BERICHT ZU WELTWEITEN KOSTEN VON INSIDER-BEDROHUNGEN 2022

Unabhängig durchgeführt von:

Ponemon INSTITUTE

proofpoint.

INHALT

EINFÜHRUNG

Das Ponemon Institute stellt die Erkenntnisse aus dem *Bericht zu weltweiten Kosten von Insider-Bedrohungen* vor.

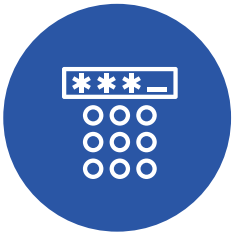
DIES IST DIE VIERTE BENCHMARK-UNTERSUCHUNG DIESER ART MIT DEM ERKLÄRTEN ZIEL, DIE FINANZIELLEN FOLGEN DURCH INSIDER-BEDROHUNGEN BESSER ZU VERSTEHEN. DANEBEN SOLL GEZEIGT WERDEN, WIE ERFOLGREICH UNTERNEHMEN DIESE RISIKEN MINIMIEREN KÖNNEN.

Die erste Untersuchung zu den weltweiten Kosten von Insider-Bedrohungen wurde 2016 durchgeführt und befasste sich ausschließlich mit Unternehmen in Nordamerika. Seitdem hat sich der Untersuchungsbereich auf Unternehmen in Europa, dem Nahen Osten, Afrika sowie dem Asien-Pazifik-Raum erweitert, wobei die Unternehmen mindestens 500 bis mehr als 75.000 Mitarbeiter haben. Dieses Jahr haben wir 1.004 IT- und IT-Sicherheitsexperten in 278 Unternehmen befragt, die mindestens ein durch einen Insider ausgelöstes, schwerwiegendes Ereignis verzeichnet haben. Insgesamt umfasst die Untersuchung 6.803 Insider-Zwischenfälle.

Im Kontext dieser Untersuchung sind Insider-Bedrohungen wie folgt definiert:

Unachtsames oder fahrlässiges Verhalten von Mitarbeitern oder Auftragnehmern

Kriminelle oder böswillige Motive eines Insiders



Diebstahl von Anmeldedaten

ZUSAMMENFASSUNG

INSIDER-BEDROHUNGEN SIND IN DEN LETZTEN ZWEI JAHREN HÄUFIGER UND KOSTSPIELIGER GEWORDEN – SO HABEN SICH DIEBSTÄHLE VON ANMELDEDATEN BEISPIELSWEISE SEIT 2020 VERDOPPELT.

Doch obwohl die Zahl der Insider-Bedrohungen in allen drei Bereichen gestiegen ist, werden die meisten Insider-Zwischenfälle durch unachtsam oder fahrlässig handelnde Mitarbeiter verursacht.

Aus den Ergebnissen geht hervor, dass 56 % der Zwischenfälle bei den untersuchten Unternehmen auf Fahrlässigkeit zurückzuführen sind. Die durchschnittlichen jährlichen Behebungskosten betrugen zudem 6,6 Millionen US-Dollar.

Die Untersuchung hat darüber hinaus ergeben, dass die Kosten von Bedrohungen durch Insider erheblich von der Art des Zwischenfalls abhängen. Dies lässt sich größtenteils auf die nach einem Insider-Zwischenfall erforderlichen Tätigkeiten zurückführen: Kontrolle und Überwachung, Untersuchung, Eskalation, Zwischenfallreaktion, Eindämmung, Ex-Post-Analyse sowie Behebung.

Dies sind einige wichtige Statistiken zu den Kosten Insider-bezogener Zwischenfälle über einen Zeitraum von zwölf Monaten:

278 Gesamtzahl der untersuchten Unternehmen	**6.803** Gesamtzahl der Insider-bezogenen Zwischenfälle	**15,4 MIO. USD** Durchschnittliche jährliche Gesamtkosten
56 % Zwischenfälle durch Fahrlässigkeit	**26 %** Zwischenfälle durch Insider mit kriminellen Motiven	**18 %** Zwischenfälle durch Diebstahl von Anmeldedaten
6,6 MIO. USD Jährliche Kosten durch Fahrlässigkeit	**4,1 MIO. USD** Jährliche Kosten durch Insider mit kriminellen Motiven	**4,6 MIO. USD** Jährliche Kosten durch Diebstahl von Anmeldedaten

DIES SIND DIE WICHTIGSTEN ERGEBNISSE DER UNTERSUCHUNG.

Die Zeit bis zur Eindämmung eines Insider-Zwischenfalls nahm im Vergleich zur letzten Untersuchung zu.

Durchschnittlich dauerte die Eindämmung eines Zwischenfalls 85 Tage – eine Steigerung gegenüber den 77 Tagen in der letzten Untersuchung.

Nur 12 % der Zwischenfälle wurden in weniger als 30 Tagen eingedämmt.

Durchschnittliche Zeit für Zwischenfall-Eindämmung

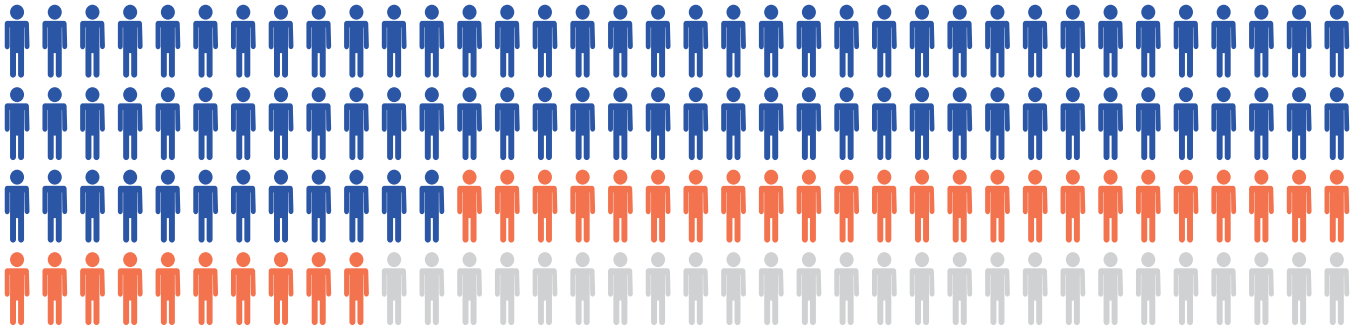
85 TAGE

12 % der Zwischenfälle wurden eingedämmt in

≤30 TAGEN

34 % der Zwischenfälle wurden eingedämmt in

≥90 TAGEN



Fahrlässig handelnde Insider sind die Hauptursache für die meisten Zwischenfälle.

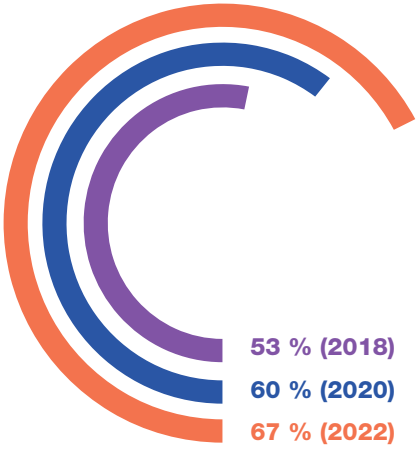
Insgesamt wurden 3.807 Angriffe (56 %) durch die Fahrlässigkeit von Mitarbeitern oder Auftragnehmern verursacht, mit durchschnittlichen Kosten pro Zwischenfall von 484.931 US-Dollar. Hierfür kann es verschiedene Gründe geben: eine unzureichende Absicherung von Geräten, die Missachtung betrieblicher Sicherheitsrichtlinien oder fehlende Patches und Upgrades.

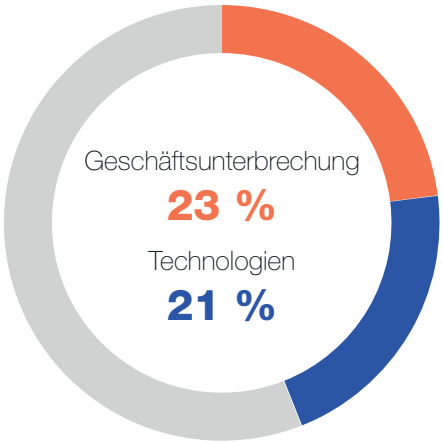
Böswillige Insider verursachten 26 % oder 1.749 Zwischenfälle mit durchschnittlichen Kosten pro Zwischenfall in Höhe von 648.062 US-Dollar.

Böswillige Insider sind Mitarbeiter oder autorisierte Personen, die ihren Datenzugang für schädliche, unethische oder rechtswidrige Zwecke nutzen. Da Mitarbeitern in der heutigen mobilen Arbeitswelt aus Produktivitätsgründen zunehmend mehr Zugriffsrechte gewährt werden, lassen sich böswillige Insider schwerer erkennen als externe Angreifer oder Hacker.

Die Zahl der Anmelde-datendiebstähle hat sich seit der letzten Untersuchung beinahe verdoppelt.

Mit durchschnittlichen Kosten von 804.997 US-Dollar pro Zwischenfall verursachen Anmeldedatendiebstähle die höchsten Behebungskosten. Die Diebe stehlen die Anmeldedaten von Anwendern, um Zugang zu kritischen Daten und Informationen zu erlangen. Viele der Anmeldedatendiebe setzen dabei bevorzugt auf Social-Engineering-Techniken, zumeist in Phishing-Angriffen. Insgesamt waren bei 1.247 Zwischenfällen (18 %) der diesjährigen Untersuchung gestohlene Anmeldedaten involviert.





Unternehmen werden mittlerweile deutlich häufiger Opfer von Zwischenfällen.

Der aktuellen Untersuchung zufolge verzeichnen 67 % der Unternehmen pro Jahr zwischen 21 und mehr als 40 Zwischenfällen. Das entspricht einem Anstieg von 60 % gegenüber 2020 bzw. 53 % gegenüber 2018.

Bei Insider-Bedrohungen stellen Störungen oder Ausfälle sowie Investitionen in Technologien die höchsten Kostenfaktoren dar.

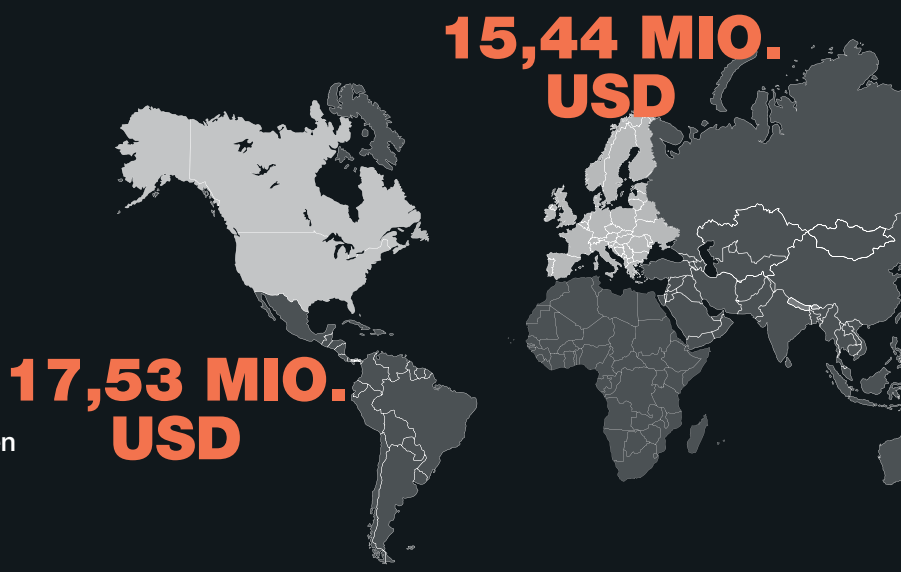
Die beiden größten Kostenfaktoren sind Geschäftsunterbrechungen aufgrund verringerter Mitarbeiterproduktivität (23 % der Gesamtkosten) sowie Technologien (21 %), wobei dies den Abschreibungswert sowie die Lizenzierung von Software und Hardware umfasst, die als Reaktion auf Insider-bezogene Zwischenfälle implementiert werden.

Unternehmen geben am meisten für die Eindämmung von Insider-Zwischenfällen aus.

Im Durchschnitt werden 184.548 US-Dollar zur Eindämmung der Folgen einer Insider-Bedrohung aufgewandt, während für Eskalation (32.228 US-Dollar) sowie Kontrolle und Überwachung (35.080 US-Dollar) am wenigsten ausgegeben wird. Zwischenfälle, die in weniger als 30 Tagen eingedämmt wurden, verursachten mit 11,23 Millionen US-Dollar die geringsten durchschnittlichen Jahreskosten für Tätigkeiten. Im Gegensatz dazu belaufen sich die durchschnittlichen jährlichen Tätigkeitskosten für mehr als 90 Tage anhaltende Zwischenfälle auf 17,19 Millionen US-Dollar.

Nordamerikanische Unternehmen geben überdurchschnittlich viel Geld für Tätigkeiten zur Abwehr von Insider-Bedrohungen aus.

Die Durchschnittskosten für Tätigkeiten zur Behebung von Insider-Bedrohungen über einen Zeitraum von zwölf Monaten betragen insgesamt 15,38 Millionen US-Dollar. Nordamerikanische Unternehmen verzeichneten mit 17,53 Millionen US-Dollar die höchsten Gesamtkosten. Auf Platz 2 lagen Unternehmen in Europa mit 15,44 Millionen US-Dollar.



Finanzdienstleister und Dienstleistungsunternehmen haben im Durchschnitt die höchsten Tätigkeitskosten.

Die durchschnittlichen Tätigkeitskosten für Finanzdienstleister und Dienstleistungsunternehmen betragen jeweils 21,25 Millionen US-Dollar und 18,65 Millionen US-Dollar. Unter „Dienstleistungen“ fällt eine Vielzahl von Unternehmen, darunter beispielsweise auch Wirtschaftsprüfungsgesellschaften, Unternehmensberater und Dienstleistungsunternehmen.

Unternehmensgröße beeinflusst die Kosten pro Zwischenfall

Die jährlichen Kosten der Zwischenfälle variieren entsprechend der Unternehmensgröße. Große Unternehmen mit mehr als 75.000 Mitarbeitern gaben im Verlauf des letzten Jahres durchschnittlich 22,68 Millionen US-Dollar aus, um Insider-bezogene Zwischenfälle zu beheben, während kleinere Unternehmen mit weniger als 500 Mitarbeitern durchschnittlich 8,13 Millionen US-Dollar aufwenden mussten.

Aus den Gesprächen mit den Teilnehmern an dieser Untersuchung ergaben sich folgende Erkenntnisse über Insider-Bedrohungen.

Für diese Untersuchung ermittelten wir nicht nur die Kosten von Insider-Bedrohungen für die Unternehmen, sondern sprachen mit den Teilnehmern auch über ihre Erfahrungen mit der Bedrohung sowie darüber, wie sie diese Risiken reduzieren.

Von allen Insider-Bedrohungsarten in dieser Untersuchung machen sich Unternehmen vor allem über Anmeldedatendiebstahl Sorgen. Anmeldedatendiebstähle haben sich seit der letzten Untersuchung beinahe verdoppelt und verursachen die höchsten Behebungskosten. 55 % der Befragten geben an, dass sie vor allem über Hacker besorgt sind, die gültige Anmeldedaten von Mitarbeitern stehlen könnten. Deutlich weniger der Befragten (21 %) machen sich wegen fahrlässig handelnder Insider Sorgen.

Fahrlässige Mitarbeiter und Anmeldedatendiebe sind die Hauptursache für die meisten Insider-Zwischenfälle. 57 % der Teilnehmer geben an, dass die Insider-Zwischenfälle durch fahrlässig handelnde Mitarbeiter entstanden, während 51 % sagen, dass böswillige Außenstehende Daten durch die Kompromittierung von Anmeldedaten oder Konten gestohlen haben.

Anfällige IoT-Geräte stellen das größte Risiko für Datenverlust dar. 63 % der Teilnehmer machen sich Sorgen wegen unverwalteter IoT-Geräte, die zum Verlust vertraulicher Daten führen könnten. Dahinter folgt die Cloud (52 % der Befragten) und das Netzwerk (51 %).

Die meisten vertraulichen Daten befinden sich in den E-Mails der Mitarbeiter. 65 % der Teilnehmer geben an, dass ihre Mitarbeiter höchst vertrauliche Daten wie personenbezogene Informationen, geistiges Eigentum und andere kritische Geschäftsdaten in E-Mails aufbewahren.

Böswillige Insider nutzen geschäftliche E-Mails, um an vertrauliche Daten zu gelangen. 74 % der Teilnehmer sagen, dass böswillige Insider vertrauliche Daten an externe Dritte verschickt haben. Dahinter folgen Scans auf offene Ports und Schwachstellen (62 %) sowie der Zugriff auf vertrauliche Daten, die nicht im Zusammenhang mit der Position oder Funktion standen (60 %).

Da die Zahl der Insider-Bedrohungen sowie die Eindämmungsdauer weiterhin zunehmen werden, spielen hochentwickelte Technologien wie Tools für Anwenderverhalten und Automatisierung eine immer wichtigere Rolle beim Schutz vor solchen Bedrohungen. Auf Anwenderverhalten basierende Tools zur Erkennung von Insider-Bedrohungen gelten als unerlässlich oder sehr wichtig (62 % der Befragten). Darauf folgt die Automatisierung der Prävention, Untersuchung, Eskalation, Eindämmung und Behebung von Insider-Zwischenfällen (55 %) sowie KI- und Machine Learning-Technologie für die genannten Zwecke (54 %).

05

Zeichen, dass Ihr Unternehmen gefährdet ist

01 Mitarbeiter sind nicht ausreichend geschult, Gesetze, Vorschriften oder rechtliche Vorgaben für ihre Arbeit vollständig zu verstehen und anzuwenden, was sich auf die Sicherheit des Unternehmens auswirkt.

02 Mitarbeiter wissen nicht, worauf sie achten müssen, um jederzeit die Sicherheit der von ihnen genutzten Geräte zu gewährleisten. Das betrifft sowohl unternehmenseigene als auch private Geräte, die sie zu beruflichen Zwecken nutzen.

03 Mitarbeiter veröffentlichen höchst vertrauliche Daten in öffentlichen Cloud-Bereichen und gefährden dadurch das Unternehmen.

04 Mitarbeiter verstoßen gegen die Sicherheitsrichtlinien ihres Unternehmens, um sich die Arbeit zu erleichtern.

05 Mitarbeiter setzen das Unternehmen Risiken aus, indem sie ihre Geräte und Anwendungen nicht kontinuierlich patchen bzw. auf die neuesten Versionen aktualisieren.

UNSERE UNTERSUCHUNG KONZENTRIERT SICH AUF TATSÄCHLICHE INSIDER-BEZOGENE EREIGNISSE ODER ZWISCHENFÄLLE, DIE FÜR DIE UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN KOSTEN VERURSACHT HABEN.

