observeIT | proofpoint.

KOSTEN VON INSIDER-BEDROHUNGEN: BERICHT 2020

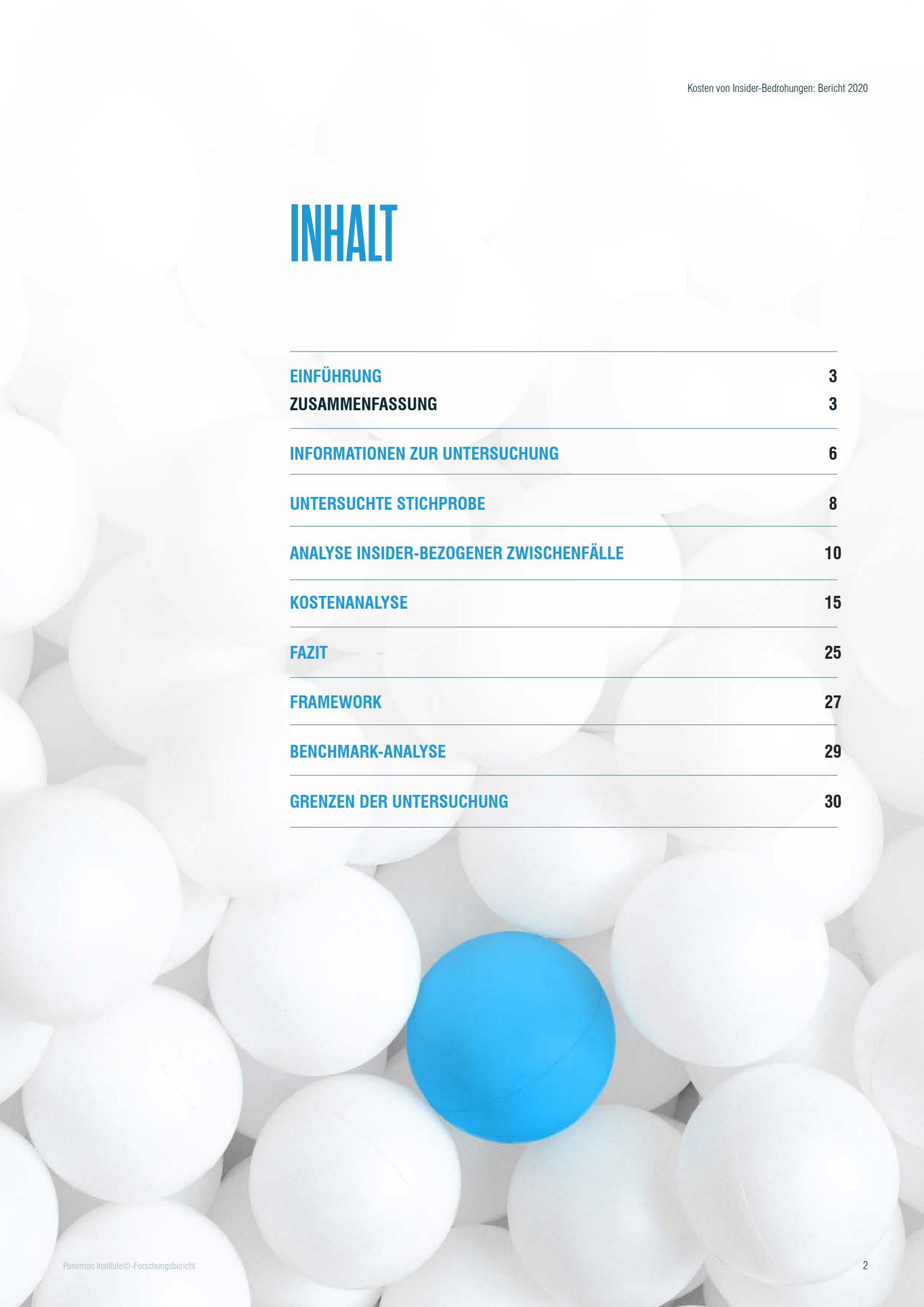
Unabhängig durchgeführt von:

Ponemon INSTITUTE

Mit Unterstützung von:

observeIT IBM Security

INHALT



EINFÜHRUNG

Das Ponemon Institute stellt die Erkenntnisse aus der weltweiten Untersuchung zu den Kosten von Bedrohungen durch Insider vor. Die von ObserveIT und IBM unterstützte Untersuchung ist die dritte Benchmark-Untersuchung dieser Art und liefert Einblicke zu den direkten und indirekten Kosten durch Insider-Bedrohungen. Die erste Untersuchung wurde 2016 durchgeführt und befasste sich ausschließlich mit Unternehmen in den USA. In der aktuellen Studie sind Unternehmen aus Nordamerika, Europa, dem Nahen Osten und Afrika sowie dem asiatisch-pazifischen Raum vertreten.

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

- Unachtsames oder fahrlässiges Verhalten von Mitarbeitern oder Auftragnehmern
- Kriminelle oder böswillige Motive eines Insiders oder
- Diebstahl von Anmeldedaten

Zusammenfassung

Die wichtigste Erkenntnis ist, dass bei allen drei oben genannten Typen von Insider-Bedrohungen die Häufigkeit sowie die damit verbundenen Kosten in den letzten zwei Jahren erheblich gestiegen sind. Beispielsweise stiegen die Gesamtkosten durch Insider-Bedrohungen laut Ponemon von 8,76 Millionen US-Dollar im Jahr 2018 um 31 % auf 11,45 Millionen US-Dollar im Jahr 2020. Hinzu kommt, dass die Anzahl der Zwischenfälle innerhalb von nur zwei Jahren um erschreckende 47 % gestiegen ist – laut Ponemon von 3.200 im Jahr 2018 auf 4.716 im Jahr 2020. Diese Daten zeigen, dass Bedrohungen durch Insider gravierender werden und – verglichen mit externen Bedrohungen – häufig zu wenig von der IT-Sicherheit in Unternehmen beachtet werden.

Wir haben 964 IT- und IT-Sicherheitsexperten in 204 Unternehmen in Nordamerika (USA und Kanada), Europa, dem Nahen Osten und Afrika sowie dem asiatisch-pazifischen Raum befragt. Die Umfrage wurde im September 2019 abgeschlossen. Jedes Unternehmen verzeichnete mindestens ein schwerwiegendes Ereignis, das von einem Insider ausgelöst wurde. Wir sprachen gezielt Unternehmen mit mindestens 1.000 Mitarbeitern an. Diese Unternehmen verzeichneten in den letzten zwölf Monaten insgesamt 4.716 Zwischenfälle durch Insider.

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

Gesamtzahl der untersuchten Unternehmen

204

Gesamtzahl der Insider-bezogenen Zwischenfälle

4.716

Durchschnittliche Gesamtkosten

11,45 Mio. USD

Zwischenfälle durch Fahrlässigkeit

62 %

Zwischenfälle durch Insider mit kriminellen Motiven

23 %

Zwischenfälle durch Diebstahl von Anmeldedaten

14 %

Jährliche Kosten durch Fahrlässigkeit

4,58 Mio. USD

Jährliche Kosten durch Insider mit kriminellen Motiven

4,08 Mio. USD

Jährliche Kosten durch Diebstahl von Anmeldedaten

2,79 Mio. USD

DIE KOSTEN FÜR ZWISCHENFÄLLE, DIE AUF DEN DIEBSTAHL VON ANMELDEDATEN ZURÜCKGEHEN, BELAUFEN SICH PRO UNTERNEHMEN AUF **DURCHSCHNITTLICH 2,79 MILLIONEN US-DOLLAR** PRO JAHR.

INSIDER MIT KRIMINELLEN ODER BÖSWILLIGEN ABSICHTEN KOSTEN DIE IN DIESER UNTERSUCHUNG BEFRAGTEN UNTERNEHMEN **DURCHSCHNITTLICH 755.760 US-DOLLAR PRO ZWISCHENFALL**.

Fahrlässig handelnde Insider verursachten den größten Teil der Zwischenfälle, doch der Diebstahl von Anmeldedaten ist mit den größten Kosten pro Zwischenfall verbunden.

Die Kosten von Bedrohungen durch Insider hängen erheblich von der Art des Zwischenfalls ab. Bei Mitarbeitern oder Auftragnehmern, die fahrlässig handeln, kosten die Zwischenfälle im Durchschnitt jeweils 307.111 US-Dollar. Da diese Art von Zwischenfall jedoch am häufigsten vorkommt (mit einem Anteil von 62 %), können sich die Gesamtkosten auf 4,58 Millionen US-Dollar pro Jahr und Unternehmen addieren.

Die Durchschnittskosten pro Zwischenfall verdreifachen sich beinahe (871.686 US-Dollar), wenn ein Betrüger Anmeldedaten abgreift und für seine Zwecke missbraucht. Die teuerste Art von Anmeldedaten-Diebstahl ist dabei Diebstahl privilegierter Anmeldedaten. In dieser Umfrage umfassten 14 % der Zwischenfälle den Diebstahl von Anmeldedaten privilegierter Anwender. Die Kosten für Zwischenfälle, die auf den Diebstahl von Anmeldedaten zurückgehen, belaufen sich pro Unternehmen auf durchschnittlich 2,79 Millionen US-Dollar pro Jahr.

Kriminelle beziehungsweise böswillig handelnde Insider kosten die in dieser Untersuchung befragten Unternehmen durchschnittlich 755.760 US-Dollar pro Zwischenfall. Kriminell agierende Insider, die regelmäßig die größte Aufmerksamkeit erhalten, sind nur für 23 % aller Zwischenfälle, die mit Bedrohungen durch Insider im Zusammenhang stehen, verantwortlich. Ihre Auswirkungen können sich jedoch im Laufe des Jahres summieren und Unternehmen im Durchschnitt 4,08 Millionen US-Dollar kosten.

Untersuchungen sind die am schnellsten wachsende Kostenstelle

Diese Aktivitäten sind mit den höchsten Kosten verbunden: Kontrolle und Überwachung, Untersuchung, Eskalation, Reaktion auf Zwischenfälle, Eindämmung, Ex-Post-Analyse und Problembehebung. Die am schnellsten wachsende Kostenstelle bei diesen Aktivitäten ist die Untersuchung – über alle Zwischenfalltypen hinweg stiegen die Durchschnittskosten innerhalb von nur zwei Jahren um 86 % auf 103.798 US-Dollar.

Die Eindämmung eines Insider-bezogenen Zwischenfalls dauert im Durchschnitt mehr als zwei Monate

Im Durchschnitt dauert es 77 Tage, bis eine Insider-Bedrohung eingedämmt ist. Nur 13 % der Zwischenfälle wurden in weniger als 30 Tagen eingedämmt.

