

FORENSIC

e-Crime-Studie 2010

Computerkriminalität in der deutschen Wirtschaft

Dr. Stefan Weiss
Goethe-Universität, Frankfurt am Main
18. Januar 2011

RISK & COMPLIANCE

Agenda

Kurzüberblick KPMG

e-Crime Studie 2010 – Computerkriminalität in Deutschland

Diskussion und Fragen

Unser Name

KPMG – diese Buchstaben stehen für die Initialen der
Gründer:

Klynveld

Peat

Marwick

Goerdeler

Netzwerk rechtlich selbstständiger, nationaler Firmen mit über 140.000 Mitarbeitern in 144 Ländern

20,11 Mrd. US-Dollar Umsatz im Jahr 2009

EMA 54 %

Americas 31 %

ASPAC 15 %

Rund 7.950 Partner

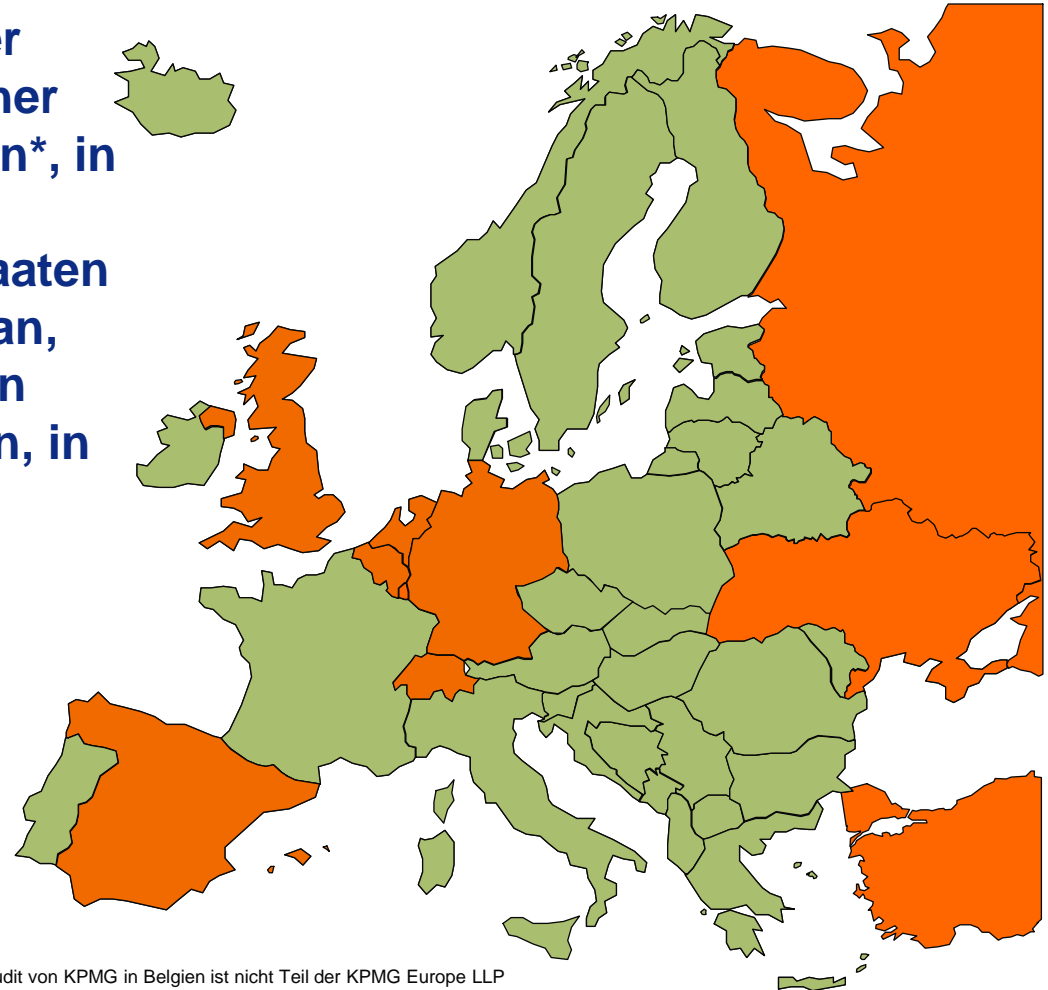
Einheitliche Struktur nach Geschäftsbereichen und Branchen weltweit

KPMG Europe LLP

Zusammenschluss europäischer Mitgliedsfirmen unter einheitlicher Leitung, derzeit KPMG in Belgien*, in Deutschland, in Teilen der Gemeinschaft unabhängiger Staaten (Armenien, Georgien, Kasachstan, Kirgistan, Russland, Ukraine), in Luxemburg, in den Niederlanden, in der Schweiz, in Spanien, in der Türkei und in UK

Rund 31.000 Mitarbeiter an 110 Standorten

4,5 Mrd. Euro Umsatz 2009**



* Der Geschäftsbereich Audit von KPMG in Belgien ist nicht Teil der KPMG Europe LLP

** Pro-forma-Zahl, die die Umsätze aller Mitgliedsgesellschaften der KPMG Europe LLP berücksichtigt

KPMG in Deutschland

Eines der führenden Wirtschaftsprüfungs- und Beratungsunternehmen

1,25 Mrd. Euro Umsatz in 2009

8.416 Mitarbeiter (zum 31.10.2009)

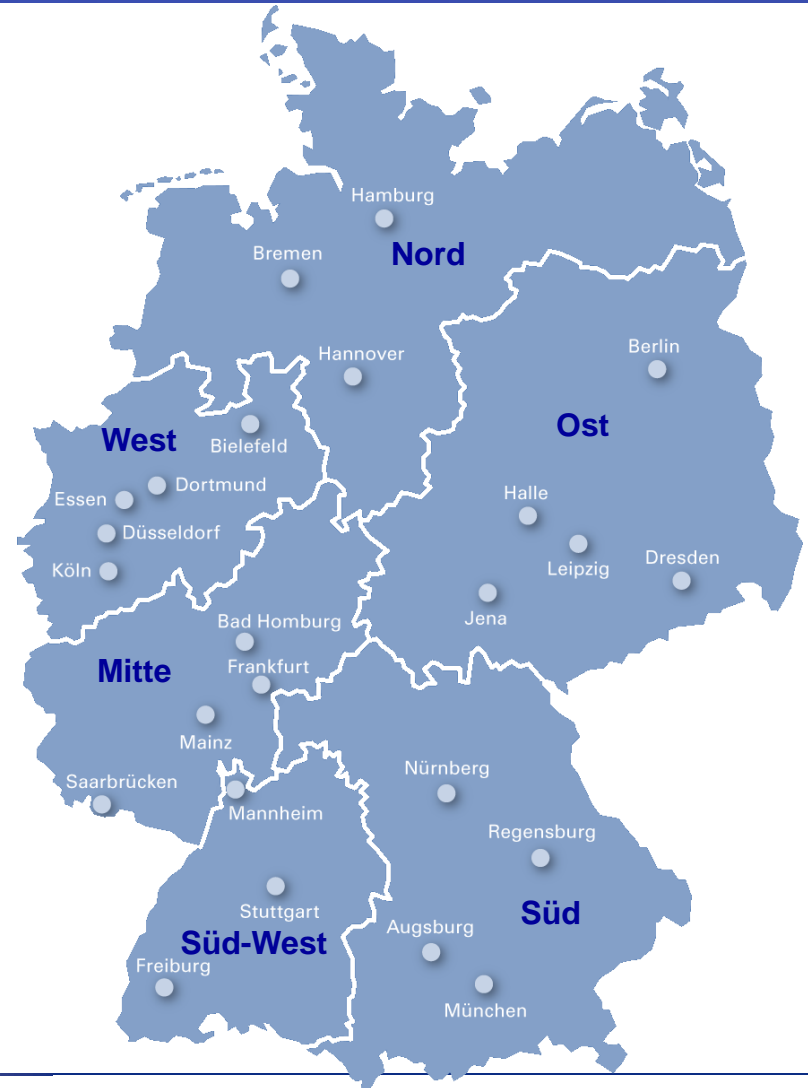
Marktanteile im Bereich Wirtschaftsprüfung (Audit)* in bekannten Indizes börsennotierter deutscher Unternehmen:

DAX30:	60 %
MDAX:	33 %
SDAX:	10 %
TecDax:	23 %

* Stand: 28. Oktober 2009; Quelle: KPMG Market & Competitor Insights

KPMG in Deutschland

Mit über 24 Standorten in sechs
Regionen sind wir in der Nähe
unserer Mandanten



Unsere Geschäftsbereiche

KPMG ist ein multidisziplinäres Unternehmen mit den Geschäftsbereichen

▶ Audit

▶ Tax

▶ Advisory

Advisory – Risk & Compliance

Internal Audit, Risk & Compliance

Forensic

IT Advisory

Financial Risk Management

Accounting Advisory

“We protect and enhance value”

Risk & Compliance – Unsere Referenzen

Allianz 



british midland
bmi



COMMERZBANK 

DAIMLER

„DekaBank

■ ■ T Deutsche Telekom

 DZ BANK

— EnBW

e-on



 Finanzgruppe

freenet 

HESSEN



Hypo  Real Estate
GROUP

IBM

LB  BW



METRO

NÜRNBERGER



LUK  FAG
SCHAEFFLER GROUP

SIEMENS

tal anx.


UniCredito Italiano

VATTENFALL 

 WestLB

Risk & Compliance – Thought Leadership



**Studie 2010
Wirtschaftskriminalität
in Deutschland**



**Data Loss Barometer
Issue 2**



**2009 European
Identity and Access
Management Survey**

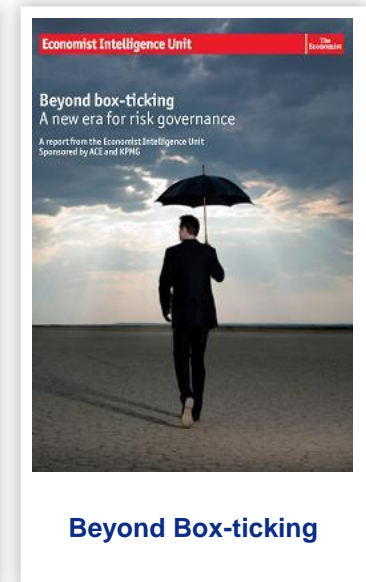
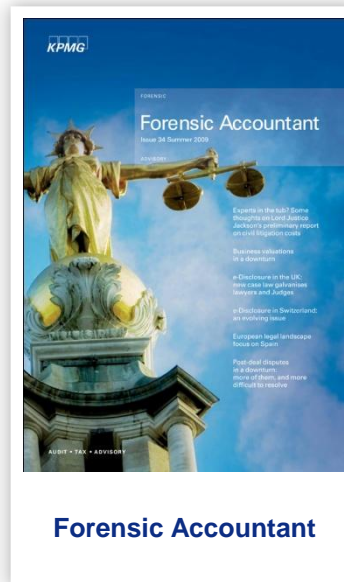
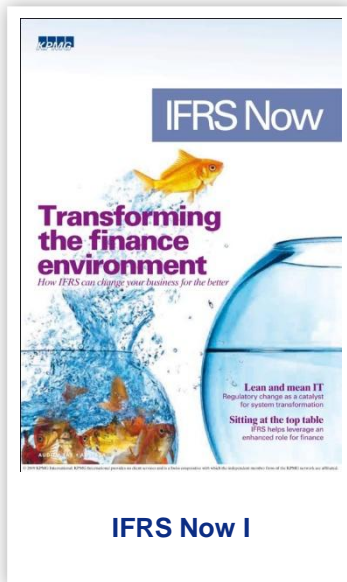


