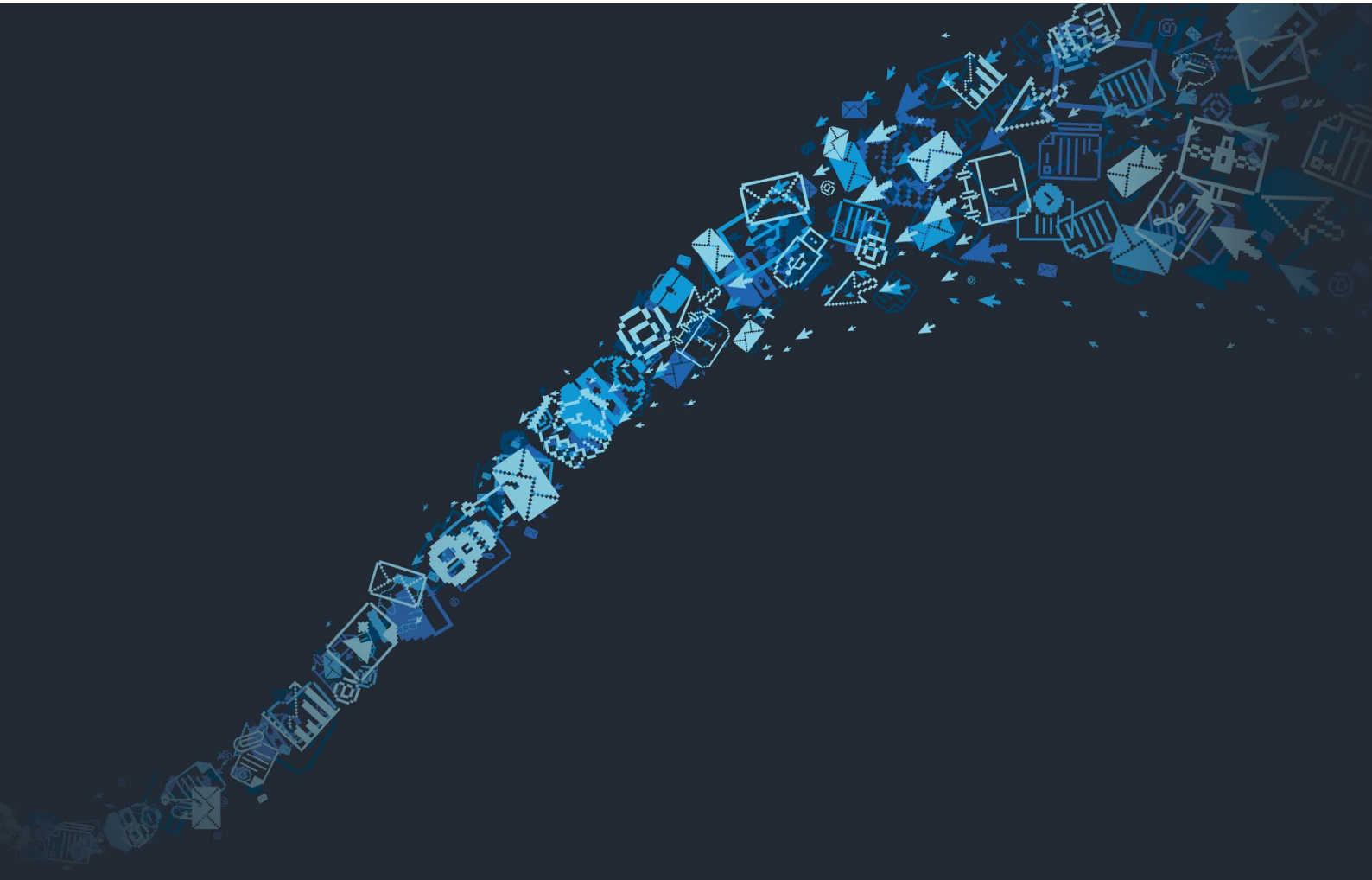
proofpoint.