Unternehmensgröße und Branche beeinflussen die Kosten pro Zwischenfall

Die Kosten der Zwischenfälle variieren entsprechend der Unternehmensgröße. Große Unternehmen (mit 25.001 bis 75.000 Mitarbeitern) gaben im Verlauf des letzten Jahres durchschnittlich 17,92 Millionen US-Dollar aus, um Insider-bezogene Zwischenfälle zu beheben, während kleinere Unternehmen (mit weniger als 500 Mitarbeitern) durchschnittlich 7,68 Millionen US-Dollar aufwenden mussten. Die Branchen mit den am schnellsten wachsenden Insider-Bedrohungen waren der Einzelhandel (38,2 % Steigerung innerhalb von zwei Jahren) und Finanzdienstleister (20,3 % Steigerung in zwei Jahren).

Alle Arten von Insider-Risiken nehmen zu

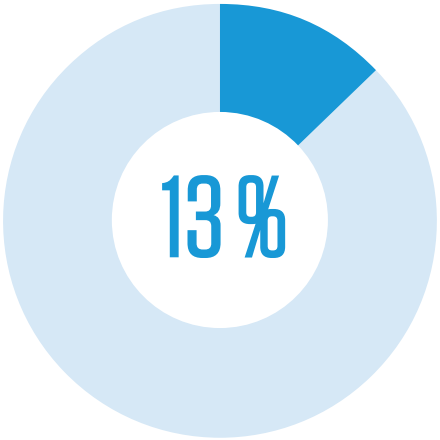
Seit 2018 ist die Zahl von Zwischenfällen mit fahrlässig handelnden Mitarbeitern oder Auftragnehmern von 13,2 auf 14,5 pro Unternehmen gestiegen. Die durchschnittliche Zahl der Anmeldedaten-Diebstähle hat sich in den letzten zwei Jahren von 1,0 auf 2,7 Zwischenfälle pro Unternehmen fast verdreifacht. Gleichzeitig verzeichneten 60 % der befragten Unternehmen mehr als 30 Zwischenfälle pro Jahr.

Fünf Zeichen, dass Ihr Unternehmen gefährdet ist

1. Mitarbeiter sind nicht ausreichend geschult darin, Gesetze, Vorschriften oder rechtliche Vorgaben für ihre Arbeit vollständig zu verstehen und anzuwenden, was sich auf die Sicherheit des Unternehmens auswirkt.
2. Mitarbeiter wissen nicht, worauf sie achten müssen, um jederzeit die Sicherheit der von ihnen genutzten Geräte – sowohl unternehmenseigene als auch eigener Endgeräte, die sie zu beruflichen Zwecken nutzen – zu gewährleisten.
3. Mitarbeiter veröffentlichen höchst vertrauliche Daten in öffentlichen Bereichen der Cloud und gefährden dadurch das Unternehmen.
4. Mitarbeiter verstoßen gegen die Sicherheitsrichtlinien ihres Unternehmens, um sich die Arbeit zu erleichtern.
5. Mitarbeiter setzen Ihr Unternehmen Risiken aus, indem sie ihre Geräte und Anwendungen nicht kontinuierlich patchen bzw. auf die neuesten Versionen aktualisieren.

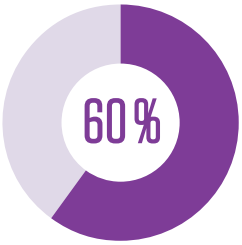
77 TAGE

um eine Insider-Bedrohung vollständig zu beheben



der Zwischenfälle wurden eingedämmt in weniger als

30 TAGEN



30

der Unternehmen verzeichneten mehr als 30 Zwischenfälle pro Jahr

INFORMATIONEN ZUR UNTERSUCHUNG

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 2019 abgeschlossen. Unsere aktuelle Benchmark-Stichprobe umfasste 204 separate Unternehmen, wobei in diesen Unternehmen insgesamt 964 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
- Mit jeweils mindestens 1.000 Mitarbeitern
- Standorte in folgenden Regionen: Nordamerika, Europa, Naher Osten und Afrika sowie im asiatisch-pazifischen Raum
- Zentrale IT-Funktion mit Kontrolle über lokale bzw. Cloud-Umgebung
- Mindestens ein schwerwiegenden Zwischenfall durch fahrlässige, böswillige oder kriminelle Insider

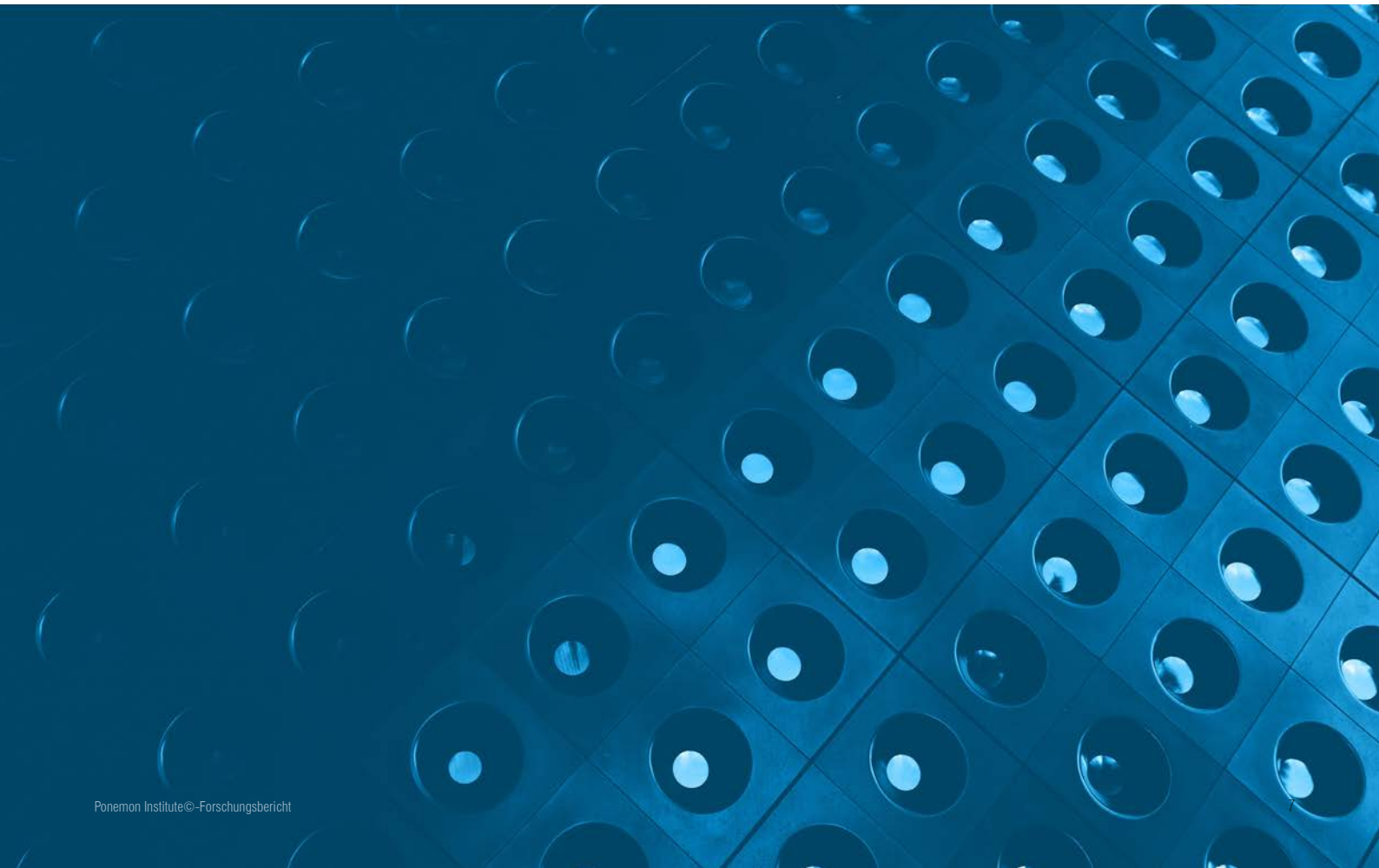
FÜR DIE STUDIE WURDEN DIAGNOSTISCHE INTERVIEWS UND **KOSTENZUORDNUNG NACH TÄTIGKEITEN** ZUR **ERFASSUNG UND EXTRAPOLATION DER KOSTENDATEN DURCHGEFÜHRT.**

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 204 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 Kostenzuordnung nach Tätigkeiten zur Erfassung und Extrapolation der Kostendaten. Das Ponemon Institute übernahm alle Phasen dieses Untersuchungsprojekts, das folgende Schritte umfasste:

- Arbeitssitzungen mit ObserveIT und IBM, um Fragengebiete auszuarbeiten
- Auswahl von Benchmark-Unternehmen
- Entwicklung eines Frameworks zur Kostenzuordnung nach Tätigkeiten
- Verwaltung des Studienprogramms
- Analyse aller Ergebnisse mit entsprechenden Zuverlässigkeitsprüfungen
- Vorbereitung eines Berichts, der alle wichtigen Ergebnisse zusammenfasst



UNTERSUCHTE STICHPROBE

Bei der Benchmark-Untersuchung ist die Analyseeinheit das Unternehmen. Das folgende Kreisdiagramm 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 Unternehmensberater.