Mit unseren Methoden wollen wir die direkten sowie indirekten Kosten erfassen, einschließlich (und nicht beschränkt auf) folgende Bedrohungen für das Unternehmen:

- Diebstahl oder Verlust von geschäftskritischen Daten oder geistigem Eigentum
- Folgen von Ausfallzeiten auf die Produktivität von Unternehmen
- Schäden an Geräten und anderen Ressourcen
- Kosten für die Erkennung und Wiederherstellung von Systemen und grundlegenden Geschäftsprozessen
- Rechtliche und gesetzliche Folgen, einschließlich Kosten von Rechtsstreitigkeiten
- Verlorenes Vertrauen bei wichtigen Verantwortlichen
- Schädigung des Marktwerts und der Reputation

Für diese Untersuchung kommt ein ABC-Framework (Activity-Based Costing, Kostenzuordnung nach Tätigkeiten) zum Einsatz. Die eigentliche Umfrage wurde im Zeitraum von zwei Monaten durchgeführt und im September 2021 abgeschlossen. Unsere aktuelle Benchmark-Stichprobe umfasste 278 separate Unternehmen, wobei in diesen Unternehmen insgesamt 1.004 Interviews mit hochrangigen Mitarbeitern durchgeführt wurden. Die Tätigkeitskosten für die aktuelle Umfrage wurden im Rahmen von tatsächlichen Treffen oder Vor-Ort-Besuchen bei allen Teilnehmern unter Wahrung strikter Vertraulichkeit ermittelt. Unternehmen aus folgenden Bereichen wurden untersucht:

- Mittelständische Unternehmen und Organisationen des öffentlichen Sektors
- Standorte in folgenden Regionen: Nordamerika, Europa, Naher Osten und Afrika sowie im Asien-Pazifik-Raum
- Zentrale IT-Funktion mit Kontrolle über lokale bzw. Cloud-Umgebung
- Mindestens ein schwerwiegender Zwischenfall durch fahrlässige, böswillige oder kriminelle Insider

In diesem Bericht stellen wir ein objektives Framework vor, das die vollständigen finanziellen Auswirkungen von durch Insider verursachten Ereignissen oder Zwischenfällen ermittelt. Diese drei Fallprofile nutzten wir zur Kategorisierung und Analyse Insider-bezogener Kosten für 278 Unternehmen:

- Unachtsamer oder fahrlässiger Mitarbeiter oder Auftragnehmer
- Krimineller oder böswilliger Mitarbeiter oder Auftragnehmer
- Diebstahl der Anmeldedaten von Mitarbeitern/Anwendern (d. h. Risiko durch Identitätsbetrug)

Unser erster Schritt in dieser Umfrage bestand in der Suche nach weltweiten Unternehmen. Die Studie basiert auf diagnostischen Interviews und der Kostenzuordnung nach Tätigkeiten zur Erfassung und Extrapolation der Kostendaten. Das Ponemon Institute übernahm alle Phasen dieses Untersuchungsprojekts, das folgende Schritte umfasste:

01 Arbeitssitzungen, um Fragengebiete auszuarbeiten

02 Auswahl von Benchmark-Unternehmen

03 Entwicklung eines Frameworks zur Kostenzuordnung nach Tätigkeiten

04 Verwaltung des Studienprogramms

05 Analyse aller Ergebnisse mit entsprechenden Zuverlässigkeitsprüfungen

06 Vorbereitung eines Berichts, der alle wichtigen Ergebnisse zusammenfasst

UNTERSUCHTE STICHPROBE

BEI DER BENCHMARK-UNTERSUCHUNG IST DIE ANALYSEEINHEIT DAS UNTERNEHMEN.

ABB. 1:

Branchen der teilnehmenden Unternehmen

Abb. 1 zeigt die prozentuale Verteilung der untersuchten Unternehmen in 13 Branchen. Die drei am stärksten vertretenen Branchen waren Finanzdienstleister, Dienstleistungsunternehmen und Betriebe aus dem produzierenden Gewerbe. Zu den Finanzdienstleistern gehören Banken, Versicherungen, Vermögensverwalter und Makler. Unter „Dienstleistungen“ fällt eine Vielzahl von Unternehmen, darunter beispielsweise auch Wirtschaftsprüfungsgesellschaften, Unternehmensberater und Dienstleistungsunternehmen.

n = 278 Unternehmen

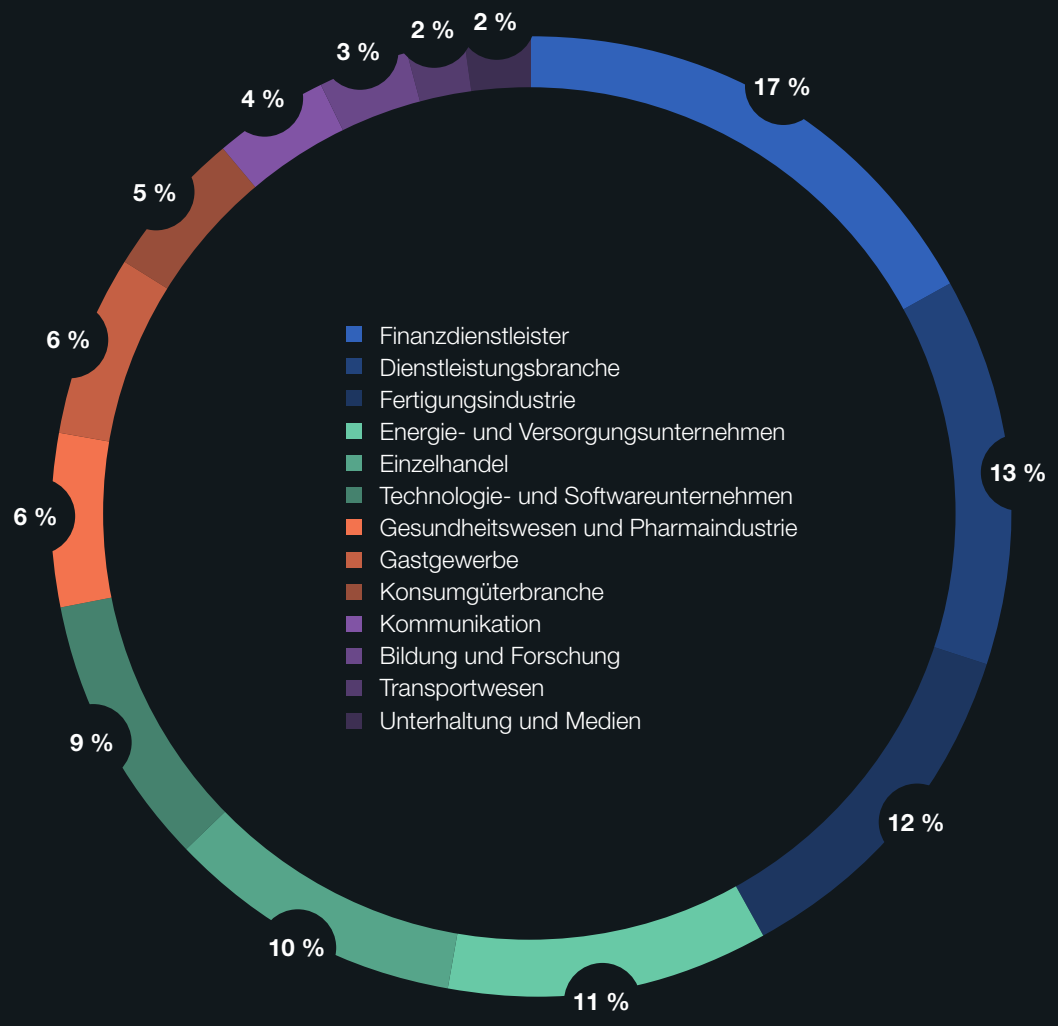


ABB. 2:

Mitarbeiterzahl der teilnehmenden Unternehmen

Abb. 2 zeigt den prozentualen Anteil der Unternehmen nach weltweiter Mitarbeiterzahl (anstelle der Unternehmensgröße). Wie sich zeigt, handelt es sich bei 43 % der Stichprobe um größere Unternehmen mit mehr als 5.000 in Vollzeit tätigen Mitarbeitern.

n = 278 Unternehmen

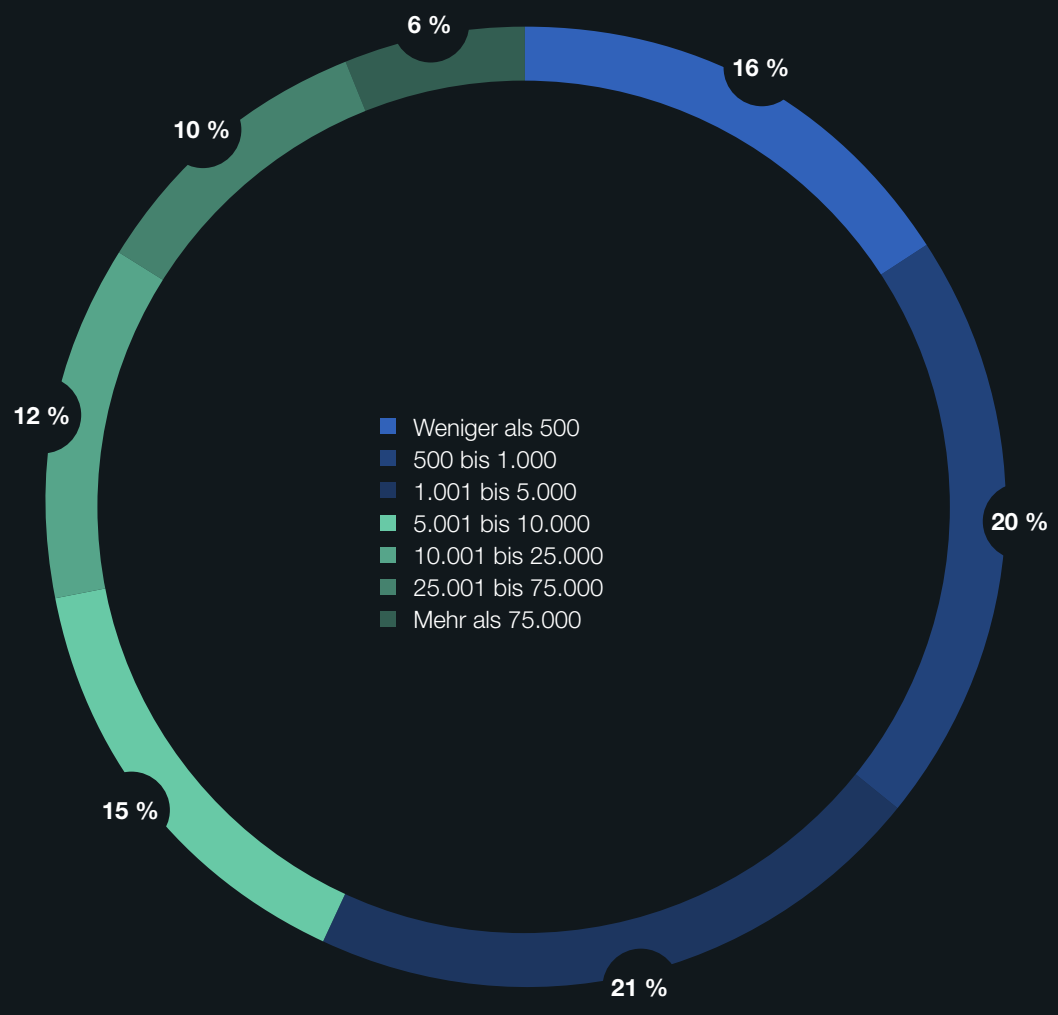


ABB. 3:

Umfrageteilnehmer nach Position oder Funktion

In Abb. 3 ist zu sehen, dass 1.004 Personen an den Interviews vor Ort teilnahmen. Pro untersuchtem Unternehmen wurde mit durchschnittlich 4,7 Personen gesprochen. Die größten Bereiche waren: CISO (15 %), IT-Operations (14 %), CIO (12 %) und IT-Techniker (11 %).

n = 1.004 Teilnehmer

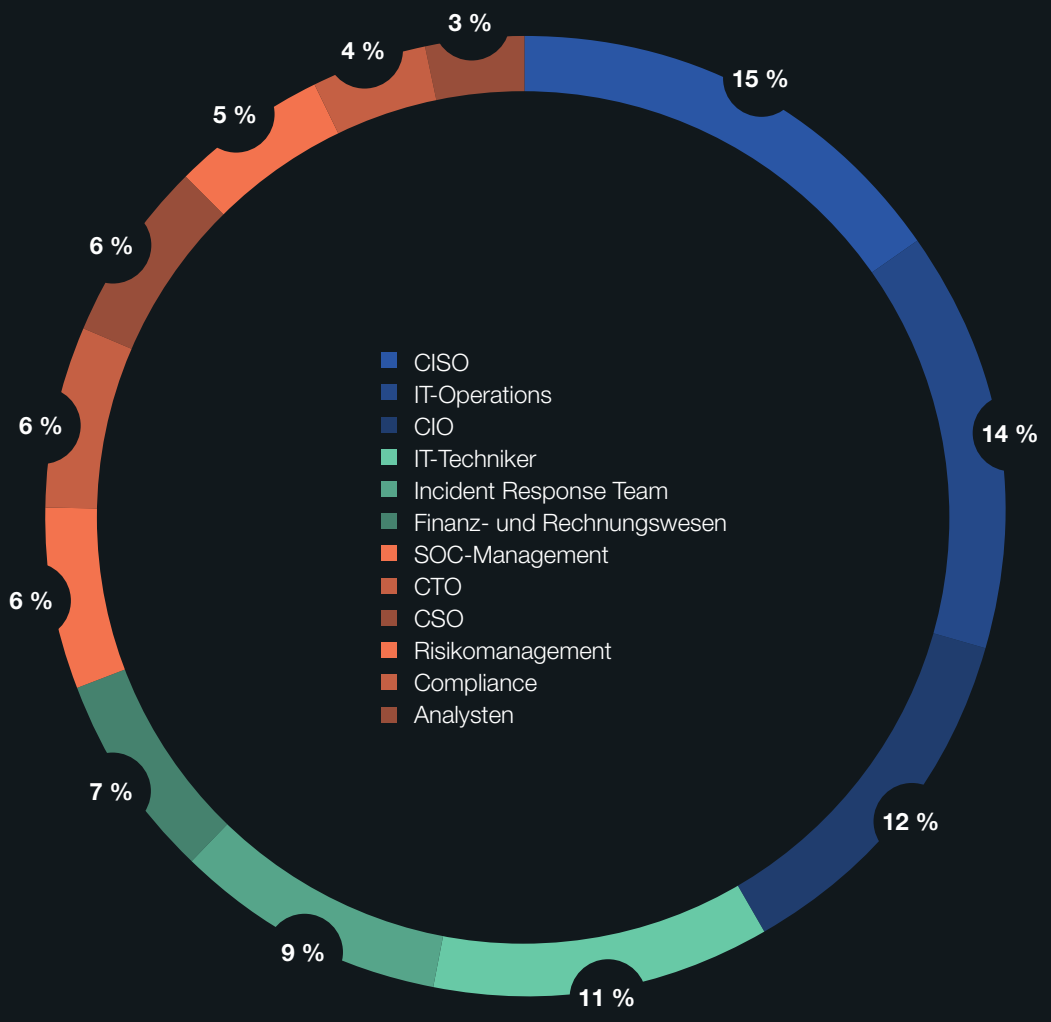
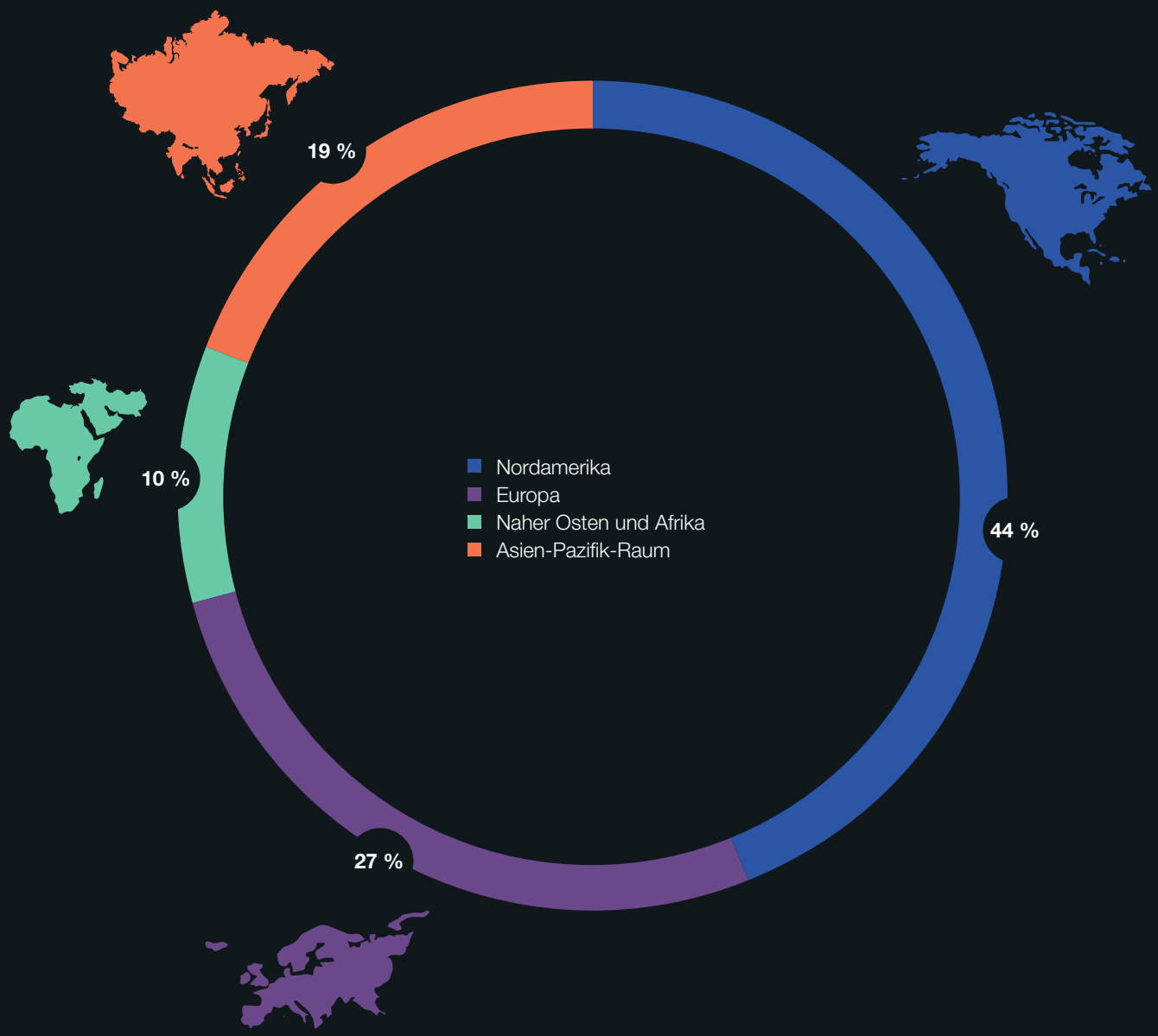


ABB. 4:

Regionale Verteilung der untersuchten Unternehmen

Abb. 4 zeigt die weltweite Verteilung der teilnehmenden Unternehmen. Nordamerika hat dabei den größten Anteil (44 %), während die wenigsten Unternehmen im Nahen Osten und in Afrika ansässig sind (10 %).

n = 278 Unternehmen



DIE WICHTIGSTEN ERKENNTNISSE

DIE GRÖSSTE ZAHL GEMELDETER ZWISCHENFÄLLE BEI EINEM EINZIGEN UNTERNEHMEN LAG BEI 46, DIE KLEINSTE BEI EINEM ZWISCHENFALL.