**KPMG Handbuch zur
Nachhaltigkeitsberichter-
stattung 2008/09**



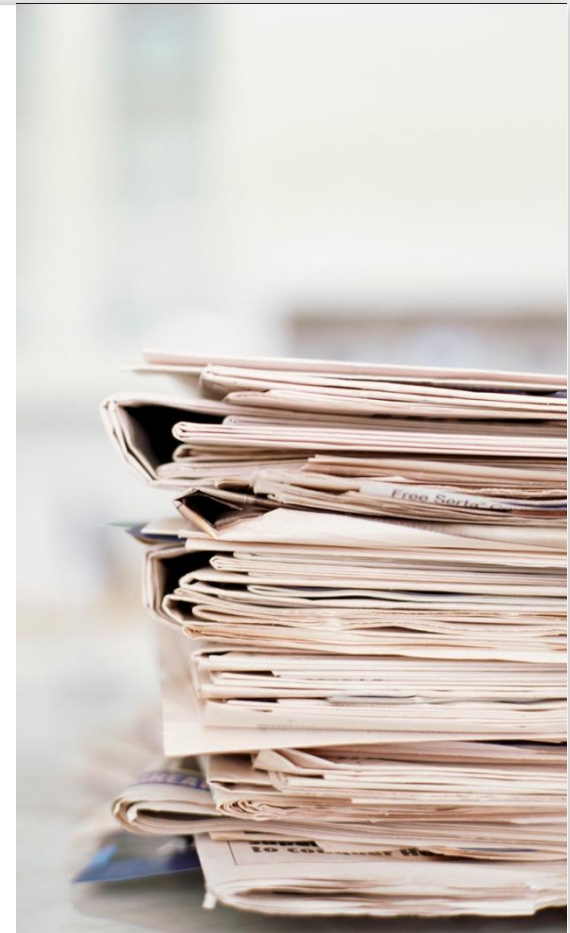
**Compliance-
Management-Systeme**

Risk & Compliance – Thought Leadership



Herausforderungen

- Zunehmend vernetzte, globale Wirtschaftsbeziehungen
- Komplexer werdende Geschäftsprozesse
- Erhöhtes Risiko wirtschaftskrimineller Handlungen
- Haftung des Vorstands oder Aufsichtsrats
- Schnelle und angemessene Reaktion auf Verdachtsfälle
- Geringe Transparenz über Integrität von Geschäftspartnern





Unser Leistungsspektrum

- Beratung bei und Durchführung von Maßnahmen in der Prävention, Aufdeckung, Aufklärung und Adressierung von wirtschaftskriminellen Handlungen
- Beweissicherung und gerichtsverwertbare Aufbereitung in Zusammenarbeit mit der KPMG Rechtsanwalts-gesellschaft
- Implementierung effizienter Anti-Fraud Maßnahmen auf Unternehmens- und Prozessebene
- Einsatz forensischer Technologie bei der Sicherung und Wiederherstellung digitaler Beweismittel, in der Analyse umfangreicher Unternehmensdaten oder bei der Bereitstellung digitaler Beweise durch sog. Evidence & Discovery Management Systeme

Agenda

Kurzüberblick KPMG

e-Crime Studie 2010 – Computerkriminalität in Deutschland

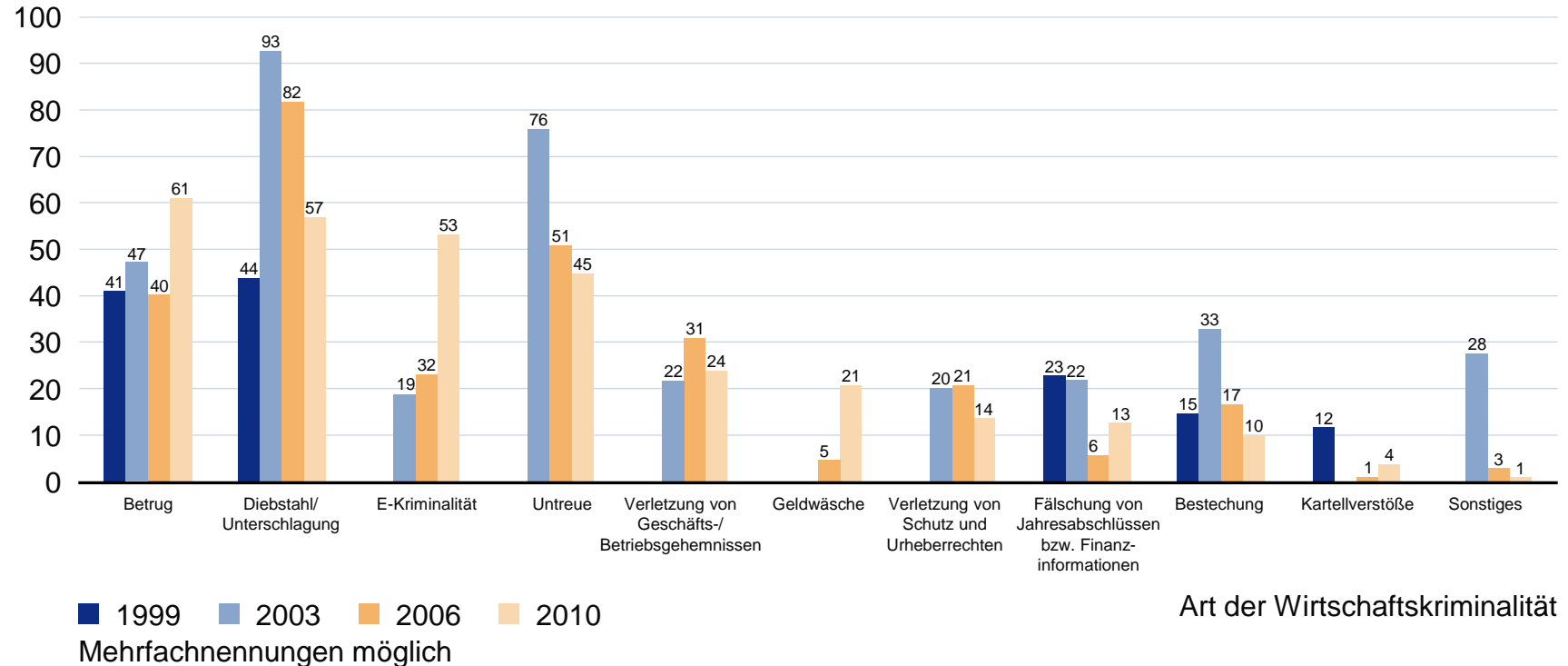
Diskussion und Fragen

Studie zur Wirtschaftskriminalität – Anfang 2010

Motivation zur Detailuntersuchung des Themas e-Crime

Häufigkeiten und Arten von Wirtschaftskriminalität

in Prozent



Eckdaten der Studiendurchführung 1/3

Konzeption



Durchführung



Erhebungsart

Persönliche Befragung

Umfrageteilnehmer

500

**Inhaber- und
familiengeführte Unternehmen**

179 (36%)

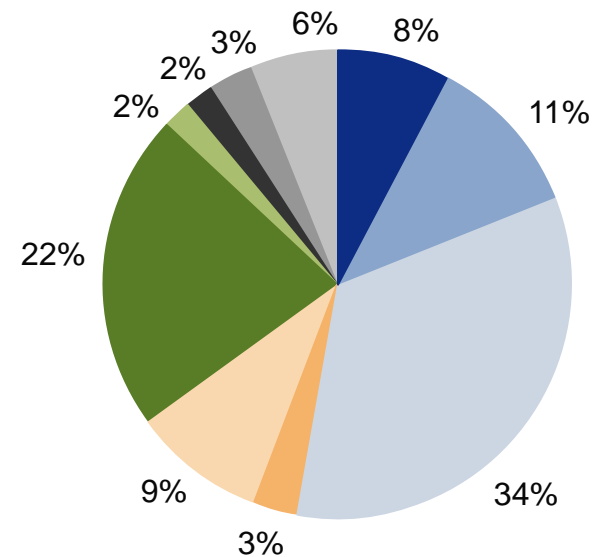
Großunternehmen

321 (64%)

Eckdaten zur Studiendurchführung 2/3

Welche Position nehmen Sie in Ihrem Unternehmen ein? (Großunternehmen)

- Leiter Controlling, Rechnungswesen
- Mitglied Vorstand / Geschäftsführung
- Leiter Recht
- Vorstand / Geschäftsführung
verantwortlich für den Bereich Finanzen
- Leiter Interne Revision
- Compliance Officer
- Leiter Personal
- Leiter Risikomanagement
- Leiter Unternehmenssicherheit
- Sonstige Position

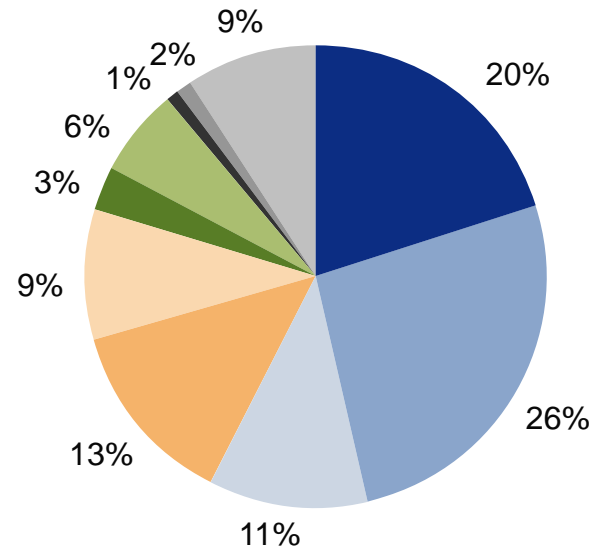


Diese Studie konzentriert sich beim Thema e-Crime erstmalig nicht auf die Technik bzw. die IT-Abteilungen

Eckdaten zur Studiendurchführung 3/3

Welche Position nehmen Sie in Ihrem Unternehmen ein? (familien- / inhabergeführte Unternehmen)

- Leiter Controlling, Rechnungswesen
- Mitglied Vorstand / Geschäftsführung
- Leiter Recht
- Vorstand / Geschäftsführung
verantwortlich für den Bereich Finanzen
- Leiter Interne Revision
- Compliance Officer
- Leiter Personal
- Leiter Risikomanagement
- Leiter Unternehmenssicherheit
- Sonstige Position



Mitglieder von Vorstand/Geschäftsführung sind bei familien-/inhabergeführten Unternehmen mit knapp 40% sehr stark vertreten

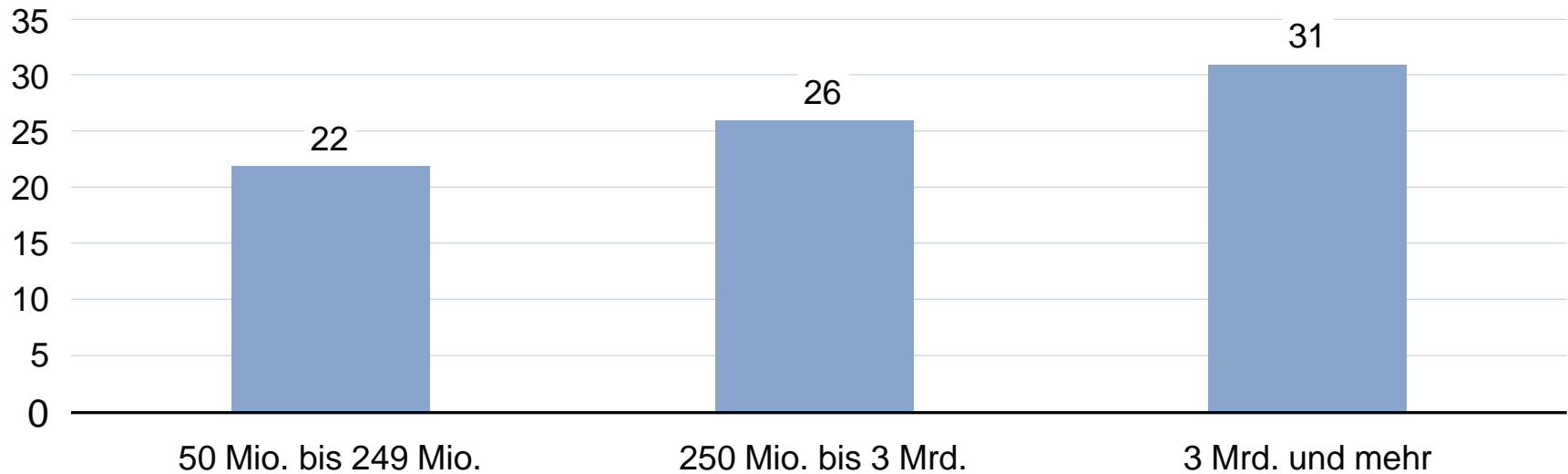
Wesentliche Ergebnisse der Studie

- ⊗ Ein Viertel der befragten Unternehmen waren in den letzten 3 Jahren von e-Crime betroffen
- ⊗ Der Diebstahl von Kunden- und Arbeitnehmerdaten ist häufigstes Delikt
- ⊗ Schadenshöhen können über 1 Mio. Euro pro Einzelfall betragen
- ⊗ In 48% der Fälle waren eigene Mitarbeiter die Täter
- ⊗ Insbesondere bei Datendiebstahl oder der Verletzung von Geschäfts- und Betriebsgeheimnissen kommen die Täter aus dem eigenen Haus
- ⊗ Vor allem exportorientierte Branchen sehen die größte Gefahr durch ausländische Spione (vor allem China und Russland)
- ⊗ Nur jeder zweite Täter wird überführt
- ⊗ Nicht einmal jedes zweite Unternehmen (48%) überprüft regelmäßig, ob die gesetzten Verhaltensregeln auch tatsächlich eingehalten werden

Betroffene Unternehmen

War Ihr Unternehmen in den vergangenen drei Jahren von e-Crime-Handlungen betroffen?