Abb. 1:

Branchen der teilnehmenden Unternehmen

n=204 Unternehmen

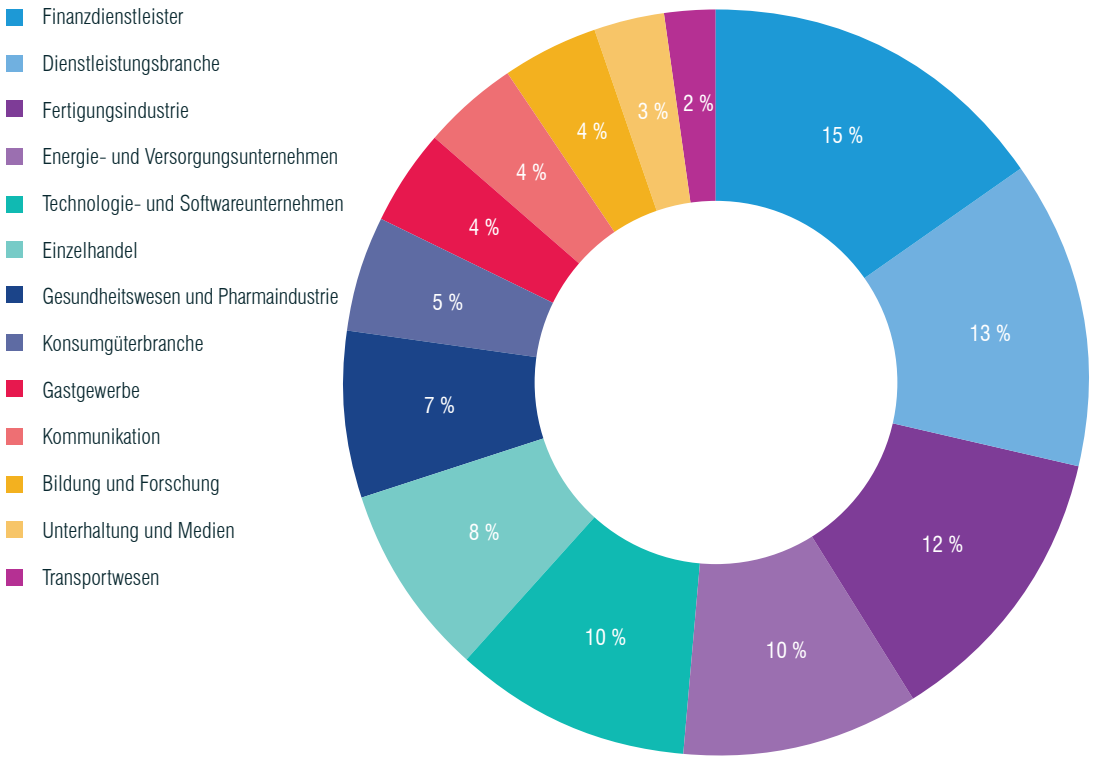
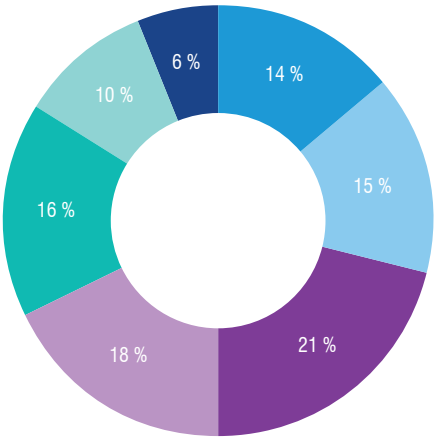


Abb. 2 zeigt den prozentualen Anteil der Unternehmen nach weltweiter Mitarbeiterzahl (anstelle der Unternehmensgröße). Wie sich zeigt, handelt es sich bei 50 % der Stichprobe um größere Unternehmen mit mehr als 5.000 in Vollzeit tätigen Mitarbeitern.

Abb. 2:

Mitarbeiterzahl der teilnehmenden Unternehmen

n=204 Unternehmen



In Abb. 3 ist zu sehen, dass 964 Personen an den Interviews vor Ort teilnahmen. Pro untersuchtem Unternehmen wurde mit durchschnittlich 4,7 Personen gesprochen. Die drei größten Bereiche waren: IT-Operations (15 %), CISOs (14 %) und IT-Techniker (14 %).

Abb. 3:

Umfrageteilnehmer nach Position oder Funktion

n=964 Personen

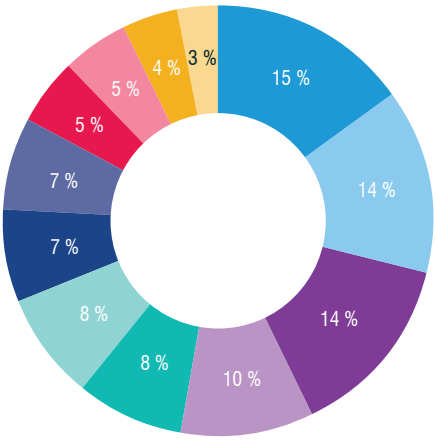
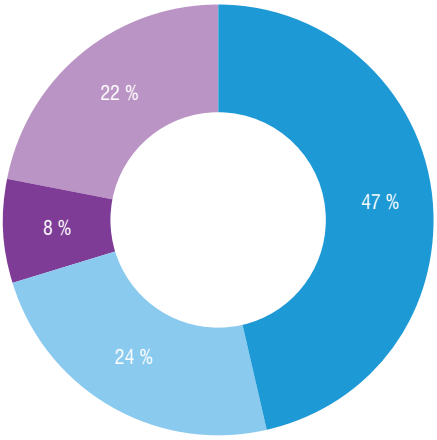


Abb. 4 zeigt die weltweite Verteilung der teilnehmenden Unternehmen. Nordamerika hat dabei den größten Anteil (47 %), während die wenigsten Unternehmen im Nahen Osten ansässig sind (8 %). Aufgrund dieser kleinen Probengröße führten wir Europa und den Nahen Osten zum Bereich EMEA zusammen.

Abb. 4:

Regionale Verteilung der untersuchten Unternehmen

n=204 Unternehmen



ANALYSE INSIDER-BEZOGENER ZWISCHENFÄLLE

Abb. 5 zeigt die Verteilung der 4.716 gemeldeten Angriffe, die wir in unserer Stichprobe analysiert haben. Insgesamt 2.962 Angriffe (62 %) waren auf Fahrlässigkeit von Mitarbeitern oder Auftragnehmern zurückzuführen. Kriminelle oder böswillige Insider waren der Grund für weitere 1.105 Angriffe (23 %).

649-mal (14 %) wurden Anmeldedaten gestohlen (d. h. Risiko durch Identitätsbetrug), wobei in 191 Fällen Anmeldedaten privilegierter Anwender gestohlen wurden. Die größte Zahl gemeldeter Zwischenfälle bei einem einzigen Unternehmen lag bei 45, die kleinste bei einem Zwischenfall.

Abb. 5:

Häufigkeit der 4.716 Zwischenfälle für die drei Insider-Profile

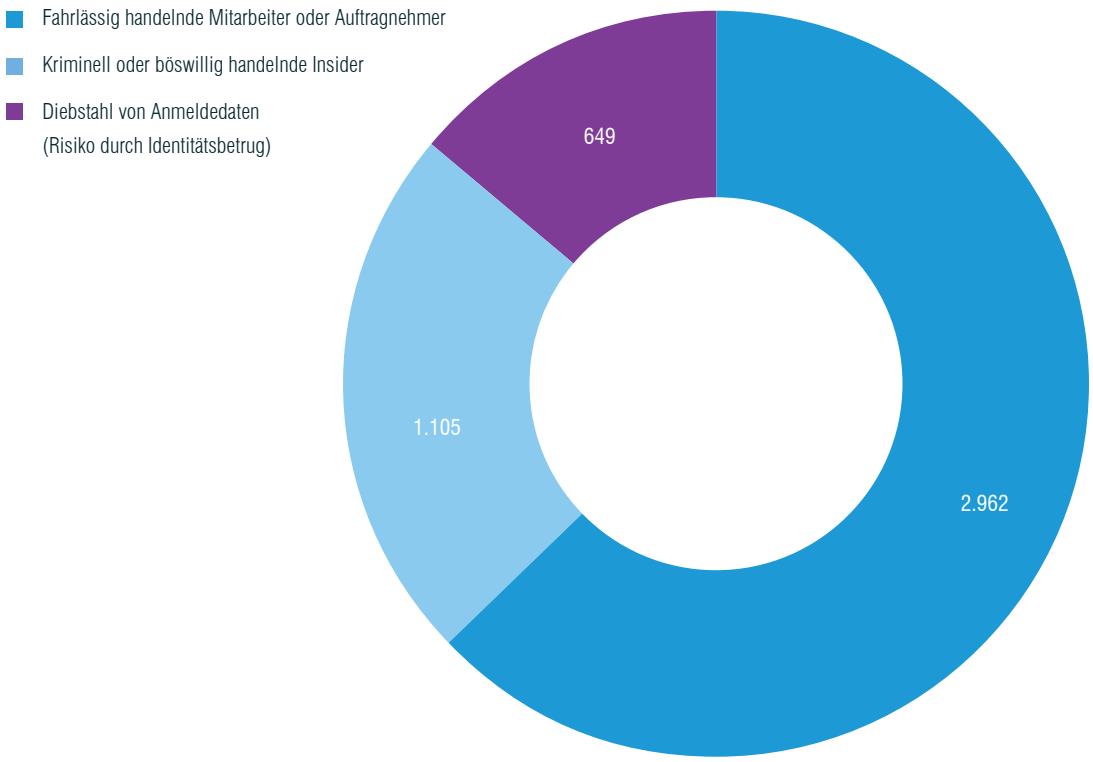
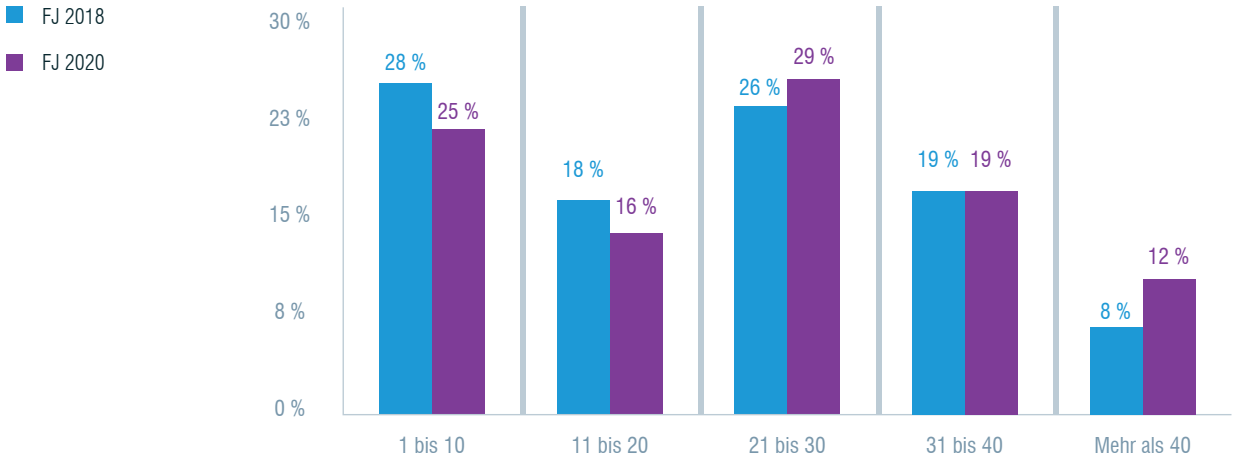


Abb. 6 zeigt ein Histogramm der Insider-bezogenen Zwischenfälle aus unserer Stichprobe von 204 Unternehmen in den vergangenen zwölf Monaten. Wie dargestellt, verzeichneten 60 % der Unternehmen im Durchschnitt mehr als 30 Zwischenfälle pro Jahr.

