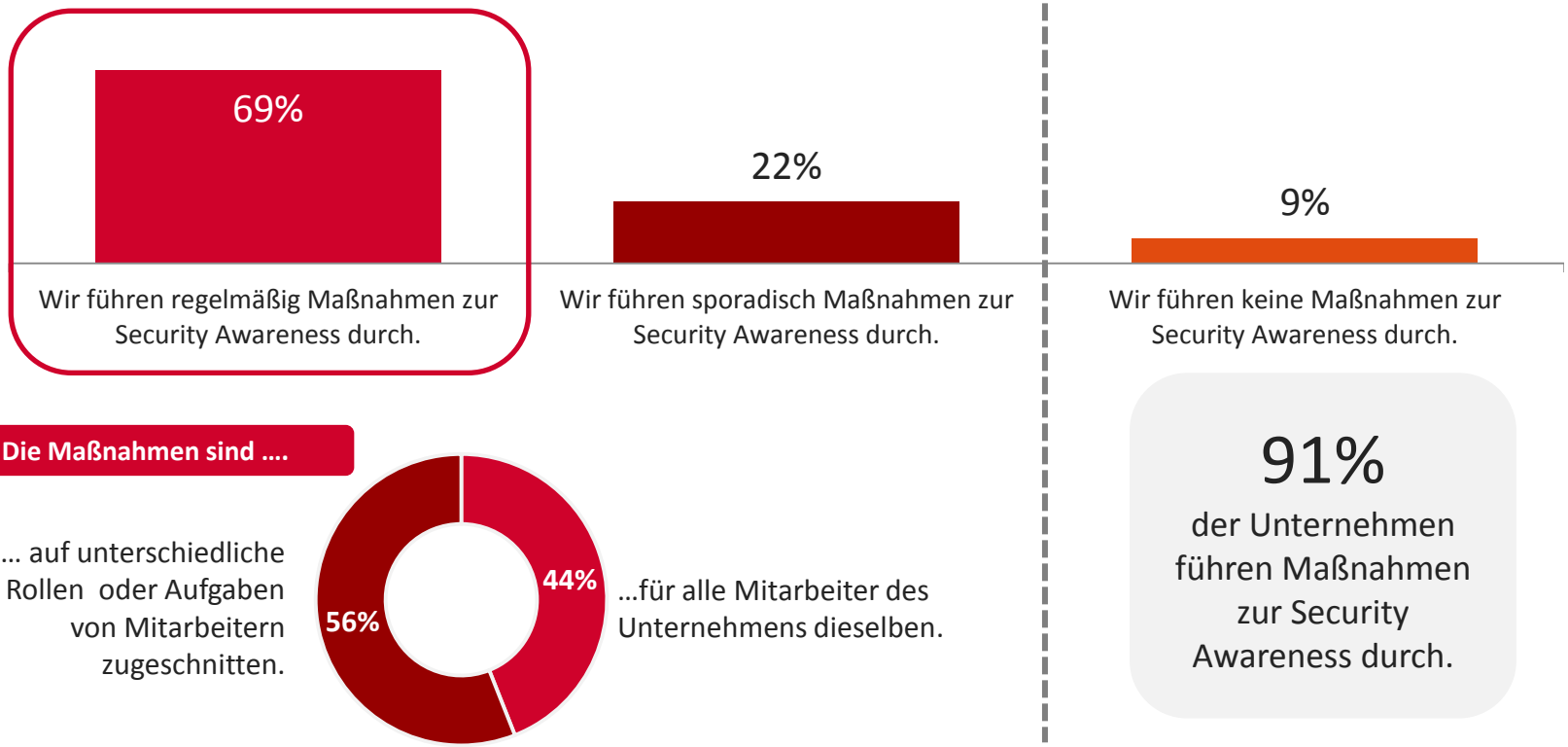
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

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 = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL EMPOWERMENT

- Informationssicherheit: Knapp 70 Prozent der Unternehmen führen regelmäßig Maßnahmen zur Security Awareness 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 = 110 (Einfachnennung) / Frage 7: Welcher Art sind diese Maßnahmen? Die Maßnahmen sind… Basis: Alle Befragten, deren Unternehmen Maßnahmen zur Security Awareness durchführen , N = 100 (Einfachnennung)

ERGEBNISSE
DIGITAL EMPOWERMENT

- 81 Prozent der Finanzdienstleister führen regelmäßig Maßnahmen zur Security Awareness durch.

Maßnahmen	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasser-versorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
Wir führen regelmäßig Maßnahmen zur Security Awareness durch.	**69%**	**81%**	**75%**	**38%**	**71%**	**0%**	**0%**
Wir führen sporadisch Maßnahmen zur Security Awareness durch.	**22%**	**17%**	**16%**	**38%**	**0%**	**83%**	**67%**
Wir führen keine Maßnahmen zur Security Awareness durch.	**9%**	**2%**	**9%**	**25%**	**29%**	**17%**	**33%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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 = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL EMPOWERMENT

- Unternehmen ab 5.000 Mitarbeitern sind bei der Durchführung von Maßnahmen zur Security Awareness am besten aufgestellt.

Maßnahmen		Unternehmensgröße		
	Total	500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	110	41	50	19
Wir führen regelmäßig Maßnahmen zur Security Awareness durch.	**69%**	**76%**	**70%**	**53%**
Wir führen sporadisch Maßnahmen zur Security Awareness durch.	**22%**	**10%**	**22%**	**47%**
Wir führen keine Maßnahmen zur Security Awareness durch.	**9%**	**15%**	**8%**	**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 = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL EMPOWERMENT

- Security Awareness: Unternehmen mit 500 bis unter 1.000 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	100	35	46	19
…für alle Mitarbeiter des Unternehmens dieselben.	**44%**	**34%**	**50%**	**47%**
… auf unterschiedliche Rollen oder Aufgaben von Mitarbeitern zugeschnitten.	**56%**	**66%**	**50%**	**53%**

Die Maßnahmen sind…	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasserversorgung
Basis	100	53	29	6 ⚠	5 ⚠	5 ⚠	2 ⚠
…für alle Mitarbeiter des Unternehmens dieselben.	**44%**	**60%**	**21%**	**0%**	**40%**	**80%**	**0%**
… auf unterschiedliche Rollen oder Aufgaben von Mitarbeitern zugeschnitten.	**56%**	**40%**	**79%**	**100%**	**60%**	**20%**	**100%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