Umsatz in Prozent

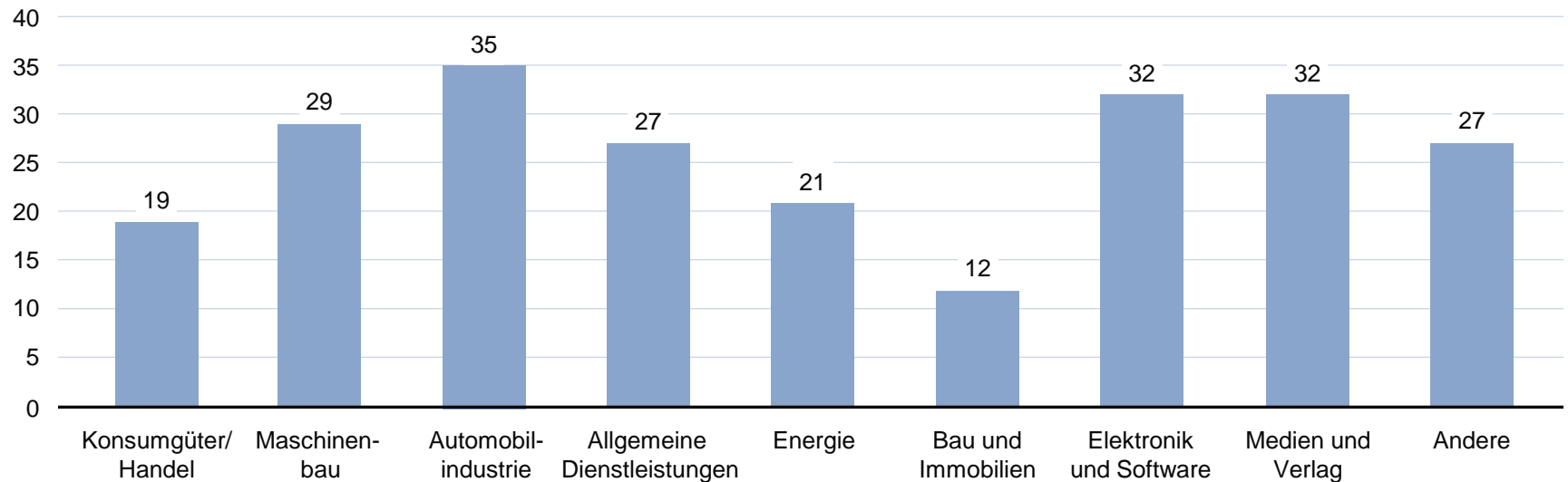


Ein Viertel der befragten Unternehmen war in den letzten drei Jahren von e-Crime betroffen

Schwerpunkte nach Branchen

War Ihr Unternehmen in den vergangenen drei Jahren von e-Crime-Handlungen betroffen? (nach Branchen)

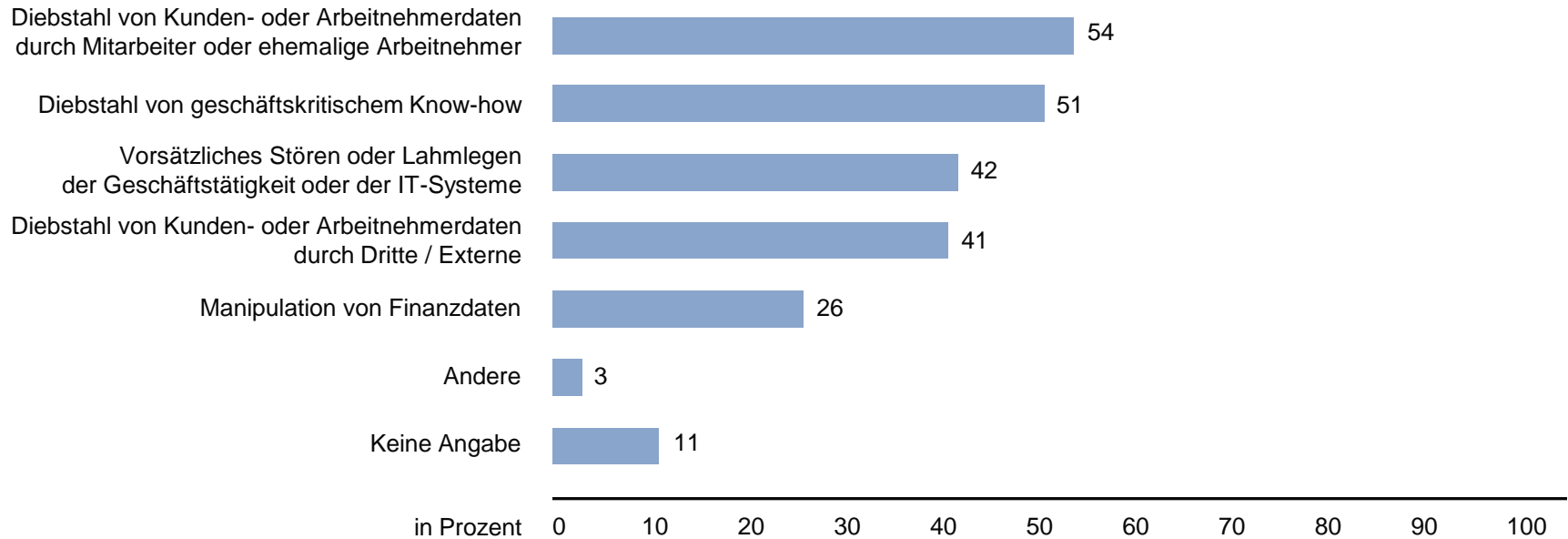
in Prozent



Branchenschwerpunkte sind die Automobilindustrie, Elektronik und Software, Medien und Verlage und der Maschinenbau

e-Crime Risiken mit hohem Schadenspotenzial

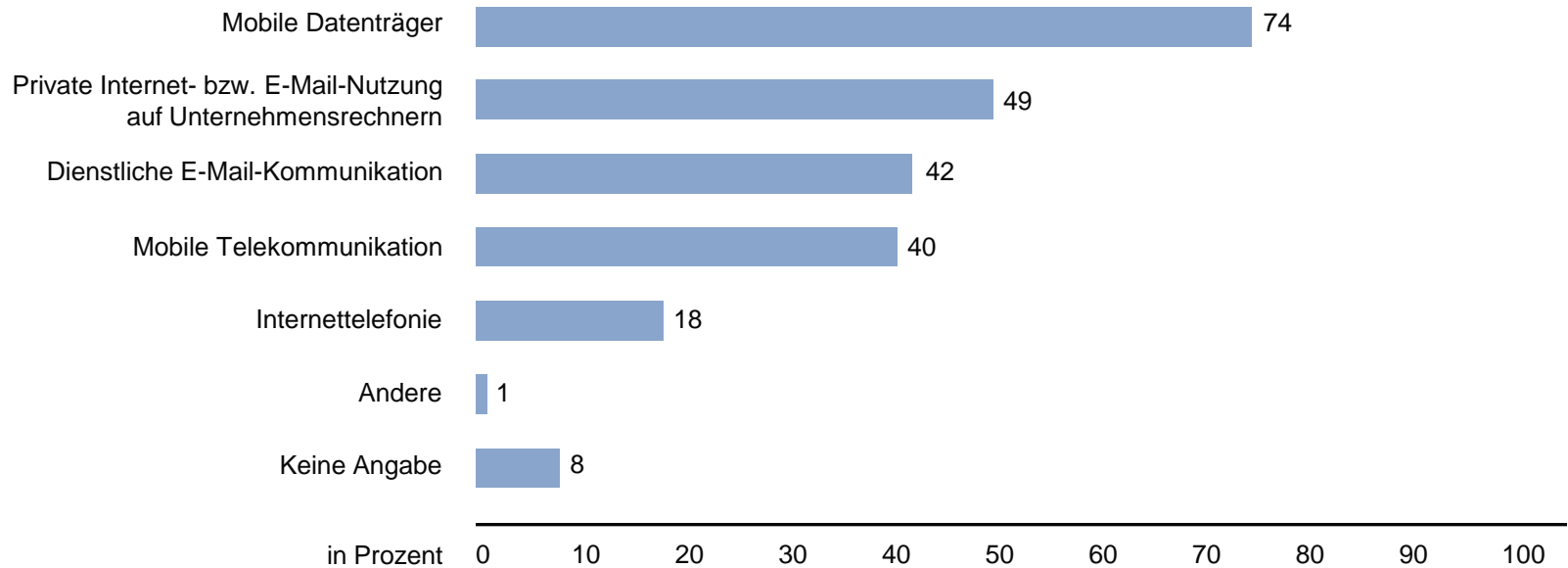
Welche der folgenden e-Crime-Risiken schätzen Sie für Ihr Unternehmen als besonders bedrohlich, das heißt mit hohem Schadenspotenzial ein?



Höchstes Schadenspotenzial beim Diebstahl von Kunden- oder Arbeitnehmerdaten durch Mitarbeiter oder ehemalige Arbeitnehmer

Gefahren in der Technologie

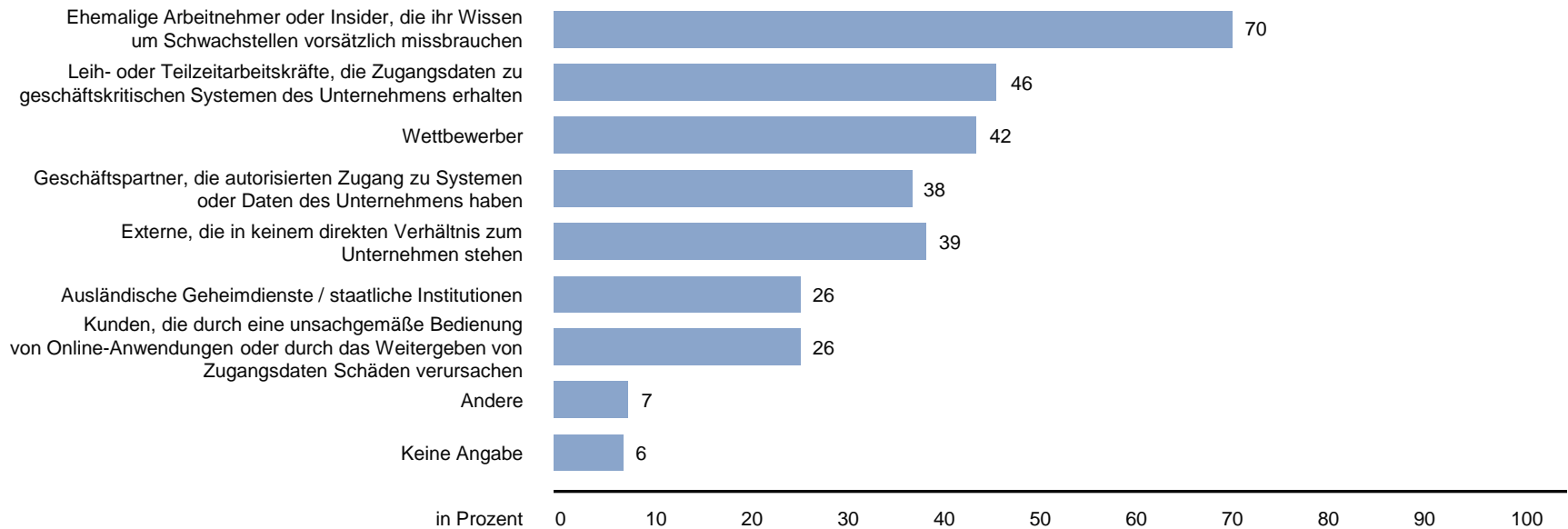
Welche der folgenden Informationstechnologien sehen Sie für Ihr Unternehmen als besonders risikobehaftet an, durch e-Crime Schaden zu nehmen?