Abb. 6:

Anteilige Häufigkeit von Insider-bezogenen Zwischenfällen pro Unternehmen

Für drei Profile konsolidiert

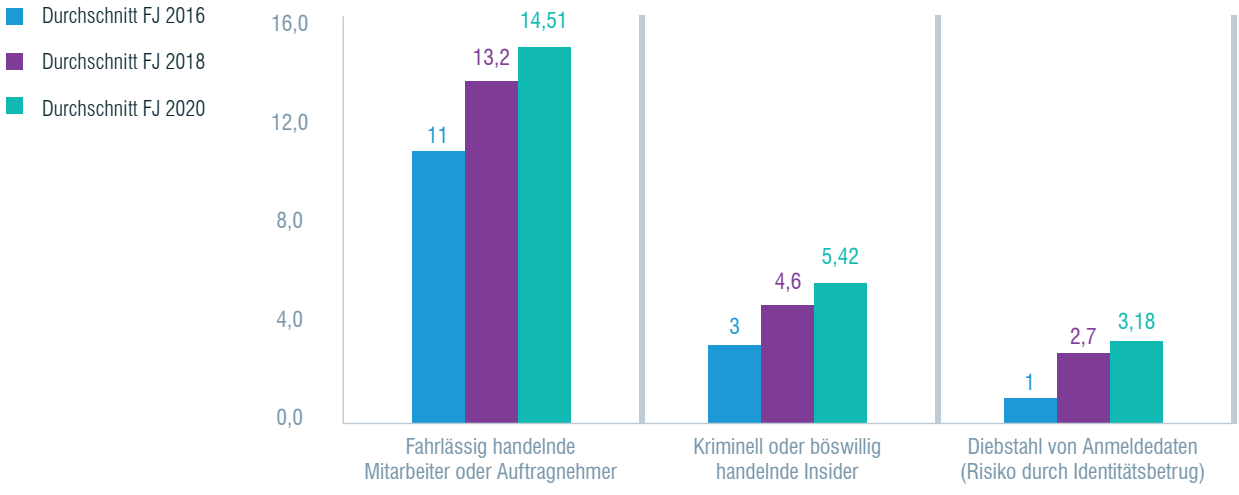


Alle Arten von Bedrohungen durch Insider nehmen stetig zu

In Abb. 7 ist zu sehen, dass seit 2016 die durchschnittliche Zahl der Zwischenfälle durch fahrlässig handelnde Mitarbeiter oder Auftragnehmer von 10,5 auf 14,5 im Jahr 2020 gestiegen ist. Die durchschnittliche Zahl der Zwischenfälle pro Unternehmen, die auf Anmeldedaten-Diebstahl zurückzuführen sind, hat sich in den letzten drei Jahren von 1,0 auf 3,2 Zwischenfälle verdreifacht.[1]

Abb. 7:

Häufigkeit der drei Profile von Insider-bezogenen Zwischenfällen



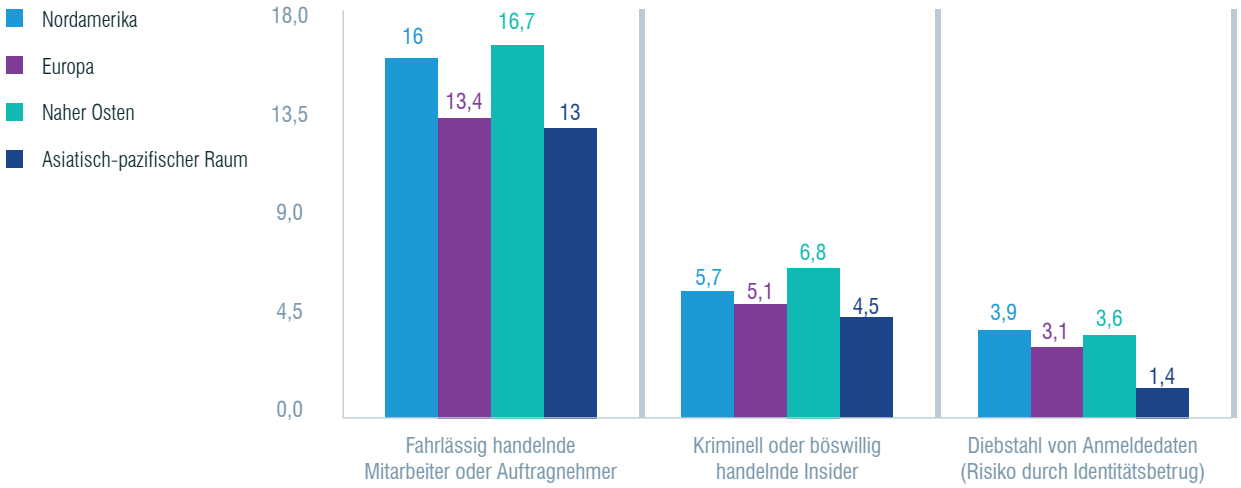
1 Die Daten für 2016 beziehen sich auf Unternehmen in den USA. Die Daten für 2020 umfassen Nordamerika, Europa, den Nahen Osten und Afrika sowie den asiatisch-pazifischen Raum. Wir gehen davon aus, dass die Daten vergleichbar sind, da die im Bericht für 2016 untersuchten US-amerikanischen Unternehmen international tätig sind.

Unternehmen im Nahen Osten verzeichneten die meisten Insider-bezogenen Zwischenfälle, solche im asiatisch-pazifischen 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 verzeichnen die meisten Fälle von Anmeldedaten-Diebstahl.

Abb. 8:

Durchschnittliche Häufigkeit von Zwischenfällen für die drei Profile

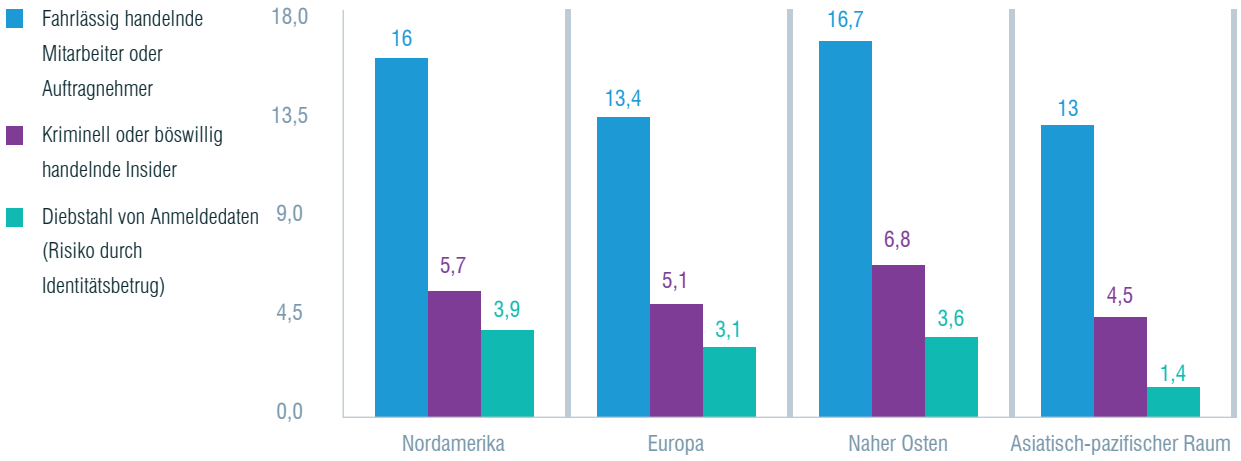


Die Häufigkeit von Bedrohungen durch Insider unterscheidet sich je nach Region

Wie in Abb. 9 gezeigt, verzeichneten Unternehmen in Nordamerika und dem Nahen Osten die größte Zahl Insider-bezogener Zwischenfälle in den vergangenen zwölf Monaten – ganz im Gegensatz zu Unternehmen im asiatisch-pazifischen Raum.

Abb. 9:

Häufigkeit der drei Profile von Insider-bezogenen Zwischenfällen nach Region



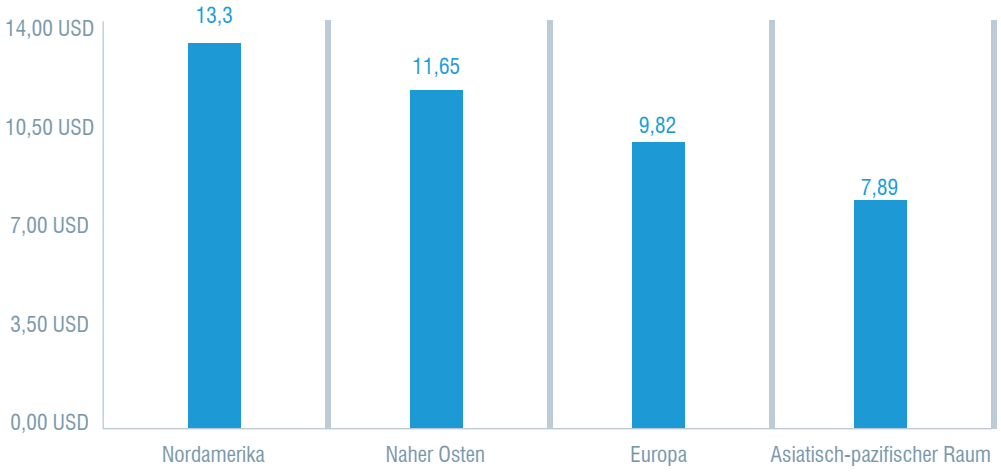
Durchschnittliche jährliche Kosten lagen bei nordamerikanischen Unternehmen über dem Durchschnitt

Die Gesamtkosten der vier untersuchten Regionen pro Jahr sind in Abb. 10 dargestellt. Nordamerikanische Unternehmen verzeichneten mit 13,3 Millionen US-Dollar die höchsten Gesamtkosten. Auf Platz 2 lagen Unternehmen im Nahen Osten mit 11,65 Millionen US-Dollar. Europa und der asiatisch-pazifische Raum lagen deutlich unter den Durchschnittskosten aller 204 Unternehmen.