techconsult
TECHNOLOGY MARKET ANALYSTS

STUDIE

Cybersecurity in Deutschland: Menschen und Daten besser schützen



proofpoint.com/de

Inhaltsverzeichnis

Informationen zur Studie

Impressum
techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de
Tel.: +49 561 8109 0
Fax: +49 561 8109 101
Web: www.techconsult.de

Erscheinungsdatum
10/2022
Autor
Ercan Hayvali

Einleitung

Die Cyber-Bedrohungslandschaft in Deutschland entwickelt sich rasant: Cyberkriminelle haben es zunehmend auf Menschen als Einfallstor für ihre Angriffe abgesehen und nicht primär auf Schwachstellen in der IT-Infrastruktur.

Über 95 Prozent[1] der erfolgreichen Cyberangriffe wurden erst durch eine menschliche Aktion ermöglicht. Menschen sind somit der wichtigste Angriffspunkt für Cyberkriminelle, die Unternehmen schaden wollen. Und in den meisten Fällen brechen Kriminelle gar nicht ein. Sie werden durch einen versehentlichen Klick oder ein wiederverwendetes Passwort hereingelassen.

Darüber hinaus hat der neue Alltag des „ortsunabhängigen Arbeitens“ in Folge der Pandemie die Angriffsflächen von Unternehmen vergrößert. Da Mitarbeiter von verschiedenen Plattformen, Geräten und Standorten auf Geschäftsinformationen und -systeme zugreifen, war der Schutz sensibler und geschäftskritischer Daten noch nie so schwierig wie heute.

Denn Daten gehen nicht von selbst verloren. Es sind immer Menschen, durch deren Aktivitäten es zu Datenverlust kommt. So werden Daten entweder von einem externen Angreifer über kompromittierte Anmeldedaten gestohlen, durch einen unvorsichtigen Benutzer an einen unbefugten Dritten weitergeleitet oder von einem böswilligen Mitarbeiter entwendet, der sie nicht selten an einen Konkurrenten weitergibt. Es ist heute wichtiger denn je, sich vor all diesen Bedrohungen zu schützen und technische Maßnahmen zu ergreifen, um sicherzustellen, dass sensible Daten geschützt sind.

Um diese Gefahrenlage besser beurteilen zu können und zu verstehen, wie sich personenzentrierte Cyberangriffe auf Unternehmen auswirken und wo die Probleme bei der Informationssicherheit in Deutschland liegen, hat Techconsult im Auftrag von Proofpoint eine Befragung unter 200 IT-Managern und Entscheidern aus deutschen Unternehmen mit mindestens 1.000 Mitarbeitern durchgeführt.

Die Studie untersucht:

- Wie häufig treten derzeit Cyberangriffe auf und welche Folgen haben sie?
- Vor welchen internen und externen Bedrohungen müssen sich Unternehmen schützen?
- Sind die bestehenden Schulungsmaßnahmen im Bereich Cybersicherheit ausreichend und wie müssen sie gestaltet sein, um erfolgreich zu sein?
- Was können Unternehmen tun, um den Bedrohungen durch böswillige Mitarbeiter erfolgreich zu begegnen?
- Wo liegen derzeit die größten Cybersecurity-Mängel in deutschen Unternehmen?