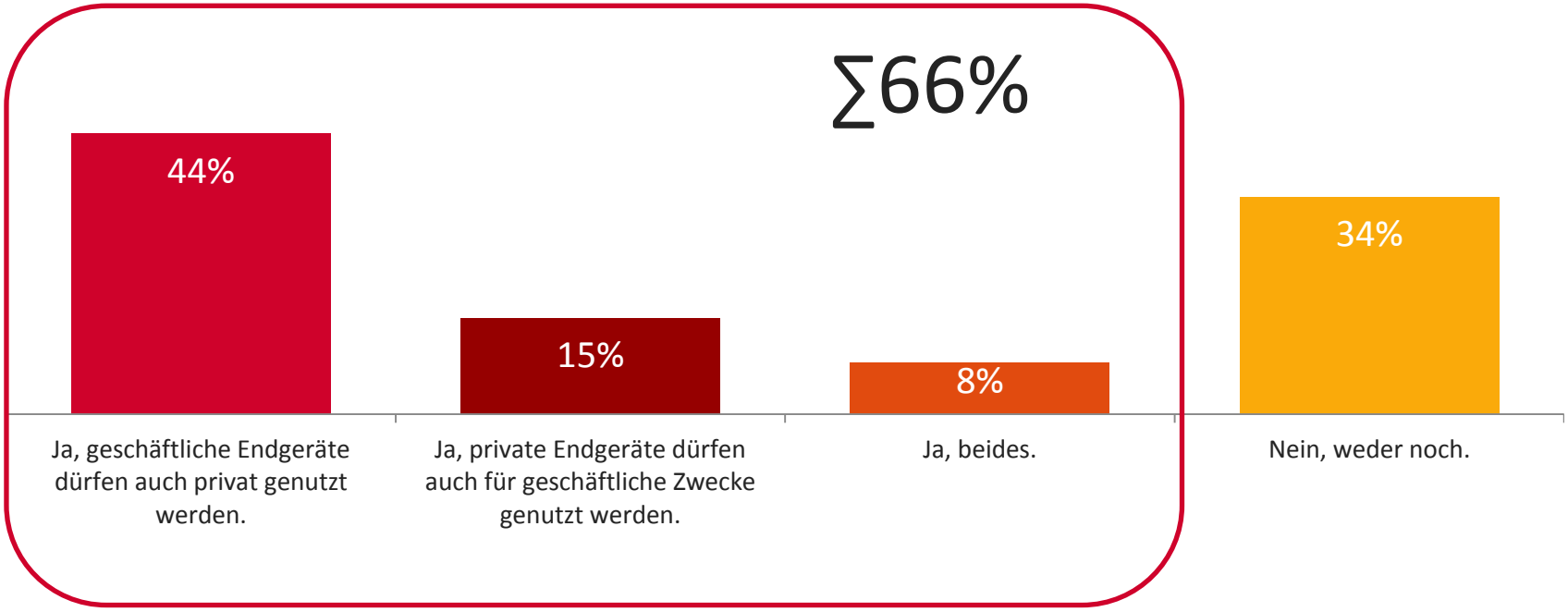
5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

Frage 7: Welcher Art sind diese Maßnahmen? Die Maßnahmen sind…
Basis: Alle Befragten, deren Unternehmen Maßnahmen zur Security Awareness durchführen, N = 100 (Einfachnennung)

ERGEBNISSE
DIGITAL EMPOWERMENT

- Mobile Devices: In zwei Drittel der Unternehmen wird Geschäftliches und Privates auf mobilen Endgeräten vermischt.



Frage 9: Kommen wir zum Thema Mobile Devices. Ist es in Ihrem Unternehmen erlaubt, geschäftliche Endgeräte auch privat zu nutzen oder private Endgeräte auch für geschäftliche Zwecke zu verwenden?
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL EMPOWERMENT

- Mobile Endgeräte: 44 Prozent der Unternehmen mit 500 bis unter 1.000 Mitarbeitern verbieten eine Mischung von Geschäftlichem und Privatem.

Mobile Endgeräte		Unternehmensgröße		
	Total	500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	110	41	50	19
Ja, geschäftliche Endgeräte dürfen auch privat genutzt werden.	**44%**	**32%**	**56%**	**37%**
Ja, private Endgeräte dürfen auch für geschäftliche Zwecke genutzt werden.	**15%**	**12%**	**14%**	**21%**
Ja, beides.	**8%**	**12%**	**4%**	**11%**
Nein, weder noch.	**34%**	**44%**	**26%**	**32%**

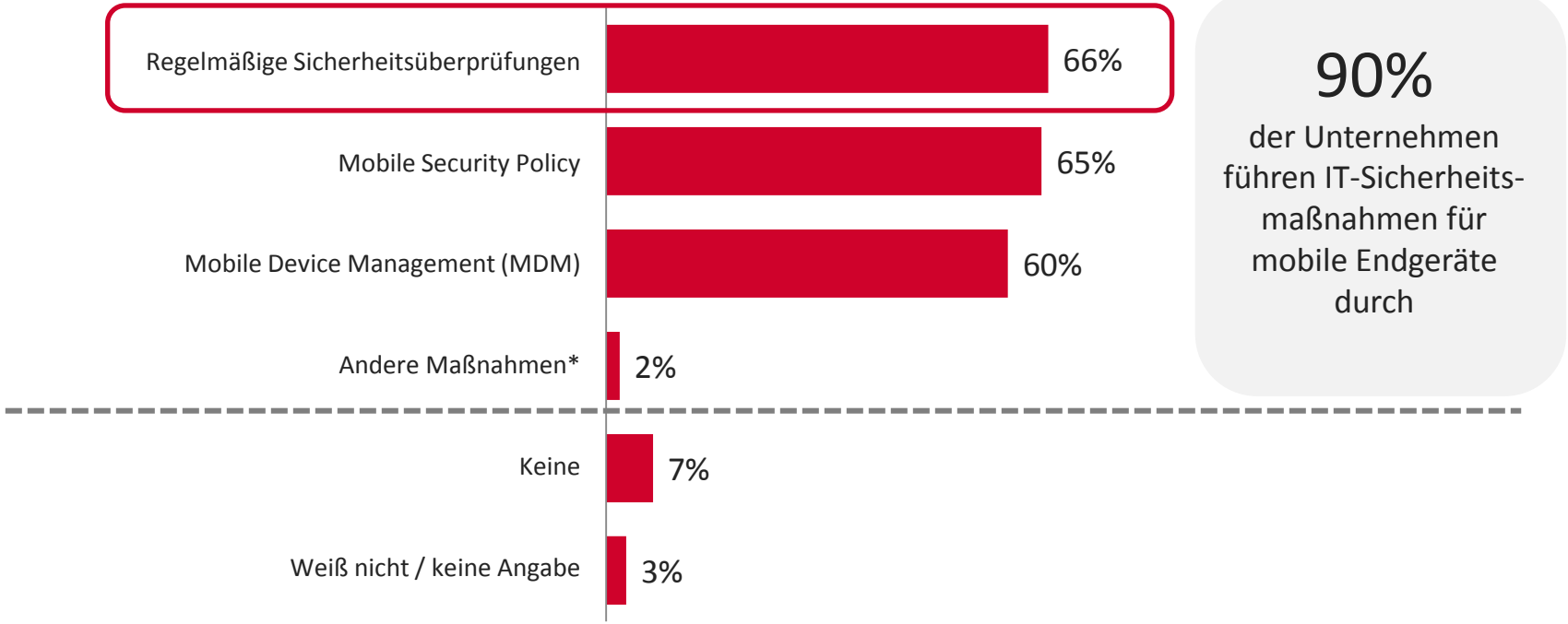
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 9: Kommen wir zum Thema Mobile Devices. Ist es in Ihrem Unternehmen erlaubt, geschäftliche Endgeräte auch privat zu nutzen oder private Endgeräte auch für geschäftliche Zwecke zu verwenden? Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL EMPOWERMENT

