POTENZIALANALYSE
UNTERNEHMEN SCHÜTZEN – RISIKEN MINIMIEREN

Delivering Transformation. Together.

sopra steria
CONSULTING

AGENDA

1. BEFRAGUNGSDESIGN
    1. METHODE UND STICHPROBE
    2. ZUSAMMENSETZUNG DER STICHPROBE
2. ZUSAMMENFASSUNG
3. ERGEBNISSE

1. BEFRAGUNGSDESIGN

Methode & Zusammensetzung der Stichprobe

METHODE UND STICHPROBE

Methode

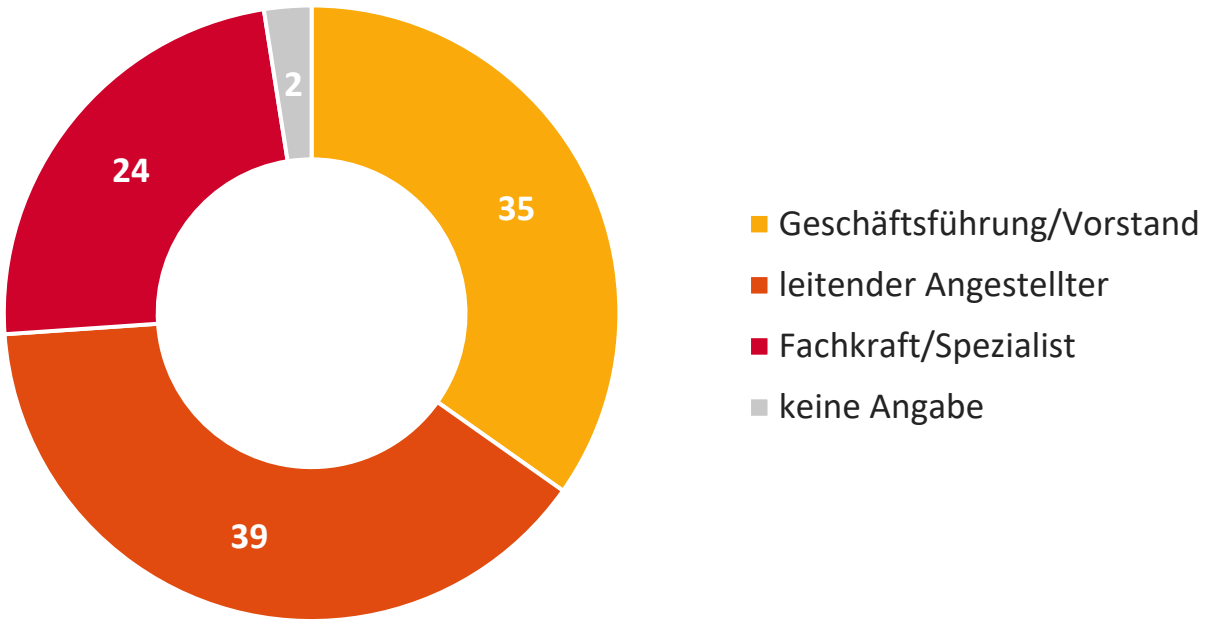
- Online-Befragung
- Befragungsdauer: 10 Minuten
- Befragungszeitraum: September 2018

Stichprobe

- Stichprobenumfang: **N = 308**, entsprechend der folgenden Kriterien:
- Branchenzugehörigkeit: Banken, Versicherungen, sonstige Finanzdienstleistungen, Energie- und Wasserversorgung, Telekommunikation/Medien, öffentliche Verwaltung, Automotive, sonstiges verarbeitendes Gewerbe
  - Position im Unternehmen: Geschäftsführung/Vorstand, leitender Angestellter oder Fachkraft/Spezialist
  - Tätigkeitsbereich im Unternehmen: Vorstand/Geschäftsführung, Strategieentwicklung/Business Development, IT, Vertrieb/Verkauf, Marketing, Finanzen/Controlling
- keine Quotierung der Stichprobe

ZUSAMMENSETZUNG DER STICHPROBE I

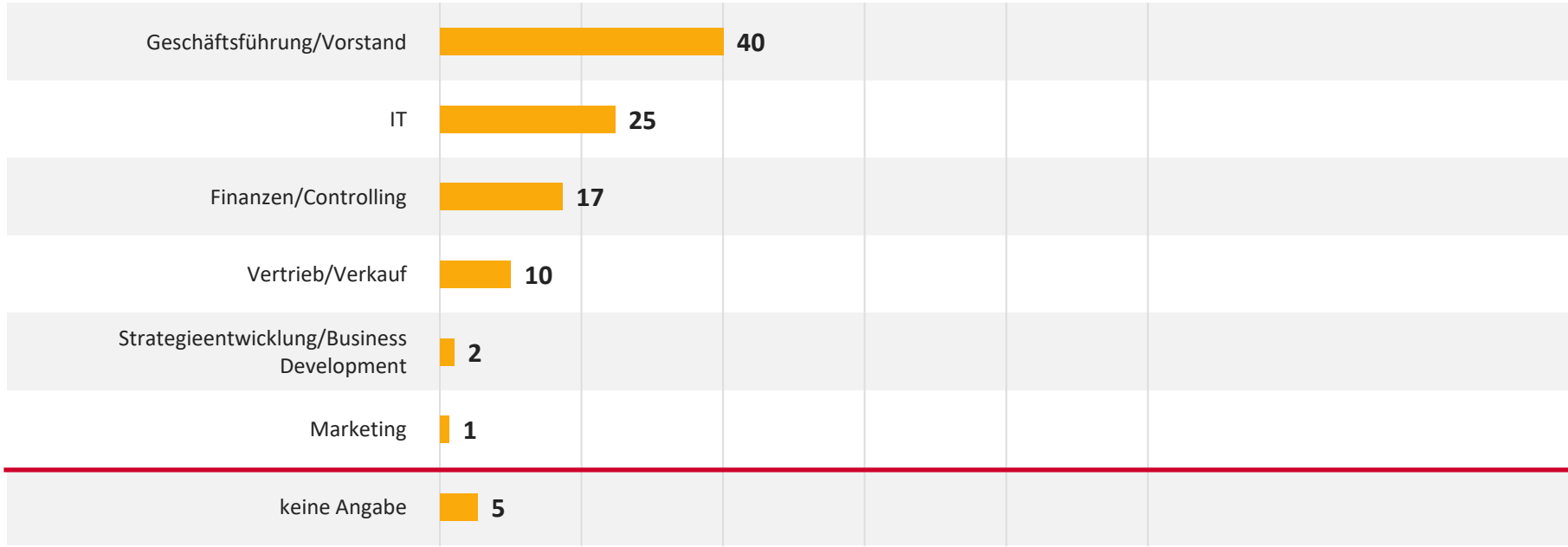
Position im Unternehmen



Basis: alle Befragten; n = 161;
Angaben in Prozent

ZUSAMMENSETZUNG DER STICHPROBE II

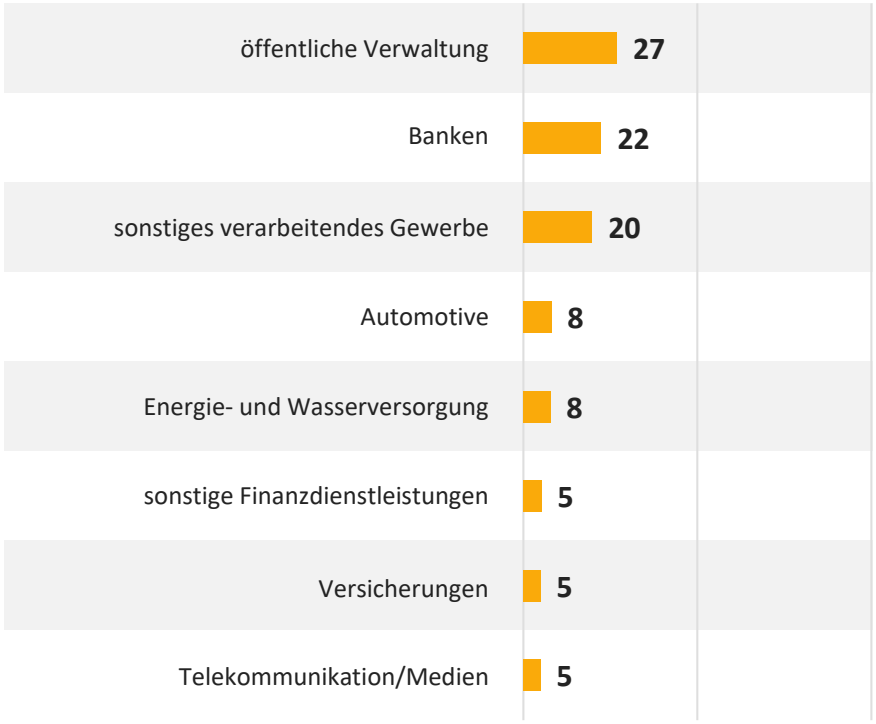
Tätigkeitsbereich im Unternehmen



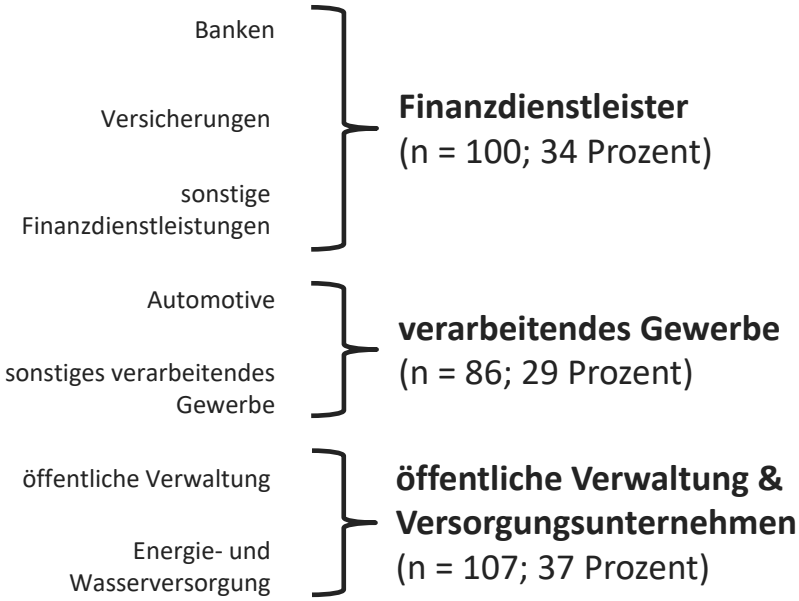
Basis: alle Befragten; n = 150;
Angaben in Prozent

ZUSAMMENSETZUNG DER STICHPROBE III

Branchenzugehörigkeit



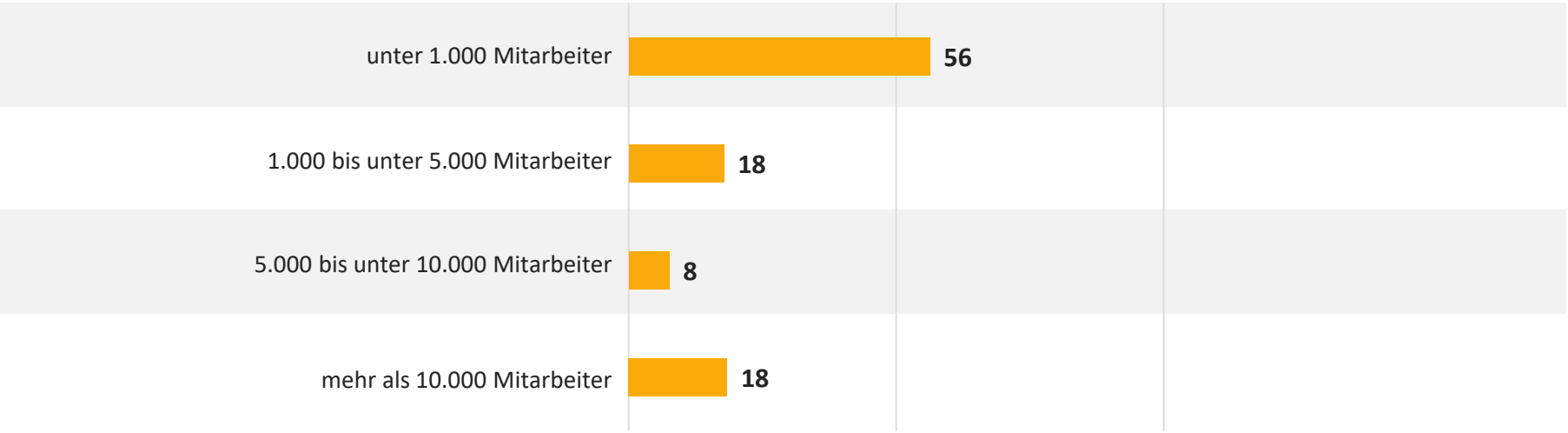
Clusterbildung



Basis: alle Befragten; n = 308;
Angaben in Prozent

ZUSAMMENSETZUNG DER STICHPROBE IV

Unternehmensgröße



Basis: alle Befragten; n = 304;
Angaben in Prozent

2. ZUSAMMENFASSUNG

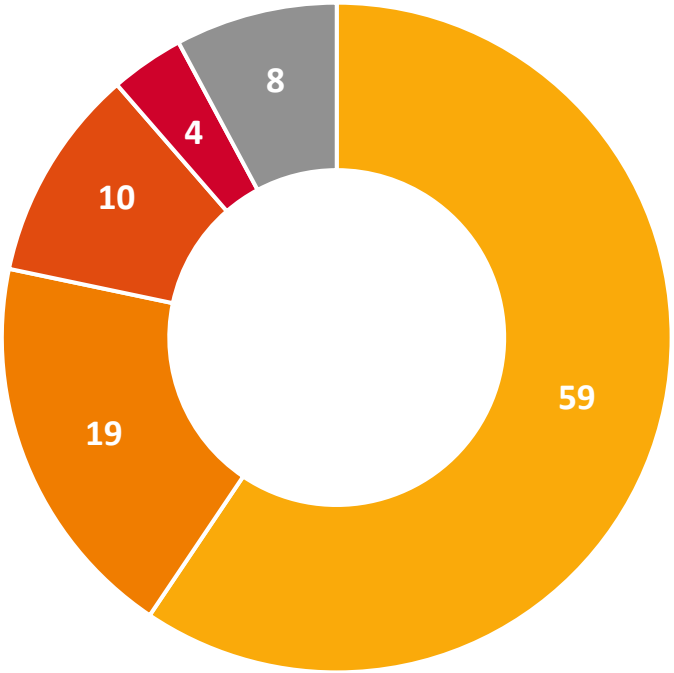
ZUSAMMENFASSUNG

- 59 Prozent der befragten Unternehmen haben eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet.
- Die Komplexität der unternehmenseigenen IT-Infrastruktur erschwert die Umsetzung der IT-Sicherheitsstrategie in zwei Drittel der befragten Unternehmen.
- Für mehr als die Hälfte der befragten Unternehmen (53 Prozent) ist ein IT-Sicherheitskonzept die essenzielle Grundlage für alle IT-Projekte.
- 36 Prozent der befragten Unternehmen sensibilisieren ihre Mitarbeiter für das Thema IT-Sicherheit.
- Im Alltagsgeschäft der befragten Unternehmen sind vor allem bösartige Software (Malware; 82 Prozent) und unerwünschte E-Mails (68 Prozent) eine Bedrohung für die IT-Sicherheit.
- In 73 Prozent der befragten Unternehmen sind interne Mitarbeiter für die IT-Sicherheit zuständig. 21 Prozent vertrauen hingegen auf externe Dienstleister.
- 39 Prozent der befragten Unternehmen haben in den vergangenen zwölf Monaten mindestens einen mit IT-Sicherheit zusammenhängenden Vorfall registriert.
- 34 Prozent der befragten Unternehmen schätzen das Risiko, Opfer einer schwerwiegenden Cyber-Attacke zu werden, als sehr gering beziehungsweise gering ein. 28 Prozent beurteilen das Risiko für ihr Unternehmen hingegen als hoch beziehungsweise sehr hoch.
- Mögliche, durch Cyber-Vorfälle verursachte Schäden werden derzeit lediglich von 17 Prozent der befragten Unternehmen versichert. 22 Prozent planen, eine entsprechende Versicherung abzuschließen. Für weitere 30 Prozent ist das derzeit kein Thema.
- Ein Drittel der befragten Unternehmen war in den vergangenen zwölf Monaten Opfer eines Cyber-Angriffs.
- Cyber-Angriffe verursachten bei der Mehrheit der befragten Unternehmen (52 Prozent) Kosten, die bei der Behebung der damit zusammenhängenden Schäden entstanden.
- Um Konformität mit der EU-DSGVO gewährleisten zu können, haben 72 Prozent ihre unternehmensinterne IT-Sicherheit an entsprechende Anforderungen angepasst.
- Um Data Leakage vorzubeugen, setzen 77 Prozent der befragten Unternehmen auf die Sensibilisierung ihrer Mitarbeiter.
- Mehr als die Hälfte der Befragten (56 Prozent) erwartet für die kommenden drei Jahre eine Steigerung des Budgets für IT-Sicherheit in ihrem Unternehmen.
- In Bezug auf die IT-Sicherheit neuer Technologien wird die Blockchain am häufigsten als sicher eingestuft (47 Prozent). Demgegenüber werden Sprachassistenten von 85 Prozent der Befragten als unsichere Technologie wahrgenommen.