Abb. 10:

Durchschnittliche Tätigkeitskosten nach Region

Durchschnitt=11,45 USD | In Millionen USD



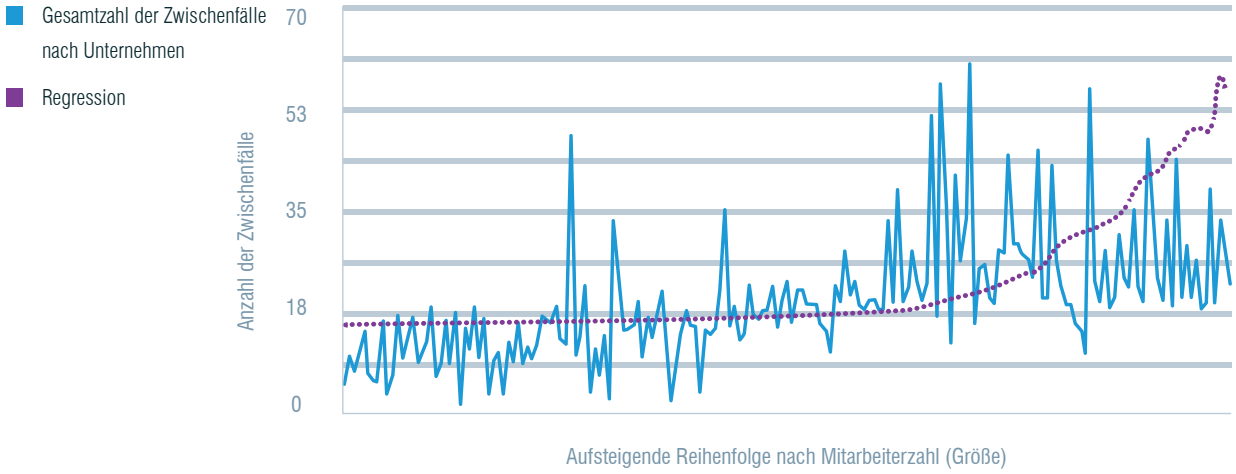
Je größer das Unternehmen, desto mehr Insider-bezogene Zwischenfälle

Abb. 11 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.

Abb. 11:

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

Durchschnitt=11,45 USD | In Millionen USD

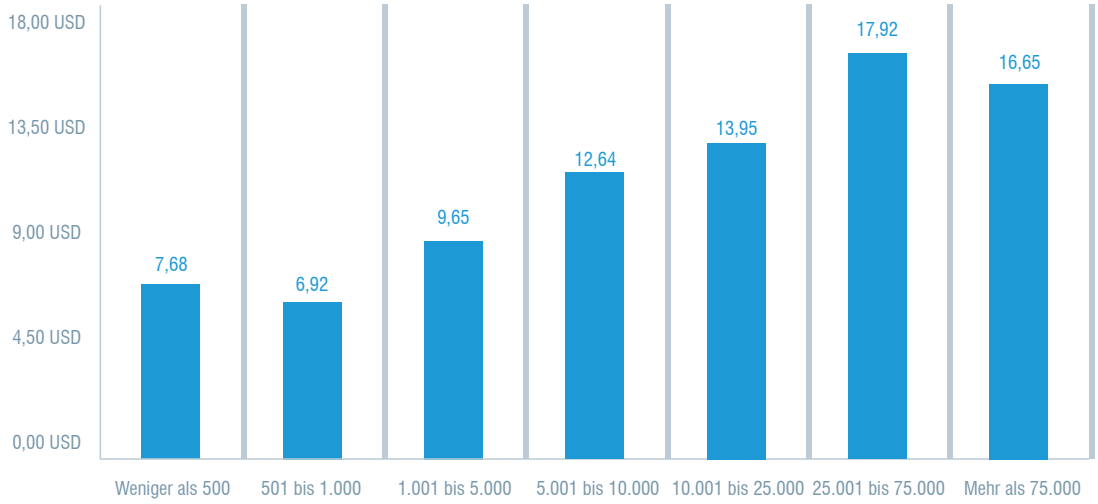


Die bereinigten jährlichen Gesamtkosten für den weltweiten Mitarbeiterstamm der befragten Unternehmen sind in Abb. 12 dargestellt. Unternehmen mit 25.001 bis 75.000 Mitarbeitern verzeichneten mit 17,92 Millionen US-Dollar die höchsten Gesamtkosten, während solche mit 500 bis 1.000 Mitarbeitern mit 6,92 Millionen US-Dollar die niedrigsten Kosten pro Jahr hatten.

Abb. 12:

Durchschnittliche Tätigkeitskosten nach Mitarbeiterzahl

Durchschnitt=11,45 USD | In Millionen USD



KOSTENANALYSE

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 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 Endgeräte.

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.

Unternehmen geben pro Zwischenfall im Durchschnitt 644.852 US-Dollar aus

Tabelle 1 fasst die Durchschnittskosten Insider-bezogener Zwischenfälle für die drei Zwischenfallarten und sieben Kostenstellen zusammen. Wie bereits erwähnt, stellen Eindämmung und Behebung die teuersten Kostenstellen dar, während für die Ex-Post-Analyse und Eskalation die geringsten Kosten anfallen.

Tabelle 1: Kostenstellen (pro Zwischenfall)	Fahrlässig handelnde Mitarbeiter oder Auftragnehmer	Kriminell oder böswillig handelnde Insider	Diebstahl von Anmeldedaten	Durchschnittskosten
Kontrolle und Überwachung	21.538 USD	21.857 USD	22.977 USD	22.124 USD
Untersuchung	49.441 USD	114.524 USD	147.429 USD	103.798 USD
Eskalation	9.282 USD	29.513 USD	26.619 USD	21.805 USD
Reaktion auf Zwischenfälle	62.877 USD	159.398 USD	132.677 USD	118.317 USD
Eindämmung	75.903 USD	175.962 USD	382.794 USD	211.553 USD
Ex-Post-Reaktion	21.035 USD	19.282 USD	18.121 USD	19.480 USD
Behebung	67.036 USD	235.223 USD	141.069 USD	147.776 USD
Gesamt	307.111 USD	755.760 USD	871.686 USD	644.852 USD

Unternehmen geben mehr Geld für Untersuchungen und Eskalationen aus. Tabelle 2 zeigt die prozentuale Kostensteigerung für jede Tätigkeit. Die Kosten für die Behebung sind nicht so stark gestiegen wie die für andere Tätigkeiten.

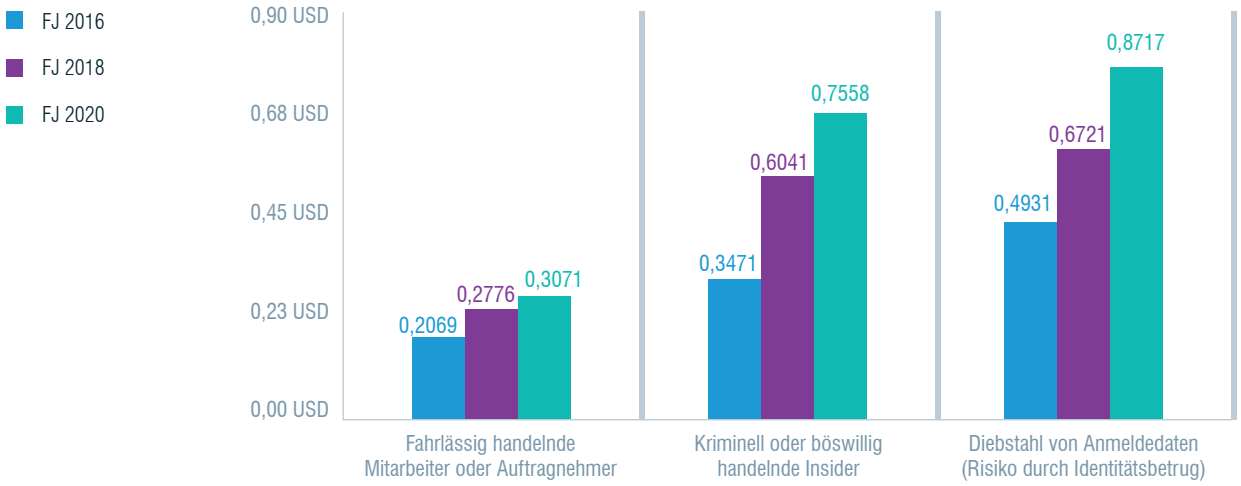
Tabelle 2: Kostenstellen nach Tätigkeitsbereich	FJ 2016	FJ 2018	FJ 2020	Nettosteigerung über drei Jahre
Kontrolle und Überwachung	9.610 USD	12.634 USD	22.124 USD	79 %
Untersuchung	41.461 USD	78.398 USD	103.798 USD	86 %
Eskalation	8.919 USD	12.542 USD	21.805 USD	84 %
Reaktion auf Zwischenfälle	66.370 USD	91.263 USD	118.317 USD	56 %
Eindämmung	122.796 USD	173.060 USD	211.553 USD	53 %
Ex-Post-Reaktion	8.498 USD	11.491 USD	19.480 USD	78 %
Behebung	91.397 USD	138.532 USD	147.776 USD	47 %
Gesamt	349.052 USD	517.920 USD	644.852 USD	60 %

Wie in Abb. 13 dargestellt, ist der Diebstahl von Anmeldedaten mit den höchsten Kosten verbunden. Sie sind mehr als 2,5-mal so teuer wie Zwischenfälle, die durch fahrlässig handelnde Mitarbeiter oder Auftragnehmer verursacht werden.

Abb. 13:

Durchschnittskosten pro Zwischenfall für die drei Profile

In Millionen USD



Pro Jahr verursacht fahrlässiges Verhalten von Mitarbeitern oder Auftragnehmern die höchsten Kosten für Unternehmen

Abb. 14 stellt die extrapolierten jährlichen Kosten Insider-bezogener Zwischenfälle für die drei Profile dar. In Bezug auf die Gesamtjahreskosten wird deutlich, dass Fahrlässigkeit von Mitarbeitern oder Auftragnehmern das Insider-Profil mit den höchsten Kosten darstellt. Der Diebstahl von Anmeldedaten ist zwar pro Zwischenfall am teuersten, auf das Jahr gerechnet aufgrund der relativ geringen Häufigkeit jedoch mit den geringsten Kosten verbunden.