[1] The Global Risks Report 2022 des Weltwirtschaftsforums

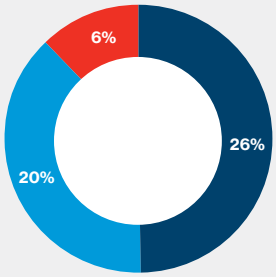
Security-Vorfälle führen zu Datenverlust und Reputationsschäden

Abbildung 1

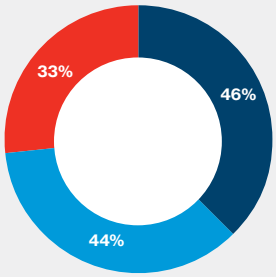
Security-Vorfälle nach Unternehmensgrößen

Basis: 200 Unternehmen

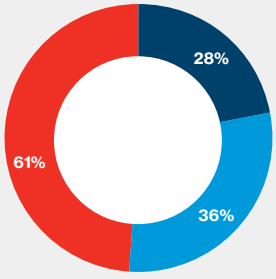
Ja, es gab mehrere Datenschutzverletzungen/Verluste sensibler Informationen.



Ja, es gab eine Datenschutzverletzung/einen Verlust von sensiblen Informationen.



Nein, es gab keine Verletzung des Datenschutzes / keinen Verlust sensibler Daten



- 1.000 bis 2.000 Beschäftigte
- 2.000 bis 5.000 Beschäftigte
- 5.000 oder mehr Beschäftigte

IT-Manager und Entscheidungsträger auf der ganzen Welt mussten in den letzten zwei Jahren ihre Cybersicherheitsstrategien ändern, um der Realität des „Arbeitens von überall“ gerecht zu werden. Viele mussten feststellen, dass Hybrid- und Remote-Arbeitsmodelle die Nutzer anfälliger für Angriffe machen. Zumindest stellen Mitarbeiter ein viel attraktiveres Ziel für Cyberkriminelle dar und vergrößern somit die Angriffsfläche einer Organisation. Auch wenn sich Unternehmen in Deutschland der wachsenden Zahl von Risiken bewusst sind, die sich aus der dynamischen Bedrohungslandschaft ergeben, ist es noch ein weiter Weg bis zu einer verlässlichen Cybersicherheit.

Security-Vorfälle sind keine Seltenheit

So gaben beispielsweise 57 Prozent der befragten IT-Sicherheitsverantwortlichen an, dass sie in den letzten 12 Monaten wenigstens eine Datenschutzverletzung und/oder den Verlust sensibler Informationen zu verzeichnen hatten. Interessanterweise scheinen Großunternehmen in Deutschland weniger häufig Opfer einer Datenpanne zu werden. So haben nur 39 Prozent der Unternehmen mit 5.000 oder mehr Mitarbeitern einen oder mehrere Sicherheitsvorfälle erlebt, während 72 Prozent der Unternehmen mit 1.000 bis 2.000 Mitarbeitern von Datenverlust durch Cybervorfälle berichten.

Bei 17 Prozent der befragten Unternehmen kam es in den letzten 12 Monaten sogar zu mehreren Datenschutzverletzungen oder dem Verlust sensibler Daten. Auch hier berichten kleinere und mittelgroße Unternehmen von überdurchschnittlich vielen Vorfällen im Vergleich zu Großunternehmen.

57 Prozent der deutschen Unternehmen in der Studie haben in den letzten 12 Monaten mindestens einen Security-Vorfall verzeichnet.

Das Auftreten solcher Sicherheitsvorfälle ist branchenübergreifend zu beobachten und könnte auch größere Dimensionen haben, als die Datenlage offenbart. Denn Datendiebstahl, Cyberattacken oder Datenverluste aufgrund von Nachlässigkeit werden oft gar nicht oder erst sehr spät erkannt. Doch welche Auswirkungen haben Sicherheitsvorfälle auf deutsche Unternehmen?

Die Folgen von Datendiebstahl und -missbrauch

ZENTRALE ERKENNTNIS

Ein Cybersecurity-Vorfall führt in 34 Prozent der Fälle zu finanziellem Schaden.