Fahrlässig handelnde Mitarbeiter oder Auftragnehmer

3.807

Insider mit kriminellen oder böswilligen Motiven

1.749

Angreifer mit gestohlenen Anmeldedaten (Risiko durch Identitätsbetrug)

1.247

ABB. 5:

Häufigkeit der drei Insider-Profile bei den 6.803 Zwischenfällen

Mitarbeiter oder Auftragnehmer sind nach wie vor die wichtigste Quelle von Bedrohungen. Abb. 5 zeigt die Verteilung der 6.803 gemeldeten Angriffe, die wir in unserer Stichprobe analysiert haben. Insgesamt 3.807 Angriffe (56 %) waren auf Fahrlässigkeit von Mitarbeitern oder Auftragnehmern zurückzuführen. Kriminelle oder böswillige Insider waren der Grund für weitere 1.749 Angriffe (26 %). Zudem gab es 1.247 Diebstähle von Anmeldedaten (18 %).

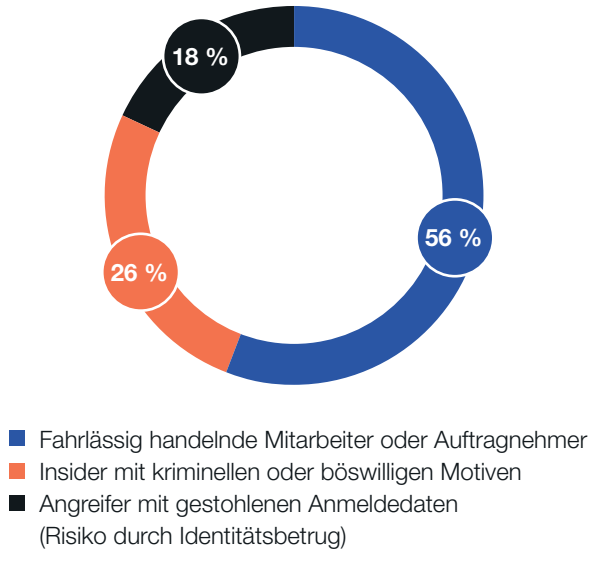
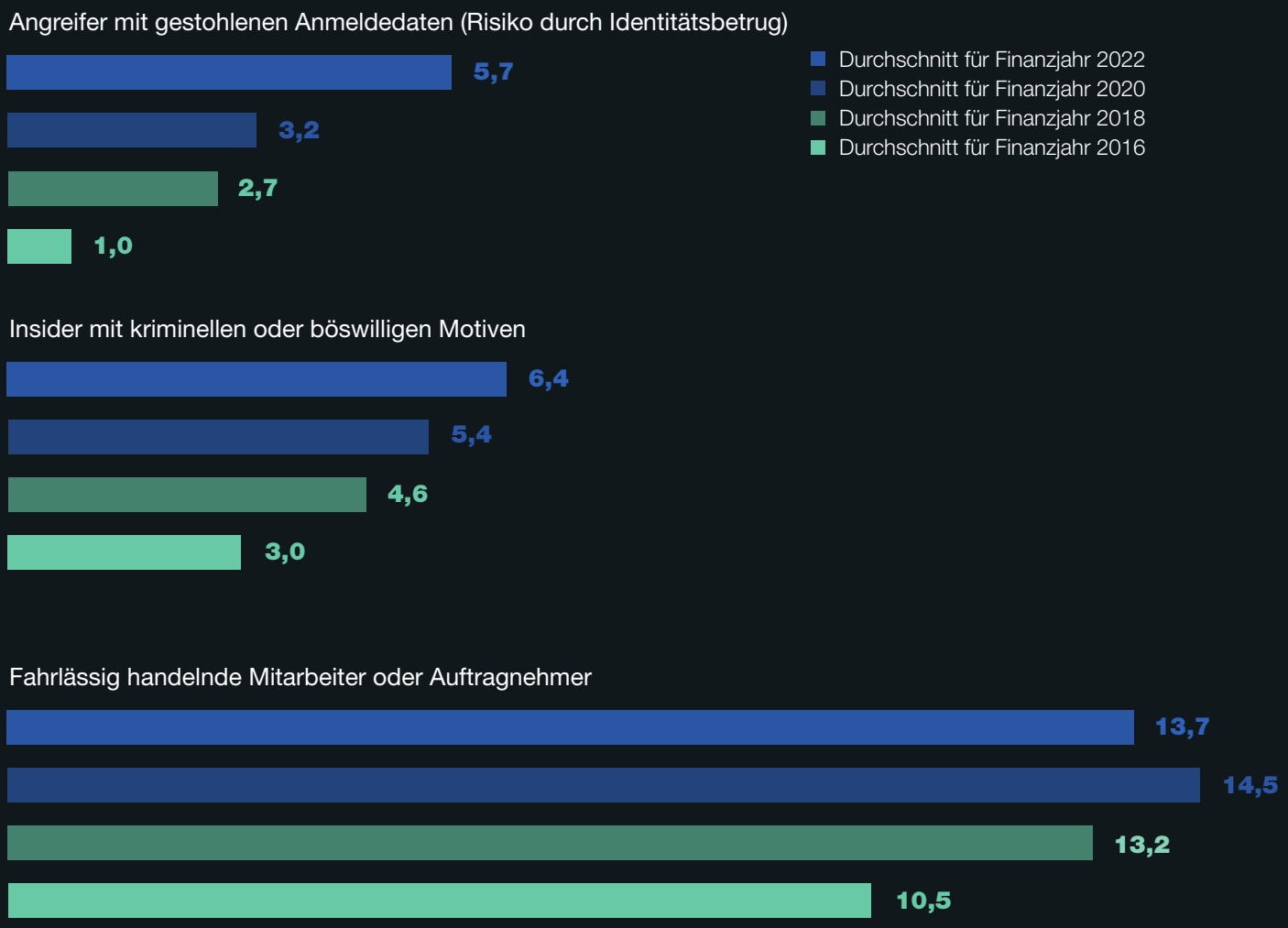


ABB. 6:

Häufigkeit der drei Profile von Insider-bezogenen Zwischenfällen

Die durchschnittliche Zahl von Anmeldedatendiebstählen hat sich beinahe verdoppelt. Wie in Abb. 6 zu sehen, stiegen Anmeldedatendiebstähle von einem Durchschnittswert von 3,2 Zwischenfällen im Jahr 2020 auf 5,7 Zwischenfälle in der aktuellen Untersuchung. Zwischenfälle durch Insider mit kriminellen oder böswilligen Motiven haben sich von 5,4 auf 6,4 erhöht.[1] Fahrlässigkeit durch Mitarbeiter oder Auftragnehmer ging von 14,5 auf 13,7 leicht zurück.



1 Die Daten für 2016 beziehen sich auf Unternehmen in den USA. Die Daten für 2022 umfassen Nordamerika, Europa, den Nahen Osten und Afrika sowie den Asien-Pazifik-Raum. Wir gehen davon aus, dass die Daten vergleichbar sind, da die im Bericht für 2016 untersuchten US-amerikanischen Unternehmen international tätig sind.

ABB. 7:

Häufigkeit von Insider-bezogenen Zwischenfällen pro Unternehmen

Die Häufigkeit von Zwischenfällen pro Unternehmen ist deutlich gestiegen. Abb. 7 zeigt die konsolidierte Durchschnittshäufigkeit von Fahrlässigkeit durch Mitarbeiter oder Auftragnehmer, Insider mit kriminellen oder böswilligen Motiven sowie Zwischenfälle mit Anmeldedatendiebstahl pro Unternehmen. Der aktuellen Untersuchung zufolge verzeichnen 67 % der Unternehmen pro Jahr zwischen 21 und mehr als 40 Zwischenfällen. Das entspricht einem Anstieg von 60 % gegenüber 2020 bzw. 53 % gegenüber 2018.

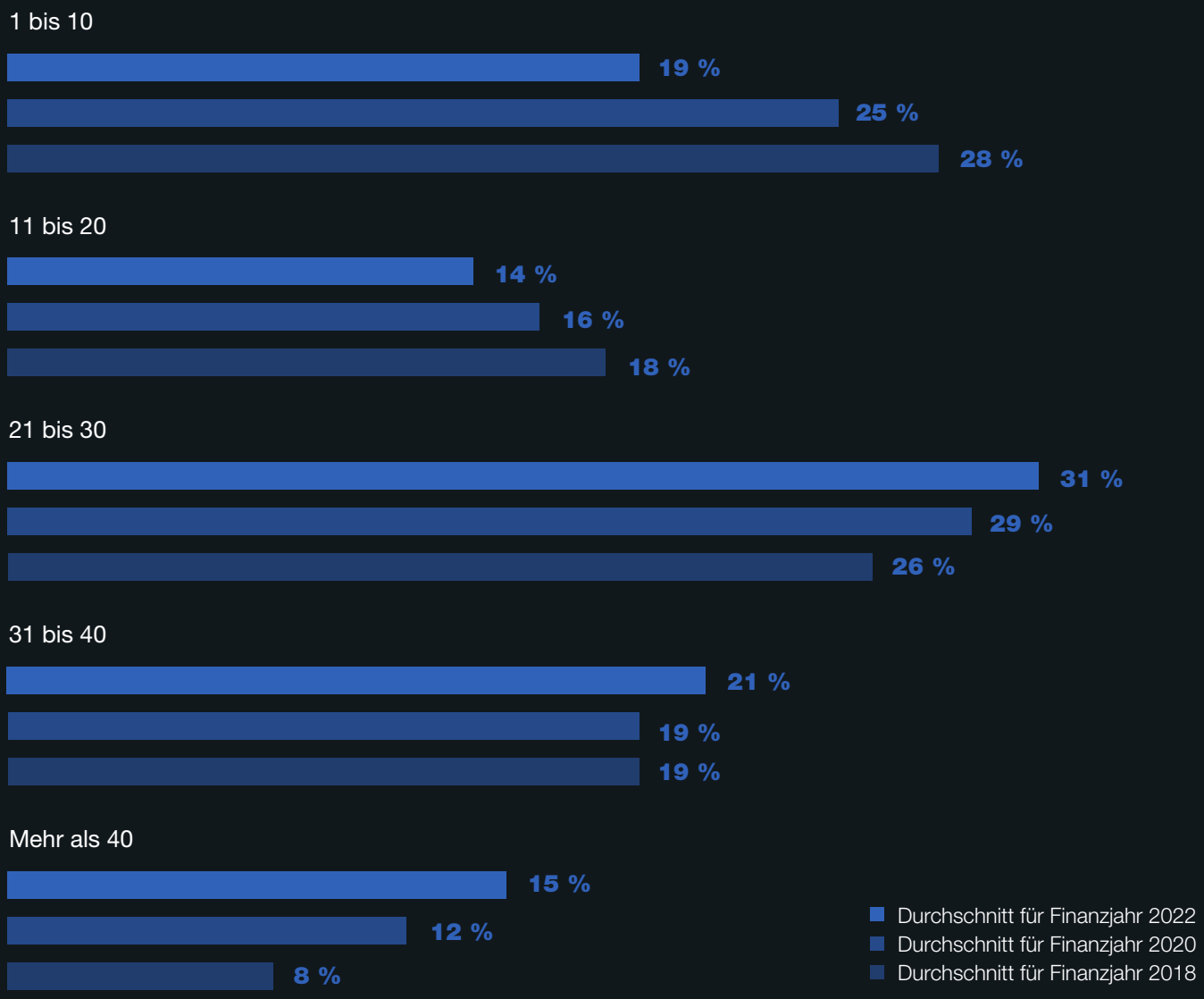


ABB. 8:

Durchschnittliche Häufigkeit von Zwischenfällen für die drei Profile nach geografischer Region

Unternehmen im Nahen Osten und in Afrika verzeichneten die meisten Insider-bezogenen Zwischenfälle, solche im Asien-Pazifik-Raum die wenigsten.
Abb. 8 stellt die Häufigkeit der Insider-bezogenen Zwischenfälle in den vier untersuchten Regionen dar. In allen Regionen hat fahrlässiges Verhalten von Mitarbeitern oder Auftragnehmern den größten Anteil. Nordamerika und der Nahe Osten sowie Afrika verzeichnen die meisten Fälle von Anmeldedaten-Diebstahl.

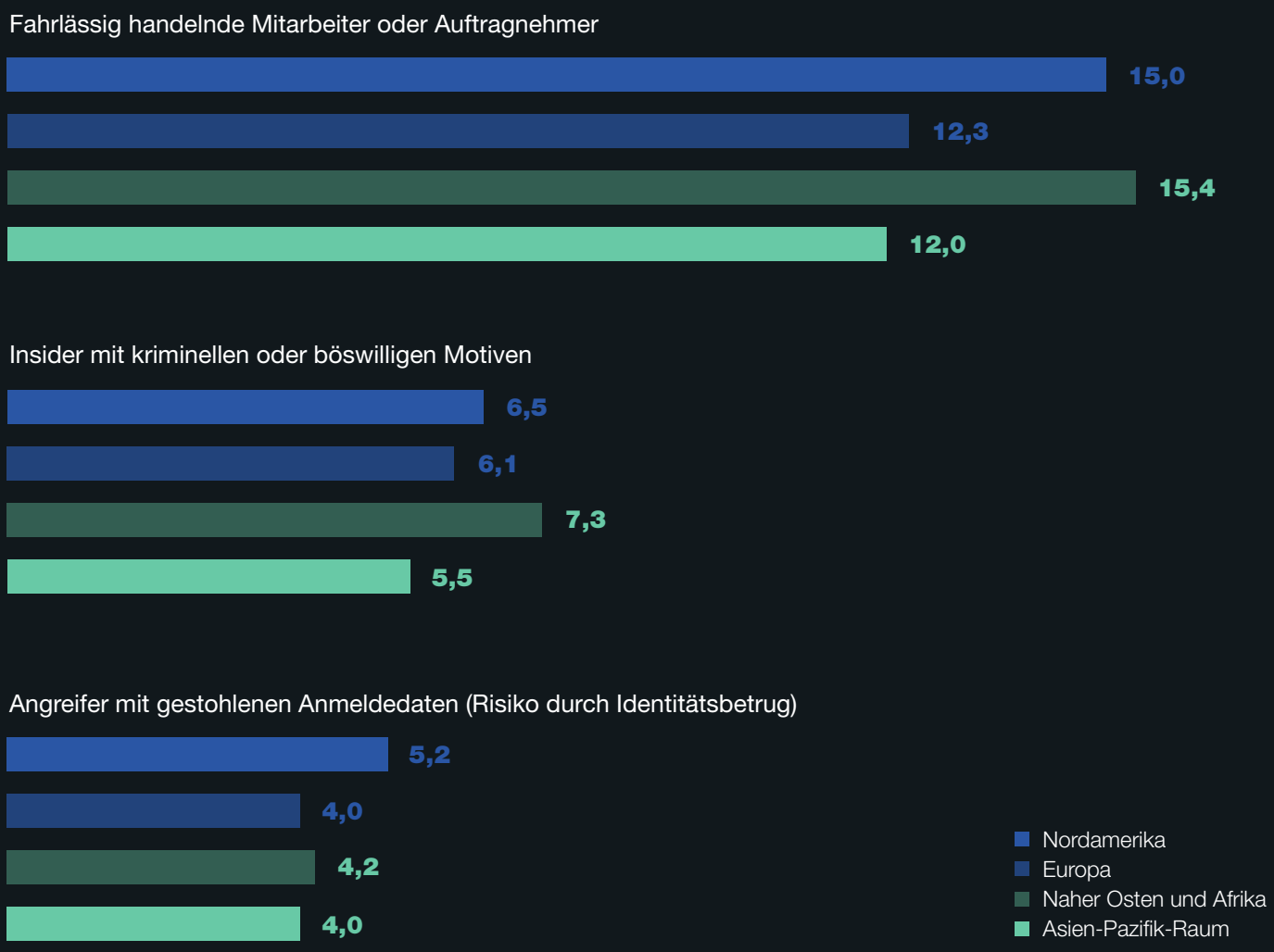


ABB. 9:

Streudiagramm Insider-bezogener Zwischenfälle nach Unternehmen

Abb. 9 stellt ein Streudiagramm der Insider-bezogenen Zwischenfälle pro Unternehmen dar. Von den 278 teilnehmenden Unternehmen hatten 152 (55 %) in den letzten zwölf Monaten durchschnittliche Gesamtkosten in Höhe von oder unterhalb des Mittelwerts von 15,4 Millionen US-Dollar. Die verbliebenen 125 Unternehmen (45 %) liegen über diesem Wert. Dies zeigt, dass die Verteilung ungleichmäßig ist.