USB Sticks werden immer kleiner, die Gefahren des Datendiebstahls hingegen immer größer

Gefahrenquellen für ein Unternehmen

Welche der folgenden Personengruppen schätzen Sie persönlich als bedeutsame Gefahrenquelle für Ihr Unternehmen ein? (nur betroffene Unternehmen)

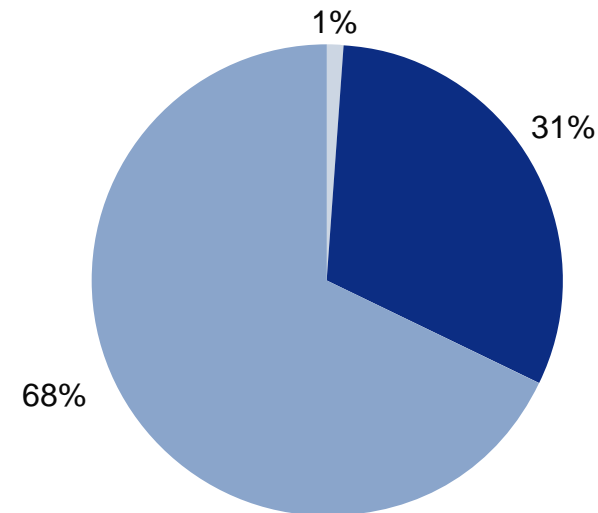


Von e-Crime betroffene Unternehmen wissen um die Gefahren, die von internen Tätern ausgehen

Rolle des Auslands

Sehen Sie die Gefahrenquellen von e-Crime-Handlungen im Wesentlichen in Verbindung mit konkreten Ländern?

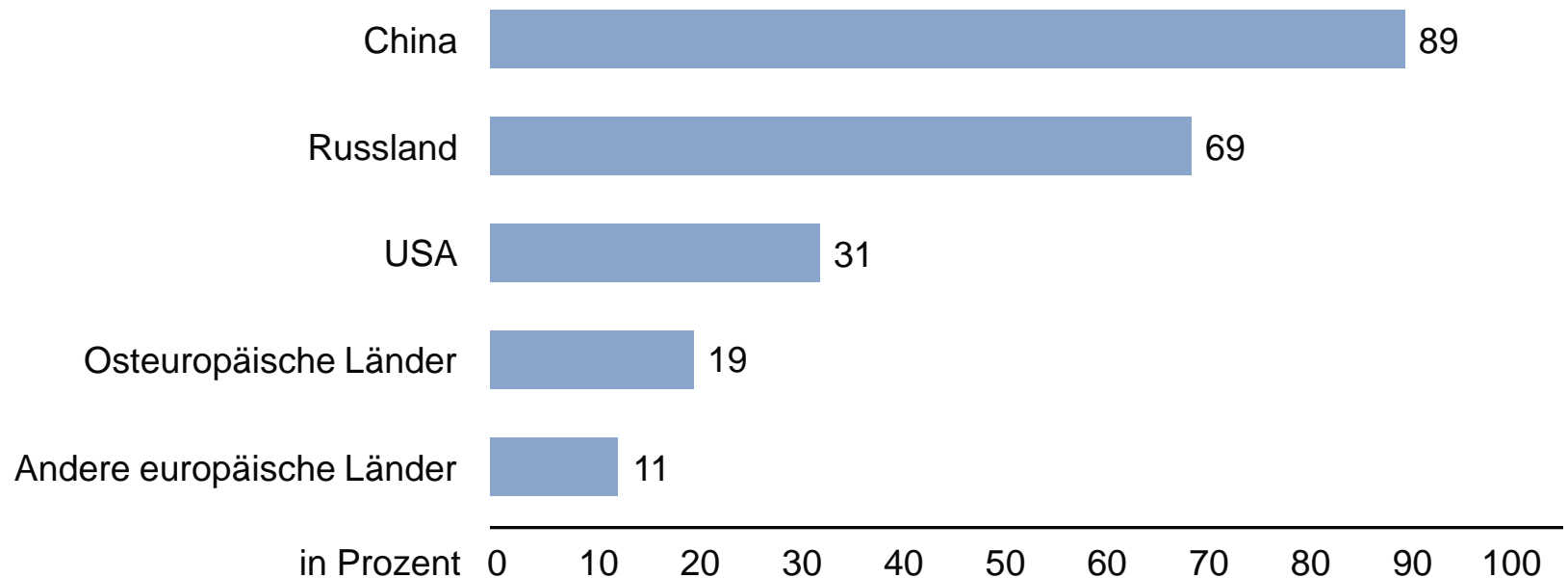
- Nein, e-Crime sehe ich nicht länderspezifisch.
- Ja, e-Crime steht in Verbindung mit bestimmten Ländern.
- Keine Angabe



Fast 70% der Umfrageteilnehmer sehen die Hauptgefahren von e-Crime Delikten nicht aus dem Ausland kommen

Länderspezifische Risiken

Befragte Unternehmen, die e-Crime-Handlungen mit bestimmten Ländern verbinden, nennen die folgenden Länder an erster Stelle.

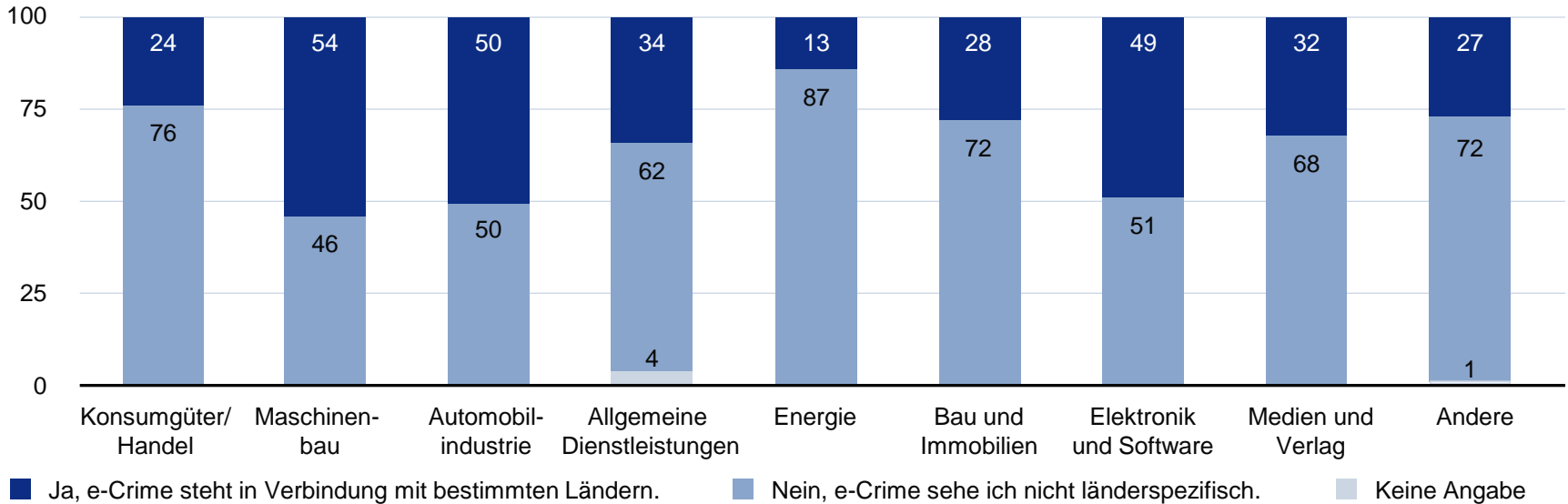


Die aufstrebenden Wirtschaftsmächte China und Russland gelten als besonders bedrohlich

Gefahren außerhalb Deutschlands (nach Branchen)

Handlungen im Wesentlichen in Verbindung mit konkreten Ländern ? (nach Branchen)

in Prozent

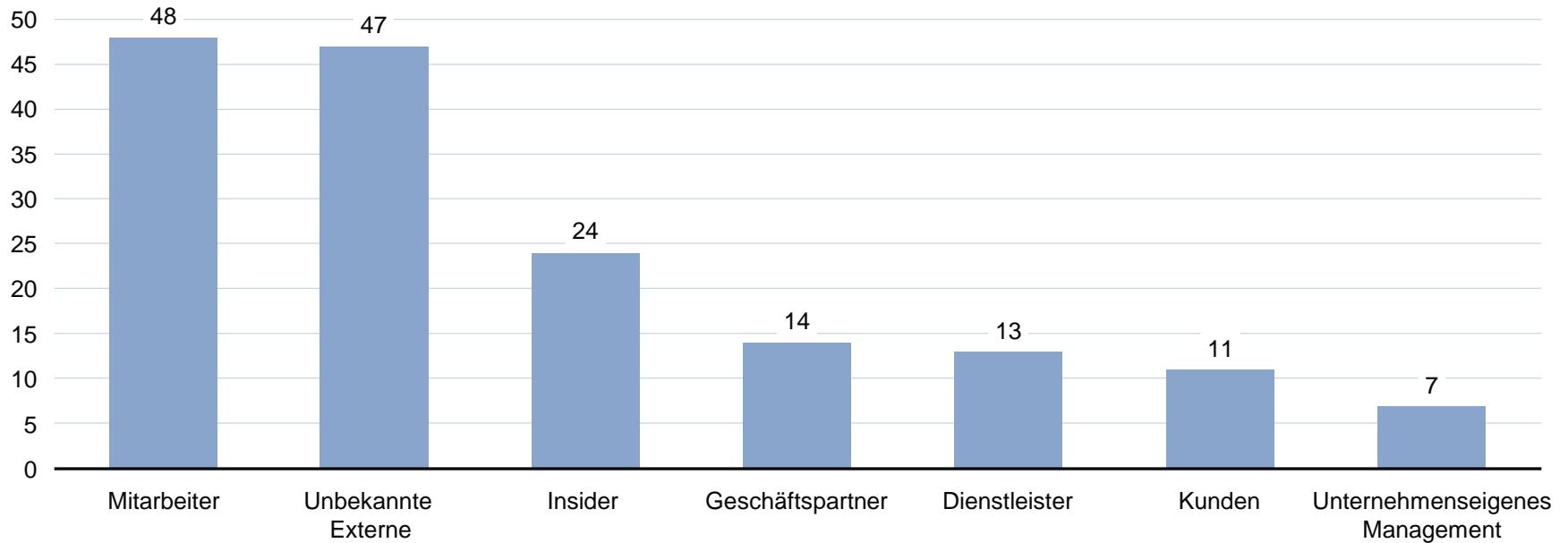


Vor allem die exportorientierten Branchen sehen e-Crime Handlungen in Verbindung mit Ländern außerhalb Deutschlands

Täterkreis

Welcher Täterkreis war bei den begangenen e-Crime-Handlungen beteiligt?