- Mobile Endgeräte: Zwei Drittel der Unternehmen führen regelmäßige Sicherheitsüberprüfungen durch.



90%
der Unternehmen führen IT-Sicherheits-maßnahmen für mobile Endgeräte 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 = 110 (Mehrfachnennungen) *Eigenes VPN-System/angepasste Software.

ERGEBNISSE
DIGITAL EMPOWERMENT

- Etwa 70 Prozent der Finanzdienstleister und Unternehmen aus dem Verarbeitenden Gewerbe haben eine Mobile Security Policy.

IT-Sicherheitsmaßnahmen für mobile Geräte	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasserversorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
Regelmäßige Sicherheitsüberprüfungen	**66%**	**69%**	**66%**	**88%**	**43%**	**67%**	**33%**
Mobile Security Policy	**65%**	**70%**	**72%**	**50%**	**86%**	**17%**	**0%**
Mobile Device Management (MDM)	**60%**	**67%**	**63%**	**25%**	**57%**	**33%**	**67%**
Andere Maßnahmen	**2%**	**2%**	**0%**	**13%**	**0%**	**0%**	**0%**
Keine	**7%**	**2%**	**13%**	**0%**	**14%**	**17%**	**33%**
Weiß nicht / keine Angabe	**3%**	**6%**	**0%**	**0%**	**0%**	**0%**	**0%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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 = 110 (Mehrfachnennungen) *Eigenes VPN-System/angepasste Software.

ERGEBNISSE
DIGITAL EMPOWERMENT

- Eine Mobile Security Policy gibt es in drei Viertel der Unternehmen ab 1.000 Mitarbeiter.

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	110	41	50	19
Regelmäßige Sicherheitsüberprüfungen	**66%**	**63%**	**72%**	**58%**
Mobile Security Policy	**65%**	**49%**	**76%**	**74%**
Mobile Device Management (MDM)	**60%**	**61%**	**62%**	**53%**
Andere Maßnahmen	**2%**	**0%**	**0%**	**11%**
Keine	**7%**	**12%**	**6%**	**0%**
Weiß nicht / keine Angabe	**3%**	**7%**	**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 = 110 (Mehrfachnennungen) *Eigenes VPN-System/angepasste Software.

ERGEBNISSE
DIGITAL EMPOWERMENT

- Mobile Endgeräte: In Unternehmen, in denen Geschäftliches und Privates vermischt werden darf, gibt es tendenziell häufiger Sicherheitsmaßnahmen.

IT-Sicherheitsmaßnahmen für mobile Geräte	Total	Nutzung mobiler Endgeräte	
		Private / geschäftliche Endgeräte dürfen geschäftlich und privat genutzt werden	Weder noch
Basis	110	73	37
Regelmäßige Sicherheitsüberprüfungen	**66%**	**68%**	**62%**
Mobile Security Policy	**65%**	**70%**	**57%**
Mobile Device Management (MDM)	**60%**	**66%**	**49%**
Andere Maßnahmen	**2%**	**3%**	**0%**
Keine	**7%**	**5%**	**11%**
Weiß nicht / keine Angabe	**3%**	**0%**	**8%**

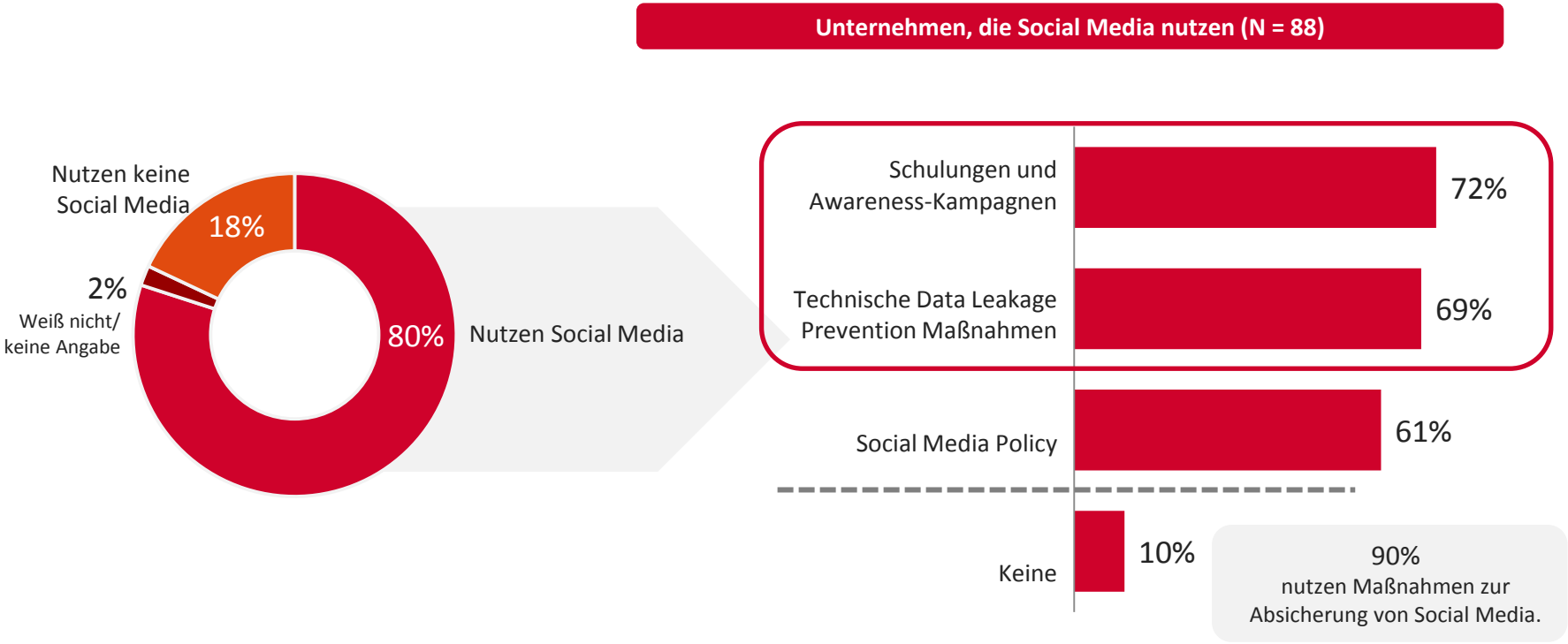
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