3. ERGEBNISSE

IT-SICHERHEIT IST BESTANDTEIL DER UNTERNEHMENSSTRATEGIE

Verfügt Ihr Unternehmen über eine IT-Sicherheitsstrategie?

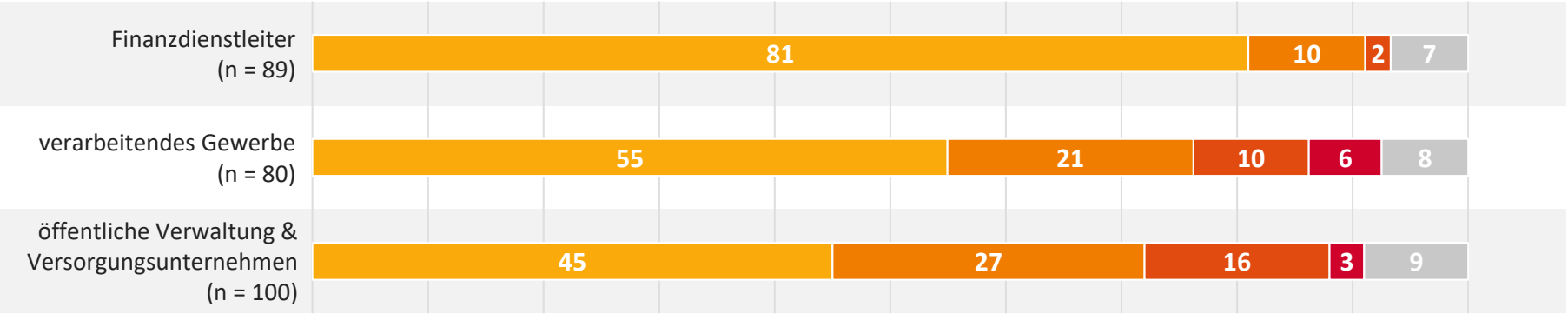


- Wir haben eine IT-Sicherheitsstrategie im Unternehmen formuliert, dokumentiert und verabschiedet.
- Eine IT-Sicherheitsstrategie befindet sich gerade in der Erstellung oder Aktualisierung.
- Wir planen eine IT-Sicherheitsstrategie.
- Wir haben keine IT-Sicherheitsstrategie und planen auch keine.
- weiß nicht/keine Angabe

Basis: alle Befragten; n = 281;
Angaben in Prozent

VOR ALLEM FÜR FINANZDIENSTLEISTER IST EINE IT-SICHERHEITSSTRATEGIE UNABKÖMMLICH

Verfügt Ihr Unternehmen über eine IT-Sicherheitsstrategie?

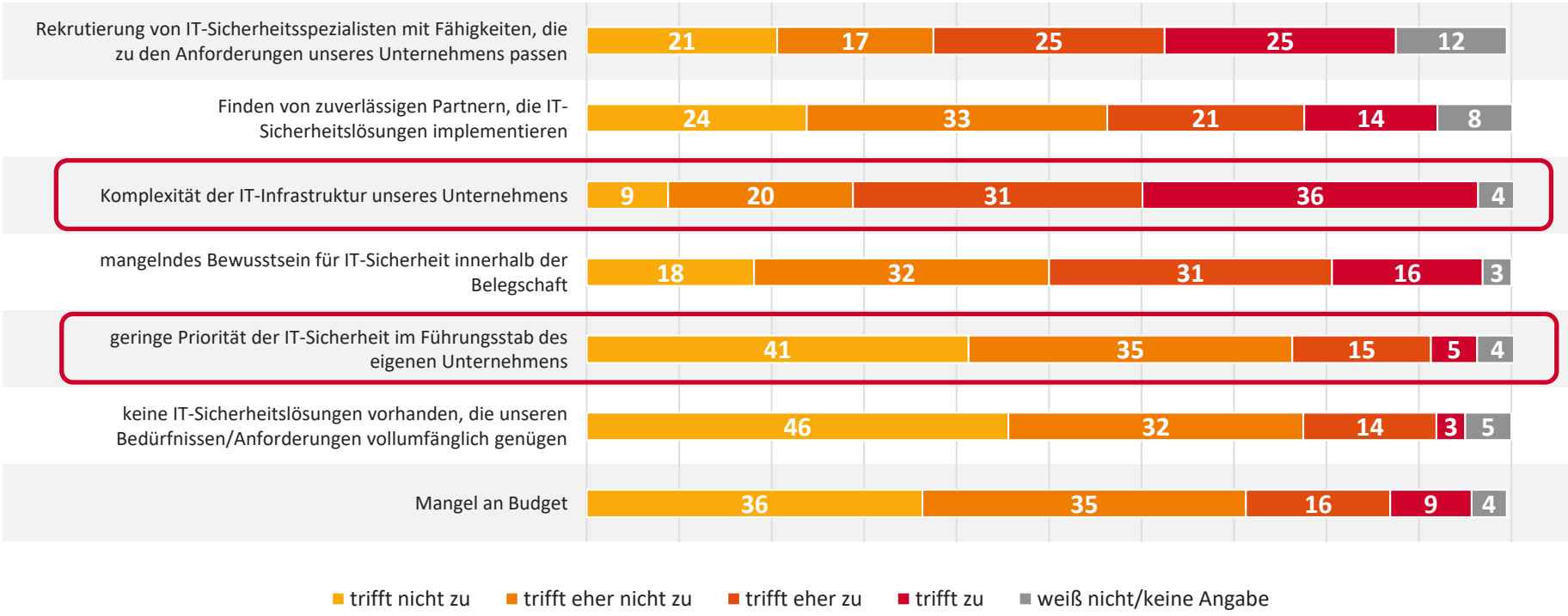


- Wir haben eine IT-Sicherheitsstrategie im Unternehmen formuliert, dokumentiert und verabschiedet.
- Eine IT-Sicherheitsstrategie befindet sich gerade in der Erstellung oder Aktualisierung.
- Wir planen eine IT-Sicherheitsstrategie.
- Wir haben keine IT-Sicherheitsstrategie und planen auch keine.
- weiß nicht/keine Angabe

Basis: alle Befragten; Angaben in Prozent

DAS THEMA IT-SICHERHEIT IST ZWAR AUF MANAGEMENTEBENE ANGEKOMMEN, KOMPLEXE IT-INFRASTRUKTUREN ERSCHWEREN ABER DIE STRATEGISCHE UMSETZUNG

Eine Reihe von Schwierigkeiten kann bei der Umsetzung einer IT-Sicherheitsstrategie auftreten. Inwieweit treffen die folgenden auf Ihr Unternehmen zu?

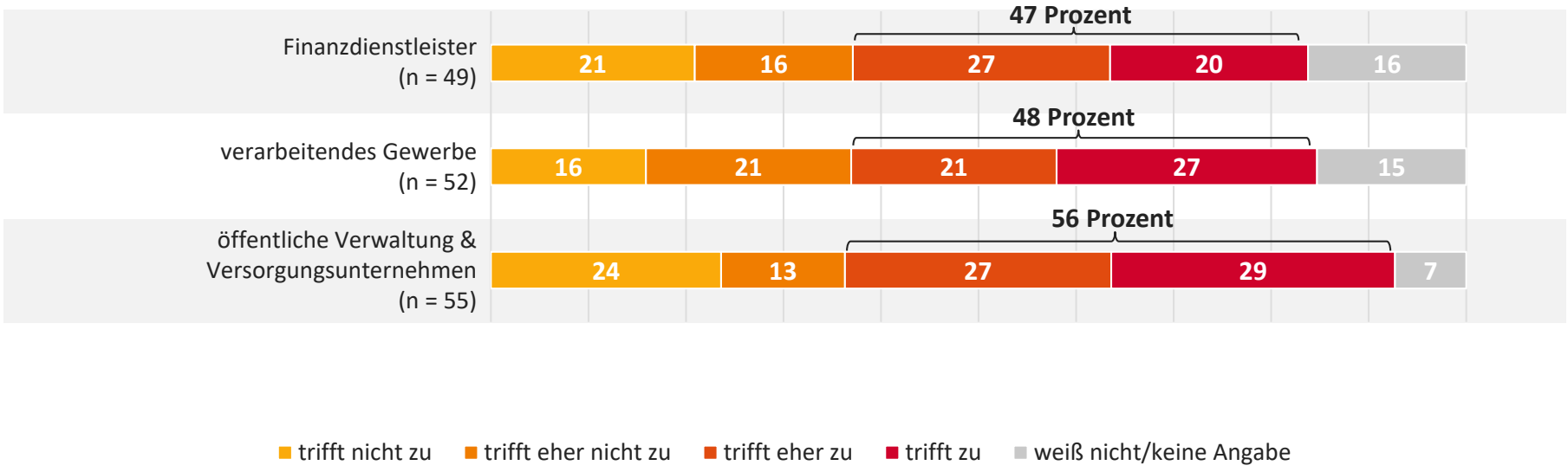


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; n = 160; Angaben in Prozent

PASSENDE IT-FACHLEUTE ZU FINDEN, IST VOR ALLEM FÜR ÖFFENTLICHE VERWALTUNG & VERSORGUNGS-UNTERNEHMEN EINE HERAUSFORDERUNG

Inwieweit trifft folgende Aussage auf Ihr Unternehmen zu?

Die **Rekrutierung von IT-Sicherheitsspezialisten mit Fähigkeiten, die zu den Anforderungen unseres Unternehmens passen**, bereitet unserem Unternehmen Schwierigkeiten bei der Umsetzung der IT-Sicherheitsstrategie.

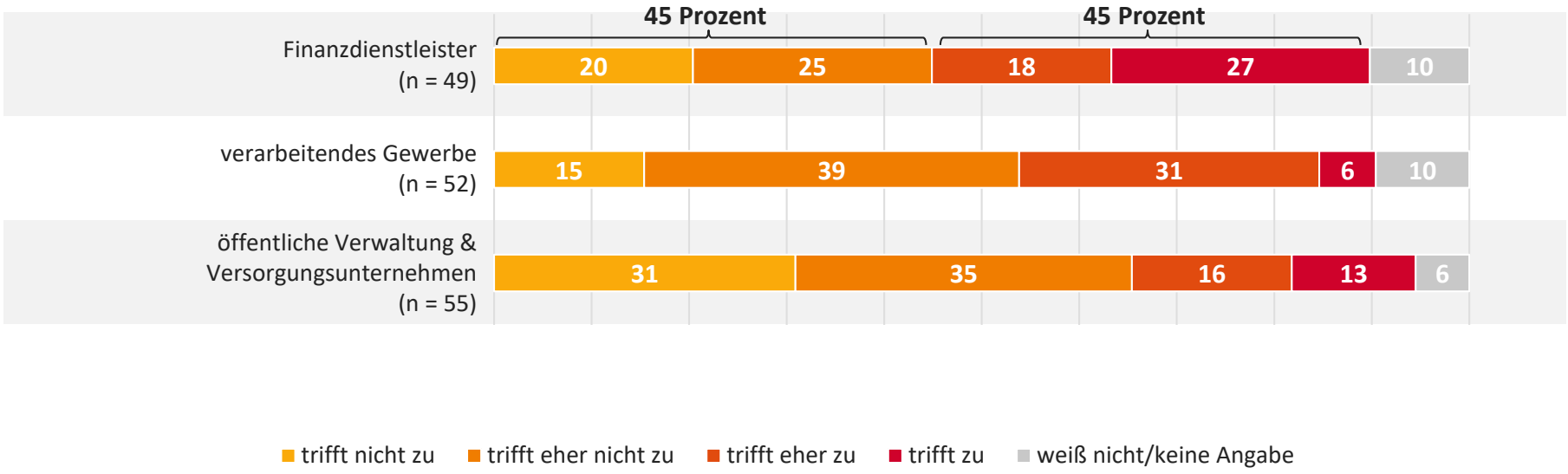


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; Angaben in Prozent

FINANZDIENSTLEISTER IM ZWIESPALT: DAS FINDEN ZUVERLÄSSIGER PARTNER GESTALTET SICH FÜR 45 PROZENT EHER SCHWIERIG. WEITERE 45 PROZENT HABEN DAMIT EHER KEIN PROBLEM.

Inwieweit trifft folgende Aussage auf Ihr Unternehmen zu?

Das **Finden von zuverlässigen Partnern, die IT-Sicherheitslösungen implementieren**, bereitet unserem Unternehmen Schwierigkeiten bei der Umsetzung der IT-Sicherheitsstrategie.

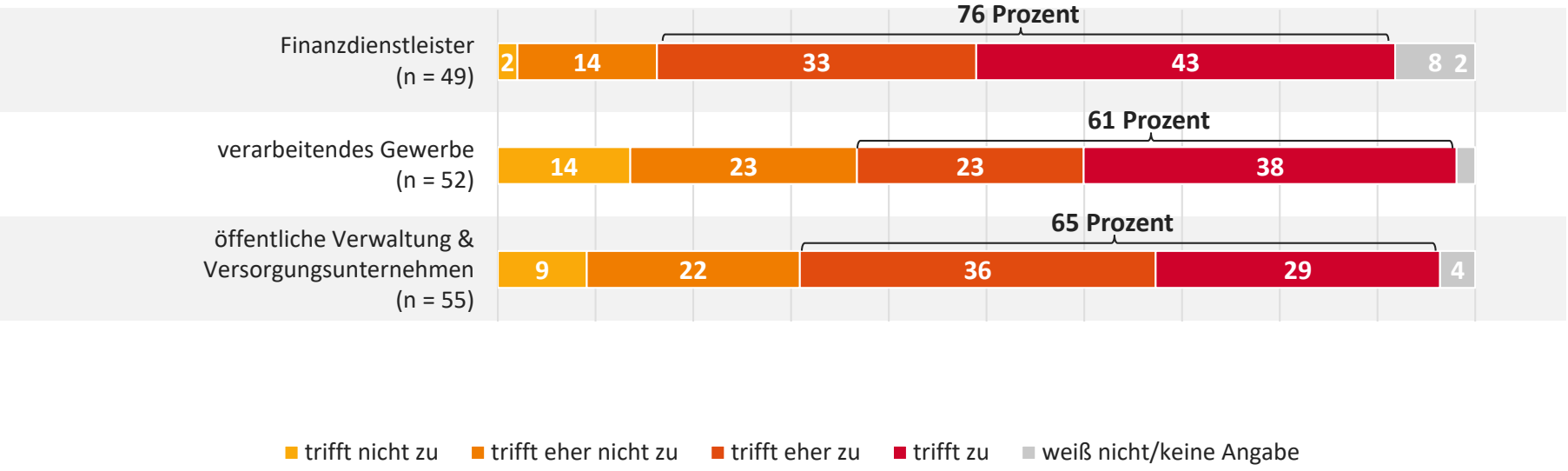


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; Angaben in Prozent

KOMPLEXE IT-INFRASTRUKTUREN ERSCHWEREN DIE UMSETZUNG EINER IT-SICHERHEITSSTRATEGIE IN ALLEN BEFRAGTEN BRANCHEN

Inwieweit trifft folgende Aussage auf Ihr Unternehmen zu?

Die **Komplexität der IT-Infrastruktur unseres Unternehmens** bereitet uns Schwierigkeiten bei der Umsetzung der IT-Sicherheitsstrategie.

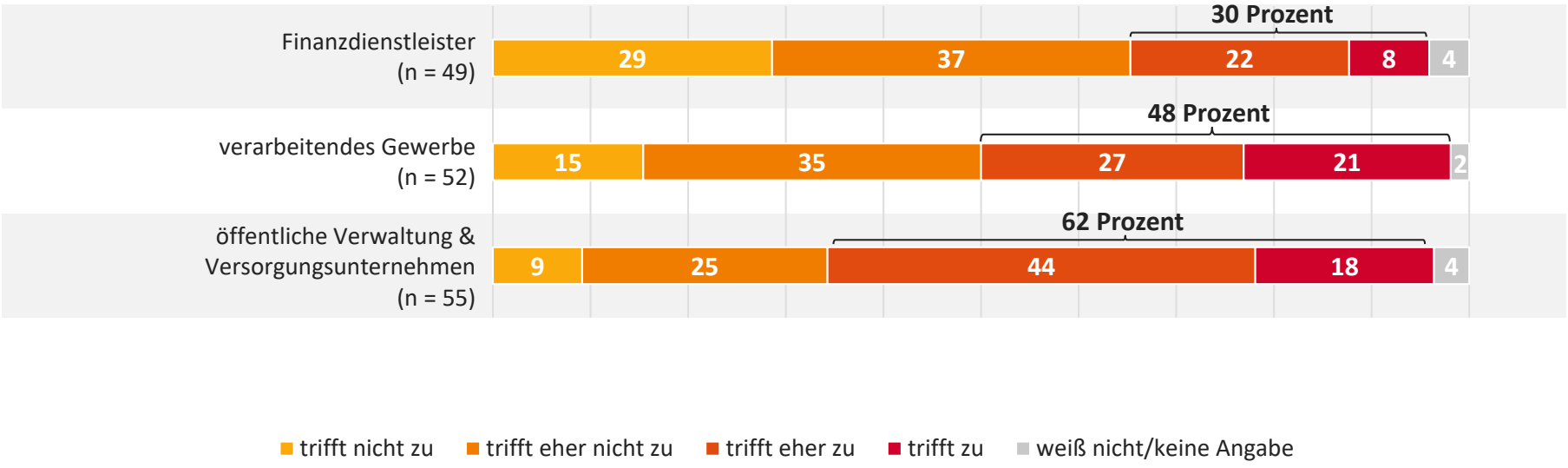


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; Angaben in Prozent

INSBESONDERE IN ÖFFENTLICHER VERWALTUNG & VERSORGUNGSUNTERNEHMEN MÜSSEN DIE MITARBEITER FÜR DAS THEMA IT-SICHERHEIT SENSIBILISIERT WERDEN

Inwieweit trifft folgende Aussage auf Ihr Unternehmen zu?