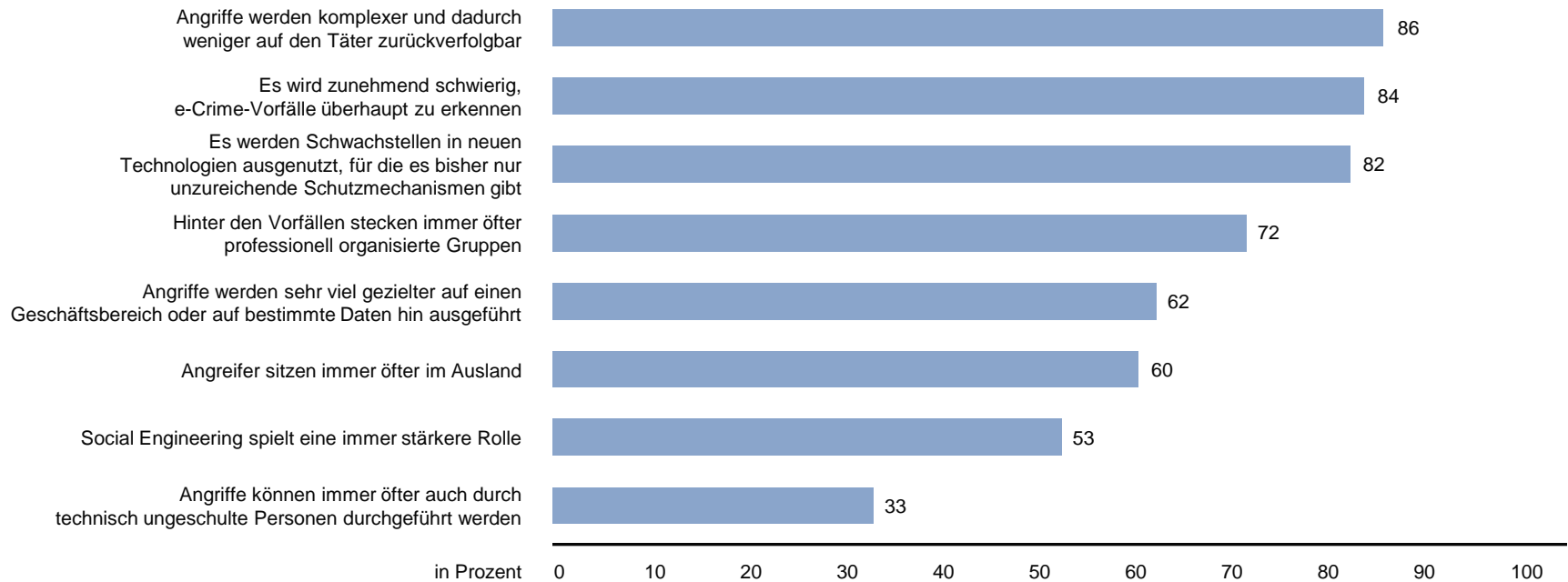
Durchschnittlicher Anteil über alle Delikttypen in Prozent



48% aller betroffenen Unternehmen nennen ihre eigenen Mitarbeiter als Täterkreis

Veränderungen in der e-Crime Bekämpfung

Wie haben sich e-Crime-Vorfälle in den letzten Jahre verändert ?

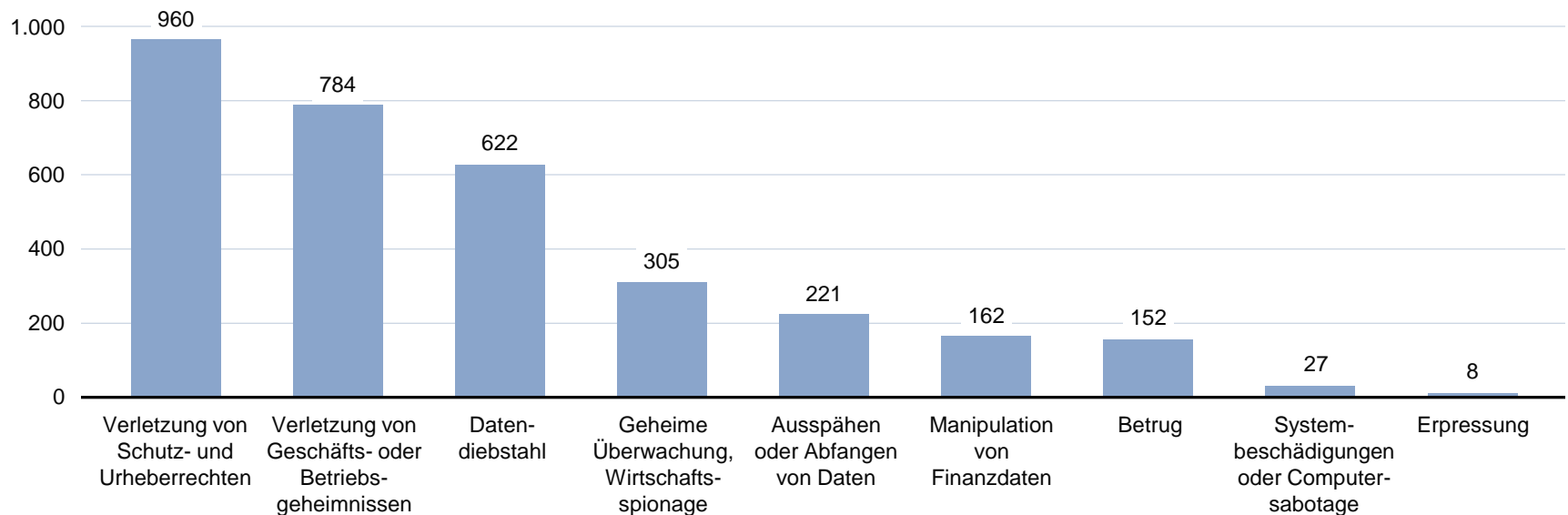


Viele Unternehmensverantwortliche fühlen sich den Angreifern im „Wettrüsten“ unterlegen

Angaben der Schadenshöhen 1/2

Welche Schadenshöhen würden Sie für die einzelnen e-Crime-Vorfälle ansetzen? (von e-Crime betroffene Unternehmen)

Durchschnitt pro Einzelfall (in 1.000 EUR)

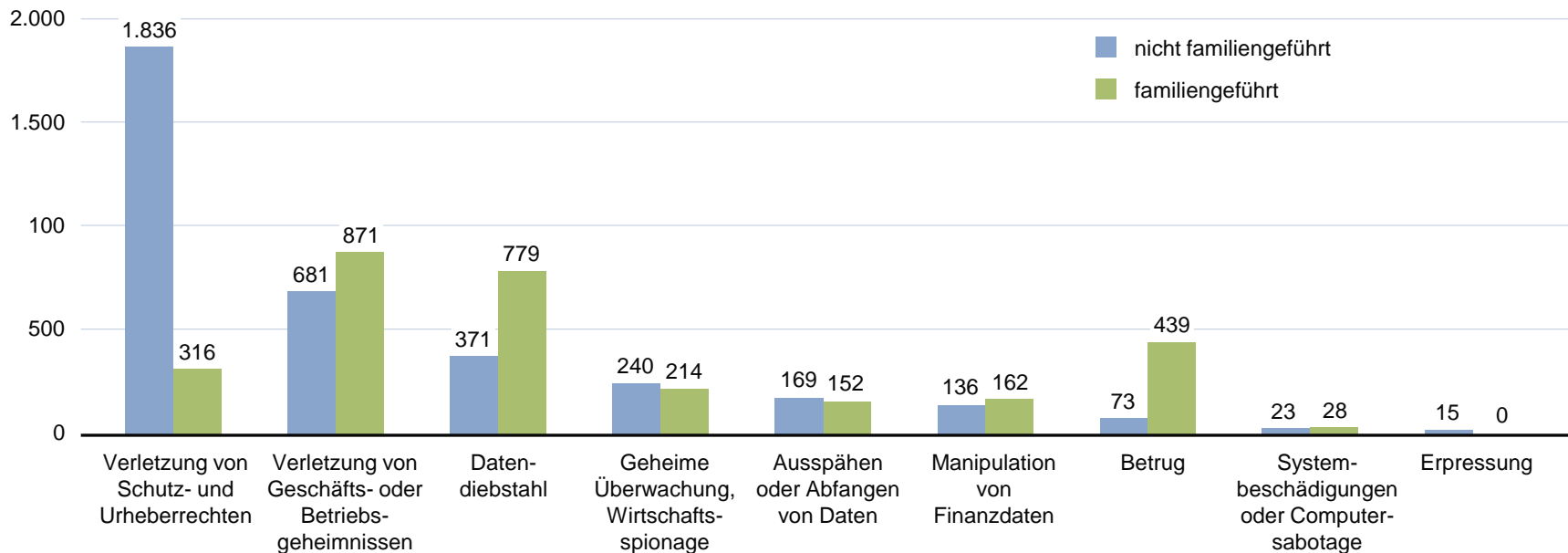


Die Schadenshöhen bewegen sich je nach Delikttyp zwischen wenigen 1.000 Euro bis zu knapp 1 Millionen Euro pro Einzelfall

Angaben der Schadenshöhen 2/2

Welche Schadenshöhen würden Sie für die einzelnen e-Crime-Vorfälle ansetzen?

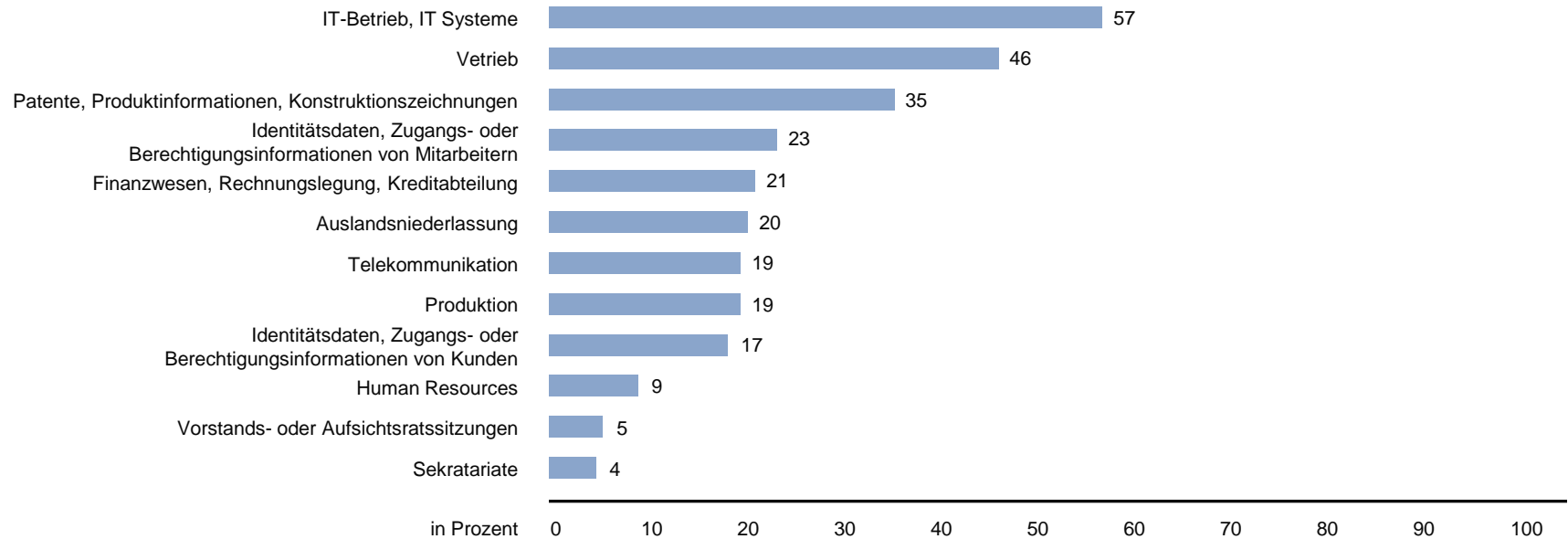
Durchschnitt pro Einzelfall (in 1.000 EUR)



Im Schnitt ist die Schadenshöhe bei familiengeführten Unternehmen um 20 Prozent höher als bei nicht familiengeführten Unternehmen