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 = 110 (Mehrfachnennungen) *Eigenes VPN-System, angepasste Software

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 und die Präsenz auf Plattformen. 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 = 110 (Berechnung Nutzer/Nicht-Nutzer) Alle Befragten, die Social Media nutzen, N = 88

ERGEBNISSE
DIGITAL PLATFORM MANAGEMENT

- Vor allem Finanzdienstleister setzen Schulungen und Awareness-Kampagnen sowie Technische Data Leakage Prevention Maßnahmen ein.

		Branche					
	Total	Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasserversorgung
Basis	88	44	27	6 ⚠	5 ⚠	5 ⚠	1 ⚠
Schulungen und Awareness-Kampagnen	**72%**	**77%**	**67%**	**50%**	**60%**	**80%**	**100%**
Technische Data Leakage Prevention Maßnahmen	**69%**	**77%**	**70%**	**67%**	**40%**	**40%**	**0%**
Social Media Policy	**61%**	**64%**	**63%**	**67%**	**60%**	**40%**	**0%**
Keine	**10%**	**5%**	**11%**	**33%**	**20%**	**20%**	**0%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

Frage 8: Ein wichtiger Bestandteil der Digitalen Exzellenz ist die Nutzung von Social Media und die Präsenz auf Plattformen. 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, die Social Media nutzen (Mehrfachnennungen)

ERGEBNISSE
DIGITAL PLATFORM MANAGEMENT

- Ungewollter Datenabfluss durch Social Media: Unternehmen ab 5.000 Mitarbeitern setzen tendenziell weniger Maßnahmen ein.

		Unternehmensgröße		
	Total	500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	88	24	46	18
Schulungen und Awareness-Kampagnen	72%	**71%**	**74%**	**67%**
Technische Data Leakage Prevention Maßnahmen	69%	**75%**	**70%**	**61%**
Social Media Policy	61%	**50%**	**67%**	**61%**
Keine	10%	**13%**	**9%**	**11%**

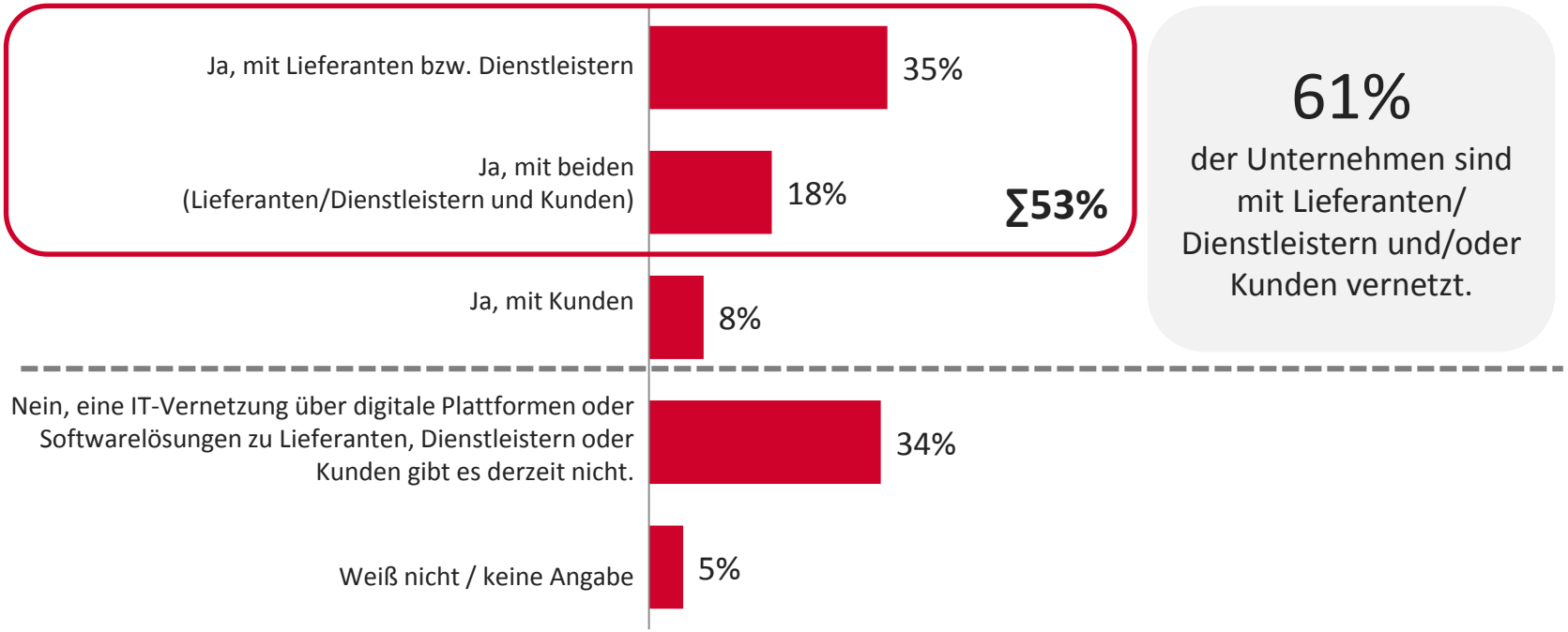
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 8: Ein wichtiger Bestandteil der Digitalen Exzellenz ist die Nutzung von Social Media und die Präsenz auf Plattformen. 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, die Social Media nutzen (Mehrfachnennungen)

ERGEBNISSE
CUSTOMER & PARTNER ENGAGEMENT

- Mehr als die Hälfte der Unternehmen ist mit seinen Lieferanten bzw. Dienstleistern über digitale Plattformen oder Software vernetzt.



61%
der Unternehmen sind mit Lieferanten/ Dienstleistern und/oder Kunden 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 oder Dienstleistern bzw. Kunden elektronisch vernetzt? Hinweis: Eine Kommunikation via E-Mail oder Fax ist hier nicht als Vernetzung zu verstehen.
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
CUSTOMER & PARTNER ENGAGEMENT

- Etwa 60 Prozent der Finanzdienstleister setzen bereits eine IT-Vernetzung über digitale Plattformen oder Softwarelösungen ein.