n = 278 Unternehmen

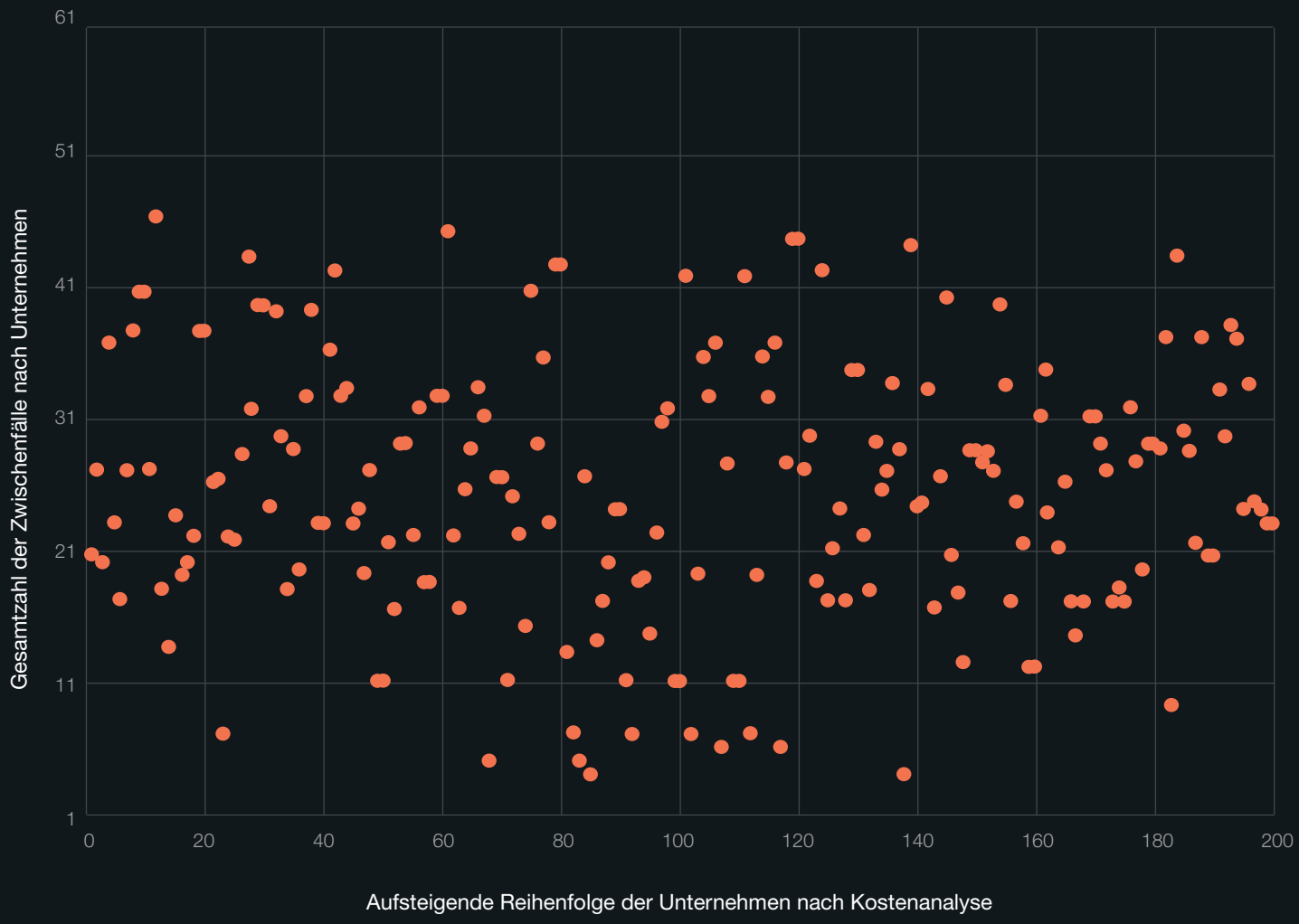


ABB. 10:

Prozentuale Verteilung bei Insider-bezogenen Zwischenfällen basierend auf der Eindämmungsdauer

Unternehmen benötigen im Durchschnitt 85 Tage, um eine Insider-Bedrohung einzudämmen. Laut Abb. 10 dauerte die Eindämmung Insider-bezogener Zwischenfälle in unserer Benchmark-Stichprobe durchschnittlich 85 Tage. Nur 12 % der Zwischenfälle wurden in weniger als 30 Tagen eingedämmt.

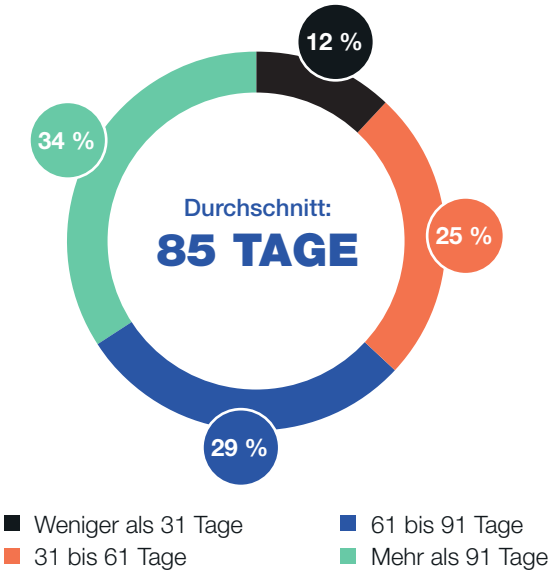


TABELLE 1:

Tools und Tätigkeiten zur Verringerung von Insider-Bedrohungen.

In unseren Interviews wurden drei Technologien genannt, die die größten Kosteneinsparungen ermöglichen: Data Loss Prevention (DLP, Datenverlustprävention), Privileged Access Management (PAM, Verwaltung privilegierter Zugriffe) sowie User and Entity Behavior Analytics (UEBA, Verhaltensanalyse von Benutzern) (siehe Tabelle 1).

Mehr als eine Antwort zulässig

TECHNOLOGIEN ZUR KOSTENREDUZIERUNG BEI DEN DREI HAUPTURSACHEN VON INSIDER-RISIKEN	ANTEIL IN PROZENT
Data Loss Prevention (DLP, Datenverlustprävention)	64 %
Privileged Access Management (PAM, Verwaltung privilegierter Zugriffe)	60 %
User and Entity Behavior Analytics (UEBA, Verhaltensanalyse von Benutzern)	57 %
Sicherheitsinformations- und Ereignis-Management (SIEM)	53 %
Endpoint Detection and Response (EDR, Endpunkterkennung und Reaktion)	50 %
Insider Threat Management (ITM, Abwehr von Insider-Bedrohungen)	41 %
Sonstiges (bitte angeben)	3 %
Gesamt	**328 %**

DIE KOSTEN DER INSIDER-ZWISCHENFÄLLE

ABB. 11:

Anteil der Kosten durch Insider nach Folgen für Unternehmen

Störungen oder Ausfälle sowie Technologien verursachen im Zusammenhang mit Insider-Bedrohungen die größten Kosten. Abb. 11 stellt den Anteil bei Zwischenfällen durch unachtsame oder fahrlässige Mitarbeiter, kriminelle Insider und den Diebstahl von Anmeldedaten in den sieben Kostenkategorien dar. Die beiden größten Kostenkategorien sind Geschäftsunterbrechungen aufgrund verringerter Mitarbeiterproduktivität (23 % der Gesamtkosten) sowie Technologien (21 %), wobei dies den Abschreibungswert sowie die Lizenzierung von Software und Hardware umfasst, die als Reaktion auf Insider-bezogene Zwischenfälle implementiert werden.

Die Prozesskosten umfassen Steuerungs- und Kontrollsystem-Tätigkeiten als Reaktion auf Bedrohungen und Angriffe. Die Gemeinkosten decken vielfältige Kosten für Support-Personal sowie die IT-Sicherheitsinfrastruktur ab.

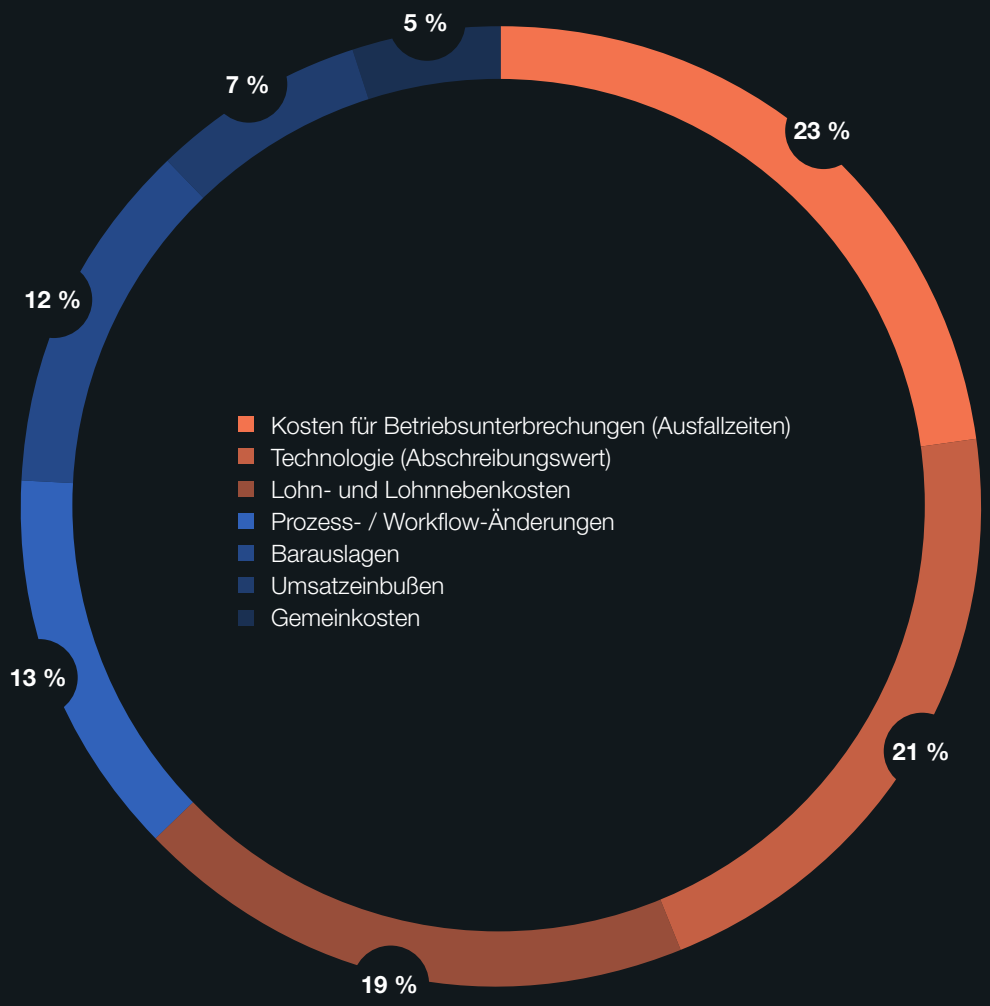


ABB. 12:

Insider-bezogene Zwischenfälle in aufsteigender Reihenfolge nach Mitarbeiterzahl (Größe)

JE GRÖSSER DAS UNTERNEHMEN, DESTO MEHR INSIDER-BEZOGENE ZWISCHENFÄLLE

Abb. 12 zeigt die Verteilung Insider-bezogener Zwischenfälle in aufsteigender Reihenfolge nach Mitarbeiterzahl (bzw. Größe) der befragten Unternehmen. Die ansteigenden Zahlen weisen darauf hin, dass die Häufigkeit der Insider-bezogenen Zwischenfälle positiv mit der Unternehmensgröße korreliert. Die Korrelation ist bei größeren Unternehmen am stärksten ausgeprägt.

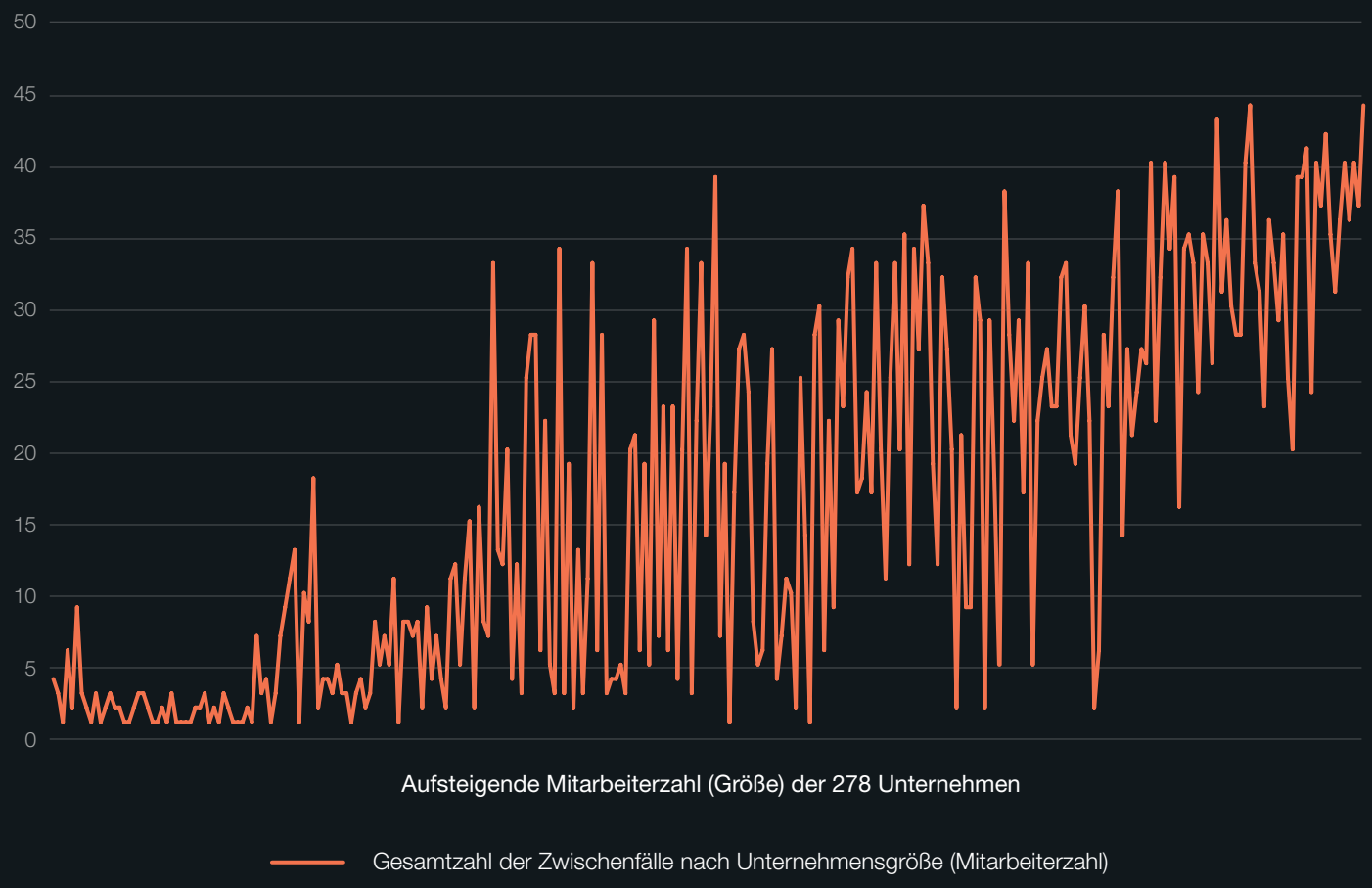


TABELLE 2:

Die durchschnittlichen Jahreskosten pro Zwischenfall für die drei Zwischenfallarten

Anmeldedatendiebstahl stellt nach wie vor den kostspieligsten Insider-Zwischenfall dar. Tabelle 2 zeigt die Durchschnittskosten pro Zwischenfall, die durchschnittliche Zahl an Zwischenfällen pro Jahr und die durchschnittlichen Jahreskosten. Fahrlässigkeit von Mitarbeitern oder Auftragnehmern tritt am häufigsten auf – allerdings verursacht diese Art von Zwischenfall im Schnitt sehr viel weniger Kosten als Anmeldedatendiebstahl und Zwischenfälle durch böswillige Insider.

Die Kosten von Zwischenfällen durch kriminelle Insider sind zwischen 2018 und 2020 von 614.192 US-Dollar auf 755.761 US-Dollar stetig gestiegen. In der aktuellen Untersuchung sind sie jedoch auf 648.062 US-Dollar gefallen. Die durchschnittliche Zahl der Anmeldedatendiebstähle hat sich seit 2018 deutlich erhöht; die Durchschnittskosten für die Behebung dieser Zwischenfälle betragen in der diesjährigen Untersuchung 804.997 US-Dollar.

FALLPROFILE AUS DEM FINANZJAHR 2018	DURCHSCHNITTS-KOSTEN PRO ZWISCHENFALL	DURCHSCHNITTLICHE ZAHL VON ZWISCHEN-FÄLLEN PRO JAHR	DURCH-SCHNITTLICHE JAHRESKOSTEN
Fahrlässig handelnde Mitarbeiter oder Auftragnehmer	277.557 $	13,2	3.663.752 $
Insider mit kriminellen oder böswilligen Motiven	614.192 $	4,6	2.825.283 $
Angreifer mit gestohlenen Anmeldedaten (Risiko durch Identitätsbetrug)	672.112 $	2,7	1.814.702 $
			8.303.737 $
FALLPROFILE AUS DEM FINANZJAHR 2020			
Fahrlässig handelnde Mitarbeiter oder Auftragnehmer	317.111 $	14,9	4.724.954 $
Insider mit kriminellen oder böswilligen Motiven	755.761 $	5,4	4.081.109 $
Angreifer mit gestohlenen Anmeldedaten (Risik durch Identitätsbetrug)	871.686 $	3,2	2.789.395 $
			11.595.458 $
FALLPROFILE AUS DEM FINANZJAHR 2022			
Fahrlässig handelnde Mitarbeiter oder Auftragnehmer	484.931 $	13,7	6.643.555 $
Insider mit kriminellen oder böswilligen Motiven	648.062 $	6,4	4.147.597 $
Angreifer mit gestohlenen Anmeldedaten (Risiko durch Identitätsbetrug)	804.997 $	5,7	4.588.483 $
			15.378.635 $

Angaben in Millionen US-Dollar

KOSTENANALYSE

DIESE UNTERSUCHUNG DECKT GRUNDLEGENDE PROZESSBEZOGENE TÄTIGKEITEN AB, DIE VERSCHIEDENE AUSGABEN UND KOSTEN IM ZUSAMMENHANG MIT DER REAKTION DES UNTERNEHMENS AUF INSIDER-BEZOGENE ZWISCHENFÄLLE NACH SICH ZIEHEN.

Die sieben Kostenstellen sind in unserem Framework wie folgt definiert:[2]

- **Kontrolle und Überwachung:** Tätigkeiten, mit denen ein Unternehmen in angemessenem Maße Zwischenfälle und Angriffe durch Insider erkennen und möglicherweise abwehren kann. Dazu gehören verrechnete (Gemein-)Kosten bestimmter Technologien, die die Behebung von Zwischenfällen oder Früherkennung von Bedrohungen unterstützen.
- **Untersuchung:** Aktivitäten, die notwendig sind, um Quelle, Umfang und Ausmaß von Zwischenfällen definitiv zu bestimmen.
- **Eskalation:** Tätigkeiten zur Bekanntmachung tatsächlicher Zwischenfälle bei wichtigen Verantwortlichen im Unternehmen. Dazu gehören auch die Schritte, mit denen eine erste Management-Reaktion organisiert wird.
- **Reaktion auf Zwischenfälle:** Tätigkeiten im Zusammenhang mit der Zusammenstellung des Vorfallreaktionsteams. Dazu gehören die notwendigen Schritte zum Formulieren einer endgültigen Management-Reaktion.
- **Eindämmung:** Tätigkeiten zur Abwehr oder Abschwächung der Folgen von Zwischenfällen oder Angriffen durch Insider, beispielsweise die Abschaltung anfälliger Anwendungen und Endpunkte.
- **Ex-Post-Reaktion:** Mit diesen Tätigkeiten sollen zukünftige Insider-bezogene Zwischenfälle und Angriffe auf das Unternehmen verhindert werden. Dazu gehören auch Maßnahmen zur Kommunikation mit wichtigen Verantwortlichen innerhalb und außerhalb des Unternehmens, z. B. die Vorbereitung von Empfehlungen, um potenzielle Schäden zu minimieren.
- **Behebung:** Bei diesen Tätigkeiten werden die Unternehmenssysteme und grundlegenden Geschäftsprozesse repariert und behoben. Dazu gehört die Wiederherstellung beschädigter Informationsressourcen und IT-Infrastrukturen.