Mangelndes Bewusstsein für IT-Sicherheit innerhalb der Belegschaft bereitet unserem Unternehmen Schwierigkeiten bei der Umsetzung der IT-Sicherheitsstrategie.

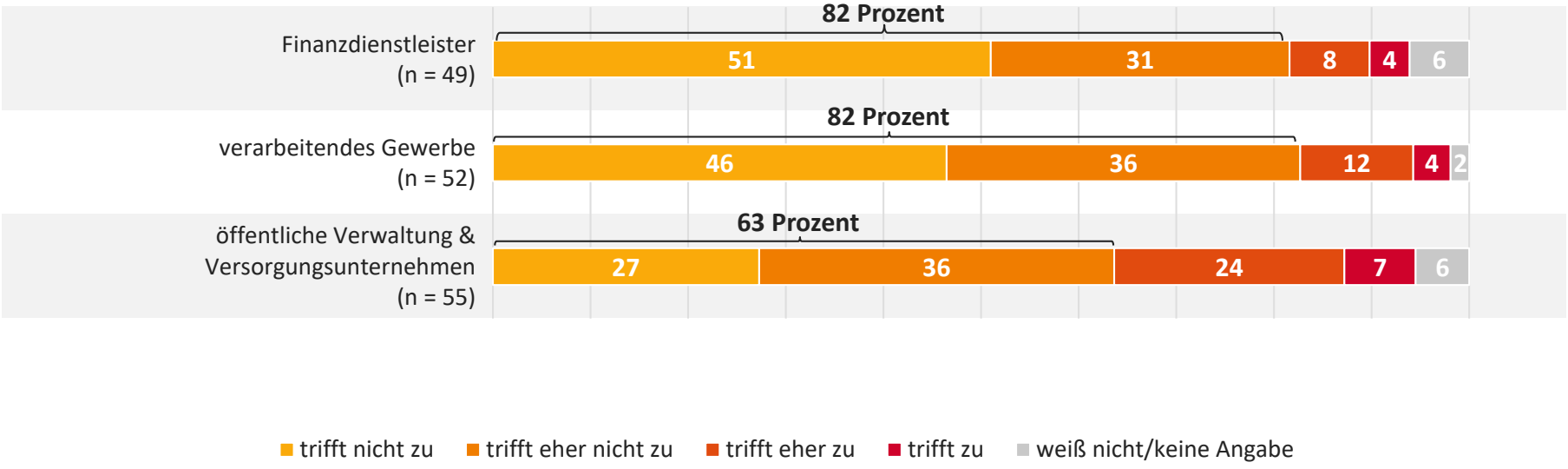


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; Angaben in Prozent

DIE BEDEUTUNG VON IT-SICHERHEIT IST BRANCHENÜBERGREIFEND AUF FÜHRUNGSEBENE ANGEKOMMEN

Inwieweit trifft folgende Aussage auf Ihr Unternehmen zu?

Die **geringe Priorität der IT-Sicherheit im Führungsstab unseres Unternehmens** bereitet uns Schwierigkeiten bei der Umsetzung der IT-Sicherheitsstrategie.

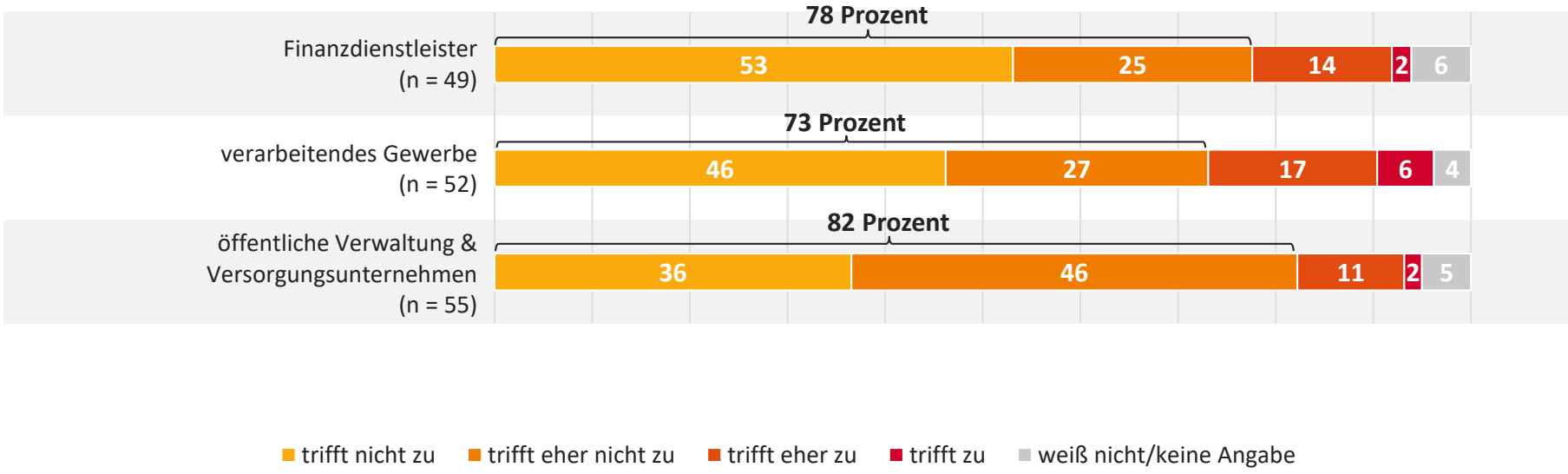


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; Angaben in Prozent

DAS ANGEBOT AN IT-SICHERHEITSLÖSUNGEN STELLT KEINE HÜRDE BEI DER UMSETZUNG DER IT-SICHERHEITSSTRATEGIE DAR

Inwieweit trifft folgende Aussage auf Ihr Unternehmen zu?

Dass **keine IT-Sicherheitslösungen vorhanden sind, die unseren Bedürfnissen/Anforderungen vollumfänglich genügen**, bereitet unserem Unternehmen Schwierigkeiten bei der Umsetzung der IT-Sicherheitsstrategie.

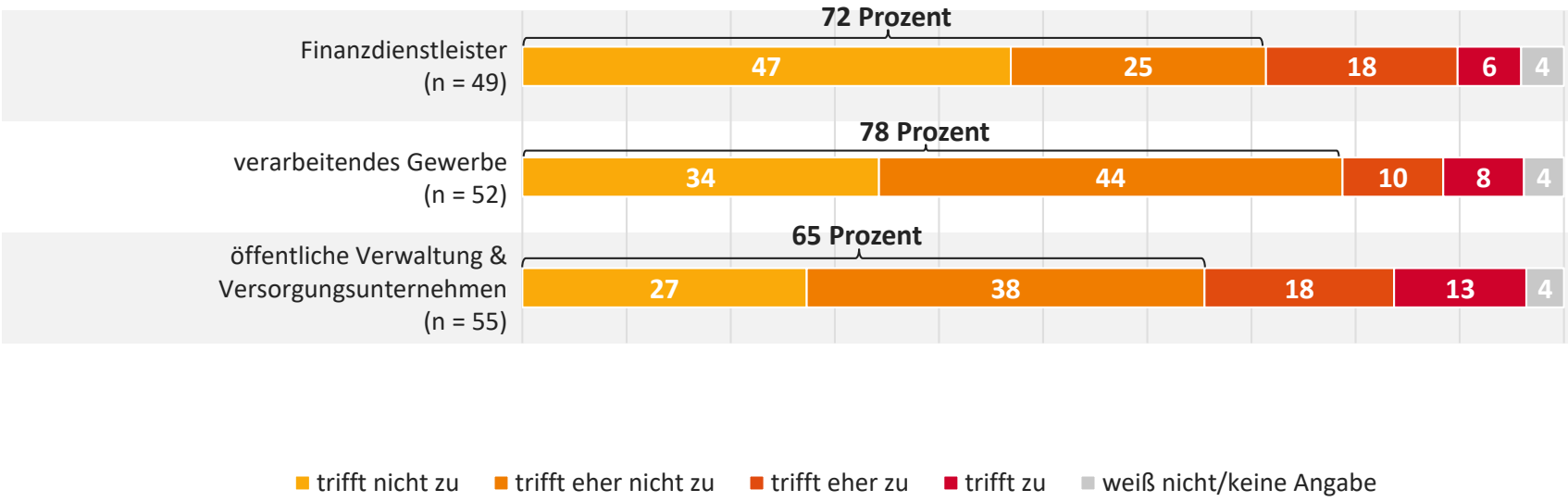


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; Angaben in Prozent

IN DEN BEFRAGTEN BRANCHEN GILT DER MANGEL AN BUDGET EHER NICHT ALS URSACHE FÜR SCHWIERIGKEITEN BEI DER UMSETZUNG DER IT-SICHERHEITSSTRATEGIE

Inwieweit trifft folgende Aussage auf Ihr Unternehmen zu?

Der **Mangel an Budget** bereitet unserem Unternehmen Schwierigkeiten bei der Umsetzung der IT-Sicherheitsstrategie.

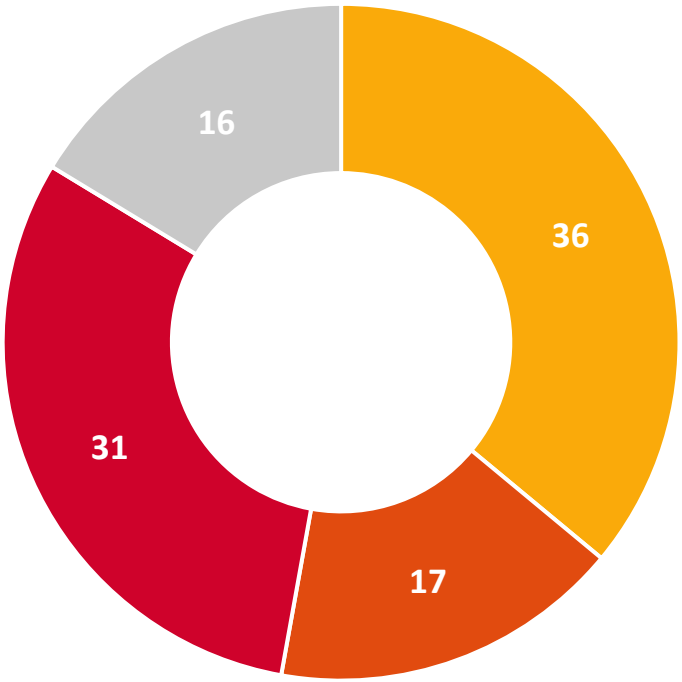


Basis: alle Befragten, deren Unternehmen eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet hat sowie gegenwärtig erstellt oder aktualisiert; Angaben in Prozent

FÜR MEHR ALS DIE HÄLFTE DER BEFRAGTEN UNTERNEHMEN IST EIN IT-SICHERHEITSKONZEPT EINE ESSENZIELLE GRUNDLAGE FÜR IT-PROJEKTE

Das Vorantreiben der Digitalisierung und Automation von Prozessen fordert spezielle IT-Sicherheitsmaßnahmen. Wie ist die Situation in Ihrem Unternehmen?

In meinem Unternehmen…

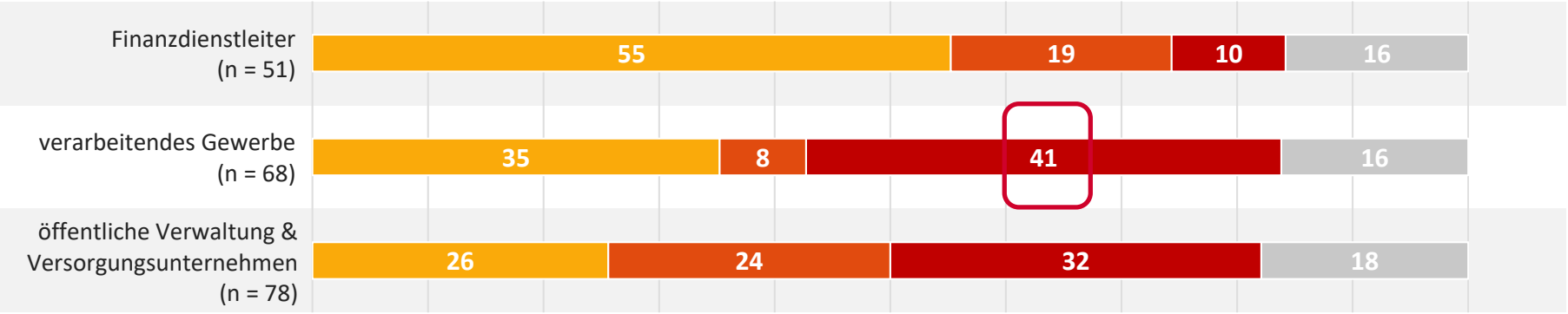


- … dürfen IT-Projekte nur bei Vorliegen eines IT-Sicherheitskonzepts gestartet werden.
- … muss ein IT-Sicherheitskonzept in einer bestimmten Frist nach Implementierung einer Anwendung oder eines IT-Systems vorliegen.
- … ist ein IT-Sicherheitskonzept für Anwendungen oder IT-Systeme nicht zwingend vorgeschrieben.
- weiß nicht/keine Angabe

Basis: alle Befragten; n = 207;
Angaben in Prozent

IN VIER VON ZEHN UNTERNEHMEN DES VERARBEITENDEN GEWERBES IST EIN IT-SICHERHEITSKONZEPT NICHT ZWINGEND VORGESCHRIEBEN

Das Vorantreiben der Digitalisierung und Automation von Prozessen fordert spezielle IT-Sicherheitsmaßnahmen. Wie ist die Situation in Ihrem Unternehmen? In meinem Unternehmen…

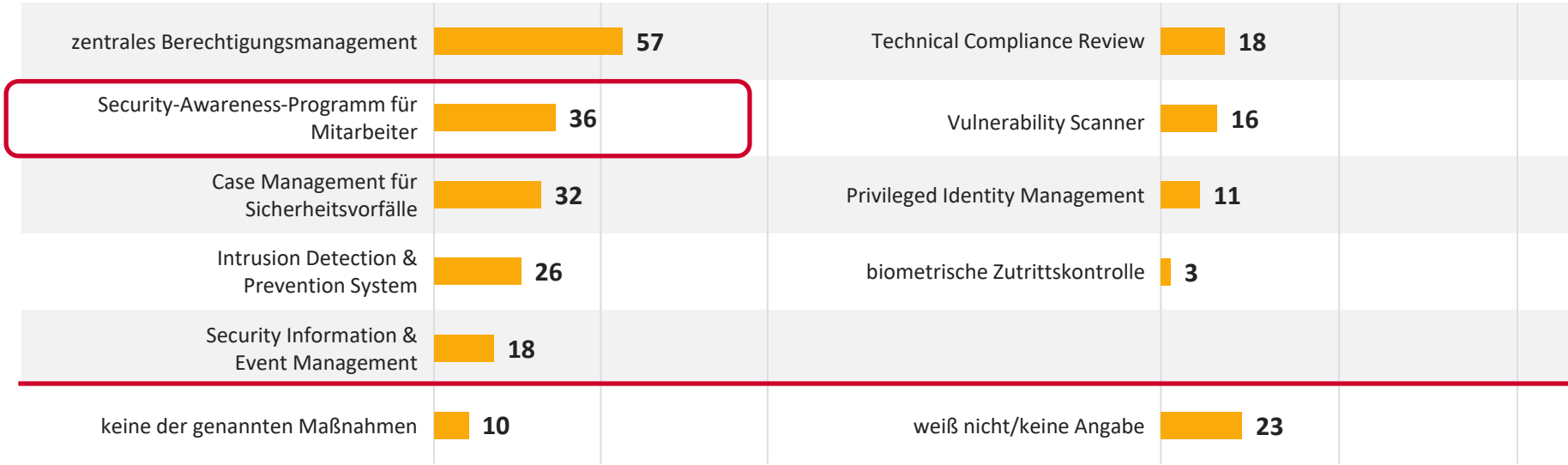


- … dürfen IT-Projekte nur bei Vorliegen eines IT-Sicherheitskonzepts gestartet werden.
- … muss ein IT-Sicherheitskonzept in einer bestimmten Frist nach Implementierung einer Anwendung oder eines IT-Systems vorliegen.
- … ist ein IT-Sicherheitskonzept für Anwendungen oder IT-Systeme nicht zwingend vorgeschrieben.
- weiß nicht/keine Angabe

Basis: alle Befragten; Angaben in Prozent

EIN DRITTEL DER BEFRAGTEN UNTERNEHMEN SENSIBILISIERT MITARBEITER FÜR DAS THEMA IT-SICHERHEIT

Welche IT-Sicherheitsmaßnahmen wurden in den vergangenen drei Jahren in Ihrem Unternehmen eingeführt?