IT-Vernetzung	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasserversorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
Ja, mit Lieferanten bzw. Dienstleistern	**35%**	**41%**	**28%**	**38%**	**43%**	**33%**	**0%**
Ja, mit beiden (Lieferanten/Dienstleistern und Kunden)	**18%**	**15%**	**25%**	**25%**	**0%**	**17%**	**33%**
Ja, mit Kunden	**8%**	**13%**	**6%**	**0%**	**0%**	**0%**	**0%**
Nein, eine IT-Vernetzung über digitale Plattformen oder Softwarelösungen zu Lieferanten, Dienstleistern oder Kunden gibt es derzeit nicht.	**34%**	**24%**	**41%**	**38%**	**57%**	**33%**	**67%**
Weiß nicht / keine Angabe	**5%**	**7%**	**0%**	**0%**	**0%**	**17%**	**0%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

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

ERGEBNISSE
CUSTOMER & PARTNER ENGAGEMENT

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

IT-Vernetzung	Total	Unternehmensgröße		
		500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	110	41	50	19
Ja, mit Lieferanten bzw. Dienstleistern	**35%**	**27%**	**46%**	**26%**
Ja, mit beiden (Lieferanten/Dienstleistern und Kunden)	**18%**	**7%**	**18%**	**42%**
Ja, mit Kunden	**8%**	**5%**	**14%**	**0%**
Nein, eine IT-Vernetzung über digitale Plattformen oder Softwarelösungen zu Lieferanten, Dienstleistern oder Kunden gibt es derzeit nicht.	**34%**	**51%**	**22%**	**26%**
Weiß nicht / keine Angabe	**5%**	**10%**	**0%**	**5%**

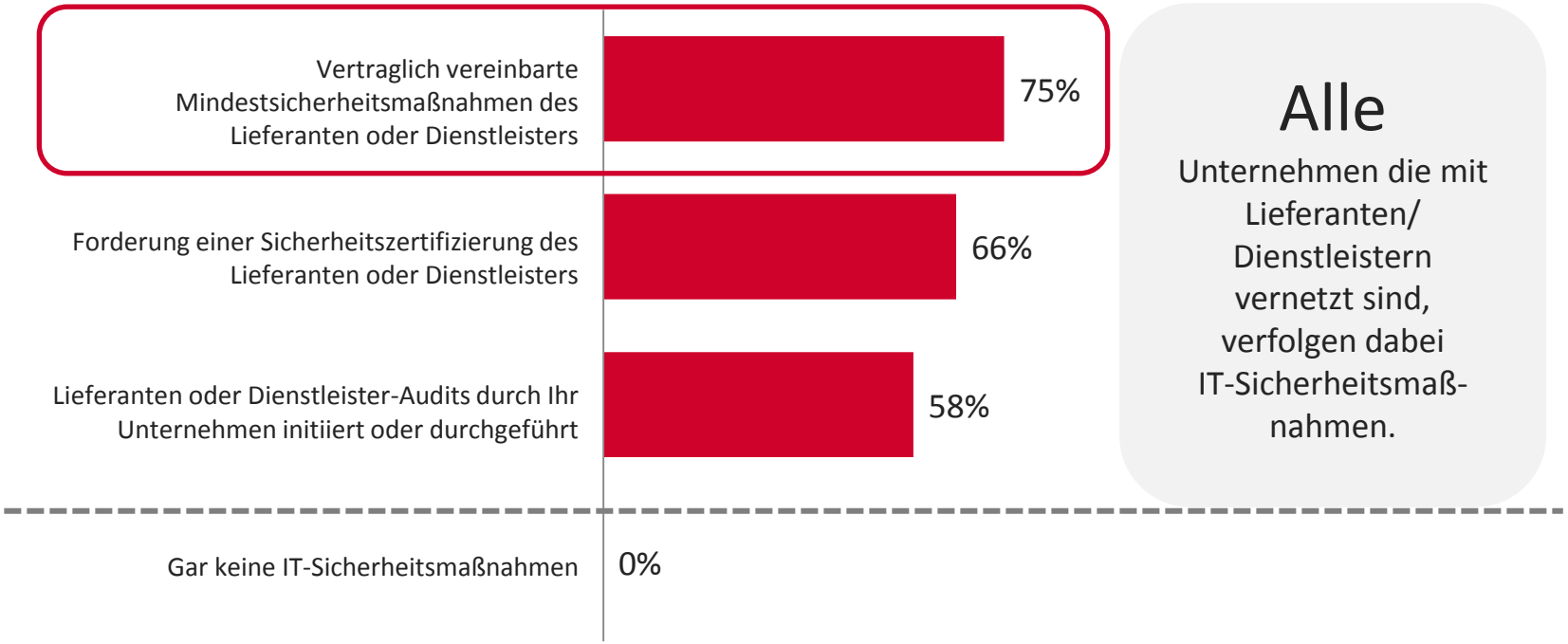
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

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 oder Dienstleistern bzw. Kunden elektronisch vernetzt? Hinweis: Eine Kommunikation via E-Mail oder Fax ist hier nicht als Vernetzung zu verstehen.
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
CUSTOMER & PARTNER ENGAGEMENT

- IT-Vernetzung: Drei Viertel 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 = 59 (Mehrfachnennungen)

ERGEBNISSE
CUSTOMER & PARTNER ENGAGEMENT

- IT-Vernetzung: 70 Prozent der Finanzdienstleister führen Lieferanten- oder Dienstleister-Audits als Sicherheitsmaßnahme durch.

IT-Vernetzung: IT-Sicherheitsmaßnahmen	Total	Branche					
		Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasserversorgung
Basis	59	30	17	5 ⚠	3 ⚠	3 ⚠	1 ⚠
Vertraglich vereinbarte Mindestsicherheitsmaßnahmen des Lieferanten oder Dienstleisters	**75%**	**70%**	**76%**	**60%**	**100%**	**100%**	**100%**
Forderung einer Sicherheitszertifizierung des Lieferanten oder Dienstleisters	**66%**	**57%**	**76%**	**80%**	**67%**	**67%**	**100%**
Lieferanten oder Dienstleister-Audits durch Ihr Unternehmen initiiert oder durchgeführt	**58%**	**70%**	**47%**	**40%**	**67%**	**33%**	**0%**
Gar keine IT-Sicherheitsmaßnahmen	**0%**	**0%**	**0%**	**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 = 59 (Mehrfachnennungen)