Ein Blick auf die in Abbildung 2 dargestellten Ergebnisse macht deutlich, dass Sicherheitsvorfälle eine Vielzahl von unerwünschten Folgen haben können. So haben über 37 Prozent der Unternehmen durch Datendiebstahl und Datenmissbrauch einen Reputationsverlust erlitten. Besonders ausgeprägt ist dies mit 45 Prozent in der Unternehmensgröße von 1.000 bis 2.000 Mitarbeitern, während nur ein Drittel (32 Prozent) der Großunternehmen mit 5.000 oder mehr Mitarbeitern negative Folgen für seinen Ruf verzeichnen musste. Unter den Branchen ist der Einzelhandel am stärksten von Reputationsschäden betroffen.

Eine weitere schwerwiegende Folge stellt für 35 Prozent der befragten IT-Sicherheitsverantwortlichen der Verlust wichtiger Daten dar. Infolge einer Datenpanne kann eine große Anzahl von Dokumenten und Informationen, die für das Geschäft oder den Erfolg des Unternehmens entscheidend sein können, in die falschen Hände geraten und dem Unternehmen langfristigen Schaden zufügen.

Mehr als jedes dritte Unternehmen (34 Prozent) hat durch einen in den letzten 12 Monaten stattgefundenen Cybersecurity-Vorfall einen direkten oder indirekten finanziellen Schaden erlitten. Nur 3 Prozent der befragten Unternehmen hatten keinerlei Konsequenzen aus Datendiebstahl und -missbrauch zu beklagen.

REPUTATIONSSCHÄDEN NACH BRANCHEN

45%
Handel

40%
Öffentliche Verwaltungen, Non-Profit, Gesundheits- und Sozialwesen

37%
Dienstleistung

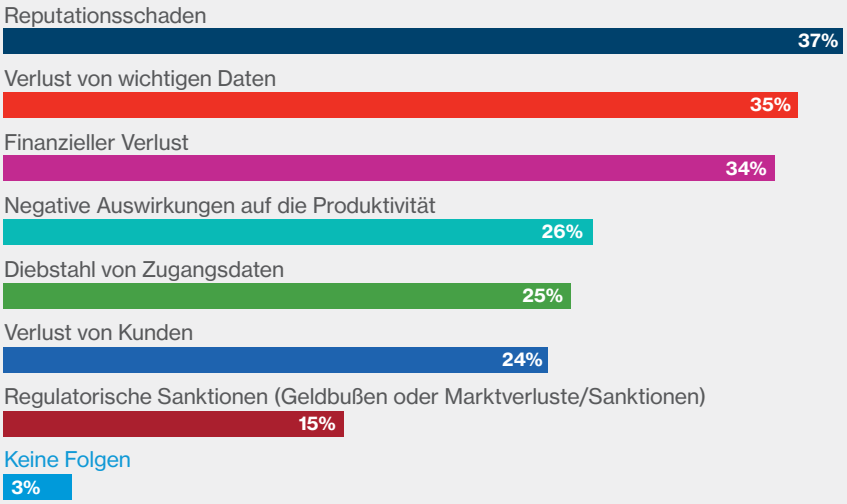
35%
Industrie

25%
Banken und Versicherungen

Abbildung 2

Folgen von Datendiebstahl und Datenmissbrauch

Basis: 200 Unternehmen



Menschen sind der größte Risikofaktor

ZENTRALE ERKENNTNIS

Mitarbeiter mit kriminellen oder böswilligen Absichten sind in 30 Prozent der Fälle die Hauptursache für eine Datenpanne.

Über 95 Prozent[1] der erfolgreichen Cyberangriffe erfordern eine menschliche Aktion. Darum sind Menschen der wichtigste Angriffspunkt für Cyberkriminelle, die Unternehmen schaden wollen, und somit für Unternehmen der wichtigste Faktor für geeignete Sicherheitsstrategien und -maßnahmen.

Mitarbeiter aller Ebenen und Funktionen können Unternehmen auf vielfältige Weise gefährden. Sie können beispielsweise schwache Passwörter verwenden, Anmeldeinformationen weitergeben, auf bösartige Links klicken oder nicht autorisierte Anwendungen herunterladen.