2 Die internen Kosten werden anhand der Arbeitszeit als Ersatz für direkte und indirekte Kosten extrapoliert. Auf diese Weise wird auch der Gemeinkostenanteil der Fixkosten berechnet, z. B. mehrjährige Investitionen in Technologien.

TABELLE 3:

Durchschnittlicher Trend der Tätigkeitskosten pro Zwischenfall für die sieben Kostenstellen.

Unternehmen geben am meisten für die Eindämmung von Insider-Zwischenfällen aus. Wie bereits erwähnt, hat sich in dieser Untersuchung die durchschnittliche Eindämmungsdauer für einen Zwischenfall von 77 auf 85 Tage erhöht. Tabelle 3 fasst die Durchschnittskosten Insider-bezogener Zwischenfälle für die drei Zwischenfallarten und sieben Kostenstellen zusammen. Wie bereits angeführt, stellen die Eindämmung und Untersuchung eines Zwischenfalls die teuersten Kostenstellen dar, während für die Ex-Post-Analyse und Eskalation die geringsten Kosten anfallen. Die Tätigkeitskosten haben sich seit 2016 um 80 % erhöht.

KOSTENSTELLEN NACH TÄTIGKEITSBEREICH	FJ 2016	FJ 2018	FJ 2020	FJ 2022
Kontrolle und Überwachung	9.620 $	12.634 $	22.124 $	35.080 $
Untersuchung	41.461 $	78.398 $	103.798 $	128.056 $
Eskalation	8.919 $	12.542 $	21.805 $	32.228 $
Reaktion auf Zwischenfälle	66.371 $	91.263 $	118.317 $	120.391 $
Eindämmung	122.796 $	173.161 $	211.553 $	184.548 $
Ex-Post-Reaktion	8.498 $	11.491 $	19.480 $	26.563 $
Behebung	91.397 $	138.532 $	147.776 $	119.131 $
Gesamt	**349.152 $**	**517.921 $**	**644.853 $**	**645.997 $**

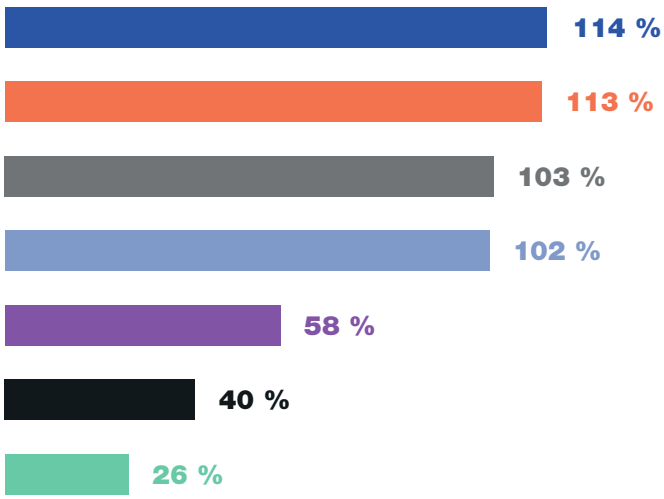


ABB. 13:

Anteil des Nettoanstiegs der durchschnittlichen Jahreskosten von Finanzjahr 2016 bis Finanzjahr 2022

Die Reaktion auf einen Insider-Zwischenfall ist seit 2016 deutlich teurer geworden. Wie Abb. 13 zeigt, sind die Kosten für Kontrolle und Überwachung sowie Eskalation seit 2016 am stärksten gestiegen – jeweils um 114 % und 113 %. Der durchschnittliche jährliche Anstieg der Tätigkeitskosten beläuft sich seit 2016 auf 80 %.

TABELLE 4:

Kosten der sieben Tätigkeitsbereiche nach Zwischenfallart für 2022

Die Eindämmung von Insider-Zwischenfällen macht den höchsten Kostenanteil bei Anmeldedatendiebstählen (Risiko durch Identitätsbetrug) und bei fahrlässig verursachten Zwischenfällen aus. In Tabelle 4 werden die durchschnittlichen Jahreskosten für die sieben Tätigkeitsbereiche nach Art des Zwischenfalls dargestellt.

FINANZJAHR 2022: KOSTENSTELLEN NACH TÄTIGKEITSBEREICH	FAHRLÄSSIG HANDELNDE MITARBEITER / AUFTRAG-NEHMER	KRIMINELLER / BÖSWILLIGER INSIDER	ANGREIFER MIT GESTOHLENEN ANMELDEDATEN (IDENTITÄTS-BETRUG)	DURCH-SCHNITTS-KOSTEN
Kontrolle und Überwachung	34.517 $	34.511 $	36.213 $	35.080 $
Untersuchung	121.511 $	126.545 $	136.111 $	128.056 $
Eskalation	29.121 $	31.112 $	36.451 $	32.228 $
Reaktion auf Zwischenfälle	112.345 $	119.711 $	129.118 $	120.391 $
Eindämmung	151.311 $	149.814 $	252.518 $	184.548 $
Ex-Post-Reaktion	23.515 $	26.733 $	29.441 $	26.563 $
Behebung	12.611 $	159.636 $	185.145 $	119.131 $
Gesamt	**484.931 $**	**648.062 $**	**804.997 $**	**645.997 $**

ABB. 14:

Durchschnittliche Jahreskosten 2022 pro Zwischenfall für die drei Zwischenfallarten

Die durchschnittlichen Tätigkeitskosten sind beim Diebstahl von Anmeldedaten am höchsten. Abb. 14 zeigt den Unterschied zwischen den Tätigkeitskosten für Fahrlässigkeit durch Mitarbeiter oder Auftragnehmer und denen für Anmeldedatendiebstahl.

Angaben in US-Dollar

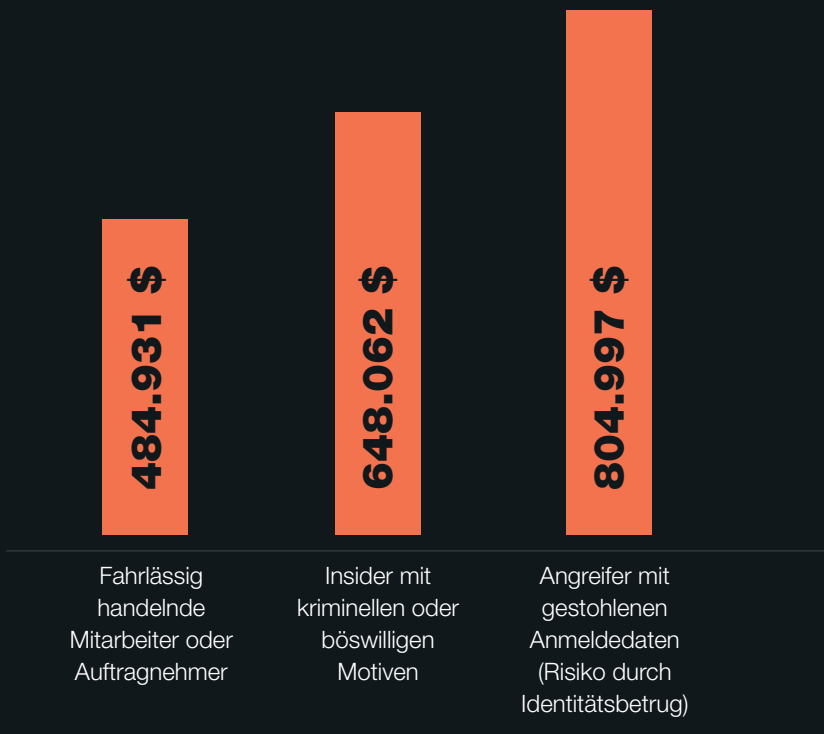


ABB. 15:

Durchschnittliche Tätigkeitskosten nach Region

NORDAMERIKANISCHE UNTERNEHMEN GEBEN ÜBER-DURCHSCHNITTLICH VIEL GELD FÜR TÄTIGKEITEN ZUR ABWEHR VON INSIDER-BEDROHUNGEN AUS.

Die Durchschnittskosten für Tätigkeiten zur Behebung von Insider-Bedrohungen über einen Zeitraum von zwölf Monaten betragen insgesamt 15,38 Millionen US-Dollar. Wie in Abb. 15 gezeigt, verzeichneten nordamerikanische Unternehmen mit 17,53 Millionen US-Dollar die höchsten Gesamtkosten. Auf Platz 2 lagen Unternehmen in Europa mit 15,44 Millionen US-Dollar. Der Asien-Pazifik-Raum lag mit 11,90 Millionen US-Dollar deutlich unter den Durchschnittskosten aller 278 Unternehmen.

Durchschnitt = 15,38 $ (in Millionen US-Dollar)

ABB. 16:

Durchschnittliche Tätigkeitskosten nach Mitarbeiterzahl

Großunternehmen geben am meisten für die Tätigkeiten zur Behebung einer Insider-Bedrohung aus. Wie in Abb. 16 gezeigt, wenden Unternehmen mit einer Mitarbeiterzahl von 25.000 bis 75.000 erheblich mehr Geld für Tätigkeiten auf, die zur Behebung eines Zwischenfalls nötig sind – im Durchschnitt 23 Mio. US-Dollar.

Durchschnitt = 15,38 $ (in Millionen US-Dollar)

Für drei Profile konsolidiert

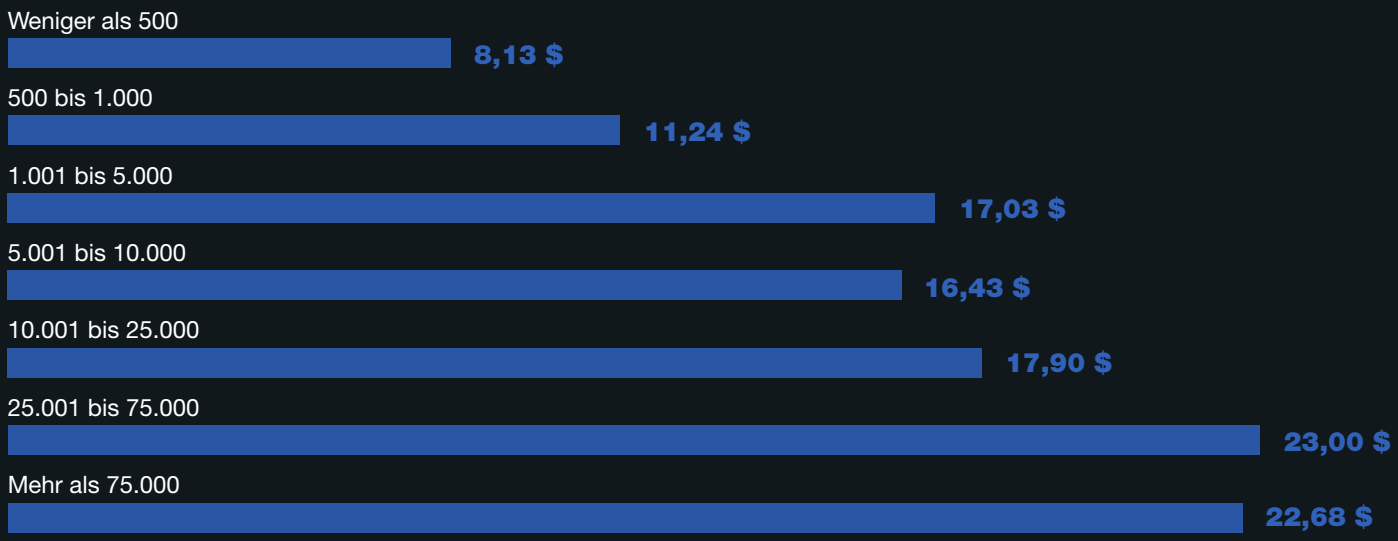
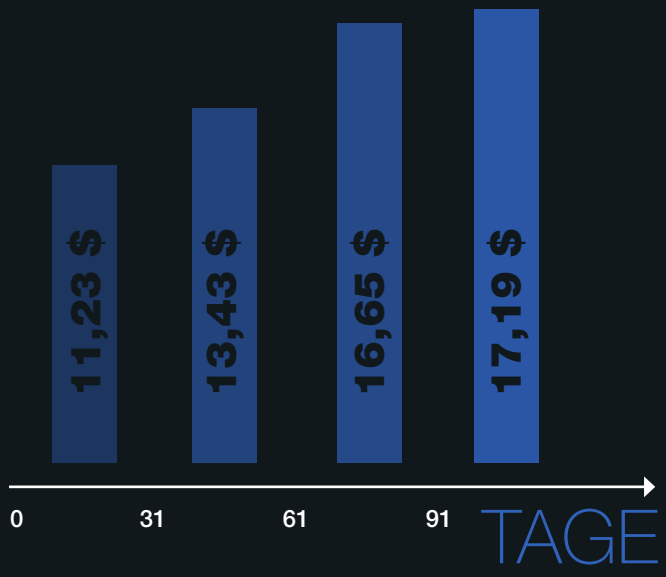


ABB. 17:

Durchschnittliche Tätigkeitskosten nach Eindämmungsdauer in Tagen

Je schneller die Eindämmung, desto geringer die Tätigkeitskosten. Die Jahresgesamtkosten korrelieren positiv mit der Eindämmungsdauer durch Insider-bezogene Zwischenfälle.
Wie Abb. 17 zeigt, waren Zwischenfälle mit einer Eindämmungsdauer von mehr als 90 Tagen mit den höchsten Gesamtkosten pro Jahr verbunden (17,19 Millionen US-Dollar). Im Gegensatz dazu wurden bei Zwischenfällen mit weniger als 30 Tagen Eindämmungsdauer die geringsten Gesamtkosten verzeichnet (11,23 Millionen US-Dollar).
Die durchschnittlichen Jahreskosten liegen bei 15,38 Millionen US-Dollar.



Durchschnitt = 15,38 $ (in Millionen US-Dollar)

ABB. 18:

Anteilige Kosten Insider-bezogener Zwischenfälle nach Tätigkeitsbereich

Ein Drittel aller Kosten fallen auf die Eindämmung. Das folgende Kreisdiagramm zeigt die anteiligen Kosten von sieben Kostenstellen. Laut Abb. 18 fallen für die Eindämmung 29 % der Gesamtjahreskosten für Insider-bezogene Zwischenfälle an. Tätigkeiten im Zusammenhang mit der Untersuchung und Reaktion auf Zwischenfälle stellen 20 % bzw. 19 % der Gesamtkosten dar.

n = 278 Unternehmen

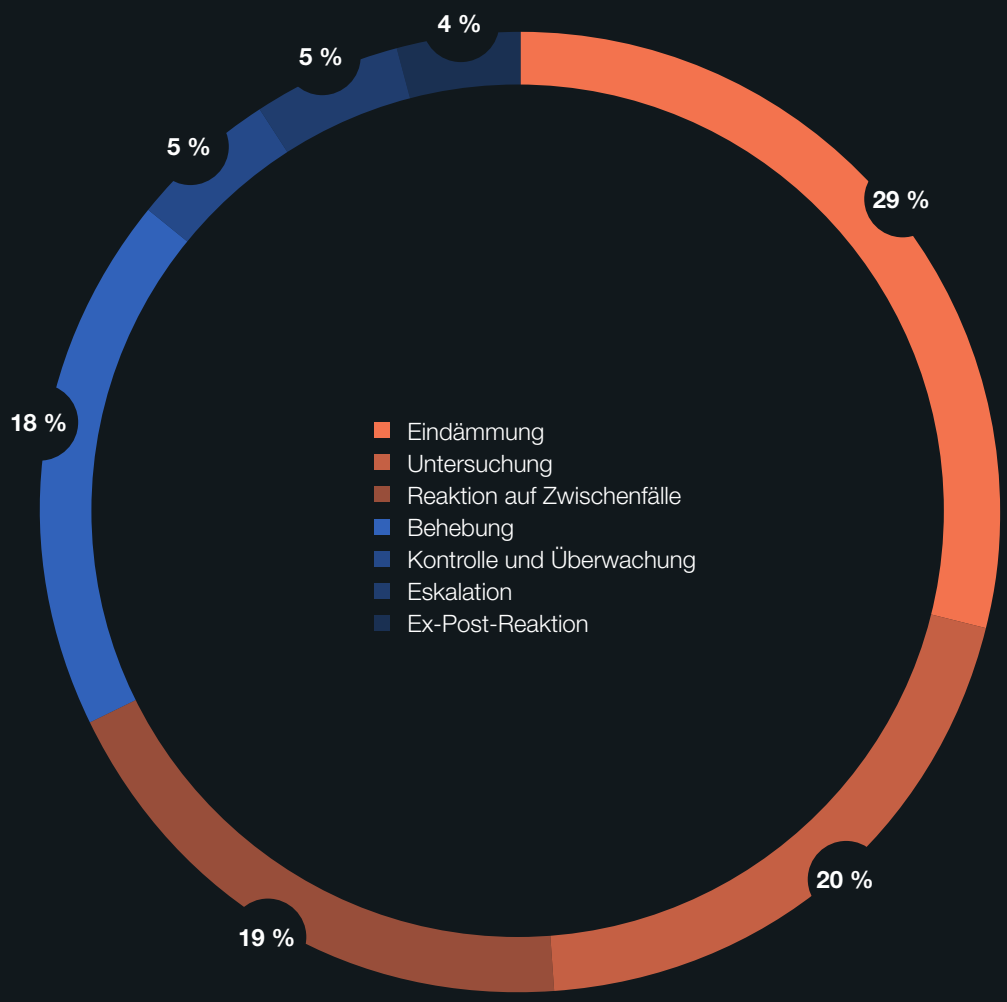


ABB. 19:

Jährliche Tätigkeitskosten nach Branche

FÜR FINANZDIENSTLEISTER UND DIENSTLEISTUNGSUNTERNEHMEN SIND DIE TÄTIGKEITSKOSTEN DEUTLICH HÖHER.

Wie Abb. 19 zeigt, betragen die durchschnittlichen Kosten für diese Unternehmen 21,25 Millionen bzw. 18,65 Millionen US-Dollar – sehr viel mehr als der Durchschnitt von 15,4 Millionen US-Dollar. Zu Dienstleistungsunternehmen zählen beispielsweise Anwaltskanzleien sowie Beratungs- und Wirtschaftsprüfungsunternehmen.