⚠ Geringe Fallzahl

ERGEBNISSE
CUSTOMER & PARTNER ENGAGEMENT

- Vernetzung mit Zulieferern: Je größer das Unternehmen desto häufiger werden 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	59	14	32	13
Vertraglich vereinbarte Mindestsicherheitsmaßnahmen des Lieferanten oder Dienstleisters	**75%**	**64%**	**72%**	**92%**
Forderung einer Sicherheitszertifizierung des Lieferanten oder Dienstleisters	**66%**	**64%**	**63%**	**77%**
Lieferanten oder Dienstleister-Audits durch Ihr Unternehmen initiiert oder durchgeführt	**58%**	**71%**	**59%**	**38%**
Gar keine IT-Sicherheitsmaßnahmen	**0%**	**0%**	**0%**	**0%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

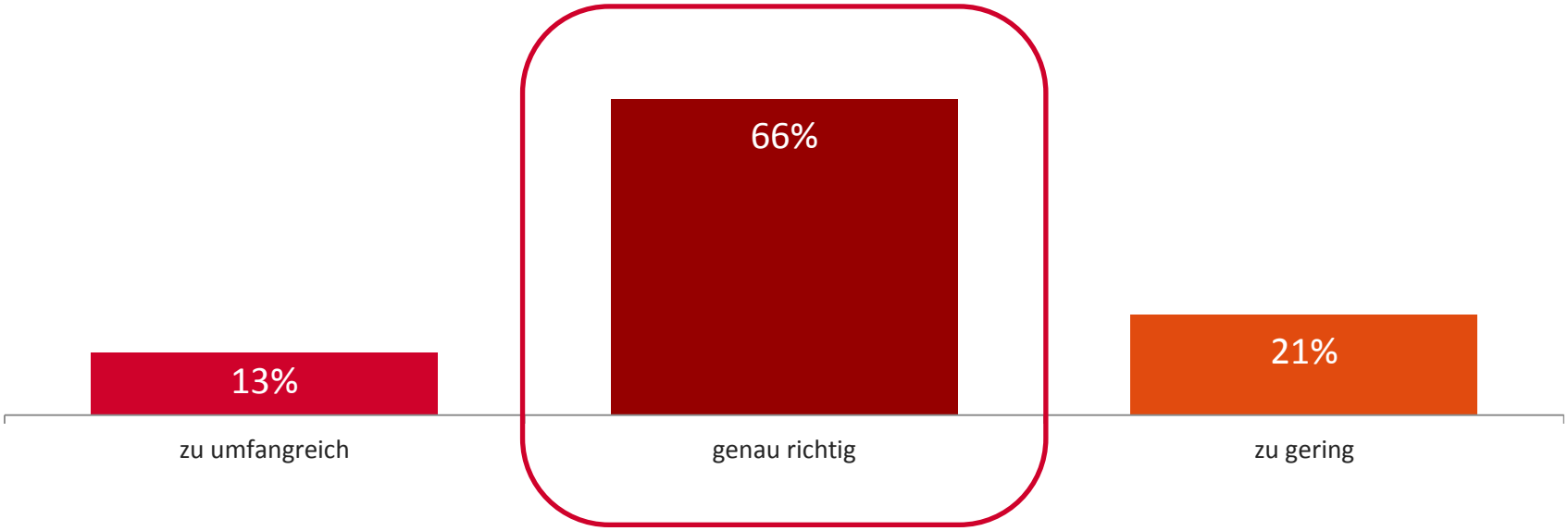
5 Prozentpunkte und mehr über Gesamtdurchschnitt

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 = 59 (Mehrfachnennungen)

ERGEBNISSE
DIGITAL COMPLIANCE

- IT-Sicherheitsgesetz: Zwei Drittel 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 = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL COMPLIANCE

- IT-Sicherheitsgesetz: Drei von zehn IT-Entscheidern der zweiten und dritten Führungsebene bewerten 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	110	66	29	15
zu umfangreich	**13%**	**11%**	**17%**	**13%**
genau richtig	**66%**	**74%**	**55%**	**53%**
zu gering	**21%**	**15%**	**28%**	**33%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Geringe Fallzahl

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 = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL COMPLIANCE

- Vor allem IT-Entscheider aus Unternehmen ab 5.000 Mitarbeitern beurteilen die staatliche Regulierung für die IT-Sicherheit als zu gering.

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	110	41	50	19
zu umfangreich	**13%**	**7%**	**16%**	**16%**
genau richtig	**66%**	**71%**	**74%**	**37%**
zu gering	**21%**	**22%**	**10%**	**47%**

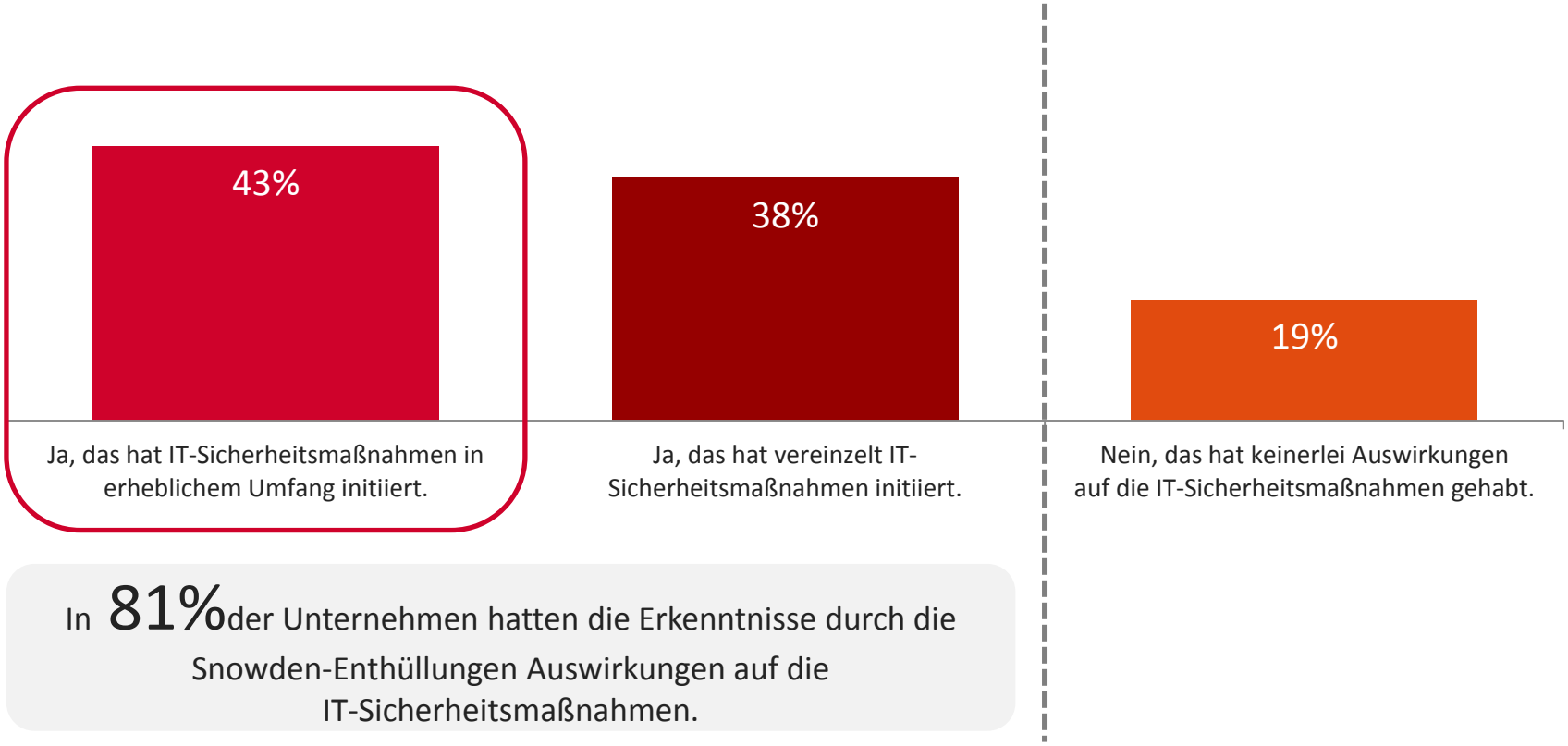
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