Während 43 Prozent der Unternehmen, die in den letzten 12 Monaten Opfer von Datendiebstahl und -missbrauch wurden, externe Angriffe durch Cyberkriminelle als Hauptursache ausmachen, zeigen die vorliegenden Ergebnisse, dass deutsche Unternehmen zunehmend mit Risiken von innen konfrontiert sind. Mehr denn je ist es wichtig, sich vor Insider-Bedrohungen zu schützen.

Beschäftigte als primäre Ursache für Security-Vorfälle

Die Ergebnisse zeigen, dass Mitarbeiter deutsche Organisationen zunehmend vor Cybersecurity-Herausforderungen stellen. Dies kann zum Teil darauf zurückgeführt werden, dass Cyberangriffe immer raffinierter werden und die Methoden, mit denen Cyberkriminelle Mitarbeiter in eine Falle locken, immer mehr der legitimen Unternehmenskommunikation ähneln. Auch wenn die Bedrohung von innen ausgeht, sind längt nicht alle Insider-Bedrohungen böswillig. Viele Mitarbeiter sind sich nicht bewusst, dass ihre Handlungen einem Insider-Angriff gleichkommen und ihr Unternehmen gefährden.

34%

Mehr als ein Drittel der befragten Unternehmen berichten von einem Cyberangriff mit gestohlenen Zugangsdaten.

Bei 41 Prozent der Unternehmen waren fahrlässige und unvorsichtige Mitarbeiter der Grund für die aufgetretenen Datendiebstähle. So werden beispielsweise infizierte E-Mail-Anhänge geöffnet, gefälschte Webseiten oder Formulare aufgerufen und ausgefüllt, oder Beschäftigte fallen auf gefälschte E-Mails herein und geben sensible Informationen preis. Auch hier unterscheiden sich die Ergebnisse je nach Unternehmensgröße: Großunternehmen geben deutlich häufiger eigene nachlässige Mitarbeiter als Ursache an (52 Prozent) als Unternehmen mit 1.000 bis 2.000 Mitarbeitern (34 Prozent).

Insgesamt berichtet mehr als ein Drittel (34 Prozent) der deutschen Unternehmen von einem Cyberangriff mit gestohlenen Zugangsdaten. Der Diebstahl kann u.a. durch Social Engineering geschehen, bei dem interne oder vertrauliche Informationen von Mitarbeitern unter Vorspiegelung falscher Tatsachen erlangt werden.

Besorgniserregend ist, dass ein großer Anteil der von Mitarbeitern ausgehenden Cyber-Bedrohungen absichtlich erfolgt. Tatsächlich gaben 30 Prozent der Befragten an, dass Mitarbeiter mit böswilligen oder kriminellen Absichten die Hauptursache für eine erlittene Datenpanne waren.

[1] The Global Risks Report 2022 des Weltwirtschaftsforums

ZENTRALE ERKENNTNISSE

Das Anklicken bösartiger Links (46 Prozent) und das Herunterladen unbekannter Anhänge und Dateien (41 Prozent) sind verbreitete Verhaltensweisen von Beschäftigten.

Fahrlässiges Verhalten als Türöffner für Cyber-Kriminelle

Mit fortschrittlichen E-Mail-Sicherheitslösungen lassen sich zwar bösartige Links in E-Mails oft schon vor der Zustellung in den Posteingang der Mitarbeiter herausfiltern, und auch Isolationstechnologie kann helfen, das Risiko des Downloads von Schadsoftware zu minimieren. Die vorliegenden Ergebnisse zeigen jedoch, dass diese Mittel noch längst nicht in allen Unternehmen angewandt werden. So gaben 46 Prozent der befragten IT-Sicherheitsverantwortlichen an, dass ihre Beschäftigten auf bösartige Links in E-Mails klicken und 41 Prozent, dass Angestellte Anhänge und Dateien aus unbekannten Quellen herunterladen. Diese Verhaltensweisen sind hoch riskant und können als Einfallstor für Malware, z. B. Ransomware, dienen, die nicht nur lokalen Schaden anrichten, sondern auch das gesamte Unternehmensnetzwerk infizieren kann.