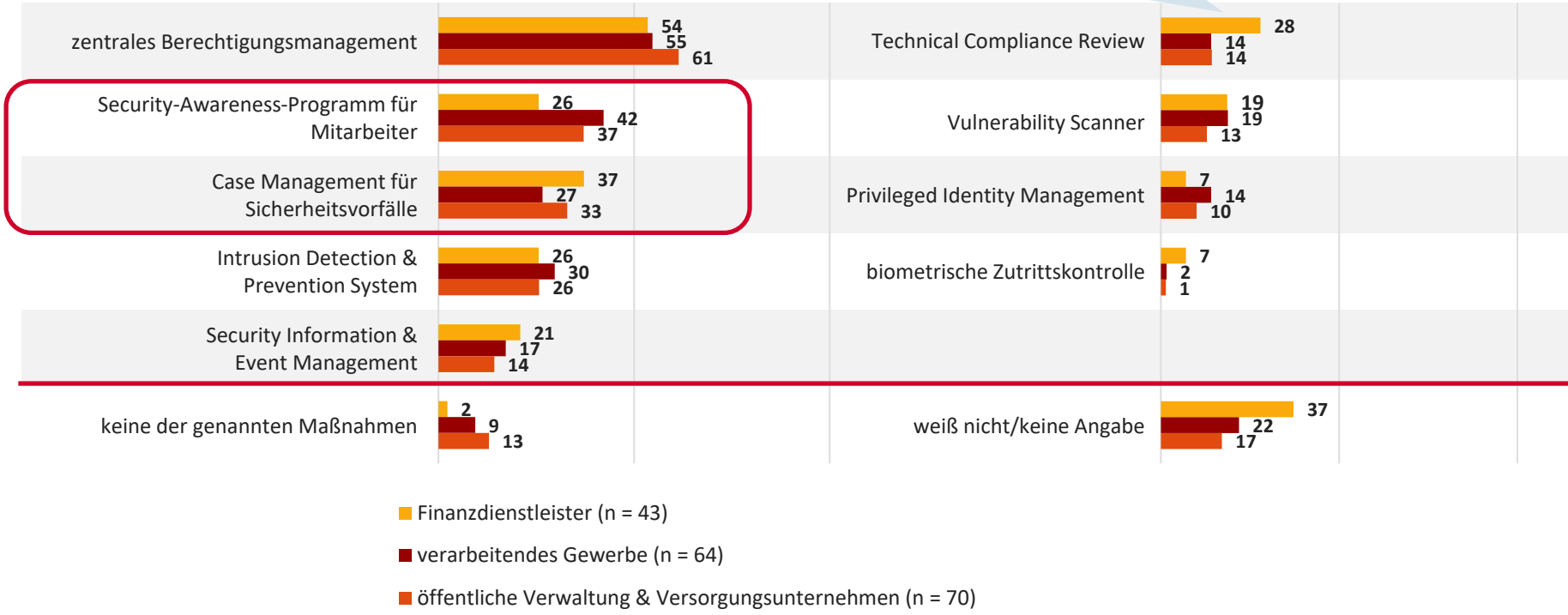


Basis: alle Befragten; n = 184;
Angaben in Prozent; Mehrfachantworten möglich

FINANZDIENSTLEISTER SETZEN SELTENER AUF SENSIBILISIERUNGS-KAMPAGNEN FÜR IHRE MITARBEITER, BETREIBEN ABER HÄUFIGER CASE MANAGEMENT FÜR SICHERHEITSVORFÄLLE

Welche IT-Sicherheitsmaßnahmen wurden in den vergangenen drei Jahren in Ihrem Unternehmen eingeführt?

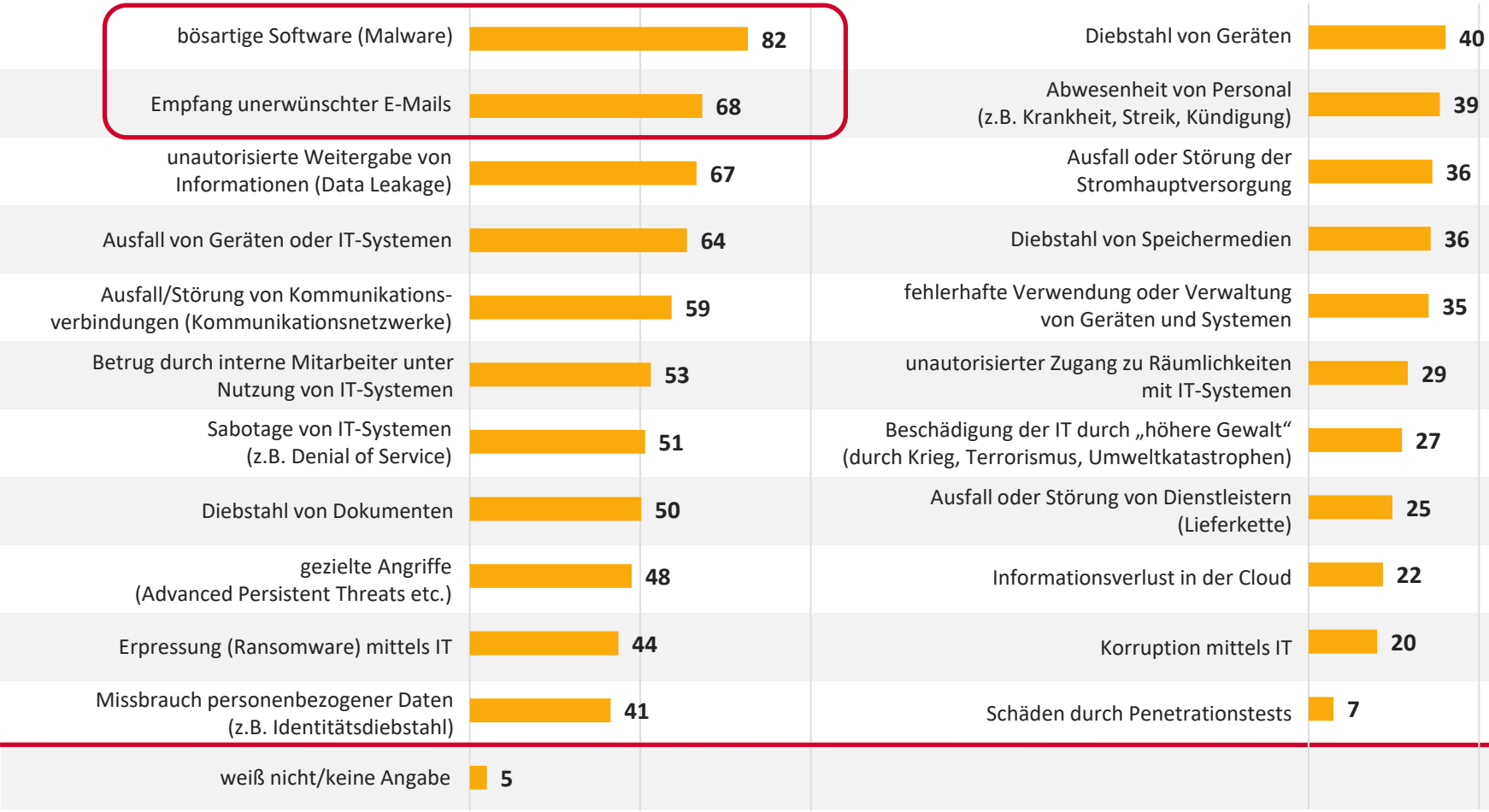
Vor allem im stark regulierten Finanzsektor spielt Compliance eine wichtige Rolle.



Basis: alle Befragten; Angaben in Prozent; Mehrfachantworten möglich

IM ALLTAGSGESCHÄFT DER BEFRAGTEN UNTERNEHMEN SIND VOR ALLEM MALWARE UND SPAM EIN PROBLEM

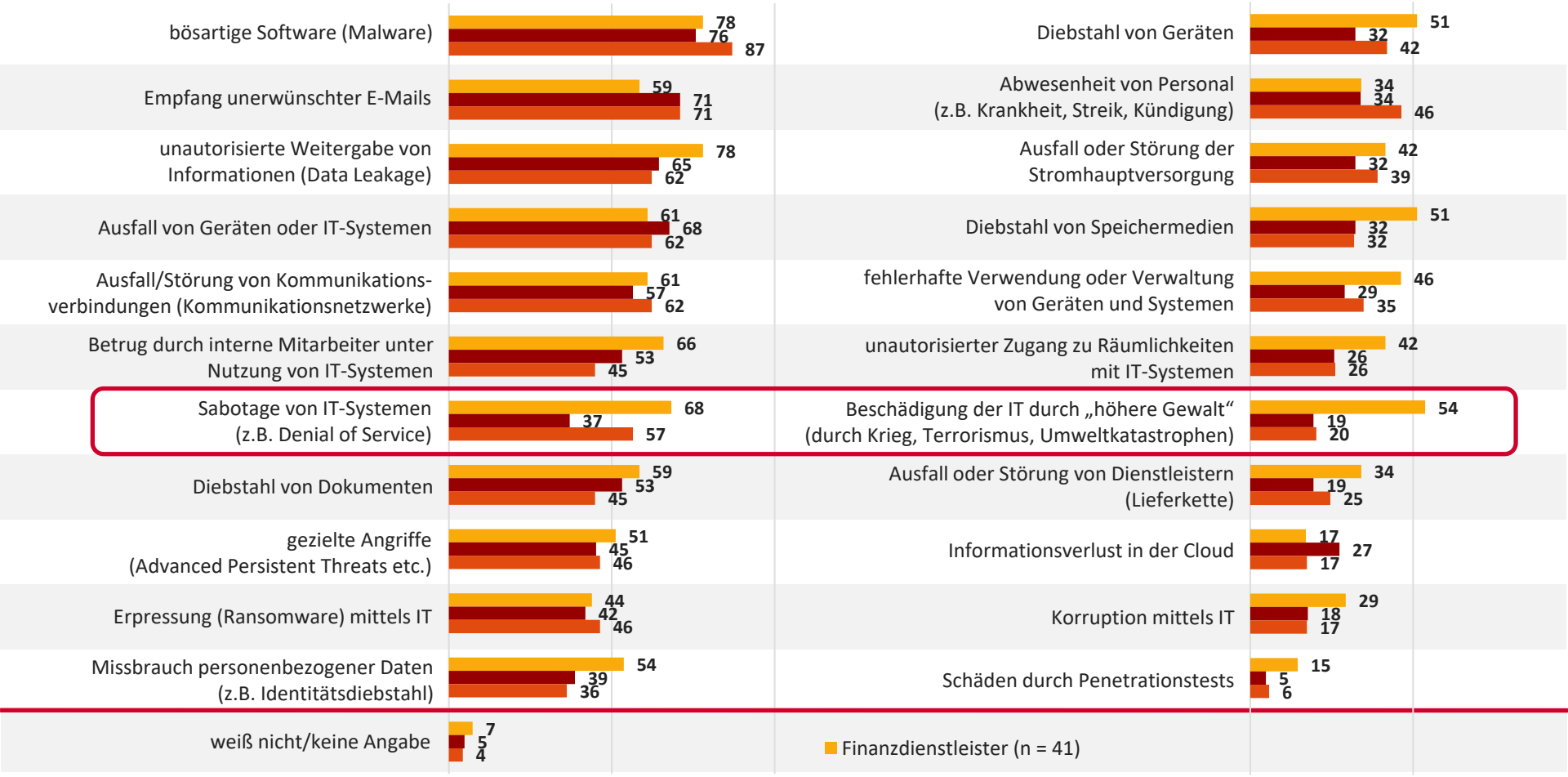
Welche Bedrohungsszenarien sind für Ihr Unternehmen relevant?



Basis: alle Befragten; n = 179;
Angaben in Prozent; Mehrfachantworten möglich

IM BRANCHENVERGLEICH IST DIE BEDROHUNG DER IT DURCH SABOTAGE UND „HÖHERE GEWALT“ FÜR FINANZDIENSTLEISTER AM RELEVANTESTEN

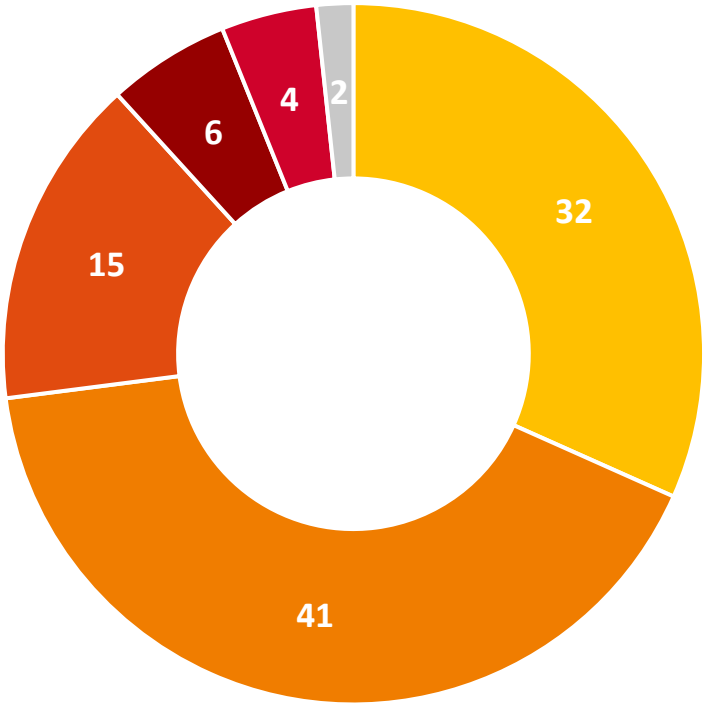
Welche Bedrohungsszenarien sind für Ihr Unternehmen relevant?



Basis: alle Befragten; Angaben in Prozent; Mehrfachantworten möglich

IN 73 PROZENT DER BEFRAGTEN UNTERNEHMEN KÜMMERN SICH AUSSCHLIEßLICH INTERNE MITARBEITER UM DIE IT-SICHERHEIT

Wer ist für die IT-Sicherheit in Ihrem Unternehmen verantwortlich?

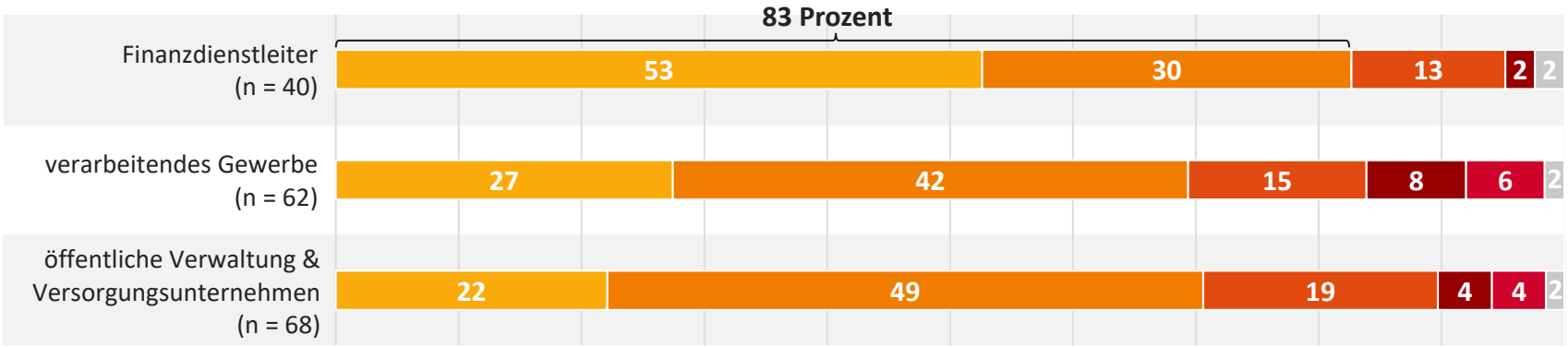


- Mitarbeiter aus interner, auf IT-Sicherheit spezialisierter Organisationseinheit
- Mitarbeiter aus interner IT-Abteilung
- externer Dienstleister, der durch unternehmenseigenen IT-Sicherheitsmanager unterstützt wird
- externer Dienstleister ohne Beteiligung unternehmenseigener Mitarbeiter
- Wir haben keinen Verantwortlichen für IT-Sicherheit in unserem Unternehmen.
- weiß nicht/keine Angabe

Basis: alle Befragten; n = 177;
Angaben in Prozent

FINANZDIENSTLEISTER SETZEN AM HÄUFIGSTEN AUF DAS UNTERNEHMENSINTERNE MANAGEMENT VON IT-SICHERHEIT

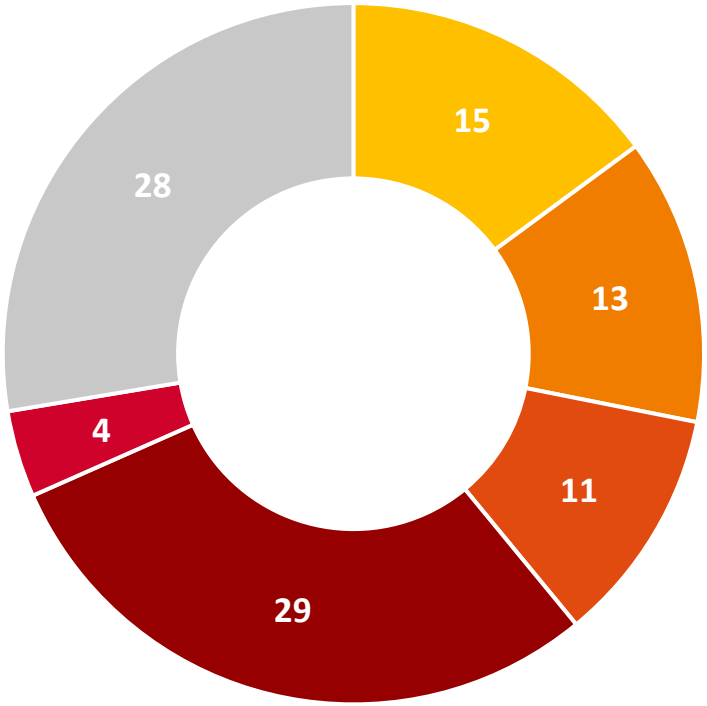
Wer ist für die IT-Sicherheit in Ihrem Unternehmen verantwortlich?