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 = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL COMPLIANCE

- Snowden-Enthüllungen mit Folgen: In vier von zehn Unternehmen haben die Erkenntnisse daraus umfangreiche IT-Sicherheitsmaßnahmen initiiert.



In **81%** der Unternehmen hatten die Erkenntnisse durch die Snowden-Enthüllungen Auswirkungen auf die IT-Sicherheitsmaßnahmen.

Frage 14: Die Snowden-Enthüllungen haben die Vertrauenswürdigkeit staatlicher Institutionen erschüttert. Das Abhören unverschlüsselter Kommunikation ist heute eine nicht mehr ignorierbare Realität. Haben diese Erkenntnisse einen Einfluss auf die Entscheidungen für IT-Sicherheitsmaßnahmen in Ihrem Unternehmen gehabt?
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL COMPLIANCE

- Vor allem bei den Finanzdienstleistern haben die Erkenntnisse aus den Snowden-Enthüllungen erhebliche IT-Sicherheitsmaßnahmen veranlasst.

		Branche					
	Total	Finanzdienst-leistungen	Sonstiges Verarbeitendes Gewerbe	Automotive	Öffentliche Verwaltung	Telekommuni-kation/Medien	Energie- und Wasser-versorgung
Basis	110	54	32	8 ⚠	7 ⚠	6 ⚠	3 ⚠
Ja, das hat IT-Sicherheitsmaßnahmen in erheblichem Umfang initiiert.	**43%**	**63%**	**19%**	**50%**	**29%**	**17%**	**0%**
Ja, das hat vereinzelt IT-Sicherheitsmaßnahmen initiiert.	**38%**	**26%**	**56%**	**25%**	**29%**	**67%**	**67%**
Nein, das hat keinerlei Auswirkungen auf die IT-Sicherheitsmaßnahmen gehabt.	**19%**	**11%**	**25%**	**25%**	**43%**	**17%**	**33%**

5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

⚠ Geringe Fallzahl

Frage 14: Die Snowden-Enthüllungen haben die Vertrauenswürdigkeit staatlicher Institutionen erschüttert. Das Abhören unverschlüsselter Kommunikation ist heute eine nicht mehr ignorierbare Realität. Haben diese Erkenntnisse einen Einfluss auf die Entscheidungen für IT-Sicherheitsmaßnahmen in Ihrem Unternehmen gehabt?
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL COMPLIANCE

- Snowden-Enthüllungen: Mehr als die Hälfte der Unternehmen mit 1.000 bis unter 5.000 Mitarbeitern hat mit umfassenden IT-Sicherheitsmaßnahmen reagiert.

		Unternehmensgröße		
	Total	500 bis unter 1.000 Mitarbeiter	1.000 bis unter 5.000 Mitarbeiter	5.000 Mitarbeiter und mehr
Basis	110	41	50	19
Ja, das hat IT-Sicherheitsmaßnahmen in erheblichem Umfang initiiert.	**43%**	**34%**	**54%**	**32%**
Ja, das hat vereinzelt IT-Sicherheitsmaßnahmen initiiert.	**38%**	**41%**	**32%**	**47%**
Nein, das hat keinerlei Auswirkungen auf die IT-Sicherheitsmaßnahmen gehabt.	**19%**	**24%**	**14%**	**21%**

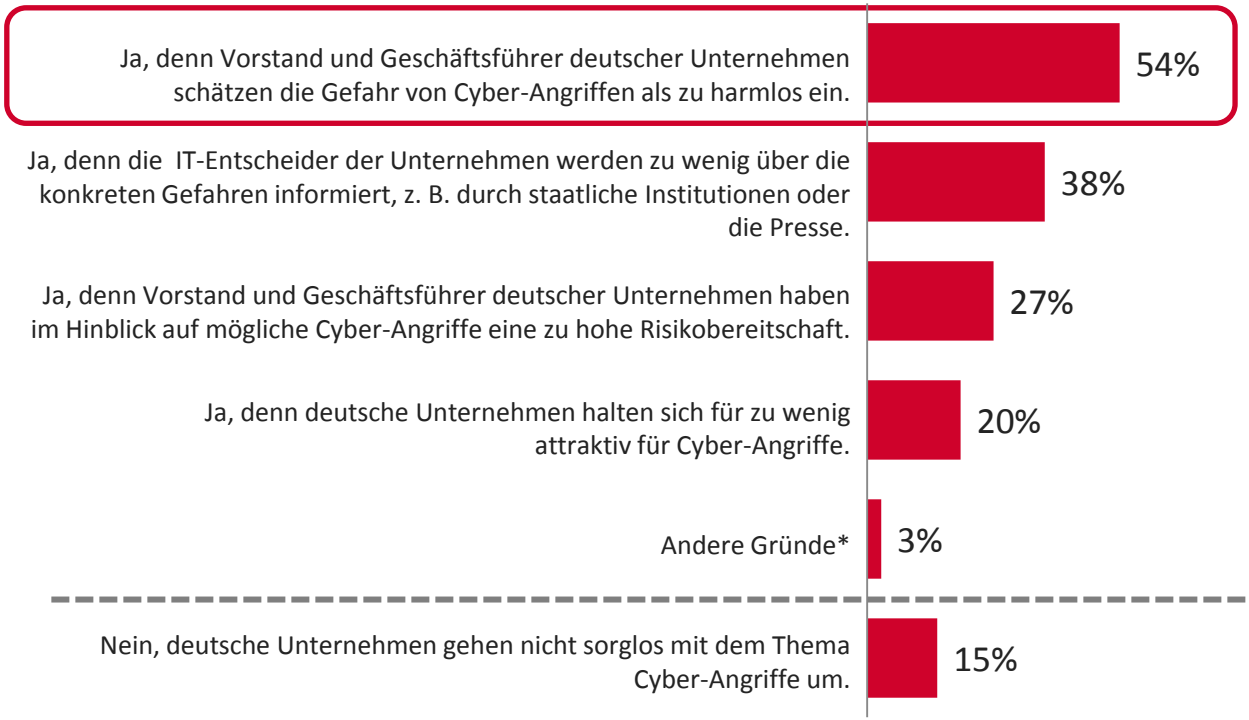
5 Prozentpunkte und mehr unter Gesamtdurchschnitt