WEITERE RISIKOREICHE VERHALTENSWEISEN VON MITARBEITERN

30%

die Verwendung unbekannter USB-Medien

27%

die Weitergabe von Zugangsdaten an andere

22%

die gemeinsame Nutzung von Firmengeräten mit Familie und Freunden

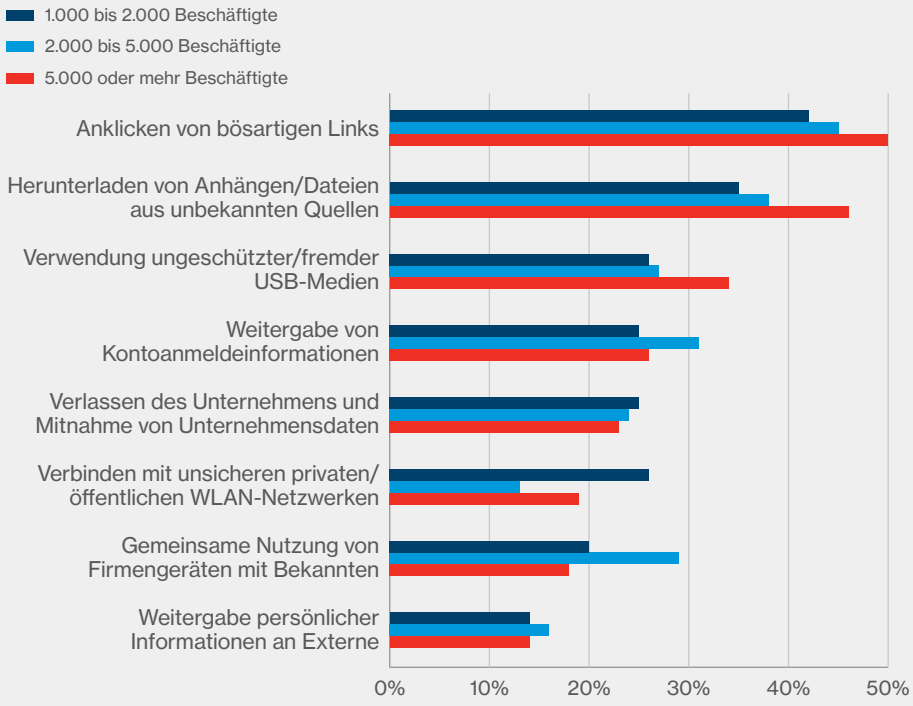
20%

die Verbindung mit unsicheren privaten oder öffentlichen WLAN-Netzwerken

Abbildung 3

Verhaltensweisen der Mitarbeiter

Basis: 200 Unternehmen



24%

Alarmierend ist, dass bei 24 Prozent der Datenpannen ehemalige Mitarbeiter sensible Daten entwenden.

Gerade im Zuge der Pandemie suchen sich viele Mitarbeiter einen neuen Arbeitsplatz. Die Ergebnisse der Studie zeigen deutlich, dass Mitarbeiter Unternehmensdaten nicht selten zu ihrem neuen Arbeitgeber mitnehmen, was eine besondere Herausforderung für die Datensicherheit darstellt. Angesichts der Auswirkungen sensibler Daten in den Händen von Konkurrenten ist es besonders alarmierend, dass bei 24 Prozent der Datenpannen, ehemalige Mitarbeiter sensible Daten mitgenommen haben.

Es fehlt an Strategien gegen Insider-Risiken

ZENTRALE ERKENNTNIS

59% der Unternehmen mit 5.000+ Mitarbeitern setzen im Kampf gegen Insiderbedrohungen auf Mitarbeiterschulungen.