Abb. 14:

Durchschnittliche Jahreskosten für die drei Profile

In Millionen USD

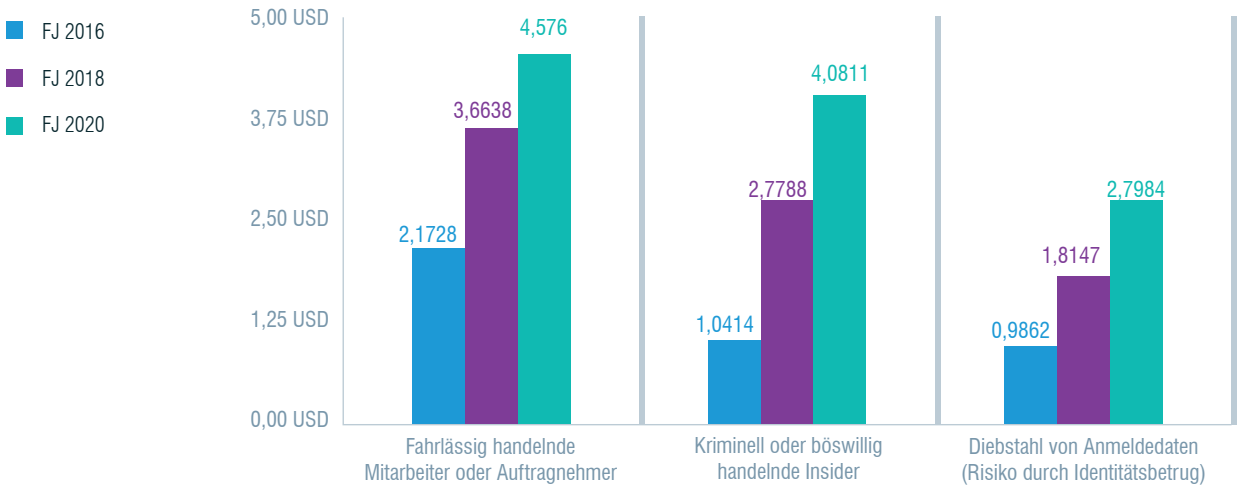
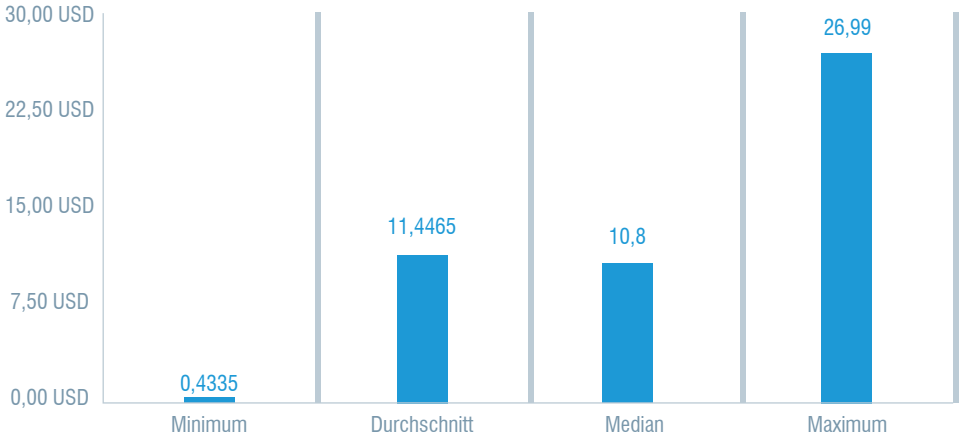


Abb. 15 stellt Median, Durchschnitt, Minimum und Maximum der Insider-Kosten (kombiniert für die drei Profile) über die vergangenen zwölf Monate dar. Der Durchschnitt liegt bei 11,45 Millionen US-Dollar, der Median bei 10,80 Millionen US-Dollar. Die Mindestkosten betragen 0,43 Millionen US-Dollar und die Maximalkosten 26,99 Millionen US-Dollar.

Abb. 15:

Statistik der untersuchten Unternehmen zu den Kosten Insider-bezogener Zwischenfälle in den vergangenen zwölf Monaten

Für drei Profile konsolidiert | In Millionen USD



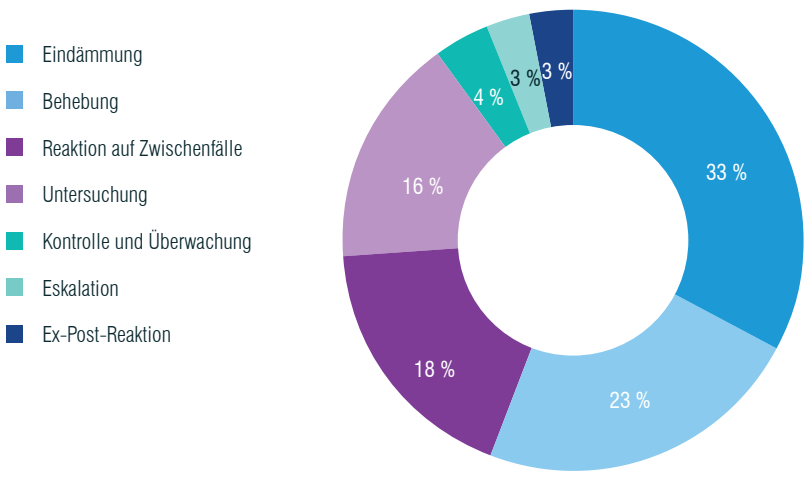
Eindämmung stellt ein Drittel aller Kosten dar

Das folgende Kreisdiagramm zeigt die anteiligen Kosten von sieben Kostenstellen. Laut Abb. 16 fallen für die Eindämmung 33 % der Gesamtjahreskosten für Insider-bezogene Zwischenfälle an. Tätigkeiten im Zusammenhang mit Behebung und der Reaktion auf Zwischenfälle stellten 23 % bzw. 18 % der Gesamtkosten dar.

Abb. 16:

Anteilige Kosten Insider-bezogener Zwischenfälle nach Tätigkeitsbereich

n=204 Unternehmen



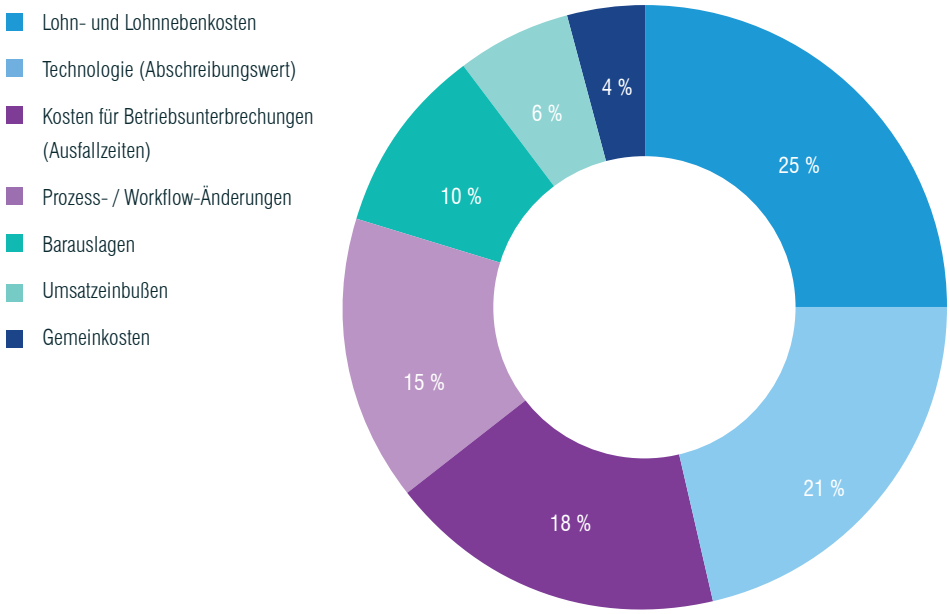
Unternehmen geben am meisten für Personal und Technologie aus, um Insider-bezogene Zwischenfälle zu beheben

Abb. 17 stellt den Anteil bei Zwischenfällen durch unachtsame oder fahrlässige Mitarbeiter, kriminelle Insider und den Diebstahl von Anmeldedaten entsprechend den sieben Kostenkategorien dar. Die Kategorie mit den höchsten Kosten (Lohn- und Lohnnebenkosten) umfasst direkte sowie indirekte Kosten für internes Personal sowie Leiharbeitskräfte und Vertragsmitarbeiter. Anschließend folgt der Kostenpunkt Technologie, was den Abschreibungswert sowie die Lizenzierung von Software und Hardware umfasst, die als Reaktion auf Insider-bezogene Zwischenfälle implementiert werden (21 %).

Die Prozesskosten umfassen Steuerungs- und Kontrollsystem-Tätigkeiten als Reaktion auf Bedrohungen und Angriffe. Zu den Kosten durch Unterbrechung gehören eingeschränkte Mitarbeiter/Benutzerproduktivität aufgrund Insider-bezogener Zwischenfälle. Die Gemeinkosten decken vielfältige Kosten für Support-Personal sowie die IT-Sicherheitsinfrastruktur ab.

Abb. 17:

Anteil der Kosten nach Standardkategorien

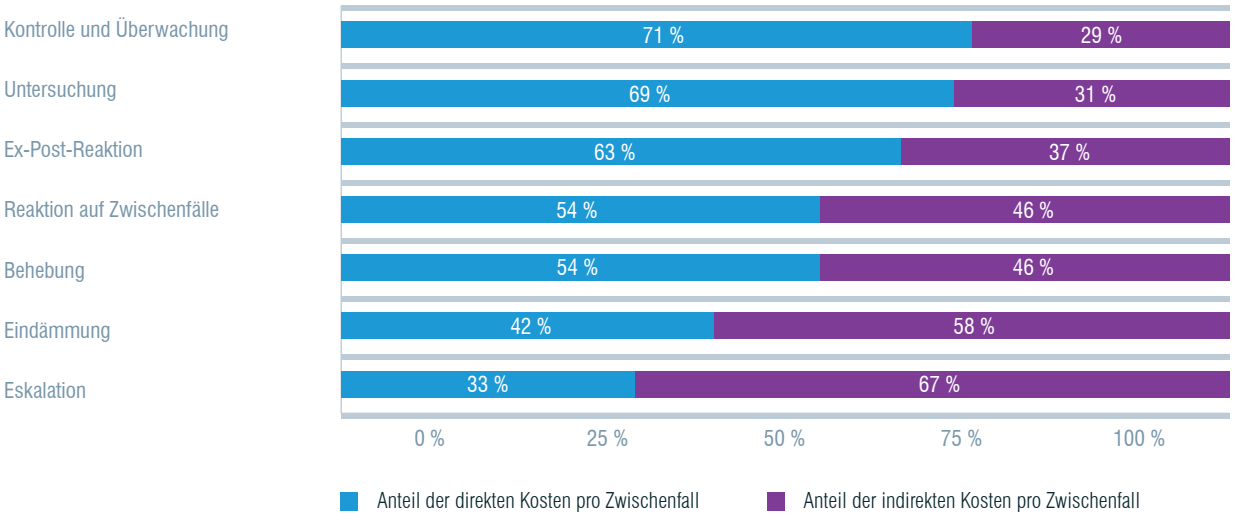


Die Unternehmen wurden gebeten, die direkten Kosten zur Durchführung einer bestimmten Tätigkeit sowie den Zeit- und Arbeitsaufwand und sonstige aufgewendete Ressourcen zu bestimmen, jedoch nicht als direkte Barauslagen (d. h. indirekte Kosten). Abb. 18 zeigt den Anteil der direkten und indirekten Kosten für sieben interne Tätigkeiten-Kostenstellen. Es zeigt sich, dass der Bereich „Kontrolle und Überwachung“ den höchsten Anteil an den direkten Kosten hat. Demgegenüber hat Eskalation den höchsten Anteil indirekter Kosten.