5 Prozentpunkte und mehr über Gesamtdurchschnitt

Frage 14: Die Snowden-Enthüllungen haben die Vertrauenswürdigkeit staatlicher Institutionen erschüttert. Das Abhören unverschlüsselter Kommunikation ist heute eine nicht mehr ignorierbare Realität. Haben diese Erkenntnisse einen Einfluss auf die Entscheidungen für IT-Sicherheitsmaßnahmen in Ihrem Unternehmen gehabt?
Basis: Alle Befragten, N = 110 (Einfachnennung)

ERGEBNISSE
DIGITAL LEADERSHIP

- Digitale Sorglosigkeit: Unternehmensleiter verharmlosen aus Sicht von mehr als der Hälfte der IT-Entscheider die Gefahr von Cyber-Angriffen.

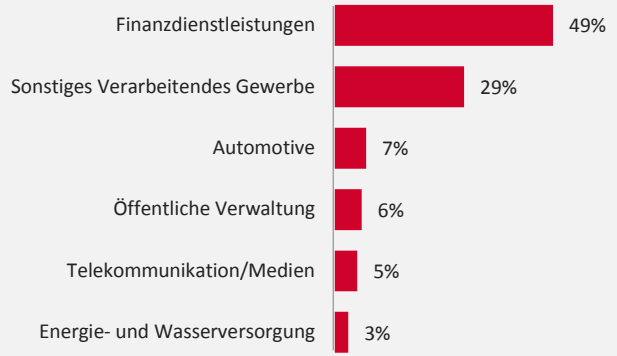


85%
der IT-Entscheider bestätigen die „Digitale Sorglosigkeit“ deutscher Unternehmen beim Thema Cyber-Angriffe.

Frage 15: Die Statistiken 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 = 110 (Mehrfachnennungen)
* Thema wird in den meisten Unternehmen sträflich vernachlässigt/Lücken sind bekannt, aber die IT-Entscheider werden ignoriert/Betrifft immer nur die anderen.

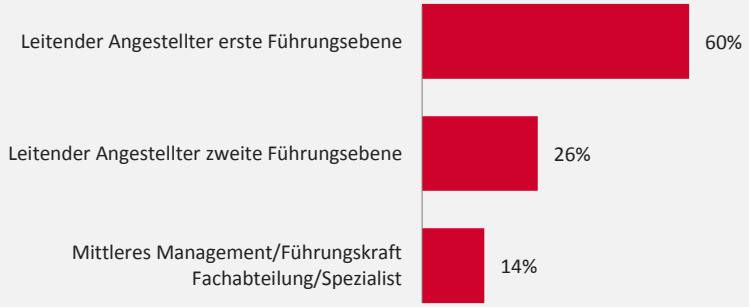
ERGEBNISSE
STATISTIK

- Branchen



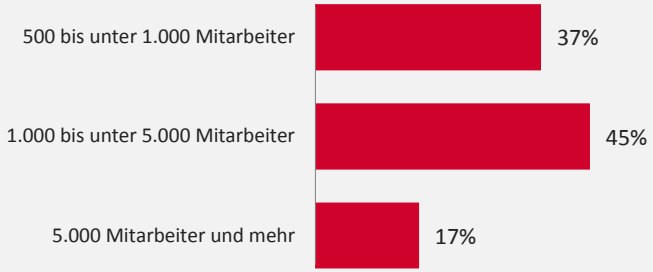
Basis: Alle Befragten, N = 110

- Position



Basis: Alle Befragten, N = 110

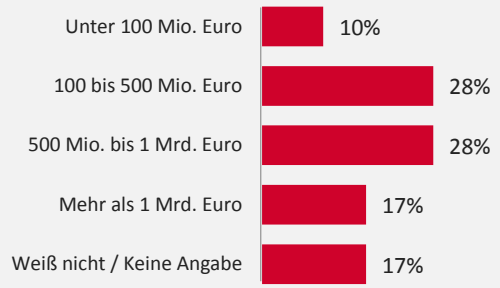
- Unternehmensgröße



Basis: Alle Befragten, N = 110

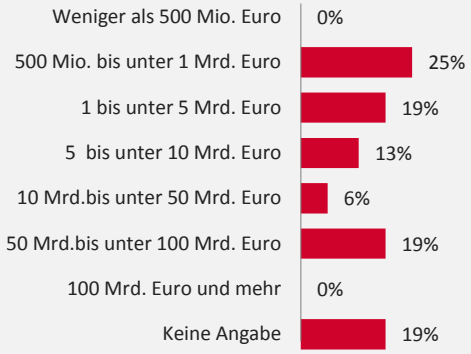
ERGEBNISSE
STATISTIK

- Jahresumsatz



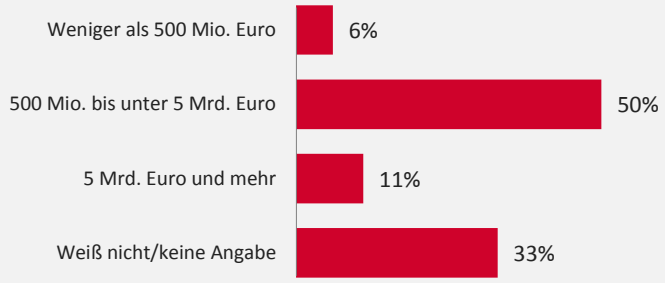
Basis: Alle Befragten, außer aus Banken und Versicherungen, N = 58

- Bilanzsumme



Basis: Basis: Alle Befragten aus Banken, N = 16

- Bruttobeitragseinnahmen



Basis: Alle Befragten aus Versicherungen, N = 36

sopra steria
CONSULTING