Basis: alle Befragten; Angaben in Prozent

MEHR ALS EIN DRITTEL HAT IN DEN VERGANGENEN ZWÖLF MONATEN MINDESTENS EINEN IT-SICHERHEITSVORFALL REGISTRIERT

Wie viele mit IT-Sicherheit in Verbindung stehende Vorfälle, die an Ihre Unternehmensleitung eskaliert werden mussten, wurden in den vergangenen zwölf Monaten in Ihrem Unternehmen registriert?

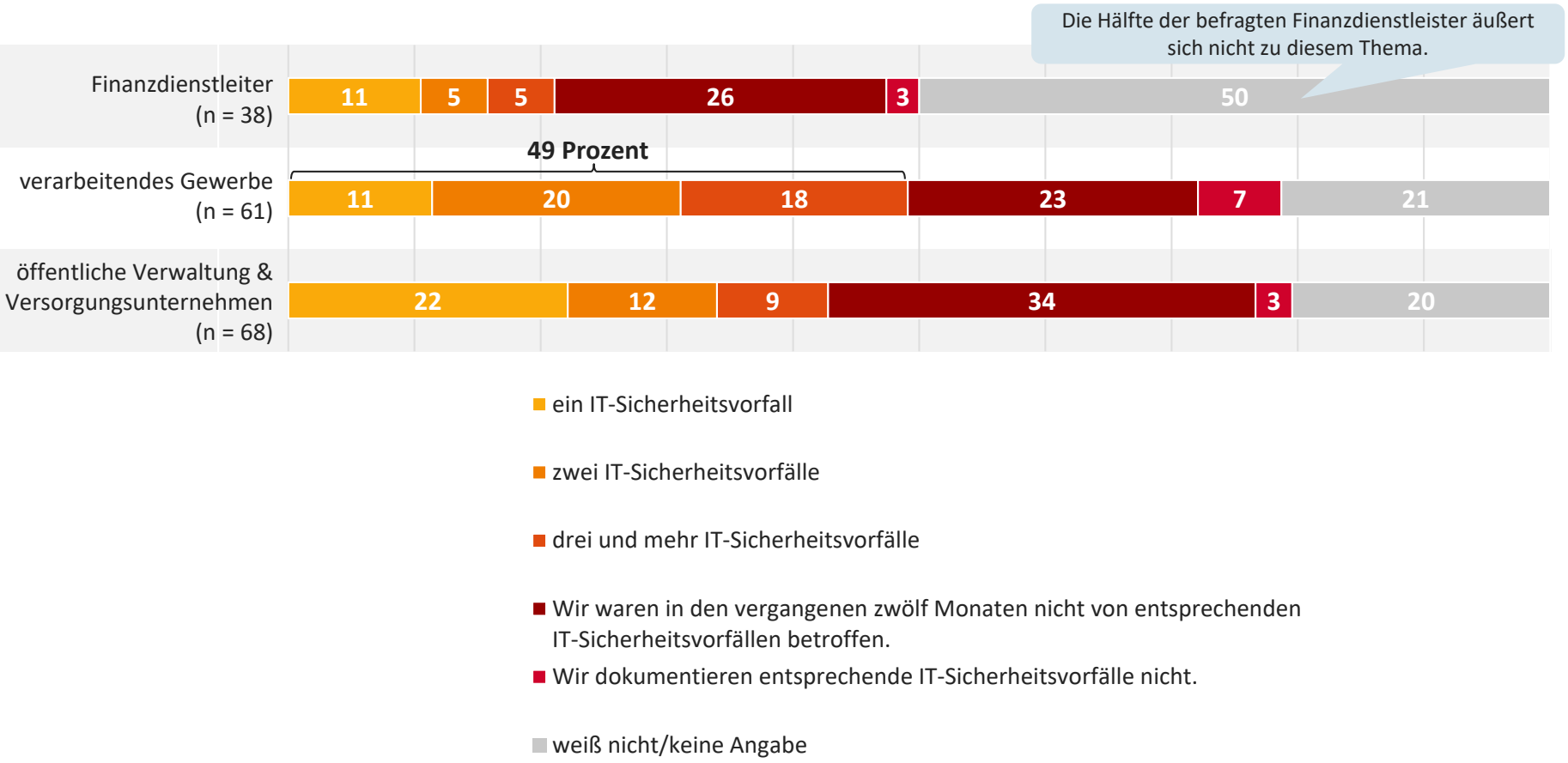


- ein IT-Sicherheitsvorfall
- zwei IT-Sicherheitsvorfälle
- drei und mehr IT-Sicherheitsvorfälle
- Wir waren in den vergangenen zwölf Monaten nicht von entsprechenden IT-Sicherheitsvorfällen betroffen.
- Wir dokumentieren entsprechende IT-Sicherheitsvorfälle nicht.
- weiß nicht/keine Angabe

Basis: alle Befragten; n = 174;
Angaben in Prozent

KNAPP DIE HÄLFTE DER BEFRAGTEN UNTERNEHMEN AUS DEM VERARBEITENDEN GEWERBE WAR VON MINDESTENS EINEM IT-SICHERHEITSVORFALL BETROFFEN

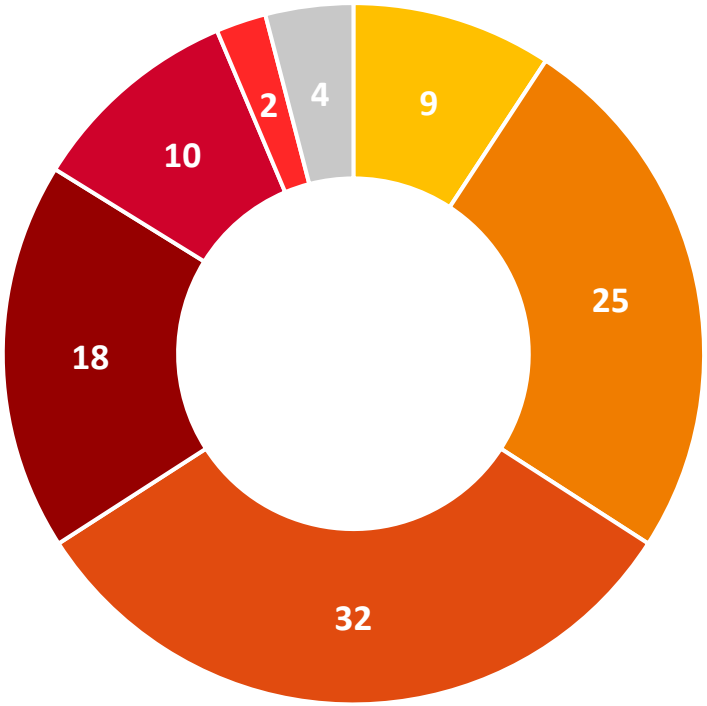
Wie viele mit IT-Sicherheit in Verbindung stehende Vorfälle, die an Ihre Unternehmensleitung eskaliert werden mussten, wurden in den vergangenen zwölf Monaten in Ihrem Unternehmen registriert?



Basis: alle Befragten; Angaben in Prozent

34 PROZENT SCHÄTZEN DAS RISIKO, OPFER EINER SCHWERWIEGENDEN CYBER-ATTACKE ZU WERDEN, ALS SEHR GERING BEZIEHUNGSWEISE GERING EIN

Wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen in den kommenden drei Jahren (2019-2021) von einer schwerwiegenden Cyber-Attacke betroffen sein wird?



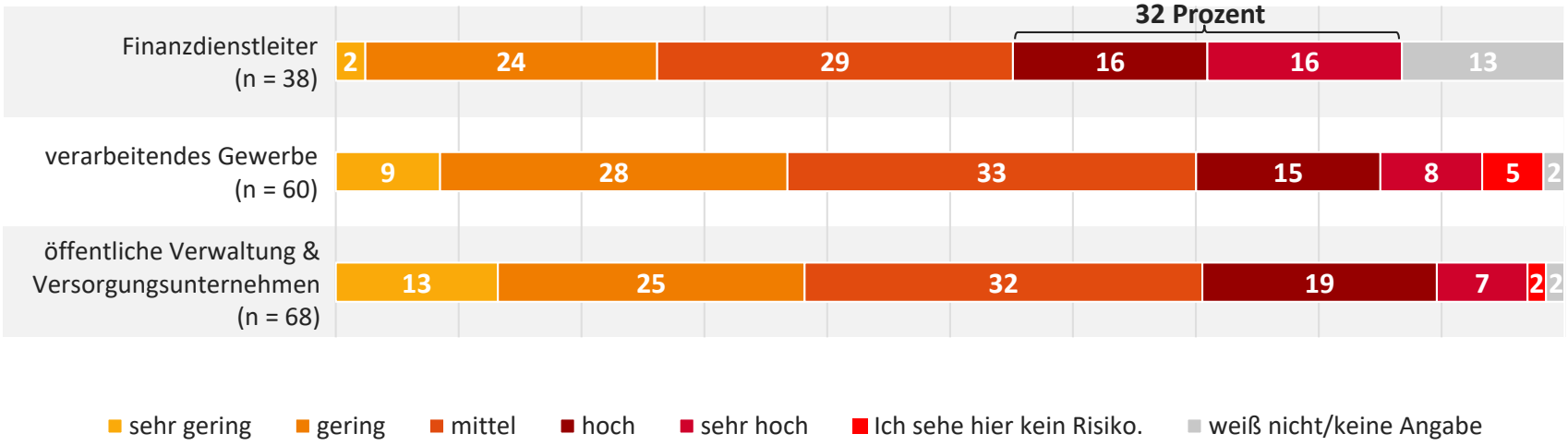
Eine Cyber-Attacke ist schwerwiegend, wenn sie einen erheblichen Reputationsschaden verursacht, zu einem Gesetzesverstoß des Unternehmens oder seines Managements führt oder einen bezifferbaren Schaden von mindestens 5% des Jahresumsatzes des Unternehmens verursacht.

- sehr gering
- gering
- mittel
- hoch
- sehr hoch
- Ich sehe hier kein Risiko.
- weiß nicht/keine Angabe

Basis: alle Befragten; n = 173;
Angaben in Prozent

KNAPP EIN DRITTEL DER FINANZDIENSTLEISTER PROGNOSTIZIERT EIN HOHES BEZIEHUNGSWEISE SEHR HOHES RISIKO FÜR DAS EIGENE UNTERNEHMEN

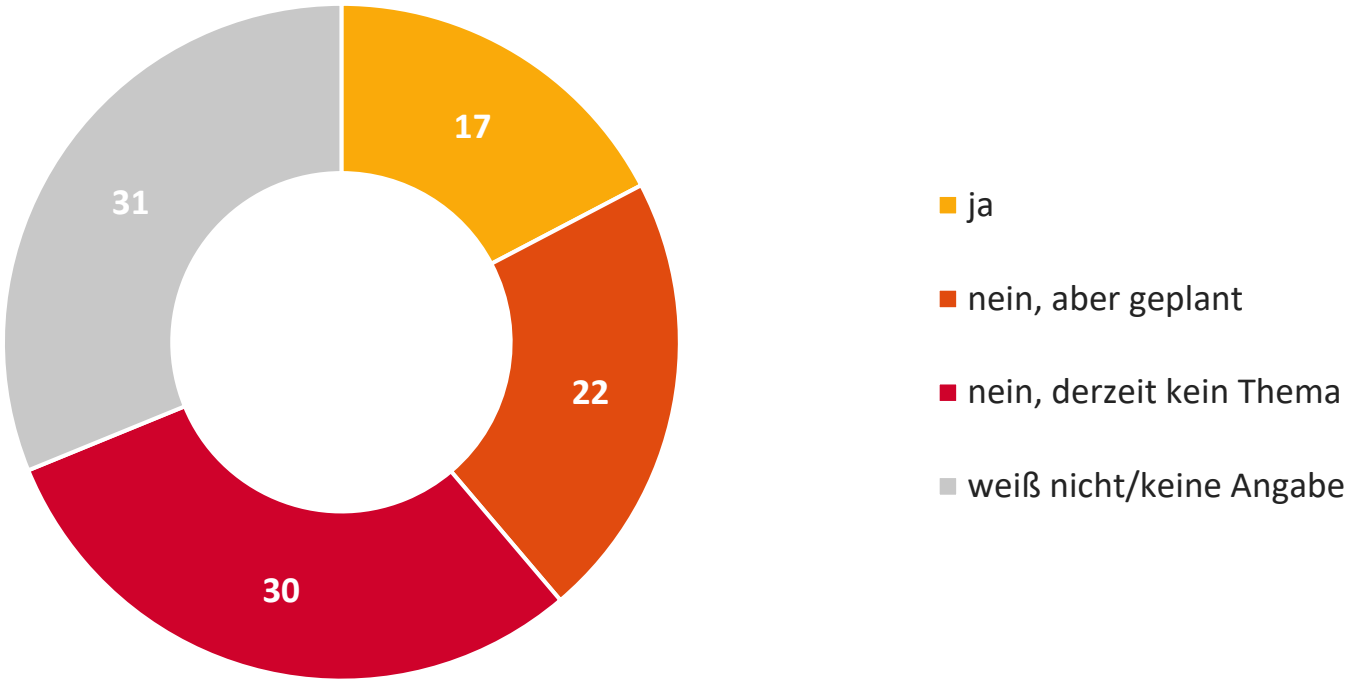
Wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen in den kommenden drei Jahren (2019-2021) von einer schwerwiegenden Cyber-Attacke betroffen sein wird?



Basis: alle Befragten; Angaben in Prozent

MÖGLICHE SCHÄDEN DURCH CYBER-VORFÄLLE WERDEN DERZEIT NOCH SELTEN VERSICHERT

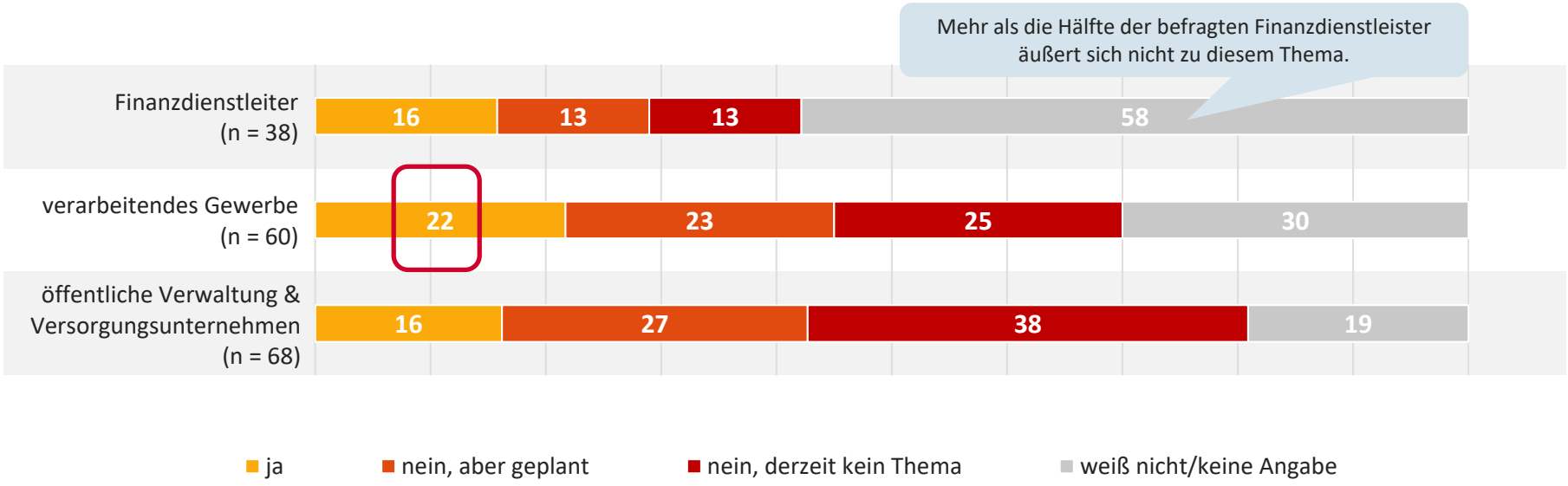
Versichert Ihr Unternehmen gegenwärtig durch Cyber-Vorfälle verursachte Schäden?