Angaben in Millionen US-Dollar

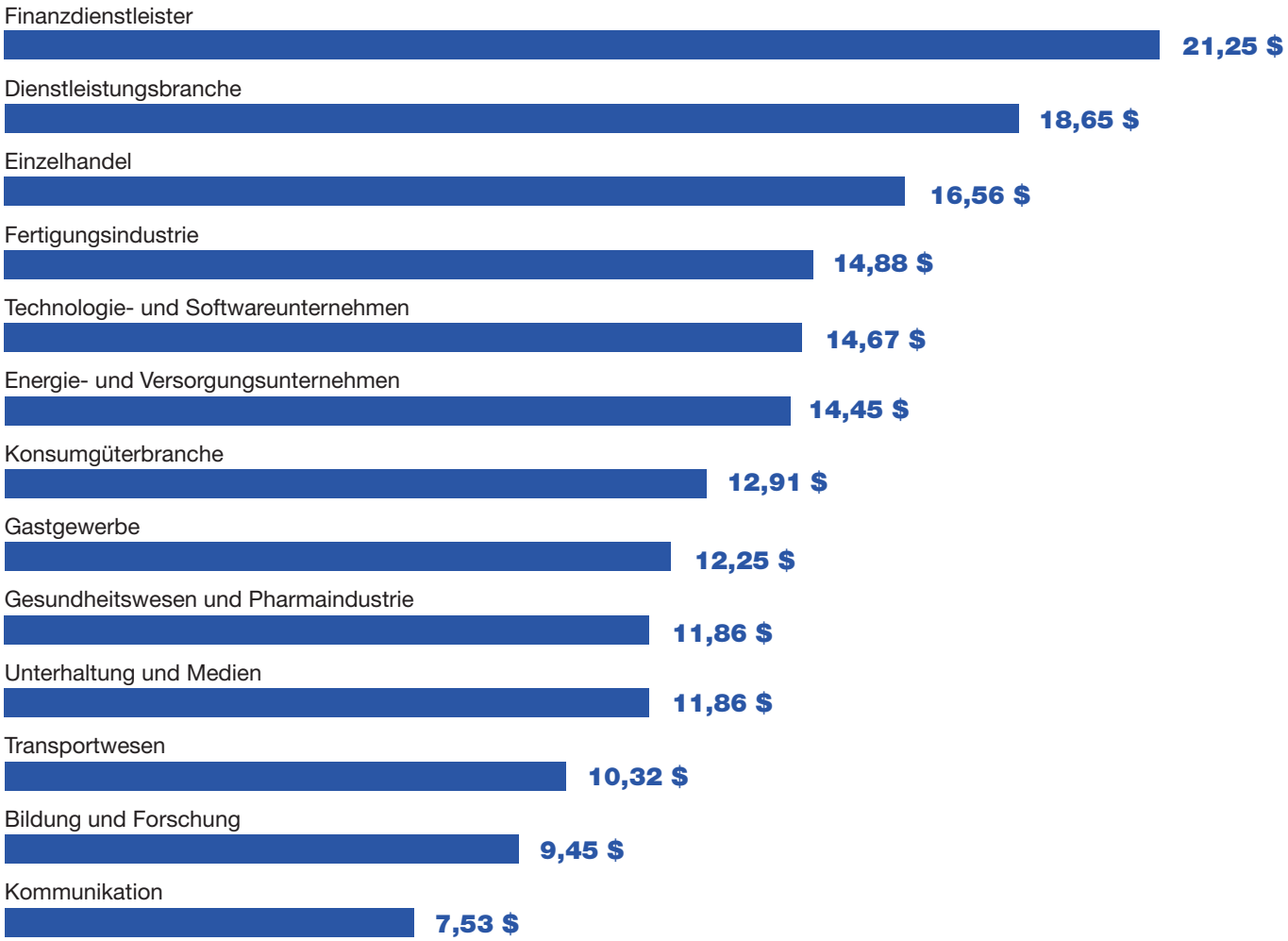
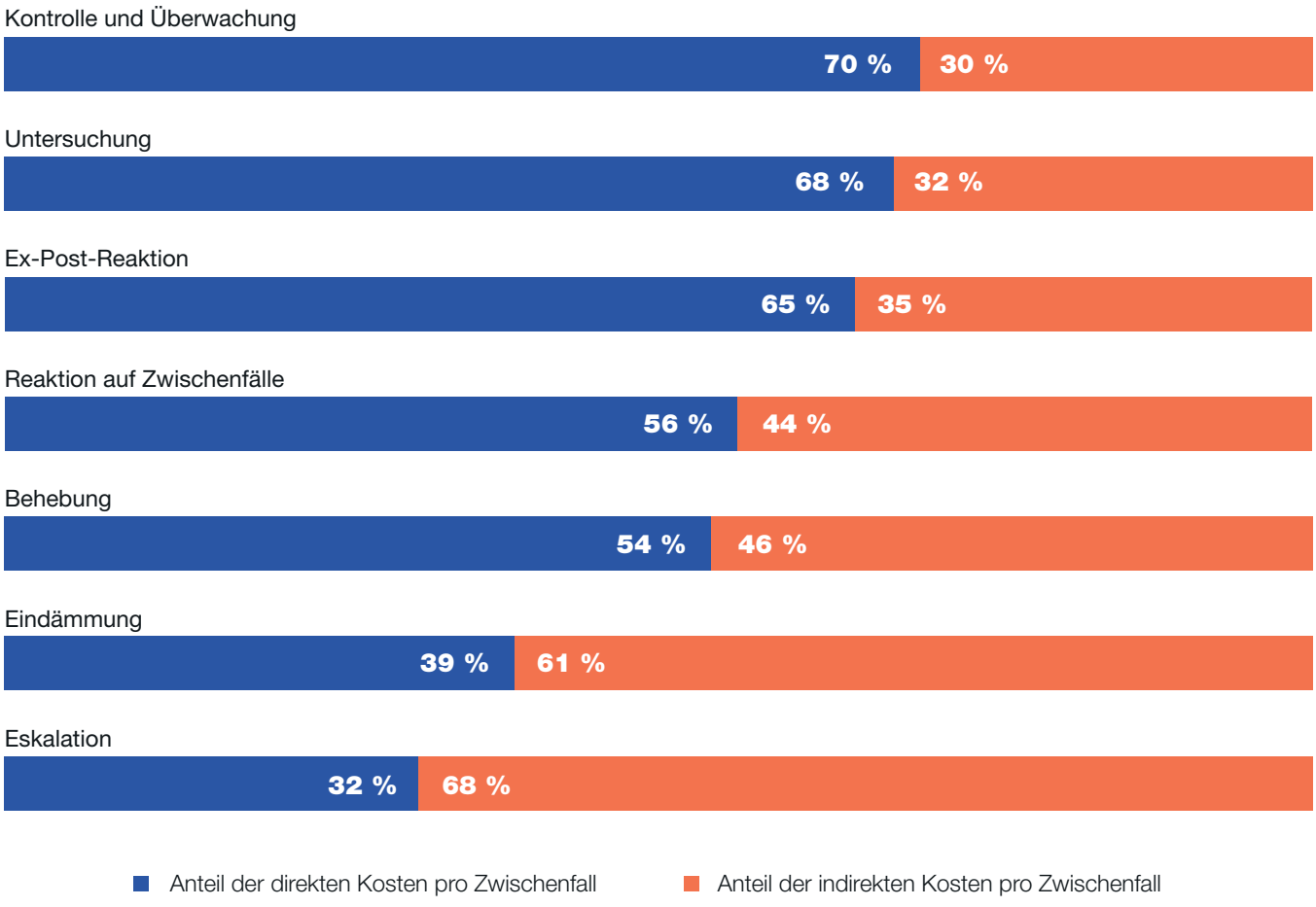


ABB. 20:

Gegenüberstellung der Anteile der direkten und indirekten Kosten für Kostenstellen

Die Unternehmen sollten die direkten und indirekten Kosten für die Durchführung der jeweiligen Tätigkeiten schätzen. Abb. 20 zeigt den Anteil der direkten und indirekten Kosten[3] für sieben interne Tätigkeiten-Kostenstellen. Die Kosten für Kontrolle und Überwachung sowie Untersuchung haben dabei den größten Anteil an den direkten Kosten (70 % bzw. 68 %). Den größten Teil der indirekten Kosten für Tätigkeiten machen Eindämmung (61 %) und Eskalation (68 %) aus.

Für drei Profile konsolidiert



3 Die direkten Kosten sind die Ausgaben für die Durchführung einer bestimmten Tätigkeit, während die indirekten Kosten aus dem Zeit- und Arbeitsaufwand sowie sonstigen aufgewendeten Unternehmensressourcen zur Behebung eines Zwischenfalls bestehen.

REDUZIERUNG VON INSIDER-BEDROHUNGEN

FÜR DIESE UNTERSUCHUNG ERMITTELTEN WIR NICHT NUR DIE KOSTEN VON INSIDER-BEDROHUNGEN FÜR DIE UNTERNEHMEN, SONDERN SPRACHEN MIT DEN TEILNEHMERN AUCH ÜBER IHRE ERFAHRUNGEN MIT DER BEDROHUNG SOWIE DARÜBER, WIE SIE DIESE RISIKEN REDUZIEREN.

ABB. 21:

Über welche Insider-Zwischenfälle machen Sie sich am meisten Sorgen?

Von allen Insider-Bedrohungsarten in dieser Untersuchung machen sich Unternehmen vor allem über Anmeldedatendiebstahl Sorgen. Wie bereits erwähnt, haben sich Anmeldedatendiebstähle seit der letzten Untersuchung beinahe verdoppelt und verursachen die höchsten Behebungskosten. 55 % der Befragten geben an, dass sie vor allem über Hacker besorgt sind, die gültige Anmeldedaten von Mitarbeitern stehlen könnten. Deutlich weniger der Befragten (21 %) machen sich wegen fahrlässig handelnder Insider Sorgen.

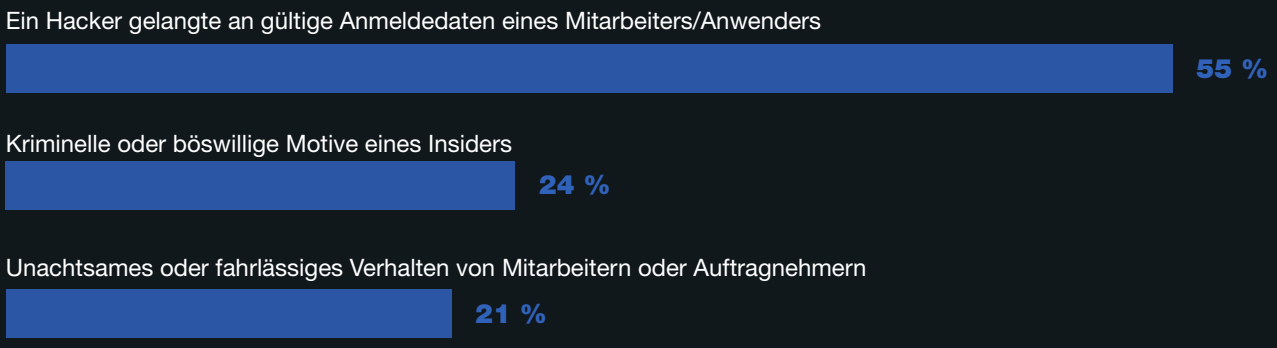


ABB. 22:

Welche der folgenden Punkte spielten bei den Zwischenfällen eine Rolle?

Fahrlässige Mitarbeiter und Anmeldedatendiebe sind die Hauptursache für die meisten Insider-Zwischenfälle. Wie Abb. 22 zeigt, geben 57 % der Teilnehmer an, dass die Insider-Zwischenfälle durch Fahrlässigkeit verursacht wurden, während 51 % sagen, dass ein böswilliger Außenstehender Daten durch die Kompromittierung von Anmeldedaten oder Konten gestohlen hat.

Mehr als eine Antwort zulässig

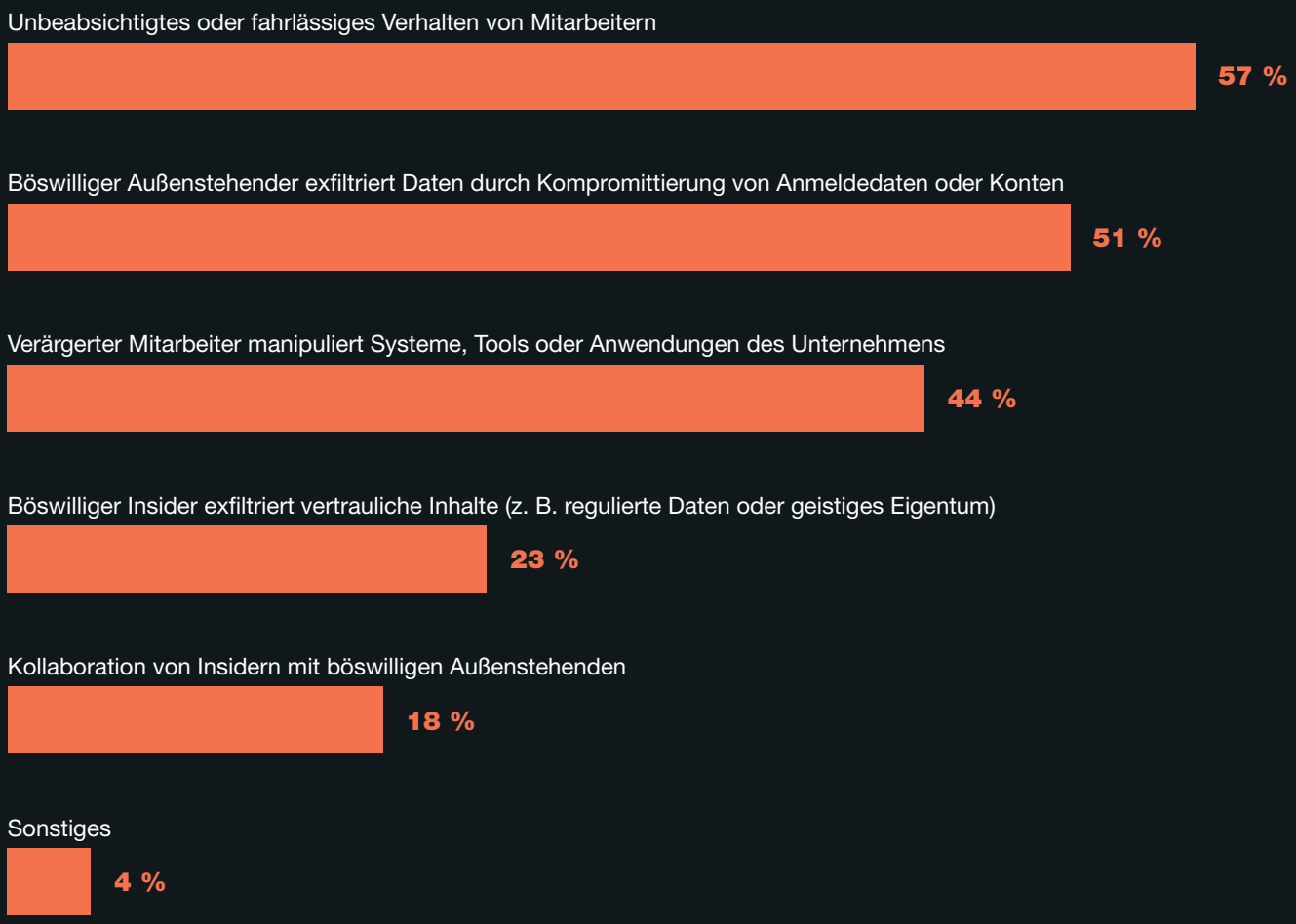


ABB. 23:

Über welche Kanäle für Insider-bezogenen Datenverlust machen Sie sich die meisten Sorgen?

Anfällige IoT-Geräte stellen das größte Risiko für Datenverlust dar. Die Vielzahl an IoT-Geräten in den Unternehmen lässt Risiken durch Insider steigen. 63 % der Teilnehmer machen sich Sorgen wegen unverwalteter IoT-Geräte, die zum Verlust vertraulicher Daten führen könnten. Wie Abb. 23 zeigt, folgen danach die Cloud (52 % der Befragten) und das Netzwerk (51 % der Befragten).

Mehr als eine Antwort zulässig

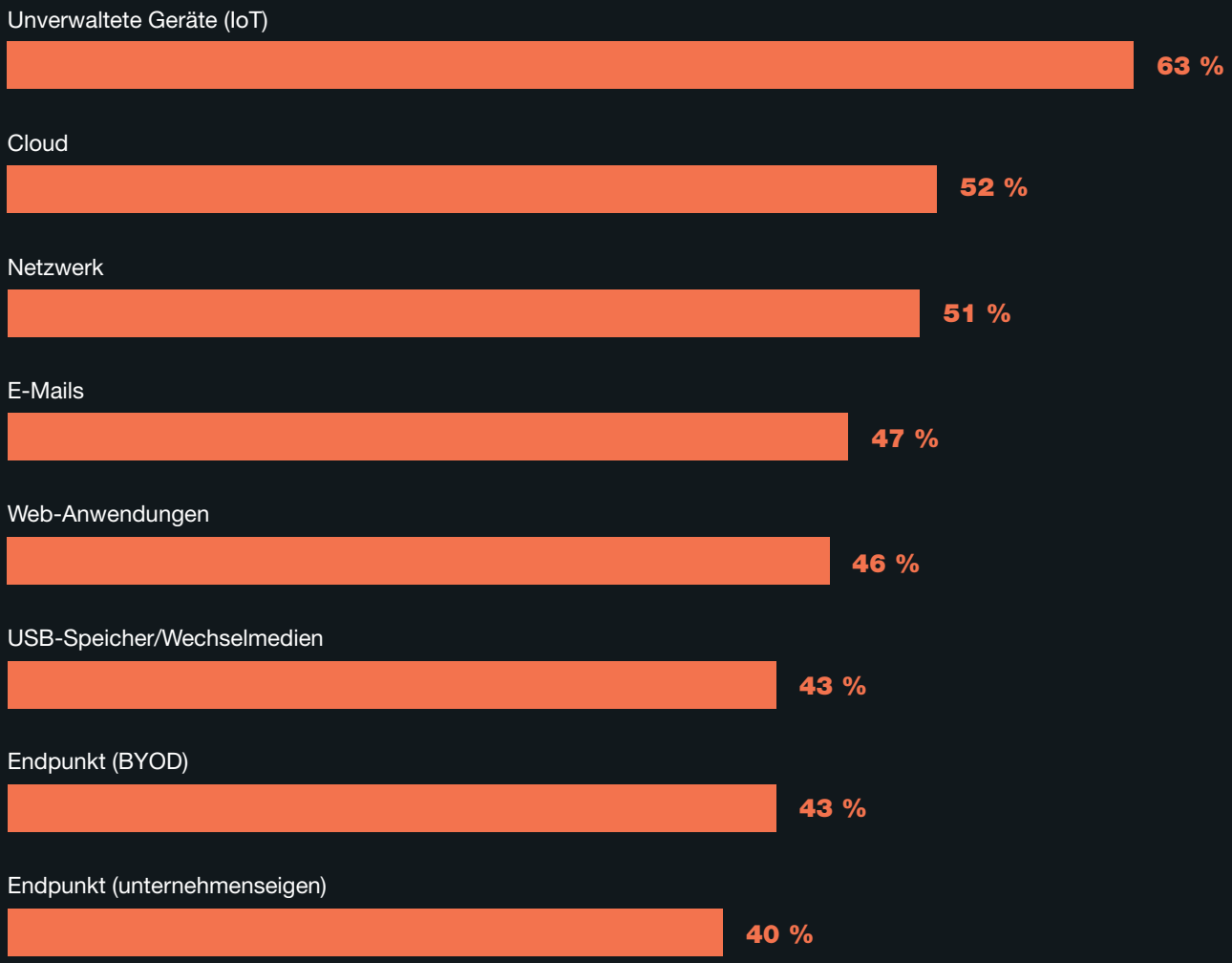


ABB. 24:

Wo speichern Ihre Anwender vertrauliche Informationen wie personenbezogene Daten, geistiges Eigentum und andere wichtige Geschäftsdaten?