Angriffsziele

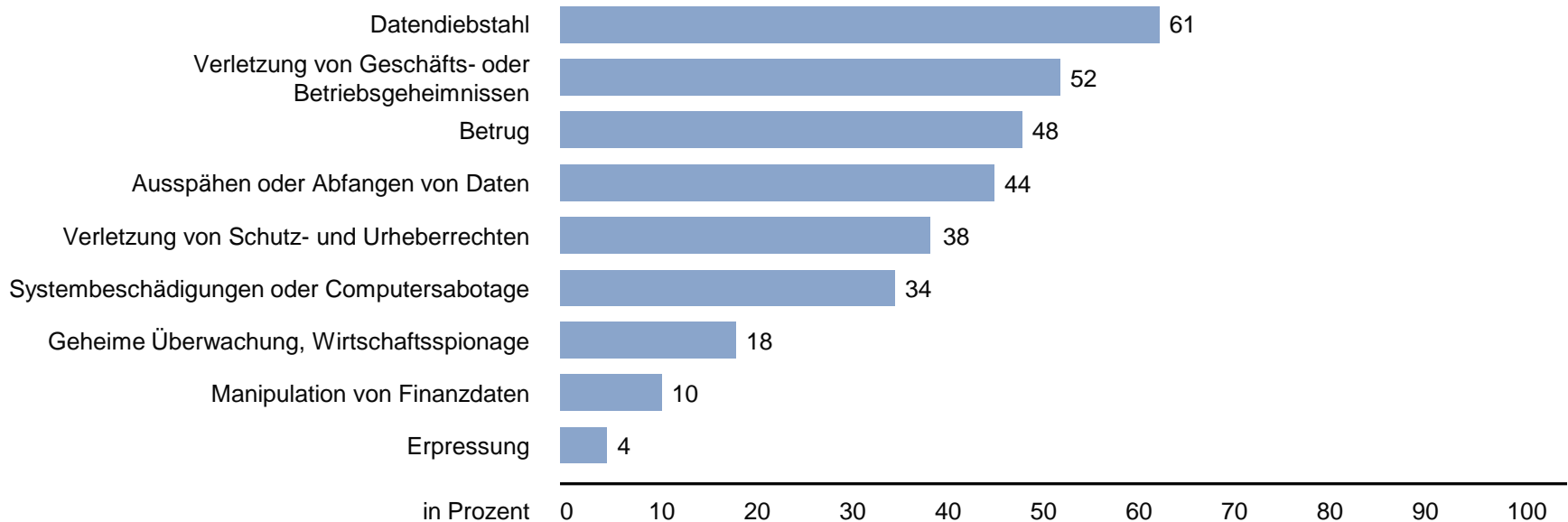
Welche Bereiche Ihres Unternehmens waren Ziel der e-Crime-Delikte? (von e-Crime betroffene Unternehmen)



IT, Vertrieb, Patente aber auch Auslandsniederlassungen gehören zu den vornehmlichen Angriffszielen

Art der tatsächlich durchgeführten e-Crime Delikte

Von welchen der genannten e-Crime-Handlungen war Ihr Unternehmen in den letzten drei Jahren betroffen? (von e-Crime betroffene Unternehmen)

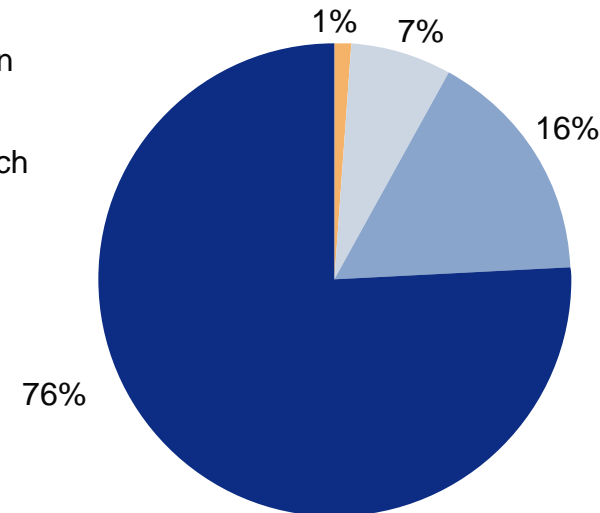


61% der von e-Crime betroffenen Unternehmen waren in den letzten drei Jahren Opfer von Datendiebstahl

Verankerung der e-Crime Bekämpfung im Unternehmen

Wie würden Sie die gegenseitige Verzahnung der einzelnen Geschäftsbereiche in Bezug auf Maßnahmen zur Prävention, Erkennung und Reaktion auf e-Crime-Delikte charakterisieren?

- Starke Verzahnung und zentrale Steuerung der Maßnahmen für alle Geschäftsbereiche
- Einige geschäftskritische Bereiche stellen eigenverantwortlich Schutzmaßnahmen, andere werden zentral betreut
- Geschäftsbereiche verantworten die Maßnahmen in Eigenregie
- Keine Angabe

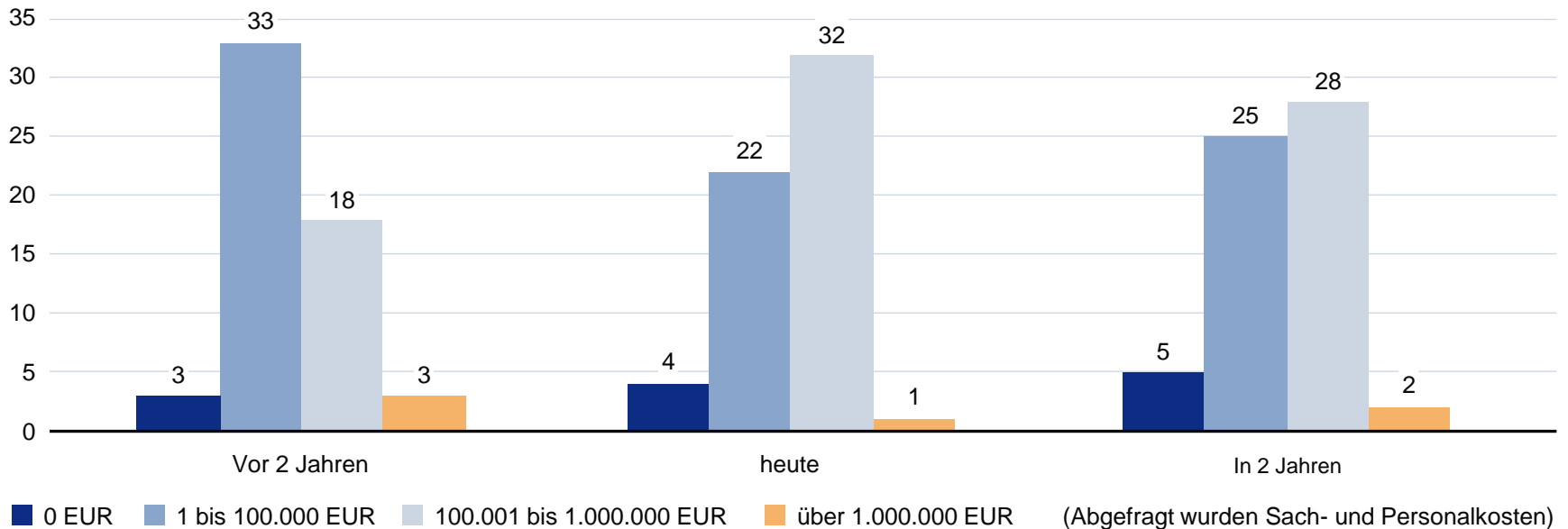


e-Crime ist ein bereichsübergreifendes und hochkomplexes Thema, dass eine Verzahnung aller Geschäftsbereiche erfordert

Investitionen in die e-Crime Bekämpfung

Wie viel investiert Ihr Unternehmen pro Jahr in die e-Crime-Bekämpfung?

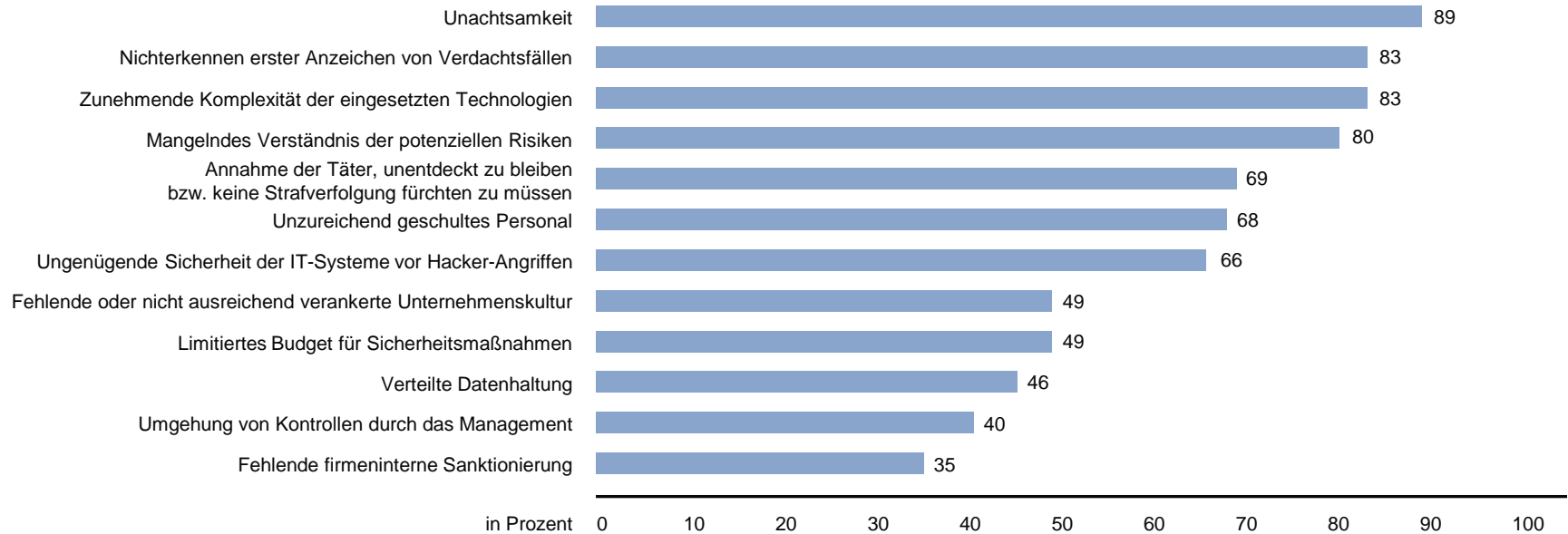
in Prozent



Trotz Krise haben die befragten Unternehmen die Ressourcen zur e-Crime Bekämpfung in den letzten zwei Jahren erweitert

Begünstigungsfaktoren für e-Crime

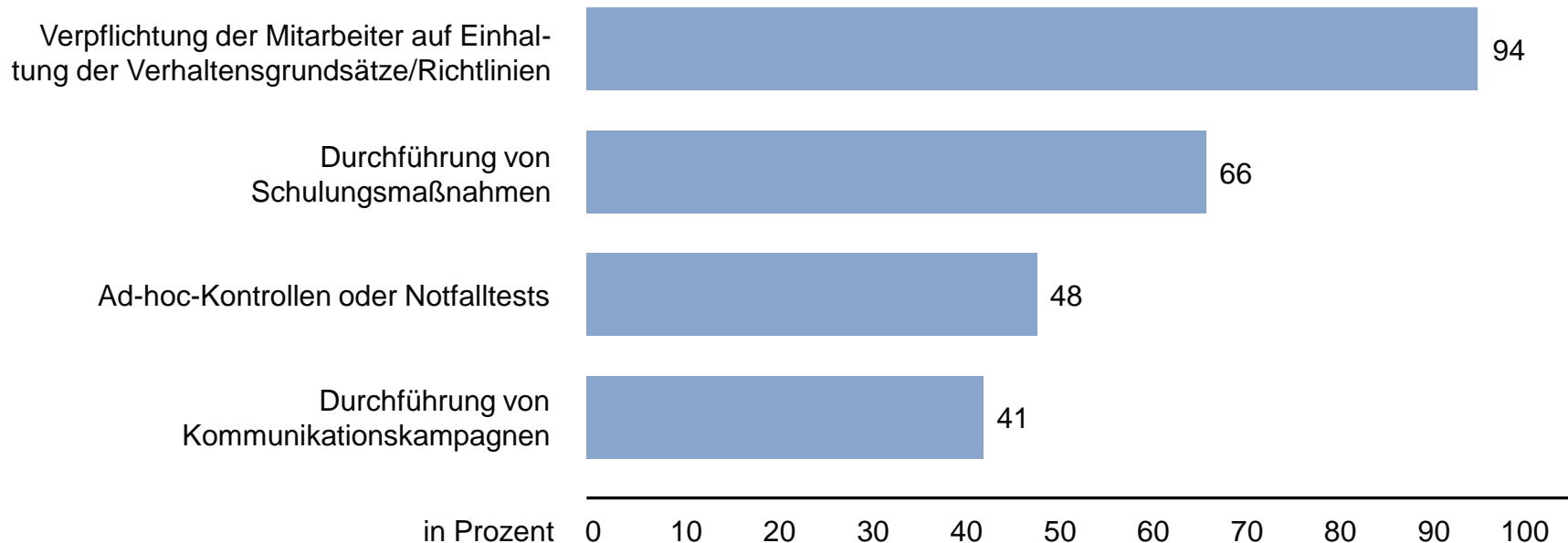
Welche Umstände begünstigen Ihrer Meinung nach das Entstehen von e-Crime besonders?