Abb. 18:

Gegenüberstellung der Anteile der direkten und indirekten Kosten für Kostenstellen

Für drei Profile konsolidiert



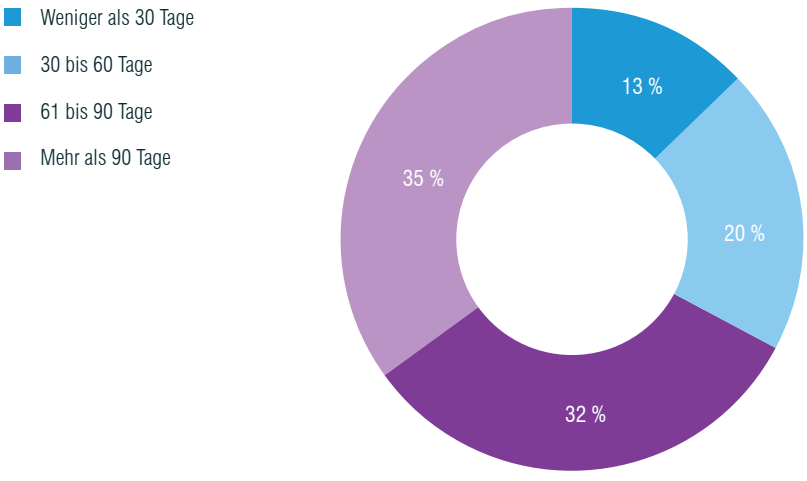
Unternehmen benötigen im Durchschnitt mehr als zwei Monate, um einen Insider-bezogenen Zwischenfall einzudämmen

Laut Abb. 19 dauerte die Eindämmung Insider-bezogener Zwischenfälle in unserer Benchmark-Stichprobe durchschnittlich 77 Tage. Nur 13 % der Zwischenfälle wurden in weniger als 30 Tagen eingedämmt.

Abb. 19:

Prozentuale Verteilung bei Insider-bezogenen Zwischenfällen basierend auf der Eindämmungsdauer

Durchschnitt=77 Tage



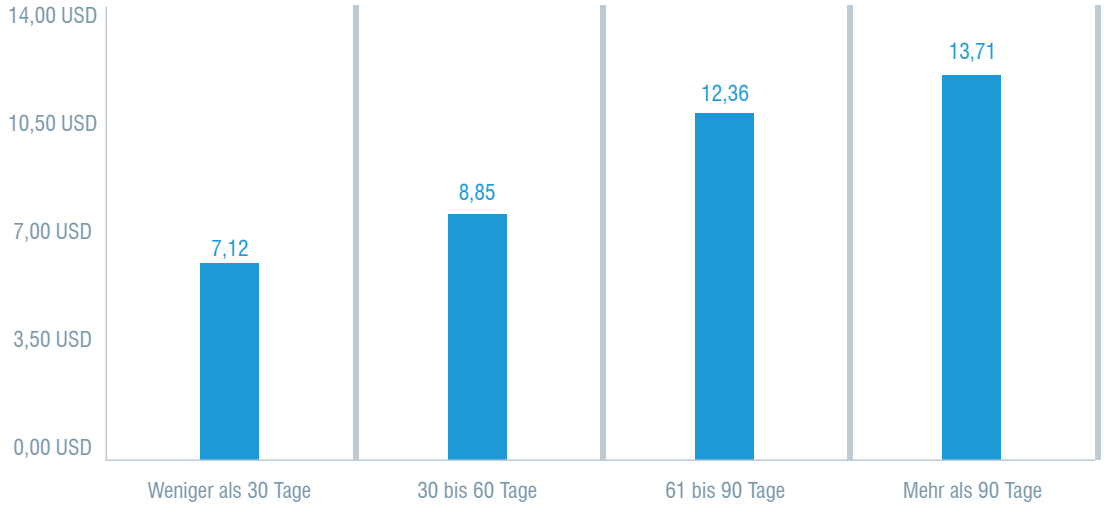
Je schneller die Eindämmung, desto geringer die Kosten

Die Jahresgesamtkosten scheinen positiv mit der Eindämmungsdauer durch Insider-bezogene Zwischenfälle zu korrelieren. Wie Abb. 20 zeigt, waren Zwischenfälle mit einer Eindämmungsdauer von mehr als 90 Tagen mit den höchsten Gesamtkosten pro Jahr verbunden (13,71 Millionen US-Dollar). Im Gegensatz dazu wurden bei Zwischenfällen mit weniger als 30 Tagen Eindämmungsdauer die geringsten Gesamtkosten verzeichnet (7,12 Millionen US-Dollar). Die durchschnittlichen Jahreskosten liegen bei 11,45 Millionen US-Dollar.

Abb. 20:

Durchschnittliche Tätigkeitskosten nach Eindämmungsdauer in Tagen

Durchschnitt=11,45 USD | In Millionen USD



Die Gesamtjahreskosten für 13 Branchen sind in Abb. 21 dargestellt.[3] Finanzdienstleister verzeichneten mit 14,50 Millionen US-Dollar die höchsten Gesamtkosten. Auf den nächsten Plätzen folgten Dienstleister sowie Technologie- und Softwareanbieter mit 12,31 Millionen US-Dollar bzw. 12,30 Millionen US-Dollar. Demgegenüber hatten Unternehmen in Bildung und Forschung mit 8,85 Millionen US-Dollar die geringsten Jahresgesamtkosten.

3 Aufgrund der kleinen Stichprobengrößen in den einzelnen Unterkategorien sind die Unterschiede zwischen Branchen nur bedingt aussagekräftig.

Abb. 21:

Jährliche Tätigkeitskosten nach Branche

Durchschnitt=11,45 USD | In Millionen USD

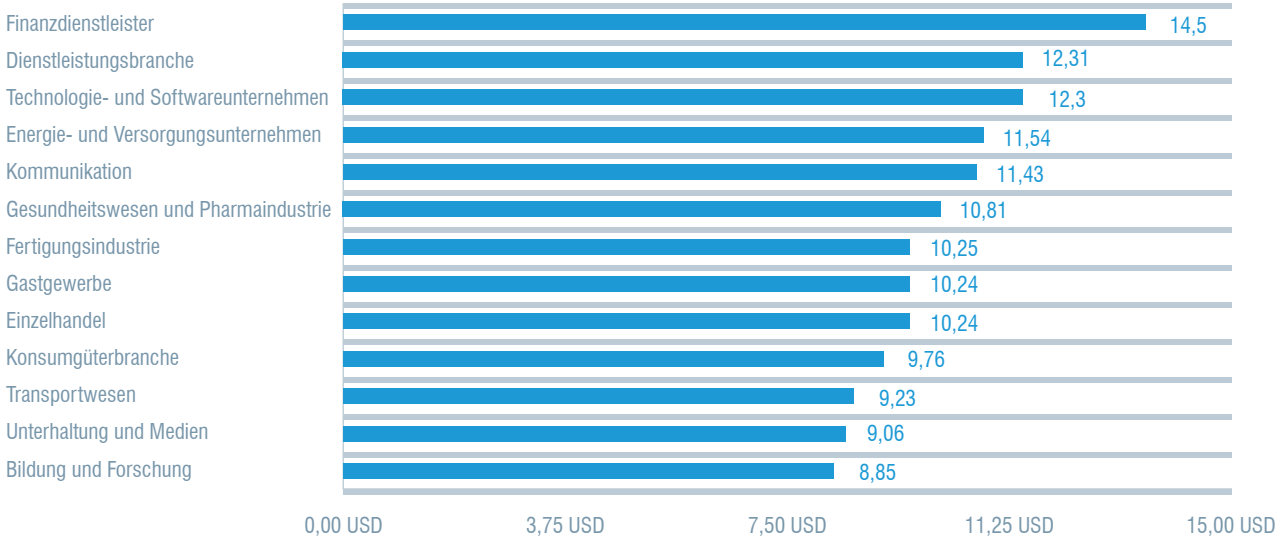
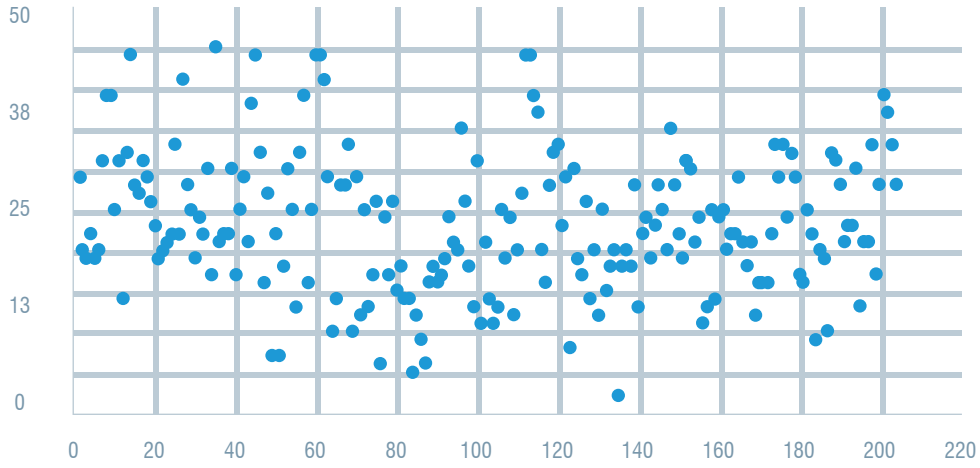


Abb. 22 stellt ein Streudiagramm der Jahresgesamtkosten von Insider-bezogenen Zwischenfällen pro Unternehmen dar. Von den 204 teilnehmenden Unternehmen hatten 124 (61 %) in den letzten zwölf Monaten durchschnittliche Gesamtkosten in Höhe oder unterhalb des Mittelwerts von 11,45 Millionen US-Dollar. Die verbliebenen 80 Unternehmen (39 %) liegen über diesem Wert. Dies zeigt, dass die Verteilung ungleichmäßig ist.

Abb. 22:

Streudiagramm Insider-bezogener Zwischenfälle nach Unternehmen

Durchschnitt=11,45 USD | In Millionen USD



Wie in Tabelle 3 dargestellt, setzt die Mehrzahl der im Bereich "Insider Threat Management" auf Schulungen zur Steigerung des Sicherheitsbewusstseins (55 %), Schutz vor Datenverlust (Data Loss Prevention, DLP) (54 %) sowie Analysen des Benutzerverhaltens (User Behavior Analystics, UBA) (50 %).