Die meisten vertraulichen Daten befinden sich in den E-Mails der Mitarbeiter. Wie in Abb. 24 zu sehen, geben 65 % der Teilnehmer an, dass Mitarbeiter höchst vertrauliche Daten wie personenbezogene Informationen, geistiges Eigentum und andere kritische Geschäftsdaten in E-Mails aufbewahren. Schulungen und Programme für Sicherheitsbewusstsein verbessern den Umgang der Mitarbeiter mit vertraulichen Daten und tragen somit entscheidend dazu bei, Fahrlässigkeit zu verringern.

Drei Antworten zulässig

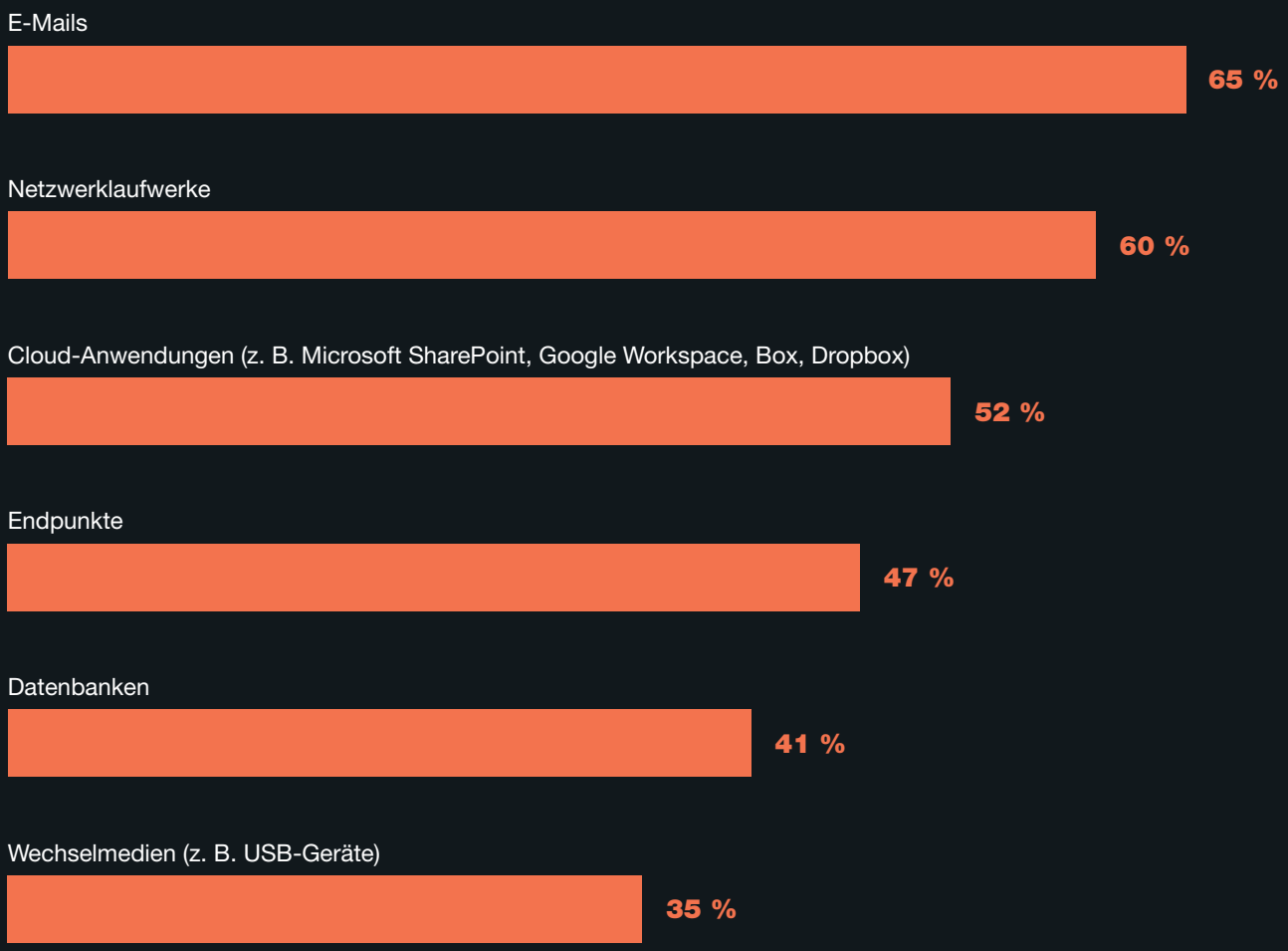


ABB. 25:

Wie arbeiten und kommunizieren Ihre Anwender mit Kollegen und Dritten?

Wie Abb. 25 zeigt, werden hauptsächlich Chat-Tools für Unternehmen (61 %) sowie E-Mails (52 %) genutzt, um intern und mit Dritten zu kommunizieren.

Drei Antworten zulässig

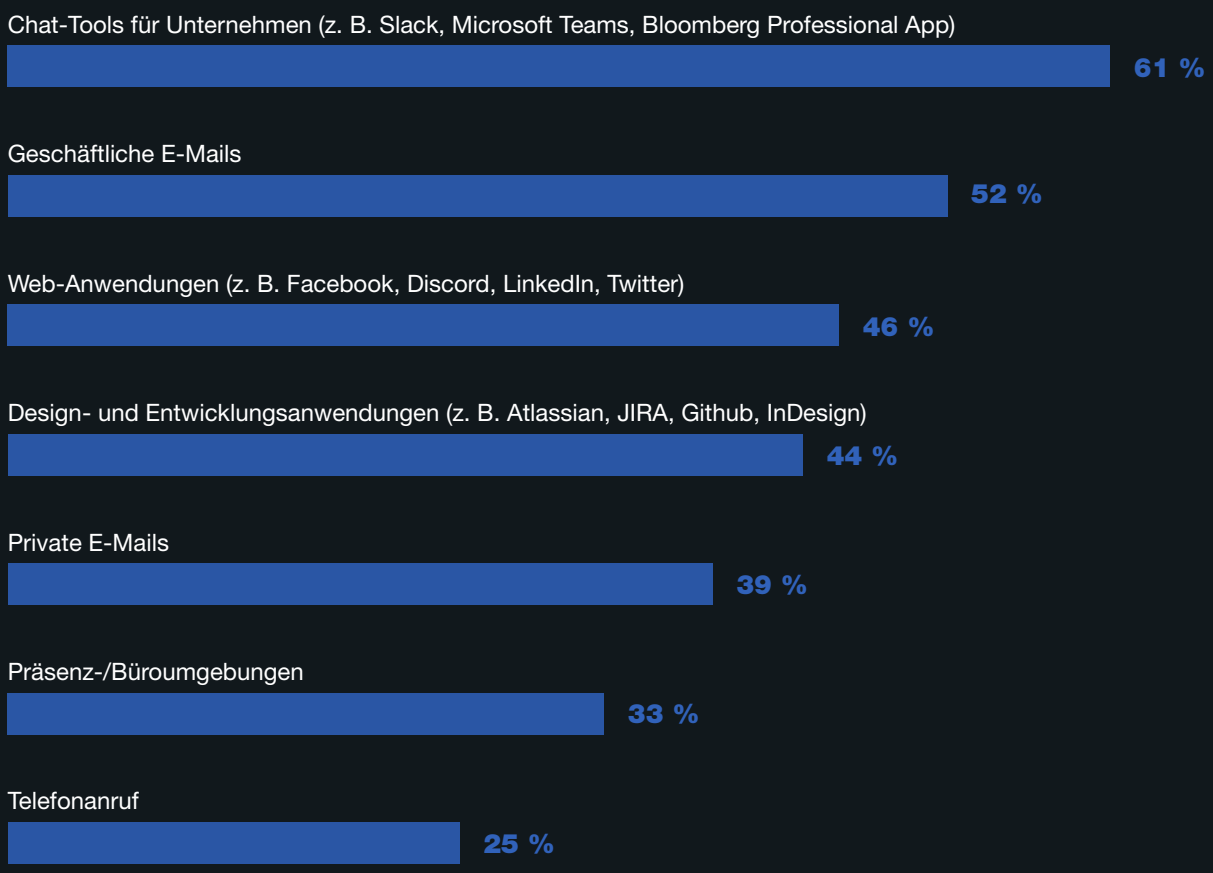


ABB. 26:

Welche der folgenden Verhaltensweisen haben böswillige Insider in Ihrem Unternehmen gezeigt?

Böswillige Insider nutzen geschäftliche E-Mails, um an vertrauliche Daten zu gelangen. Abb. 26 zeigt eine Liste der in dieser Untersuchung abgedeckten Verhaltensweisen, die böswillige Insider in den Unternehmen gezeigt haben. 74 % der Teilnehmer sagen, dass böswillige Insider vertrauliche Daten an externe Dritte verschickt haben. Dahinter folgen Scans auf offene Ports und Schwachstellen (62 %) sowie der Zugriff auf vertrauliche Daten, die nicht im Zusammenhang mit der Position oder Funktion standen (60 %).

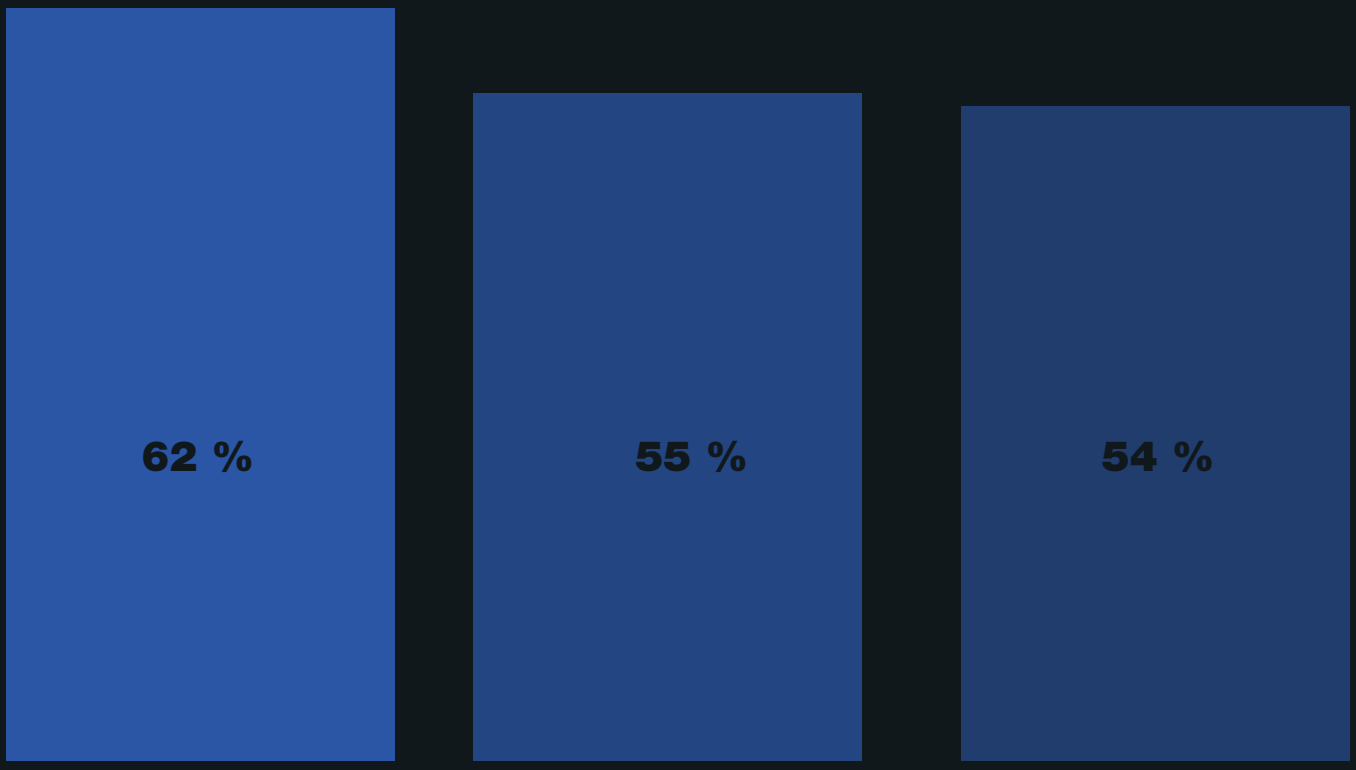
Mehr als eine Antwort zulässig

ABB. 27:

Wie wichtig sind hochentwickelte Technologien bei der Minimierung von Insider-Bedrohungen?

Da die Zahl von Insider-Zwischenfällen und die Eindämmungsdauer zunehmen, spielen hochentwickelte Technologien bei der Minimierung dieser Bedrohungen eine immer wichtigere Rolle. Wie in Abb. 27 zu sehen, gelten auf Anwenderverhalten basierende Tools zur Erkennung von Insider-Bedrohungen als unerlässlich oder sehr wichtig (62 % der Befragten). Darauf folgt die Automatisierung der Prävention, Untersuchung, Eskalation, Eindämmung und Behebung von Insider-Zwischenfällen (55 %) sowie KI- und Machine Learning-Technologie für die genannten Zwecke (54 %).

Antworten „unerlässlich“ und „sehr wichtig“ kombiniert



Auf Anwenderverhalten basierende Tools zur Erkennung von Insider-Bedrohungen

Automatisierung der Prävention, Untersuchung, Eskalation, Eindämmung und Behebung von Insider-Zwischenfällen

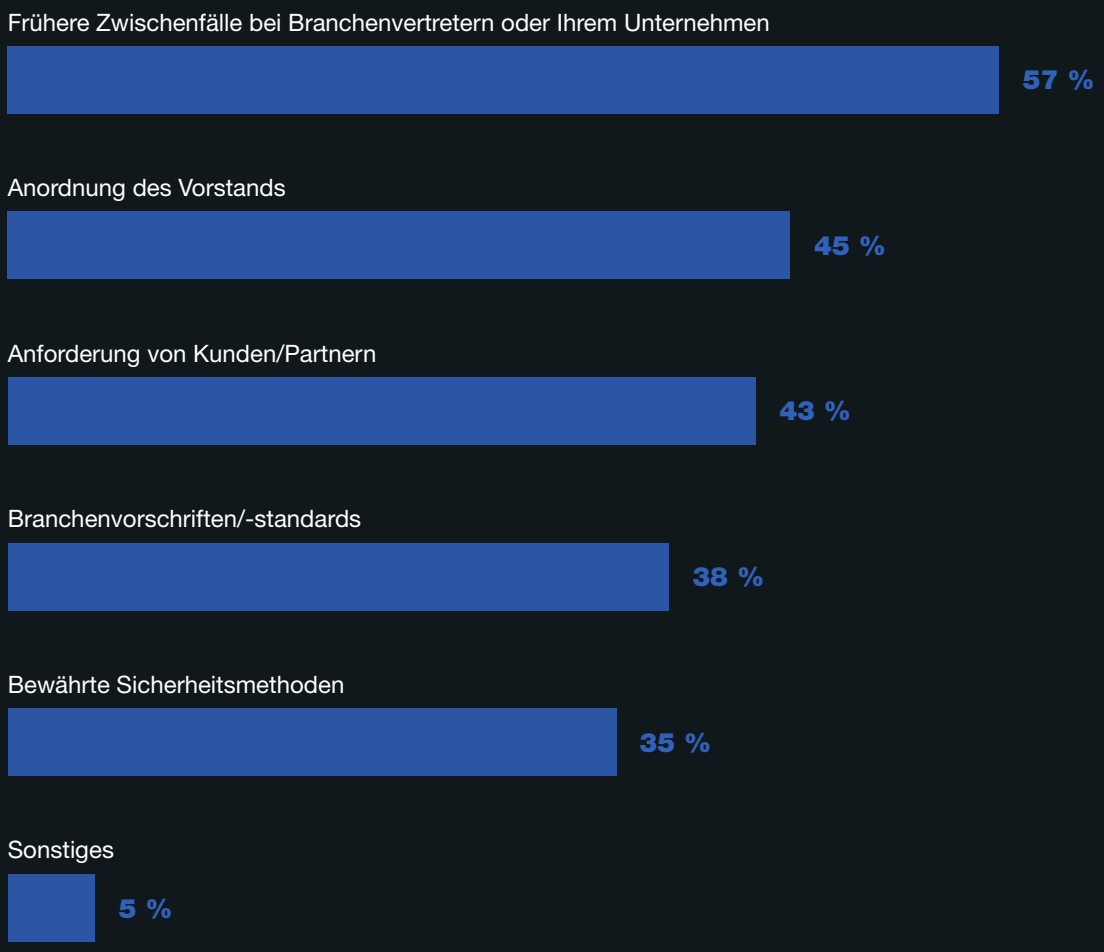
KI- und Machine Learning-Technologie, um Insider-Zwischenfälle zu verhindern, zu untersuchen, zu eskalieren, einzudämmen und zu beheben

ABB. 28:

Was war der ausschlaggebende betriebliche Faktor für Ihr Programm zur Abwehr von Insider-Bedrohungen?

Frühere Zwischenfälle motivieren die Unternehmen dazu, ein Programm zur Abwehr von Insider-Bedrohungen zu implementieren. Abb. 28 zeigt, warum sich die in dieser Untersuchung vertretenen Unternehmen um die Minimierung von Insider-Bedrohungen bemühen. Der Hauptgrund (57 %) liegt in früheren Zwischenfällen bei anderen Unternehmen. Nur 38 % der Befragten geben an, dass Branchenvorschriften und -standards für die Implementierung eines Programms zur Abwehr von Insider-Bedrohungen ausschlaggebend waren.

Mehr als eine Antwort zulässig



FAZIT

Die schnelle digitale Transformation der letzten zwei Jahre trug unbeabsichtigt zum Wachstum von Insider-Bedrohungen bei.