Die gute Nachricht ist: Viele IT-Sicherheitsverantwortliche sind sich darüber im Klaren, dass die größte Bedrohung für die IT-Infrastruktur von den eigenen Beschäftigten ausgeht.

Entsprechend widmen sie diesem Thema mehr Aufmerksamkeit und planen, ihre Sicherheitsanstrengungen in diesem Bereich auszuweiten. So geben 85 Prozent an, dass die von den Mitarbeitern ausgehenden Risiken in den nächsten zwei Jahren zu einem der größten Probleme für die Cybersicherheit werden. Dies umfasst das gesamte Spektrum des Mitarbeiterverhaltens, einschließlich böswilliger und nachlässiger Mitarbeiter.

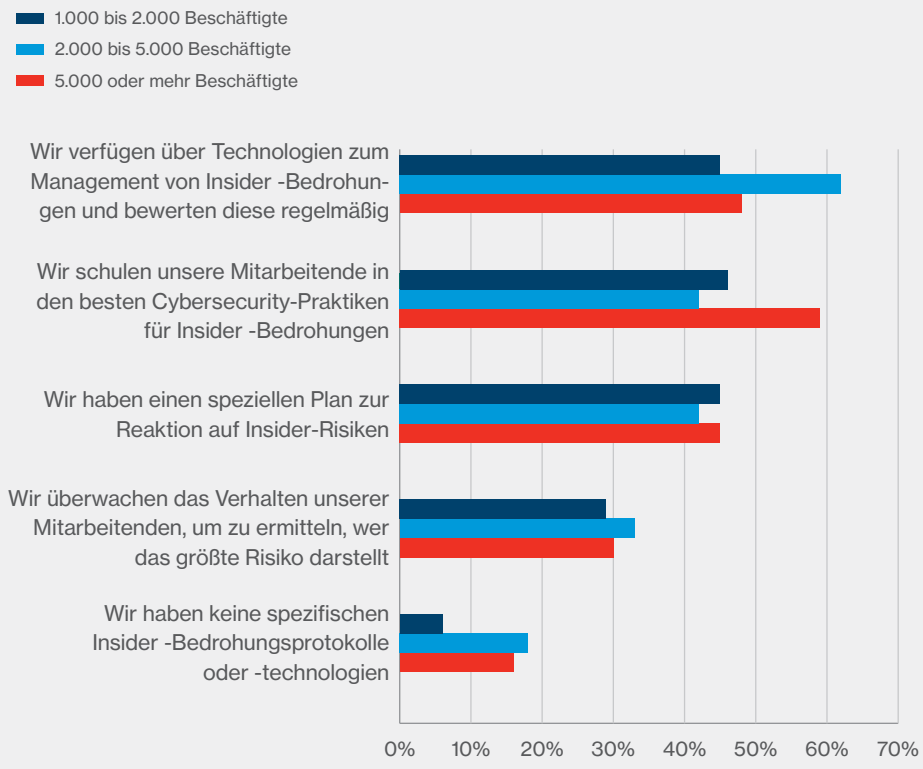
85%

Für 85 Prozent der Unternehmen ist das menschliche Risiko in den nächsten zwei Jahren ein Hauptanliegen im Bereich der Cybersicherheit.

Abbildung 4

Protokolle zur Bekämpfung von Bedrohungen

Basis: 200 Unternehmen



Im Bereich der spezifischen Sensibilisierung hinsichtlich möglicher Insider-Bedrohung haben die befragten Unternehmen bereits zahlreiche Protokolle eingerichtet. Aktuell schult jedes zweite Unternehmen (50 Prozent) seine Mitarbeiter in den besten Cybersecurity-Praktiken gegen Insider-Bedrohungen.