Basis: alle Befragten; n = 173;
Angaben in Prozent

DAS VERARBEITENDE GEWERBE HAT BISLANG AM HÄUFIGSTEN CYBER-VERSICHERUNGEN ABGESCHLOSSEN

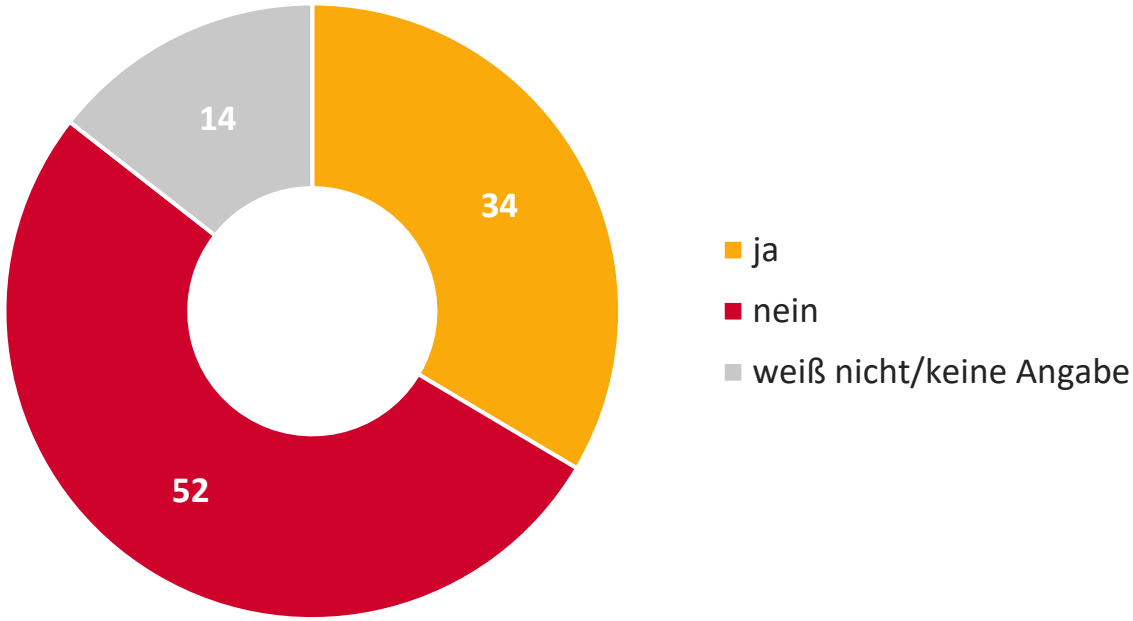
Versichert Ihr Unternehmen gegenwärtig durch Cyber-Vorfälle verursachte Schäden?



Basis: alle Befragten; Angaben in Prozent

EIN DRITTEL DER BEFRAGTEN UNTERNEHMEN WAR IN DEN VERGANGENEN ZWÖLF MONATEN OPFER EINES CYBER-ANGRIFFS

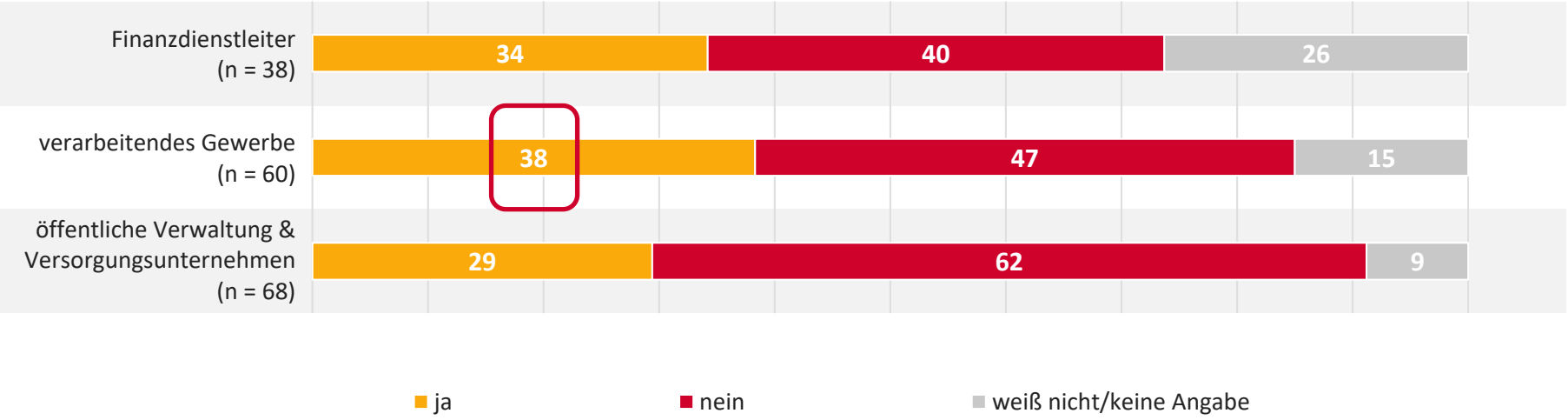
War Ihr Unternehmen in den vergangenen zwölf Monaten von einem Cyber-Angriff betroffen?



Basis: alle Befragten; n = 173;
Angaben in Prozent

DAS VERARBEITENDE GEWERBE WAR IM BRANCHENVERGLEICH AM HÄUFIGSTEN VON CYBER-ANGRIFFEN BETROFFEN

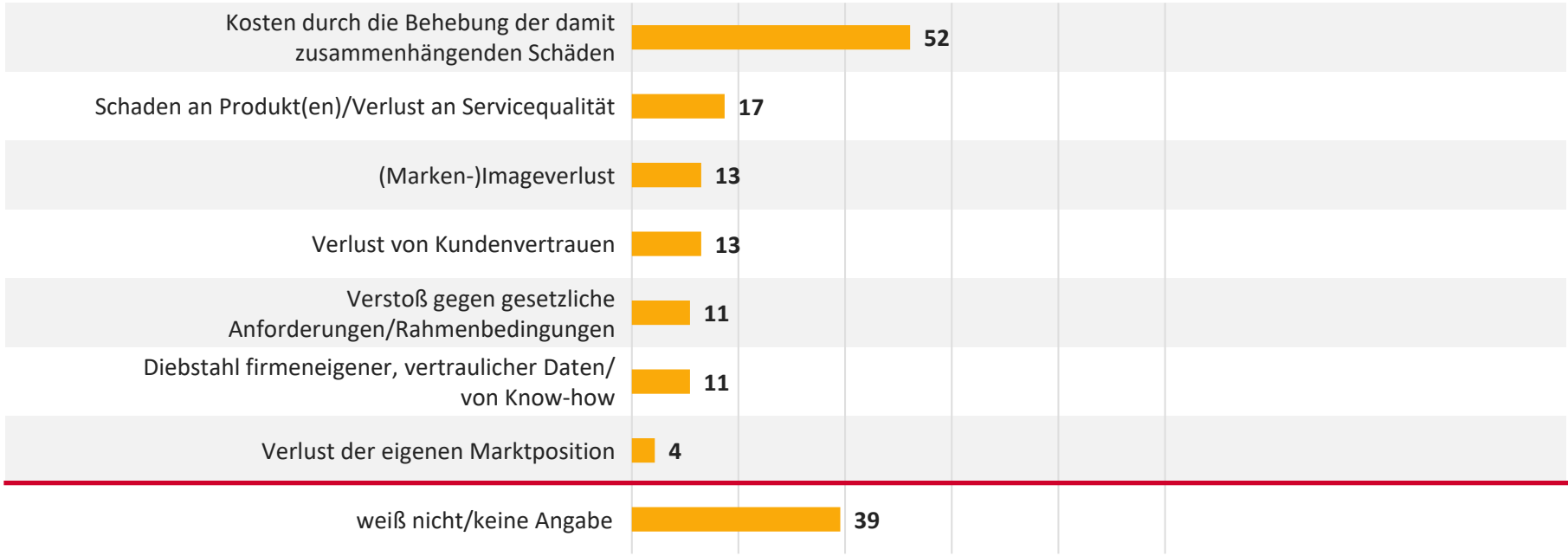
War Ihr Unternehmen in den vergangenen zwölf Monaten von einem Cyber-Angriff betroffen?



Basis: alle Befragten; Angaben in Prozent

CYBER-ANGRIFFE VERURSACHTEN VOR ALLEM FINANZIELLEN SCHADEN

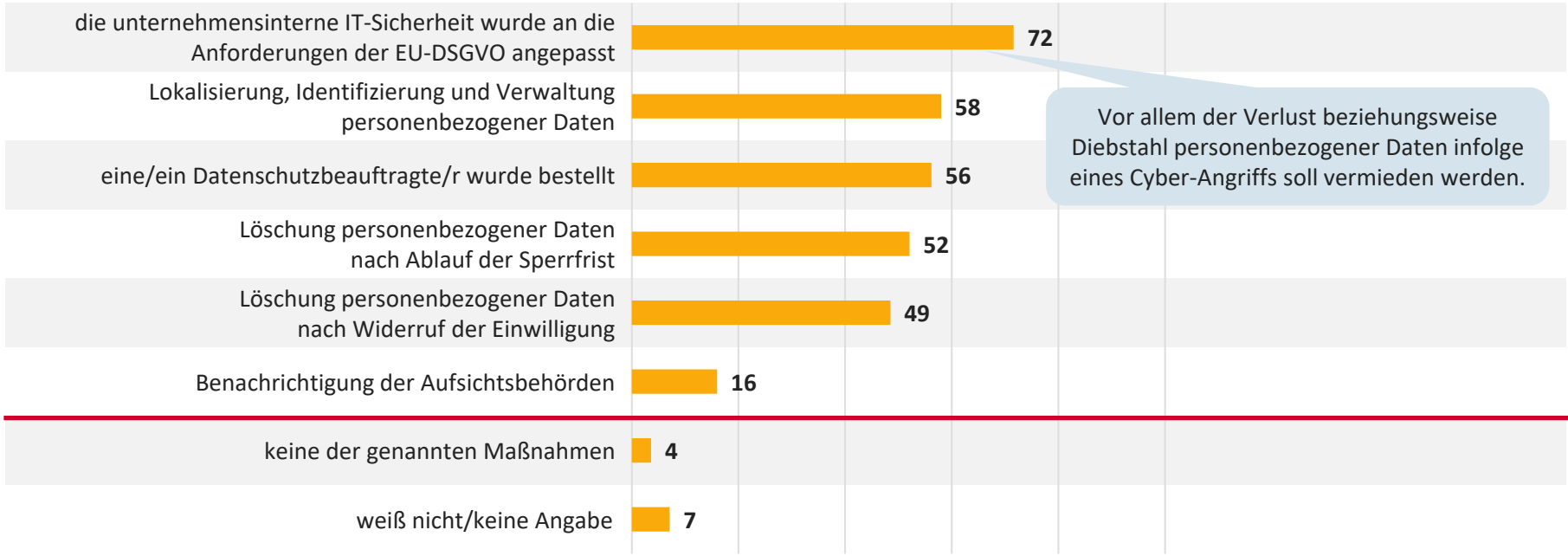
Welche Folgen hatte dieser Cyber-Angriff für Ihr Unternehmen?



Basis: alle Befragten, deren Unternehmen in den vergangenen zwölf Monaten von einem Cyber-Angriff betroffen war; n = 46; Angaben in Prozent; Mehrfachantworten möglich

DIE MEHRHEIT HAT EINE VIELZAHL AN MAßNAHMEN ERGRIFFEN, DIE KONFORMITÄT MIT DER EU-DSGVO GEWÄHRLEISTEN SOLLEN

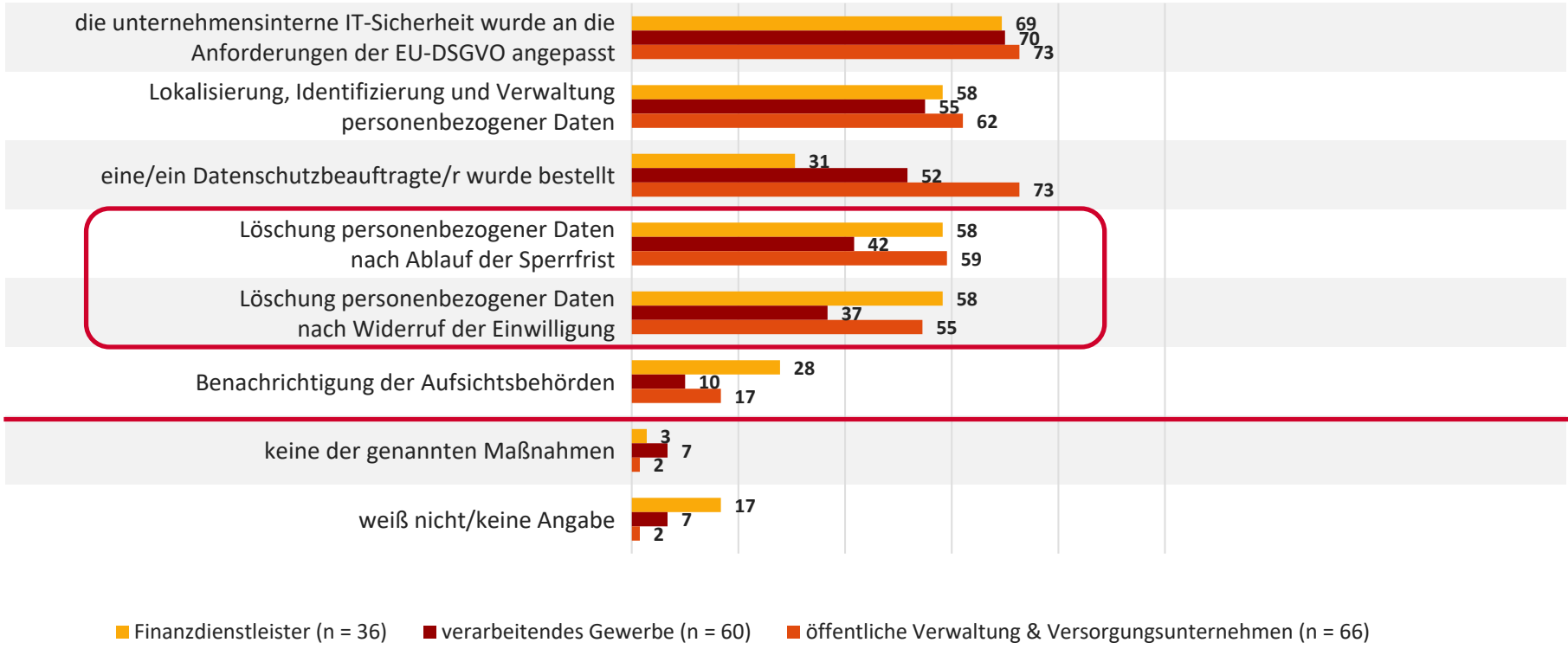
Welche Maßnahmen hat Ihr Unternehmen seit der Einführung der EU-DSGVO am 25. Mai 2018 ergriffen?