Eine noch so ausgeklügelte Informationssicherheitsstruktur ist machtlos gegen den „Faktor Mensch“

Training und Awareness

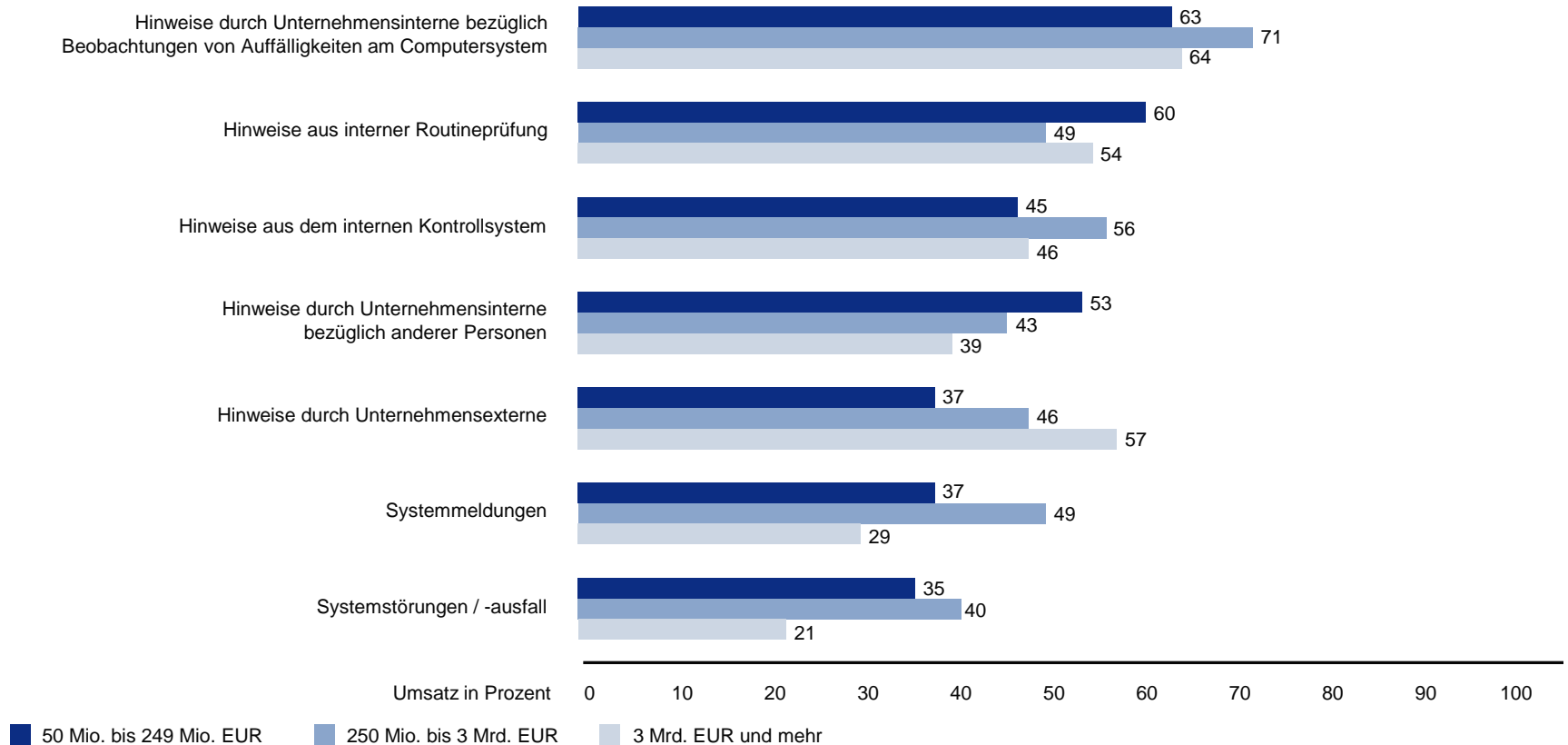
Welche Maßnahmen haben Sie zur Sensibilisierung Ihrer Mitarbeiter bezüglich bestehender e-Crime-Risiken ergriffen?



Verhaltensgrundsätze und Richtlinien sind eingeführt, doch bei der regelmäßigen Kontrolle hapert es

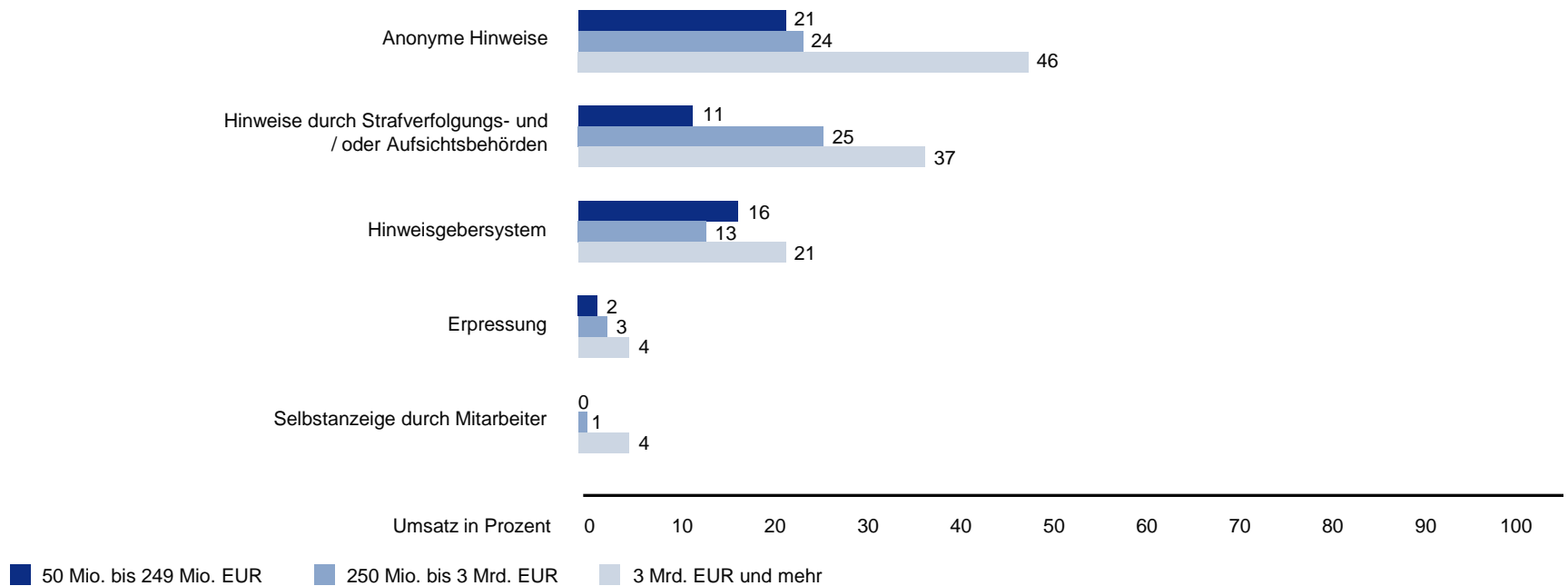
Erkennung von e-Crime Delikten (1/2)

Wodurch sind Sie auf Fälle von e-Crime erstmalig aufmerksam geworden?



Erkennung von e-Crime Delikten (2/2)

Wodurch sind Sie auf Fälle von e-Crime erstmalig aufmerksam geworden?

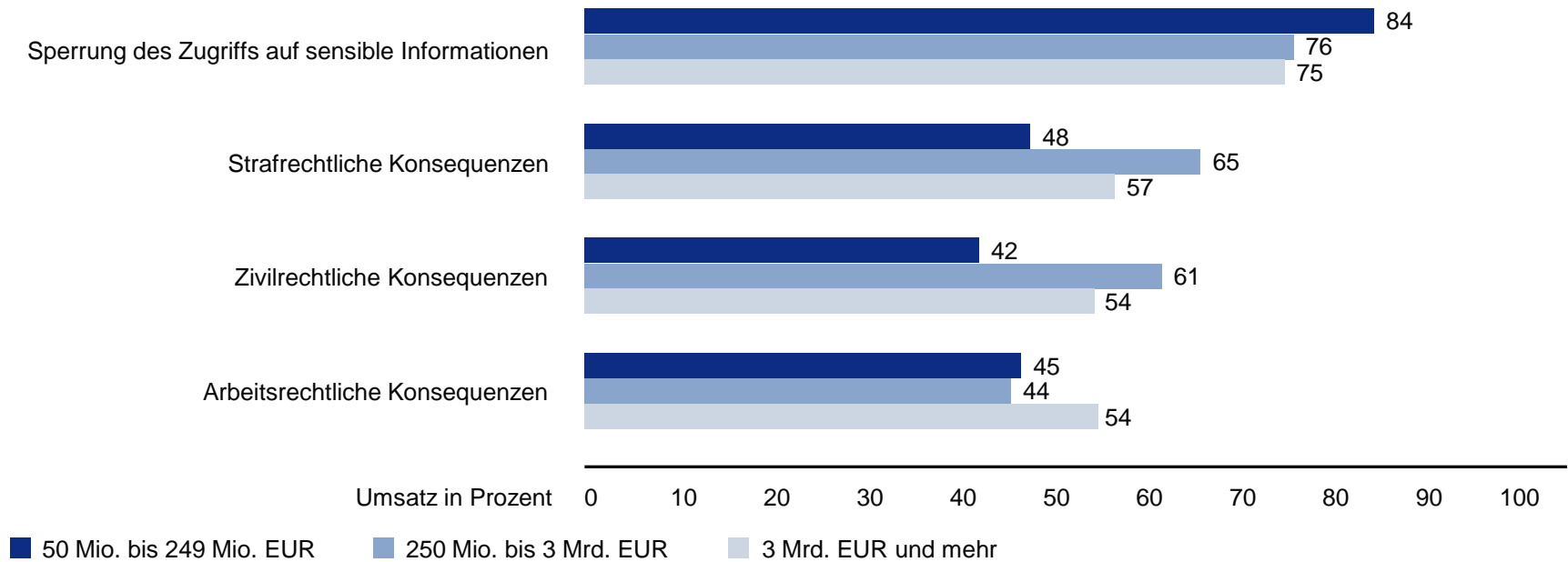


Vor allem bei großen Unternehmen spielen zunehmend anonyme Hinweisgebersysteme und Unternehmensexterne eine Rolle

Sanktionierung

Welche Sanktionen hat Ihr Unternehmen gegen die e-Crime-Täter ergriffen?

(von e-Crime betroffene Unternehmen)

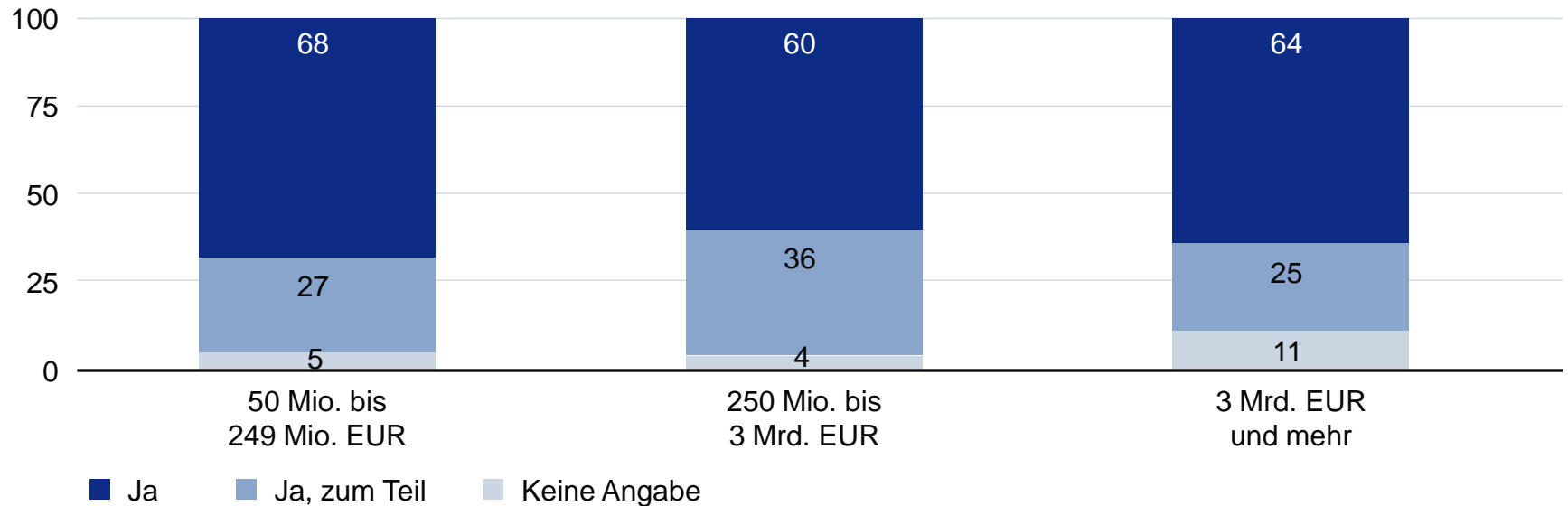


Von e-Crime betroffene Unternehmen sanktionieren Delikte meist sehr konsequent

Erstreaktion

Hat Ihr Unternehmen in der Rückschau nach Kenntnis des Verdachts beziehungsweise der Taten angemessen und zeitnah gehandelt?