Die Gefahren durch die Nutzung privater Geräte und der Cloud zeigen Unternehmen, dass der traditionelle Ansatz zur Datensicherheit nicht mehr ausreicht.

Genau deshalb ist die Implementierung eines personenzentrierten Insider Threat Management (ITM)-Programms, das auf die moderne ortsunabhängige Arbeitswelt ausgelegt ist, auch so wichtig. Ein effektives ITM-Programm funktioniert durch teamübergreifende Zusammenarbeit – einschließlich der IT-, Personal-, Compliance- und Rechtsabteilung, um nur einige zu nennen. Ein Team aus technischem als auch nicht-technischem Personal gewährleistet die Umsetzung der drei erfolgreichen Elemente eines solchen Programms:

Überblick

Implementieren Sie eine ITM-Plattform, die Ihnen einen Überblick sowie Kontext zu Datenbewegungen bietet. So können Sie die durchschnittlich benötigte Zeit zur Erkennung und Reaktion verkürzen. Mit einem besseren Verständnis der Datenbewegungen können Sie zudem die durchschnittliche Zeit zur Eindämmung einer Insider-Bedrohung effektiv verringern.

Konsistenz

Bewerten Sie die Unternehmensrisiken, einschließlich der besonders gefährdeten Insider, und schaffen Sie einen speziellen Aufgabenbereich für Insider-Bedrohungen innerhalb des Unternehmens. Im Rahmen dieses Prozesses sollte ein einheitliches und wiederholbares Verfahren etabliert werden, mit dem relevante Warnmeldungen zu Insider-Bedrohungen kontextbasiert erkannt und Reaktionen ausgelöst werden. Mit einer dedizierten Lösung für Insider-Risiken können Sie einen einheitlichen Prozess gewährleisten, der die durchschnittlich benötigten Zeit zur Erkennung und Reaktion verkürzt.

Transparenz

Um zu verstehen, was beim nächsten Mal besser funktionieren könnte, ist ein kontinuierlicher Verbesserungsprozess erforderlich. Basierend auf eigenen Erfahrungen und denen anderen Unternehmen können Sie Ihre Maßnahmen zur Risikominimierung kontinuierlich und effektiv verbessern.

Da die Zahl von Insider-Zwischenfällen und die Eindämmungsdauer zunehmen, spielen hochentwickelte Technologien bei der Minimierung dieser Bedrohungen eine immer wichtigere Rolle. Ein ITM-Programm unterstützt Ihr Unternehmen bei der zuverlässigen Erkennung von gefährlichem Verhalten und Daten-interaktionen der Anwender sowie bei der Reaktion auf Zwischenfälle. Der Aufbau eines solchen Programms spielt daher eine entscheidende Rolle bei der Verhinderung von Datenverlust und der Minimierung von Insider-Risiken.

FRAMEWORK

DIESE UNTERSUCHUNG LIEFERT INFORMATIONEN DAZU, MIT WELCHEN KOSTEN DIE BEDROHUNG DURCH INSIDER VERBUNDEN SEIN KANN.

Die Umfrage deckt die grundlegenden Systeme und geschäftlichen Tätigkeiten ab, die verschiedene Ausgaben für die Reaktion auf fahrlässiges oder kriminelles Insider-Verhalten nach sich ziehen. Laut unserer Definition in dieser Untersuchung beeinträchtigt ein Insider-bezogener Zwischenfall die grundlegenden Daten, Netzwerke oder Geschäftssysteme eines Unternehmens. Dazu gehören auch Angriffe durch externe Akteure, die es auf Anmeldedaten legitimer Mitarbeiter/ Anwender abgesehen haben (d. h. Risiko durch Identitätsdiebstahl).

Unsere Benchmark-Methoden haben das Ziel, die tatsächlichen Erlebnisse und Konsequenzen Insider-bezogener Zwischenfälle nachzuvollziehen. Basierend auf Interviews mit verschiedensten hochrangigen Personen in den untersuchten Unternehmen klassifizieren wir die Kosten entsprechend zweier unterschiedlicher Kostenflüsse:

- Die Kosten für die Minimierung von Insider-Bedrohungen, die wir als interne Kostenstellen bezeichnen
- Die Kosten durch die Folgen von Zwischenfällen, die wir als externe Effekte des Ereignisses oder Angriffs bezeichnen

Wir analysieren die internen Kostenstellen in ihrer Reihenfolge – beginnend mit Kontrolle und Überwachung der Insider-Bedrohungslage und endend mit Behebungsmaßnahmen. Ebenfalls enthalten sind die Kosten durch entgangene Geschäftschancen und Unterbrechungen des Geschäftsbetriebs. Für jeden der Kostenpunkte baten wir die Teilnehmer, die direkten und indirekten Kosten sowie (falls zutreffend) die Opportunitätskosten zu schätzen.

Diese werden wie folgt definiert:

- **Direkte Kosten:** Die direkten Auslagen, um eine bestimmte Tätigkeit abzuschließen
- **Indirekte Kosten:** Der Zeit- und Arbeitsaufwand sowie sonstige aufgewendete Unternehmens-ressourcen, jedoch ohne direkte Barauslagen
- **Opportunitätskosten:** Die Kosten durch entgangene Geschäftschancen als Konsequenz einer Rufschädigung nach dem Zwischenfall

Externe Kosten wie der Verlust von Informations-ressourcen, Geschäftsunterbrechung, Schäden an Geräten und Umsatzverlusten wurden mit Methoden zur Ermittlung von Schattenpreisen erfasst. Die Gesamtkosten haben wir sieben unterschiedlichen Kostenvektoren zugewiesen.[4]

4 Wir sind uns bewusst, dass diese sieben Kostenkategorien nicht vollständig voneinander unabhängig sind und keine umfassende Liste aller Kostenstellen darstellen.

Diese Untersuchung deckt grundlegende prozessbezogene Tätigkeiten ab, die verschiedene Ausgaben im Zusammenhang mit der Reaktion des Unternehmens auf Insider-bezogene Zwischenfälle nach sich ziehen. Die sieben internen Kostenstellen in unserem Framework sind:[5]

07
interne Kostenstellen

01 **Kontrolle und Überwachung:** Tätigkeiten, mit denen ein Unternehmen in angemessenem Maße Zwischenfälle und Angriffe durch Insider erkennen und möglicherweise abwehren kann. Dazu gehören verrechnete (Gemein-) Kosten bestimmter Technologien, die die Behebung von Zwischenfällen oder Früherkennung von Bedrohungen unterstützen.

02 **Untersuchung:** Aktivitäten, die notwendig sind, um Quelle, Umfang und Ausmaß von Zwischenfällen definitiv zu bestimmen.

03 **Eskalation:** Tätigkeiten zur Bekanntmachung tatsächlicher Zwischenfälle bei wichtigen Verantwortlichen im Unternehmen. Dazu gehören auch die Schritte, mit denen eine erste Management-Reaktion organisiert wird.

04 **Reaktion auf Zwischenfälle:** Tätigkeiten im Zusammenhang mit der Zusammenstellung des Vorfallreaktionsteams. Dazu gehören die notwendigen Schritte zum Formulieren einer endgültigen Management-Reaktion.

05 **Eindämmung:** Tätigkeiten zur Abwehr oder Abschwächung der Folgen von Zwischenfällen oder Angriffen durch Insider, beispielsweise die Abschaltung anfälliger Anwendungen und Endpunkte.

06 **Ex-Post-Reaktion:** Mit diesen Tätigkeiten sollen zukünftige Insider-bezogene Zwischenfälle und Angriffe auf das Unternehmen verhindert werden. Dazu gehören auch Maßnahmen zur Kommunikation mit wichtigen Verantwortlichen innerhalb und außerhalb des Unternehmens, z. B. die Vorbereitung von Empfehlungen, um potenzielle Schäden zu minimieren.

07 **Behebung:** Bei diesen Tätigkeiten werden die Unternehmenssysteme und grundlegenden Geschäftsprozesse repariert und behoben. Dazu gehört die Wiederherstellung beschädigter Informationsressourcen und IT-Infrastrukturen.

Zusätzlich zu den oben genannten prozessbezogenen Aktivitäten verzeichnen Unternehmen häufig externe Folgen oder Kosten aus den Nachwirkungen von Zwischenfällen. Unsere Untersuchung zeigt, dass folgende vier allgemeine Kostenvorgänge mit diesen externen Konsequenzen verbunden sind:

04
allgemeine Kostenvorgänge

01 **Kosten von Informationsverlust oder -diebstahl:** Verlust oder Diebstahl sensibler oder vertraulicher Informationen aufgrund eines Insider-Angriffs. Solche Informationen umfassen Geschäftsgeheimnisse, geistiges Eigentum (einschließlich Quellcode), Kundendaten und Personalakten. Diese Kostenkategorie umfasst auch die Kosten der Benachrichtigung bei einer Datenschutzverletzung, falls diese personenbezogenen Informationen auf illegale Weise erlangt wurden.

02 **Kosten durch Geschäftsunterbrechung:** Die wirtschaftliche Auswirkung von Ausfallzeiten oder ungeplanten Unterbrechungen, aufgrund derer das Unternehmen seine Daten nicht verarbeiten kann.

03 **Kosten durch Geräteschäden:** Die Kosten für die Wiederherstellung von Geräten und weiteren IT-Ressourcen nach Insider-Angriffen auf Informationsressourcen und kritische Infrastruktur.

04 **Umsatzverluste:** Der Verlust von Kunden (Abwanderung) und weiteren Verantwortlichen aufgrund von Systemunterbrechungen oder Abschaltungen nach einem Insider-Angriff. Zum Extrapolieren dieser Kosten nutzen wir eine Methode zur Berechnung von Schattenpreisen, die auf dem „Lebenszeitwert“ eines durchschnittlichen Kunden basiert, der für jedes teilnehmende Unternehmen definiert ist.

5 Die internen Kosten werden anhand der Arbeitszeit als Ersatz für direkte und indirekte Kosten extrapoliert. Auf diese Weise wird auch der Gemeinkostenanteil der Fixkosten berechnet, z. B. mehrjährige Investitionen in Technologien.

BENCHMARK-ANALYSE

Unser Benchmark-Instrument ist darauf ausgelegt, von IT-, Informationssicherheits- und anderen wichtigen Mitarbeitern beschreibende Informationen dazu zu erhalten, welche indirekten oder direkten Kosten durch Insider-bezogene Zwischenfälle oder tatsächlich erkannte Angriffe angefallen sind. Dabei müssen die Personen keine tatsächlichen Zahlen aus der Buchhaltung zur Verfügung stellen. Stattdessen basiert unser Ansatz auf Schätzungen und Extrapolationen anhand von Interviewdaten über einen Zeitraum von vier Wochen.

Grundlage für die Kostenschätzungen sind vertrauliche diagnostische Interviews mit wichtigen Personen innerhalb der Unternehmen, die wir in unseren Benchmarks untersuchen. Die erfassten Daten umfassen keine tatsächlichen Buchhaltungsdaten, sondern entsprechen Schätzungen der Teilnehmer basierend auf deren Wissen und Erfahrung. Die Kostenschätzungen erfolgen für jede Kategorie in zwei Phasen. In der ersten Phase werden die Teilnehmer aufgefordert, die direkten Kosten für jede Kostenkategorie zu schätzen. Dabei geben sie eine Bereichsvariable im unten gezeigten Zahlengeraden-Format an.

Verwenden der Zahlengeraden: Die unter jeder Kostenkategorie zu einer Datenschutzverletzung angegebene Zahlengerade ist eine Möglichkeit, die bestmögliche Schätzung für die Gesamtkosten zu erhalten, die für Auslagen, Personal und Gemeinkosten angefallen sind. Die Teilnehmer sollten einen Punkt zwischen den oben angegebenen oberen und unteren Grenzwerten markieren, wobei sie die oberen und unteren Grenzwerte während des Interviews jederzeit zurücksetzen konnten.

Geben Sie Ihre Schätzung der direkten Kosten für [Kostenkategorie] hier ein.

Untere Grenze _____|_____ **Obere Grenze**

Da bei dieser Methode ein numerischer Wert aus der Zahlengeraden und kein genauer Schätzwert für jede Kostenkategorie erfasst wird, bleibt die Vertraulichkeit gewährleistet. Dadurch steigt die Antwortrate. Für das Benchmark-Instrument sollten die Experten außerdem separat eine zweite Schätzung für die indirekten sowie die Opportunitätskosten angeben.

Die Kostenschätzungen wurden anschließend für jedes Unternehmen basierend auf der relativen Höhe dieser Kosten im Vergleich zu den direkten Kosten innerhalb einer bestimmten Kategorie kompiliert. Abschließend stellten wir allgemeine Fragen zu zusätzlichen Fakten, zum Beispiel zu geschätzten Umsatzverlusten durch Insider-bezogene Zwischenfälle oder Angriffe.

Umfang und Bereich der Umfragethemen beschränkten sich auf bekannte Kostenkategorien, die in verschiedenen Branchen relevant sind. Laut unserer Erfahrung erzielen Umfragen, die sich auf Prozesse konzentrieren, eine höhere Antwortrate und hochwertigere Ergebnisse. Außerdem führten wir die Umfrage auf gedruckten Fragebögen statt elektronisch durch, um die Vertraulichkeit besser gewährleisten zu können.

Um absolute Vertraulichkeit zu gewährleisten, wurden bei der Umfrage keinerlei unternehmensspezifische Informationen erfasst. Die Materialien enthielten keine Tracking-Codes oder andere Methoden, mit denen sich die Antworten mit den teilnehmenden Unternehmen verknüpfen lassen.

Um den Benchmark-Umfang überschaubar zu halten, haben wir die Fragen bewusst auf die Kostenaktivitäten beschränkt, die wir für die Bewertung als unerlässlich betrachten. Basierend auf Gesprächen mit anerkannten Experten konzentrieren sich die Fragen auf eine begrenzte Menge direkter sowie indirekter Kostenaktivitäten. Nach der Erfassung der Benchmark-Informationen wurde jedes Instrument sorgfältig auf Konsistenz und Vollständigkeit geprüft. Für diese Untersuchung wurden die Antworten einiger weniger Unternehmen nicht berücksichtigt, da sie unvollständig oder inkonsistent waren oder leere Antworten enthielten.

Die Untersuchungen begannen im September 2021. Um die Konsistenz für alle untersuchten Unternehmen zu gewährleisten, bezogen sich die Angaben zu den Erfahrungen der Unternehmen jeweils auf vier aufeinanderfolgende Wochen. Der Zeitraum ist nicht unbedingt für alle Unternehmen in dieser Untersuchung identisch. Die extrapolierten direkten und indirekten Kosten wurden von Kosten für vier Wochen auf Kosten pro Jahr umgerechnet (Verhältnis = 4/52 Wochen).

GRENZEN DER UNTERSUCHUNG

FÜR UNSERE UMFRAGE VERWENDETEN WIR EINE VERTRAULICHE UND PROPRIETÄRE BENCHMARK-METHODE, DIE BEREITS BEI FRÜHEREN UNTERSUCHUNGEN ERFOLGREICH EINGESETZT WURDE.

Die Methode unterliegt jedoch grundsätzlichen Beschränkungen, die für Schlussfolgerungen aus den Ergebnissen sorgfältig berücksichtigt werden müssen.

- **Keine statistischen Ergebnisse:** Unsere Untersuchung basiert auf einer repräsentativen, nicht statistischen Stichprobe von Unternehmen, die in den vergangenen zwölf Monaten mindestens einen Zwischenfall durch Insider verzeichnet haben. Statistische Rückschlüsse, Fehlermargen und Konfidenzintervalle können nicht auf diese Daten angewendet werden, da unsere Stichprobenmethoden nicht wissenschaftlich sind.
- **Keine Antworten:** Die aktuellen Ergebnisse basieren auf einer kleinen repräsentativen Menge an Benchmark-Daten. Für diese Untersuchung haben 159 Unternehmen den Benchmark-Prozess durchlaufen. Fehlende Antworten wurden nicht berücksichtigt, daher ist es immer möglich, dass sich Nichtteilnehmer bei den zugrundeliegenden Kosten für Datenschutzverletzungen deutlich unterscheiden.
- **Auswahl der Stichprobe:** Da unsere Stichprobenwahl einseitig ist, wird die Qualität der Ergebnisse davon beeinflusst, wie stark die Stichprobe für die Gesamtmenge der untersuchten Unternehmen repräsentativ ist. Wir sind der Meinung, dass die vorliegende Stichprobe dahingehend einseitig ist, dass die teilnehmenden Unternehmen über ausgereiftere Programme für Datenschutz und Informationssicherheit verfügen.
- **Unternehmensspezifische Informationen:** Die Benchmark-Informationen sind sensibel und vertraulich. Daher wurden keine Informationen erfasst, die eine Identifizierung des Unternehmens ermöglichen. Außerdem konnten die Teilnehmer Variablen für Kategorie-Antworten verwenden, um demografische Informationen zum Unternehmen sowie zur Branche anzugeben.
- **Nicht erfasste Faktoren:** Um das Interview-Skript kurz und knapp zu halten, entschieden wir uns gegen die Verwendung weiterer wichtiger Variablen wie führende Trends und Unternehmenseigenschaften. Es war nicht möglich festzustellen, inwieweit die nicht erfassten Variablen möglicherweise die Benchmark-Ergebnisse erklären können.
- **Extrapolierte Ergebnisse zu den Kosten:** Die Qualität der Benchmark-Untersuchung basiert auf der Integrität der vertraulichen Antworten der Personen, die sich zu Fragen zu den teilnehmenden Unternehmen geäußert haben. Während gewisse Kontrollen in den Benchmark-Prozess eingebunden werden können, ist es immer möglich, dass Antworten nicht genau oder wahrheitsgemäß sind. Zudem kann die Tatsache, dass die Kosten extrapoliert und nicht als tatsächliche Kosten angegeben wurden, zu unbeabsichtigten Ungenauigkeiten und Fehlern führen.

Ponemon INSTITUTE

Förderung kompetenter Informationsverwaltung

Das Ponemon Institute bietet unabhängige Untersuchungen und Schulungen an, die effektive Praktiken zur Informations- und Datenschutzverwaltung in Unternehmen und Behörden fördern. Wir haben uns zum Ziel gesetzt, hochwertige, empirische Untersuchungen zu wichtigen Themen durchzuführen, die die Verwaltung und Sicherheit vertraulicher Informationen zu Personen und Organisationen betreffen.

Wir gewährleisten Datenvertraulichkeit sowie Privatsphäre und fühlen uns ethischen Forschungsstandards verpflichtet. Wir erfassen keine personenbezogenen Informationen von Einzelpersonen (bzw. unternehmensbezogene Informationen in der Wirtschaftsforschung). Außerdem halten wir uns an strikte Qualitätsstandards, um zu gewährleisten, dass Umfrageteilnehmer keine sachfremden, irrelevanten oder unangemessenen Fragen erhalten.

proofpoint.

Informationen zu Proofpoint

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.