Basis: alle Befragten; n = 169;
Angaben in Prozent; Mehrfachantworten möglich

DAS VERARBEITENDE GEWERBE HAT AM SELTENESTEN EU-DSGVO-KONFORME LÖSCHUNGSPRAKTIKEN ETABLIERT

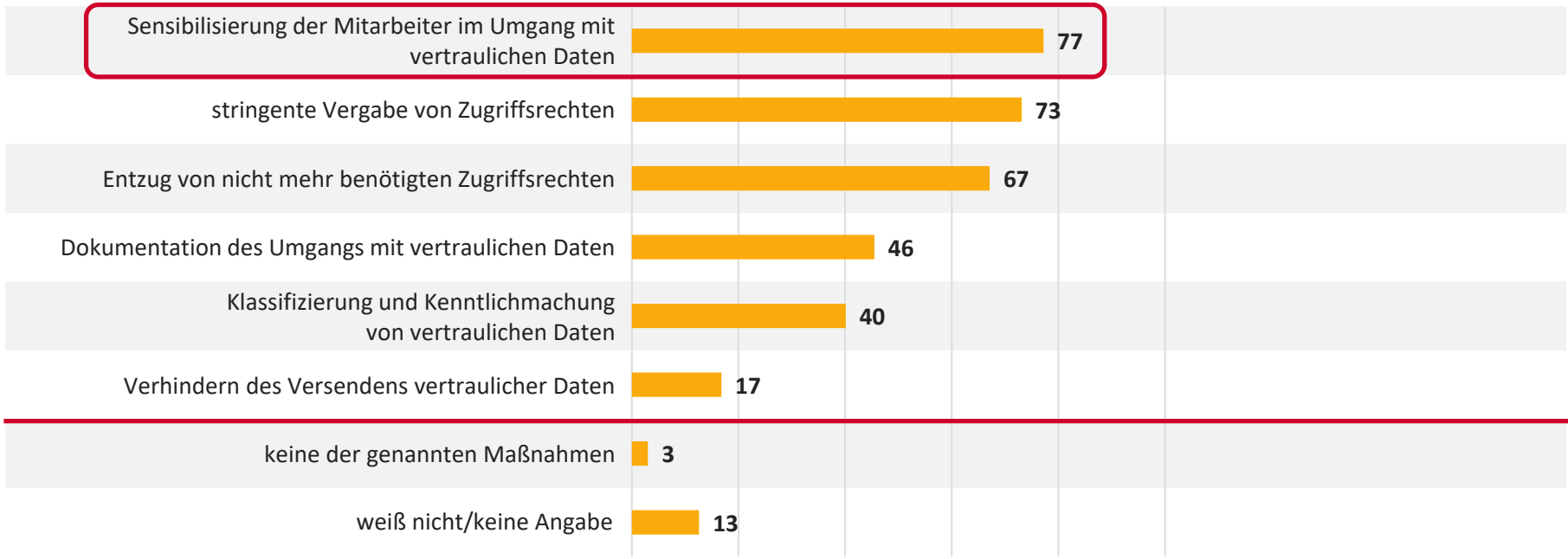
Welche Maßnahmen hat Ihr Unternehmen seit der Einführung der EU-DSGVO am 25. Mai 2018 ergriffen?



Basis: alle Befragten;
Angaben in Prozent; Mehrfachantworten möglich

MEHR ALS DREI VIERTEL DER BEFRAGTEN UNTERNEHMEN SETZEN AUF DIE SENSIBILISIERUNG DER MITARBEITER ALS PRÄVENTIONSMAßNAHME GEGEN DATA LEAKAGE

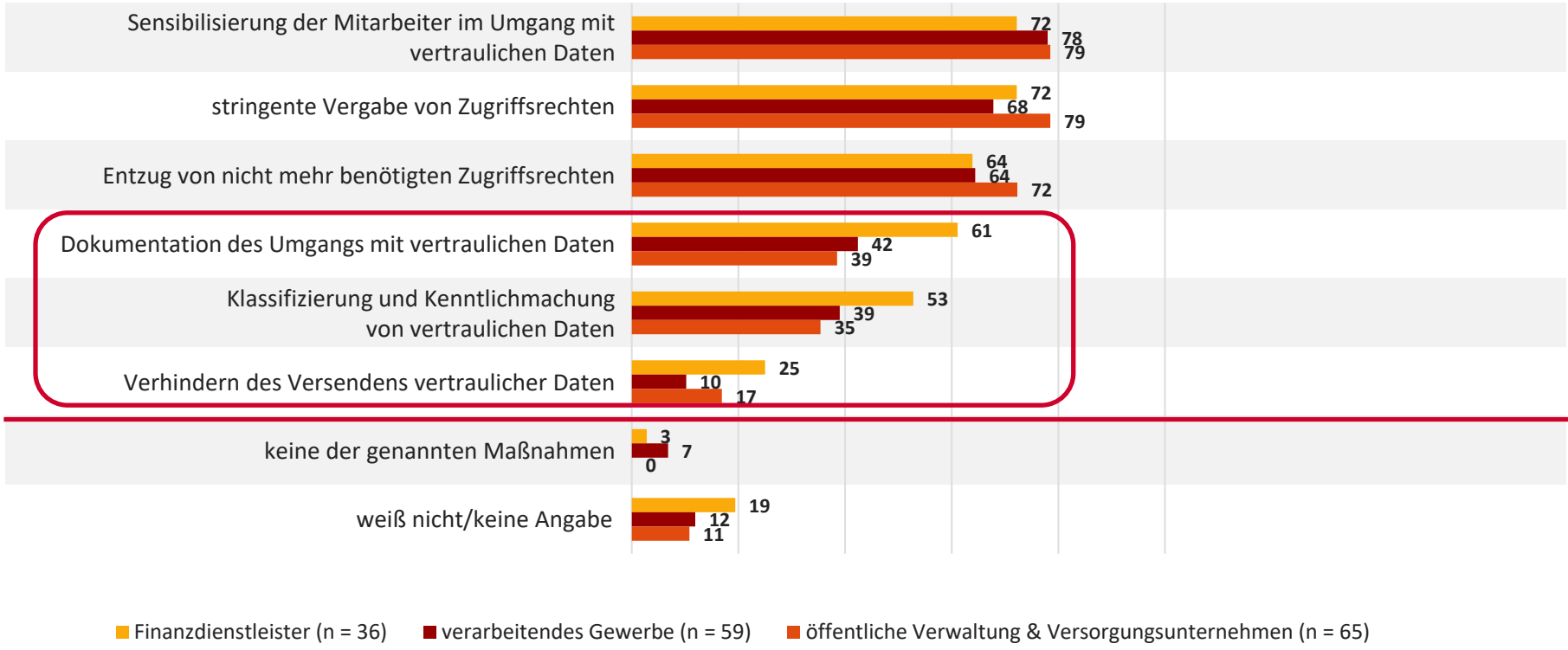
Welche Maßnahmen ergreift Ihr Unternehmen zur Data Leakage Prevention (Schutz vor dem Abfluss vertraulicher, sensibler Daten an Unbefugte)?



Basis: alle Befragten; n = 167;
Angaben in Prozent; Mehrfachantworten möglich

DER UMGANG MIT VERTRAULICHEN DATEN WIRD INSBESONDERE VON FINANZDIENSTLEISTERN DURCH KONKRETE MAßNAHMEN GEREGELT

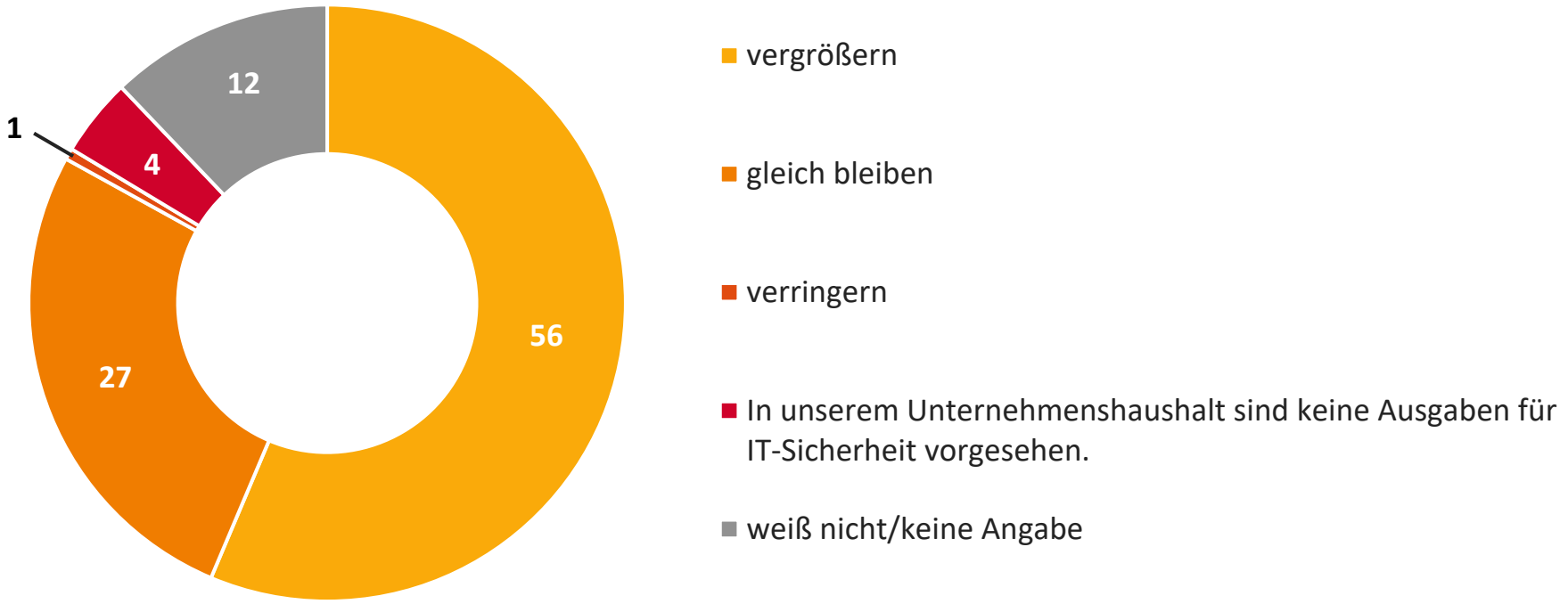
Welche Maßnahmen ergreift Ihr Unternehmen zur Data Leakage Prevention (Schutz vor dem Abfluss vertraulicher, sensibler Daten an Unbefugte)?



Basis: alle Befragten;
Angaben in Prozent; Mehrfachantworten möglich

MEHR ALS DIE HÄLFTE DER BEFRAGTEN ERWARTET FÜR DIE KOMMENDEN DREI JAHRE EINE STEIGERUNG DES BUDGETS FÜR IT-SICHERHEIT IN IHREM UNTERNEHMEN

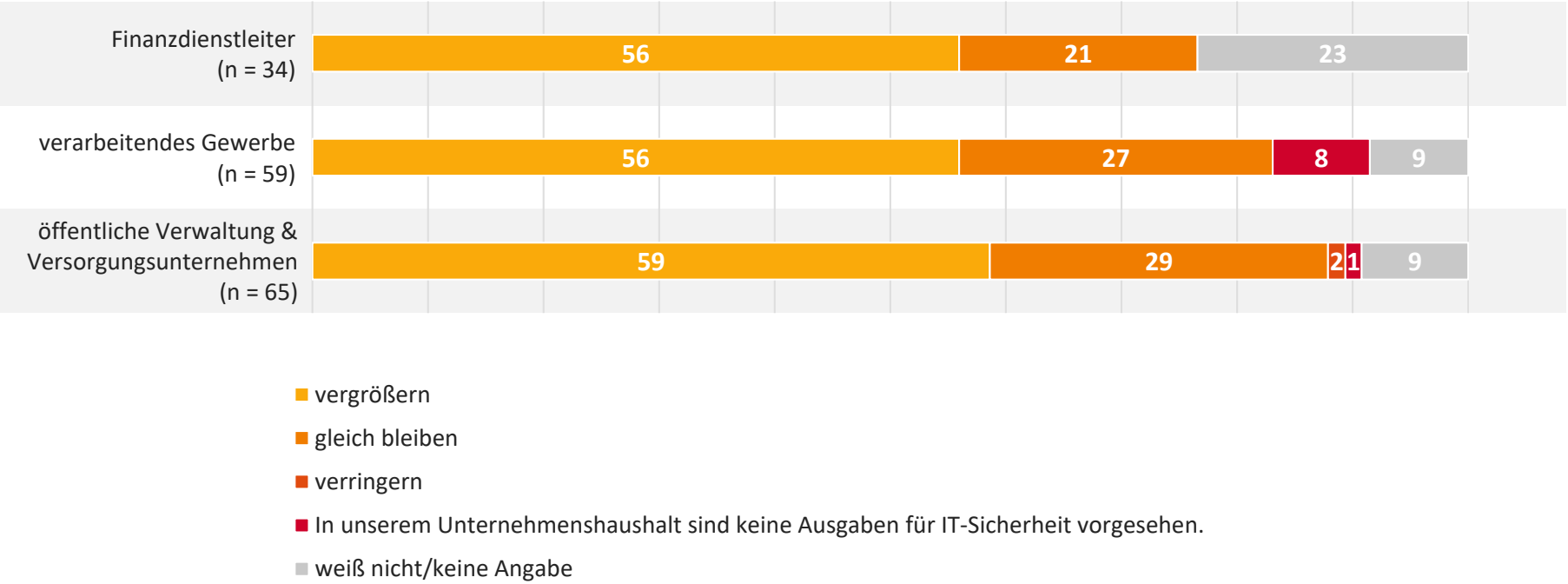
Wie wird sich das Budget Ihres Unternehmens für IT-Sicherheit in den kommenden drei Jahren (2019-2021) verändern?



Basis: alle Befragten; n = 165;
Angaben in Prozent

IT-SICHERHEIT GEWINNT AN BEDEUTUNG – BRANCHEN-ÜBERGREIFEND VOR ALLEM STEIGENDE BUDGETS ERWARTET

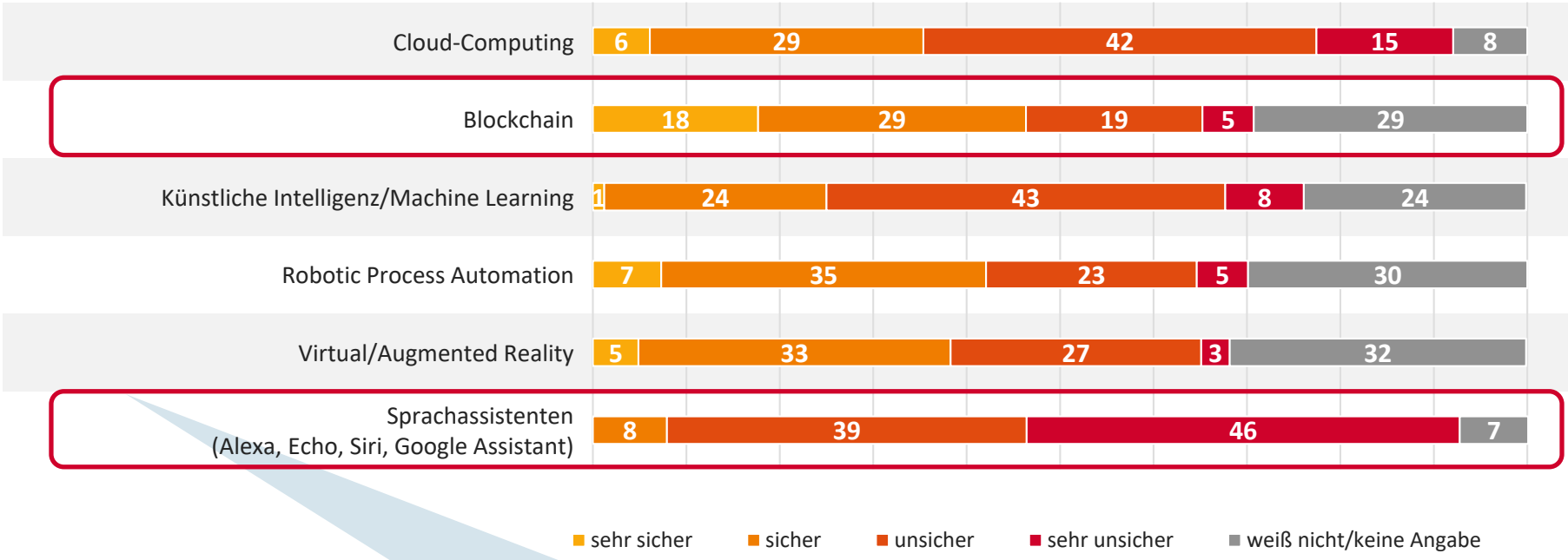
Wie wird sich das Budget Ihres Unternehmens für IT-Sicherheit in den kommenden drei Jahren (2019-2021) verändern?



Basis: alle Befragten; Angaben in Prozent

BLOCKCHAIN WIRD AM HÄUFIGSTEN ALS SICHER EINGESTUFT, SPRACHASSISTENTEN GELTEN EHER ALS UNSICHERE TECHNOLOGIE

Wie sicher stufen Sie folgende Technologien ein?