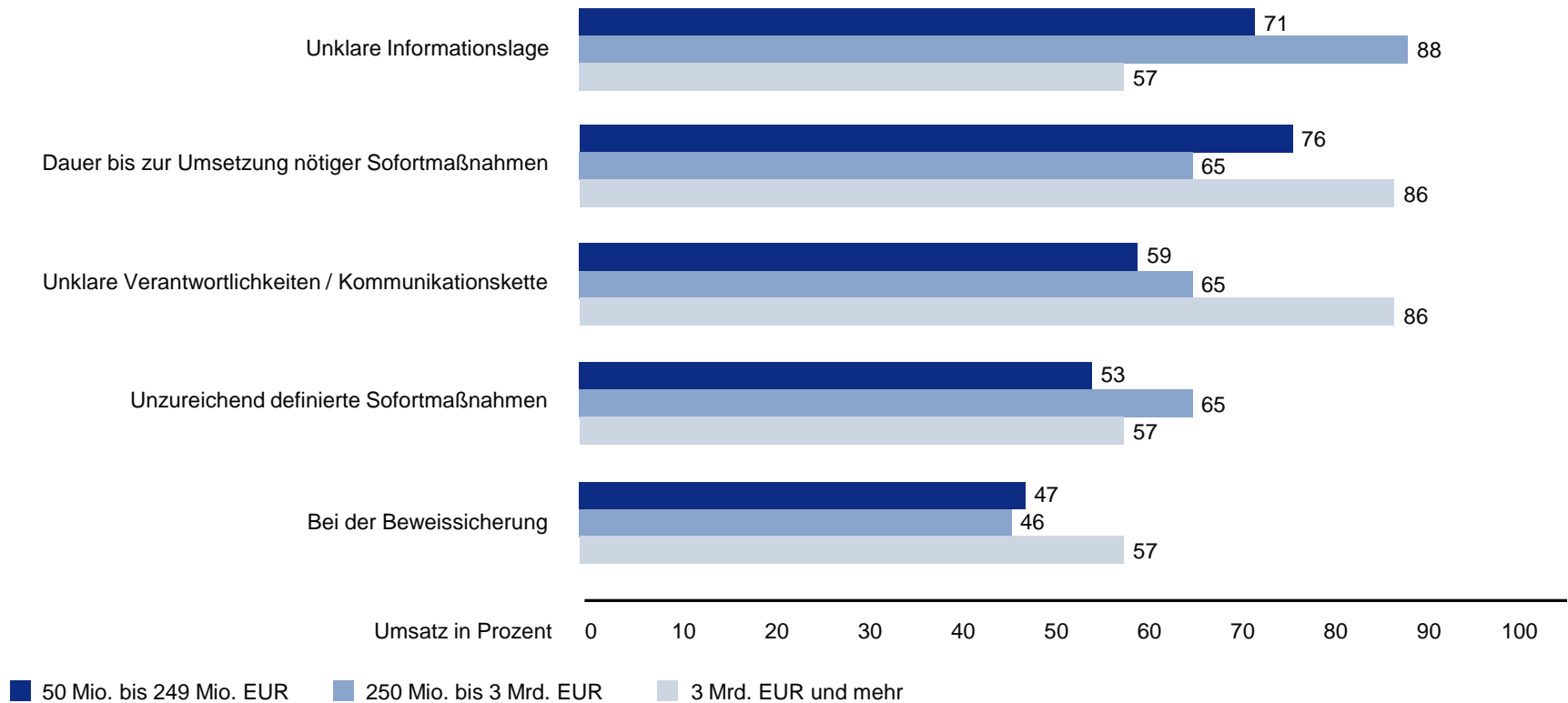
in Prozent



Ein Drittel der von e-Crime betroffenen Unternehmen halten ihre Erstreaktion für nur teilweise angemessen

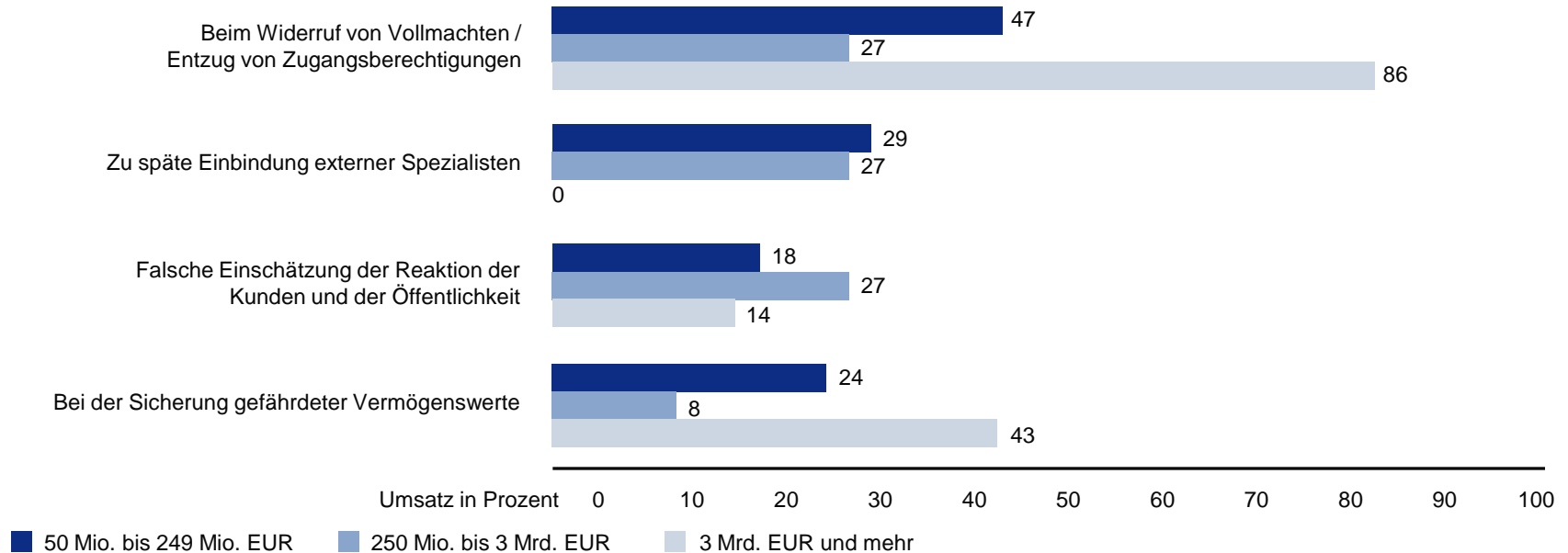
Versäumnisse in der Erstreaktion (1/2)

In welchen Bereichen gab es in der Erstreaktion aus Ihrer Sicht Versäumnisse? (Unternehmen, die nur zum Teil angemessen auf e-Crime-Delikte reagierten)



Versäumnisse in der Erstreaktion (2/2)

In welchen Bereichen gab es in der Erstreaktion aus Ihrer Sicht Versäumnisse? (Unternehmen, die nur zum Teil angemessen auf e-Crime-Delikte reagierten)

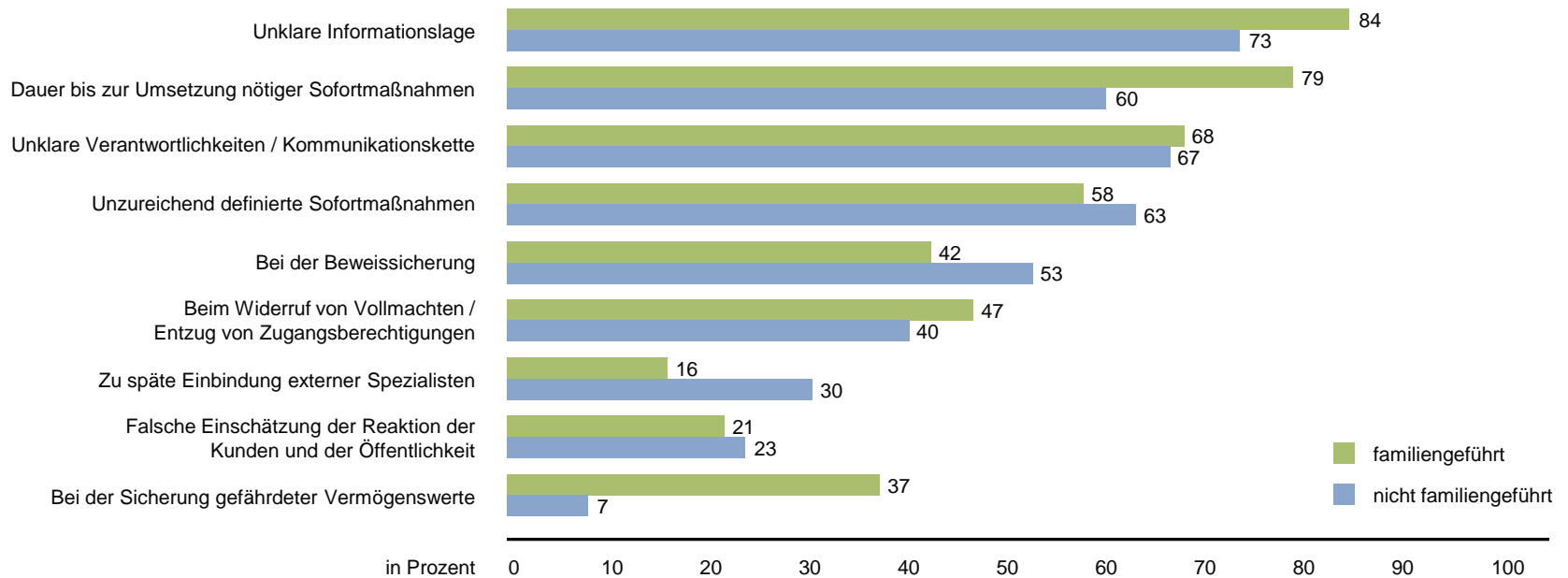


Insgesamt deuten die Umfrageergebnisse auf eine unzureichende Vorbereitung der Unternehmen auf e-Crime Delikte hin

Versäumnisse in der Erstreaktion (Vergleich mit familiengeführten Unternehmen)

In welchen Bereichen gab es in der Erstreaktion aus Ihrer Sicht Versäumnisse?

Selektion: Unternehmen, die nur zum Teil angemessen auf e-Crime-Delikte reagierten



Familiengeführte Unternehmen sind in Krisensituationen schlechter vorbereitet als nicht familiengeführte Unternehmen

Agenda

Kurzüberblick KPMG

e-Crime Studie 2010 – Computerkriminalität in Deutschland

Diskussion und Fragen

Kontakt Daten



Dr. Stefan Weiss

Director, Risk & Compliance

Marie-Curie-Straße 30
60439 Frankfurt/Main

Tel. +49 69 9587-3570

Mobil +49 174 3269 152

stefanweiss@kpmg.com

KPMG Aktiengesellschaft Wirtschaftsprüfungsgesellschaft
Member of KPMG International

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2011 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Germany. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.

Fraud Triangle

Das Fraud Triangle zeigt Faktoren, die Fraud begünstigen
(nach Donald R. Cressey, US-amerikanischer Soziologe und Kriminologe)