Tabelle 3: Tools und Aktivitäten im Kampf gegen Insider-Bedrohungen Sicherheitstools und Tätigkeiten	Zahl der Unternehmen	Anteil der Unternehmen
Awareness-Schulungen	112	55 %
Schutz vor Datenverlust (DLP)	110	54 %
Analyse des Benutzerverhaltens (UBA)	102	50 %
Kontrolle und Überwachung von Mitarbeitern	96	47 %
Security Information and Event Management (SIEM)	91	45 %
Incident Response Management (IRM)	89	44 %
Gründliche Überprüfung von Auftragnehmern	87	43 %
Austausch von Bedrohungsdaten	85	42 %
Verwaltung privilegierter Zugriffe (PAM)	80	39 %
Analyse des Netzwerk-Traffics	77	38 %

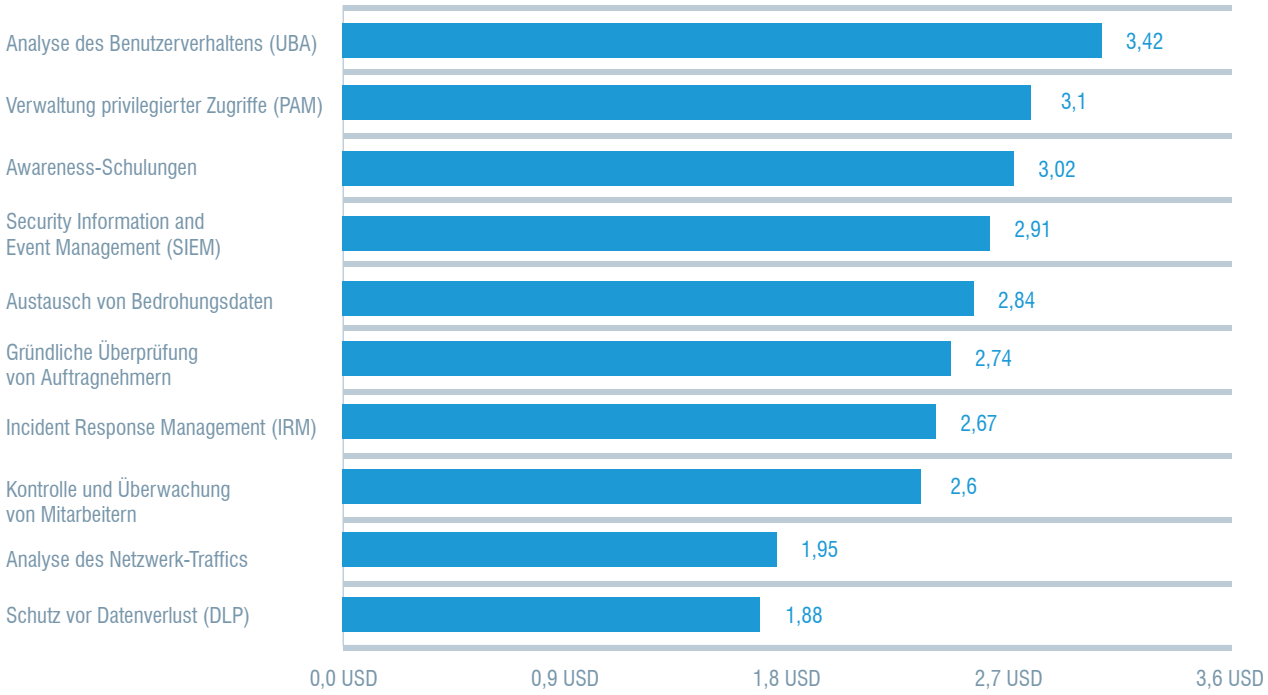
UBA, PAM und Awareness-Schulungen sind die kostengünstigsten Tools und Aktivitäten

Wie Abb. 23 zeigt, können Unternehmen im Durchschnitt 3,4 Millionen US-Dollar mit UBA-Lösungen sowie 3,1 Millionen US-Dollar mit PAM-Lösungen sparen. Die am häufigsten eingesetzten Tools und Aktivitäten sind in Abb. 23 aufgeführt. Entsprechend führen 112 Unternehmen Schulungsprogramme zur Verbesserung des Sicherheitsbewusstseins durch. 110 Unternehmen setzen DLP-Lösungen ein und 102 Unternehmen nutzen UBA-Lösungen zur Erkennung verdächtiger Netzwerkaktivitäten.

Abb. 23:

Kosteneinsparungen durch Tools und Aktivitäten zur Verringerung von Cyberrisiken

Durchschnitt=11,45 USD | In Millionen USD



SCHLUSSFOLGERUNGEN – INSIDER THREAT MANAGEMENT

Bedrohungen durch Insider nehmen zu: Die Durchschnittskosten pro Zwischenfall stiegen von 8,76 Millionen US-Dollar (2018, lt. Ponemon) auf 11,45 Millionen US-Dollar (2020), während die Eindämmung eines Zwischenfalls jetzt 77 statt 73 Tage (lt. Ponemon) in Anspruch nimmt. Daher müssen Unternehmen ein effektives Insider Threat Management-Programm aufbauen. Ein solches Programm soll gewährleisten, dass das Unternehmen bei einem Zwischenfall schnell reagieren und die Folgen für den Geschäftsbetrieb insgesamt minimieren kann.

Unabhängig davon, ob Insider-Bedrohungen auf Fahrlässigkeit oder Böswilligkeit zurückzuführen sind, können sie nicht mit Technologie allein behoben werden. Deshalb benötigen Unternehmen eine Insider Threat Management (ITM)-Lösung, die Menschen, Prozesse und Technologien verbindet und es ermöglicht, Zwischenfällen im Unternehmen schnell aufzudecken und oder gar zu verhindern.

Menschen

- Die Erkennung und Vermeidung von Insider-Bedrohungen kann nur im Team funktionieren. Gewährleisten Sie, dass die richtigen Gruppen und Verantwortlichen im Sicherheitskontrollzentrum (SOC) des Unternehmens vertreten sind.
- Beschränken Sie den Anwenderzugriff auf nicht geschäftskritische Daten oder schränken Sie die Zeitspanne ein, in der privilegierte Anwender auf diese Informationen zugreifen können.
- Suchen Sie nach verdächtigen Verhaltensindikatoren, um potenziell schädliche Insider-Bedrohungen aufzudecken.

Prozesse

- Bewerten Sie die Risiken für das Unternehmen. Schaffen Sie eine Position, die sich dediziert mit Bedrohungen durch Insider befasst, insbesondere wenn Daten besonders vertraulich oder wertvoll sind.
- Etablieren Sie einheitliche und wiederholbare Prozesse, die allen Mitarbeitern gegenüber fair sind, und nutzen Sie Technologien für den Aufbau und die Unterstützung dieser Prozesse.
- Investieren Sie in Schulungen für Ihre Anwender, um sie in Bereichen wie dem sicheren Umgang mit Daten, Sicherheitsbewusstsein und Wachsamkeit zu unterstützen.

Technologien

- Berücksichtigen Sie mögliche Leistungseinbußen sowie den Aufwand für die Verwaltung, Bereitstellung, Stabilität und Flexibilität jeder Lösung zur Abwehr von Insider-Bedrohungen.
- Wählen Sie eine Lösung, die mit dem Wachstum Ihres Unternehmens skaliert.
- Achten Sie insbesondere auf die Erfahrungen eines Anbieters in Bezug auf das Insider Threat Management.
- Bringen Sie in Erfahrung, ob die Lösung Einblicke in die Aktivitäten von Anwendern gibt – insbesondere in Bezug auf Anwender mit umfangreichen Zugriffsrechten.

DIESE UNTERSUCHUNG DER KOSTEN IST EINZIGARTIG, DA SIE **DIE GRUNDLEGENDEN SYSTEME** UND **TÄTIGKEITEN IM ZUSAMMENHANG MIT GESCHÄFTSPROZESSEN** BERÜCKSICHTIGT, DIE EINE VIELZAHL VON AUSGABEN NACH SICH ZIEHEN.

FRAMEWORK

Diese Untersuchung liefert Informationen dazu, mit welchen Kosten für ein Unternehmen die Bedrohung durch Insider verbunden sein kann. Die Umfrage deckt die grundlegenden prozessbezogenen Systeme und Tätigkeiten im Zusammenhang mit Geschäftsprozessen ab, die verschiedene Ausgaben im Zusammenhang mit der Reaktion des Unternehmens auf Fahrlässigkeit und kriminelles Verhalten von Insidern 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 Unternehmensressourcen, jedoch ohne direkte Barauslagen
- Opportunitätskosten: Die Kosten durch entgangene Geschäftschancen als Konsequenz einer Rufschädigung nach dem Zwischenfall

Externe Kosten wie der Verlust von Informationsressourcen, 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 die grundlegenden prozessbezogenen 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]

- **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 Endgeräte.
- **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.

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:

- **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.
- **Kosten durch Geschäftsunterbrechung:** Die wirtschaftliche Auswirkung von Ausfallzeiten oder ungeplanten Unterbrechungen, aufgrund derer das Unternehmen seine Daten nicht verarbeiten kann.
- **Kosten durch Geräteschäden:** Die Kosten für die Wiederherstellung von Geräten und weiteren IT-Ressourcen nach Insider-Angriffen auf Informationsressourcen und kritische Infrastruktur.
- **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. eine mehrjährige Investition in Technologien.

UNSER BENCHMARK-INSTRUMENT **ERFASST BESCHREIBENDE INFORMATIONEN** VON DER IT.

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.

Unterer Grenzwert

Oberer Grenzwert

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 stärker 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 konzentrierten 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 März 2019. Um die Konsistenz für alle untersuchten Unternehmen zu gewährleisten, bezogen sich die Angaben zu den Erfahrungen der Unternehmen jeweils auf vier aufeinanderfolgende Wochen. Der tatsächliche 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 inhärenten 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.

observeIT

INFORMATIONEN ZU OBSERVEIT

Als führender Anbieter für Lösungen zur Abwehr von Insider-Bedrohungen schützt Proofpoint | ObserveIT vor Datenverlust, schädlichen Aktionen und Markenschädigung, die durch böswillig, fahrlässig oder unbewusst falsch handelnde Insider entstehen. ObserveIT korreliert Aktivitäten und Datenbewegungen und unterstützt dadurch Sicherheitsteams bei der Identifizierung von Anwenderrisiken, bei der Erkennung von und Reaktion auf Datenschutzverletzungen durch Insider sowie bei der Beschleunigung von Reaktionen auf Sicherheitszwischenfälle. Weitere Informationen finden Sie unter: www.observeIT.com

Ponemon INSTITUTE

INFORMATIONEN ZU PONEMON INSTITUTE

Das Ponemon Institute bietet unabhängige Untersuchungen und Schulungen an, die kompetente 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 den 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.