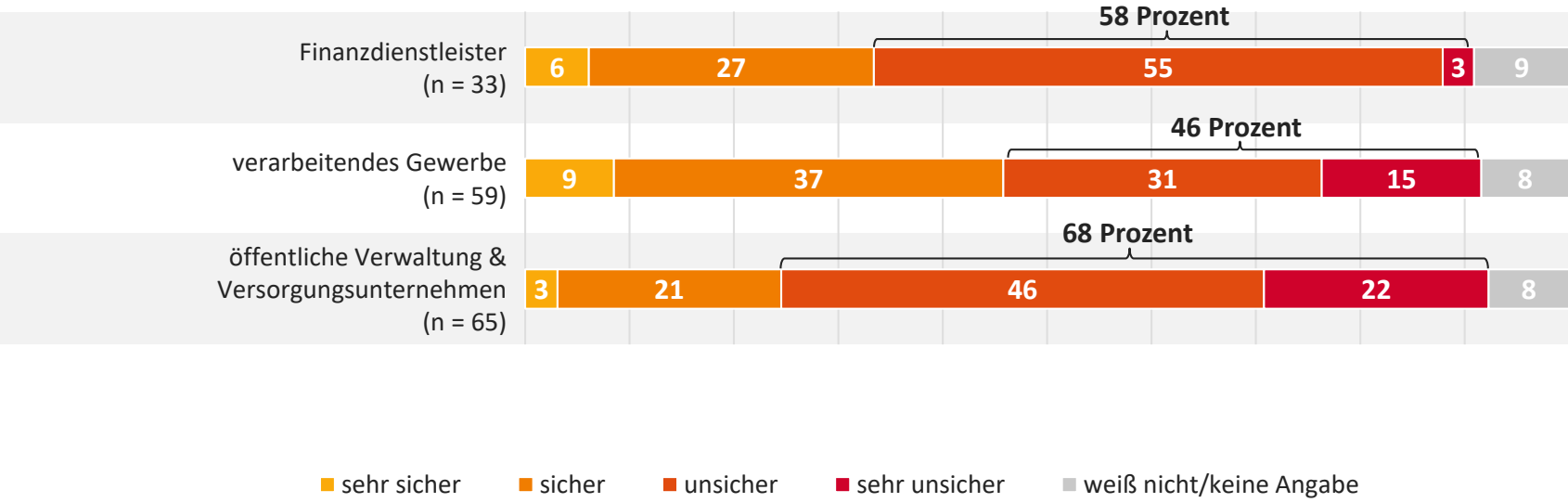


Die hier abgebildeten Ergebnisse geben die persönlichen Ansichten der Befragten in akkumulierter Form wieder. Neue Technologien können Skepsis und Unsicherheit hervorrufen. Umso wichtiger ist eine sachorientierte Aufklärung über Chancen und Risiken im Zusammenhang mit ihrer Nutzung.

Basis: alle Befragten; n = 164;
Angaben in Prozent

INSBESONDERE DIE MEHRHEIT DER ÖFFENTLICHEN VERWALTUNG & VERSORGUNGSUNTERNEHMEN ZWEIFELT DIE SICHERHEIT VON CLOUD-COMPUTING AN

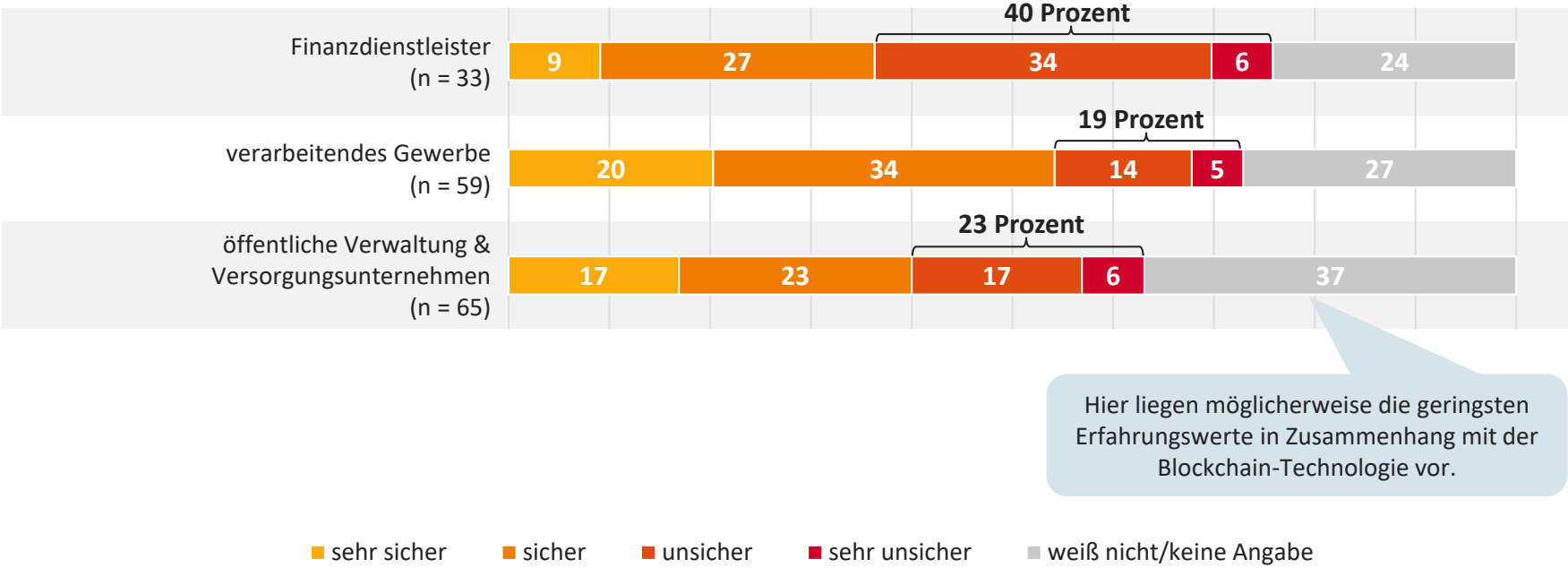
Wie sicher stufen Sie das **Cloud-Computing** ein?



Basis: alle Befragten; Angaben in Prozent

FINANZDIENSTLEISTER ÄUßERN SKEPSIS GEGENÜBER BLOCKCHAIN – VIER VON ZEHN STUFEN DIE TECHNOLOGIE ALS UNSICHER EIN

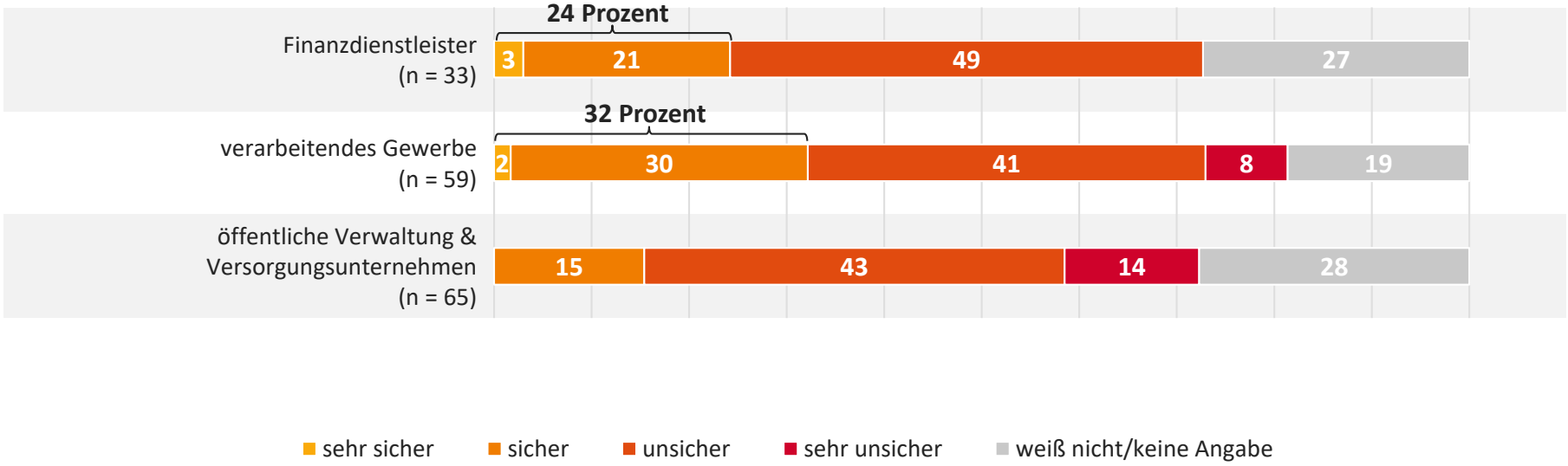
Wie sicher stufen Sie die **Blockchain** ein?



Basis: alle Befragten; Angaben in Prozent

KNAPP EIN DRITTEL DER BEFRAGTEN AUS DEM VERARBEITENDEN GEWERBE NIMMT KÜNSTLICHE INTELLIGENZ/MACHINE LEARNING ALS SICHER WAHR

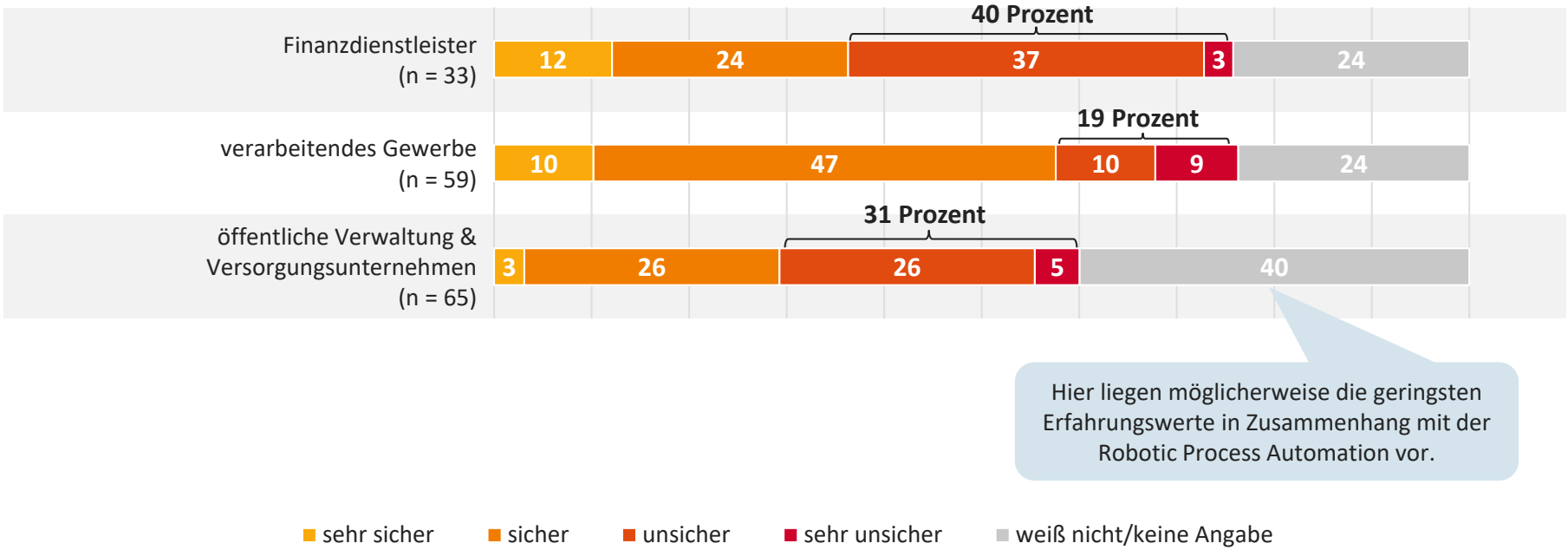
Wie sicher stufen Sie **Künstliche Intelligenz/Machine Learning** ein?



Basis: alle Befragten; Angaben in Prozent

40 PROZENT DER BEFRAGTEN FINANZDIENSTLEISTER STUFEN ROBOTIC PROCESS AUTOMATION ALS UNSICHER EIN

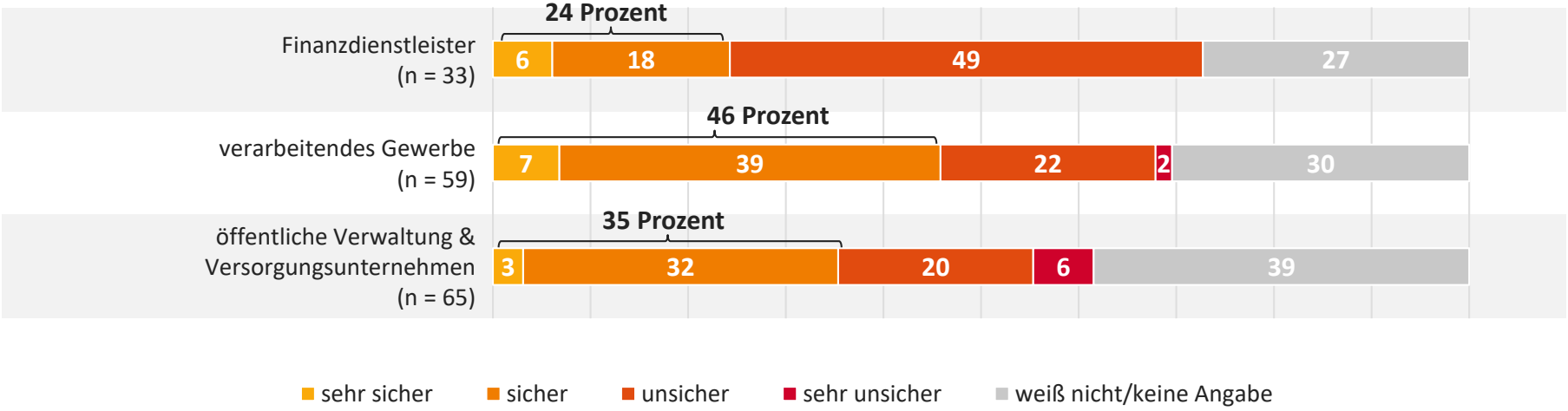
Wie sicher stufen Sie **Robotic Process Automation** ein?



Basis: alle Befragten; Angaben in Prozent

VIRTUAL/AUGMENTED REALITY HAT VOR ALLEM ANWENDUNGSPOTENZIAL IM VERARBEITENDEN GEWERBE: 46 PROZENT DER BEFRAGTEN AUS DIESER BRANCHE STUFEN DIE TECHNOLOGIE ALS SICHER EIN

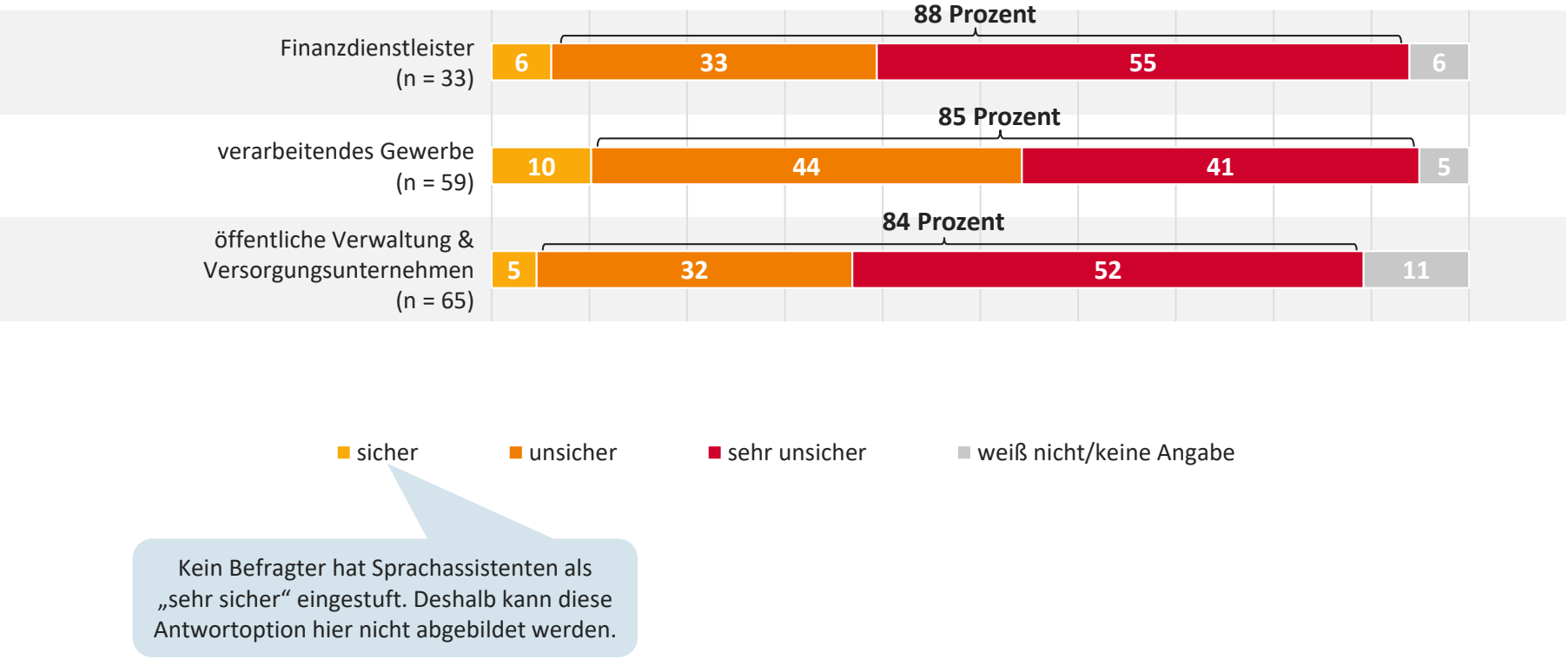
Wie sicher stufen Sie **Virtual/Augmented Reality** ein?



Basis: alle Befragten; Angaben in Prozent

BRANCHENÜBERGREIFENDE EINIGKEIT: MEHR ALS 80 PROZENT DER BEFRAGTEN STUFEN SPRACHASSISTENTEN ALS UNSICHER BEZIEHUNGSWEISE SEHR UNSICHER EIN

Wie sicher stufen Sie **Sprachassistenten (Alexa, Echo, Siri, Google Assistant)** ein?



Kein Befragter hat Sprachassistenten als „sehr sicher“ eingestuft. Deshalb kann diese Antwortoption hier nicht abgebildet werden.

Basis: alle Befragten; Angaben in Prozent