Darüber hinaus verfügen nur 51 Prozent der befragten Unternehmen über Technologien zur gezielten Bekämpfung von Insider-Bedrohungen. Besonders weit verbreitet sind diese Technologien in Unternehmen mit 2.000 bis 5.000 Mitarbeitern (62 Prozent), während nur 45 Prozent der Unternehmen mit 1.000 bis 2.000 Mitarbeitern über eine entsprechende Lösung verfügen.

Zusätzlich lassen sich spezifische Protokolle und Maßnahmenpläne gegen interne Bedrohungen definieren und im Bedarfsfall einsetzen. Jedoch verfügen lediglich 44 Prozent der befragten Unternehmen über einen spezifischen Plan, um auf Insider-Risiken zu reagieren. Dabei bestehen keine relevanten Unterschiede zwischen Organisationen unterschiedlicher Größe.

ZENTRALE ERKENNTNIS

Durch ein klares Berechtigungskonzept kann der Zugriff auf Dateien und Systeme definiert werden. Zugriffsrechte sollten nur jene Beschäftigte erhalten, die diese auch benötigen.

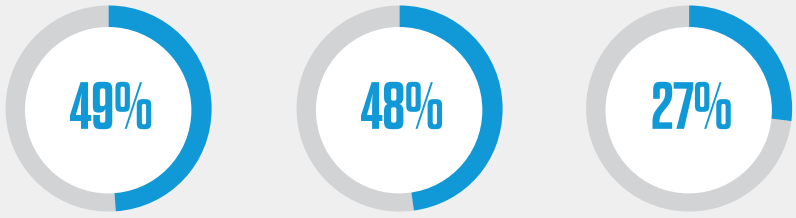
Berechtigungskonzepte schützen vor Insider-Bedrohungen

IT-Sicherheitsverantwortliche können auch den Zugang zu sensiblen Unternehmensdaten proaktiv verwalten, um Sicherheitsrisiken einzudämmen. Doch nur jedes zweite befragte Unternehmen (49 Prozent) kontrolliert kontinuierlich, welche Mitarbeiter auf sensible Daten zugreifen. Diese Kontrolle und Protokollierung würde es ihnen ermöglichen, Vorfälle einzugrenzen und den Kreis der verantwortlichen Mitarbeiter im Falle eines Datendiebstahls, -missbrauchs oder -löschens einzugrenzen.

44%
Nur 44 Prozent der Unternehmen verfügen über einen speziellen Plan zur Reaktion auf Insider-Risiken.

Abbildung 5

Einblick in sensible Unternehmensdaten
Basis: 200 Unternehmen



Wir überwachen ständig, welche Mitarbeitenden auf Daten zugreifen.

Wir schotten den Zugang zu sensiblen Daten für bestimmte Mitarbeitende ab.

Wir haben keinen genauen Überblick darüber, welche Mitarbeitende auf Daten zugreifen.

Angesichts der Bedeutung des Faktors Mensch für Cybersecurity-Vorfälle ist es alarmierend, dass nur 48 Prozent der Unternehmen den Zugang zu sensiblen Daten für bestimmte Mitarbeiter oder Mitarbeitergruppen sperren. Diese niedrige Quote ist besonders überraschend, da es sich um eine einfache Maßnahme zum Schutz sensibler Daten handelt. Noch alarmierender ist, dass ein Viertel der Unternehmen nicht genau weiß, wo ihre sensiblen Daten gespeichert sind. Darüber hinaus haben 27 Prozent der befragten Unternehmen nicht einmal einen genauen Überblick darüber, welche Mitarbeiter auf sensible Daten zugreifen. Dabei könnten Unternehmen durch proaktive Ansätze im Zugriffsmanagement ihre Dateninfrastrukturen stärken und potenziellen Bedrohungen entgegenwirken.

Unternehmen müssen sich auf eine Stärkung des Cybersecurity-Bewusstseins und bessere Security Tools konzentrieren

82%
In 82 Prozent der Unternehmen gibt es laufende Programme zur Sensibilisierung der Mitarbeiter für Cybersicherheit.

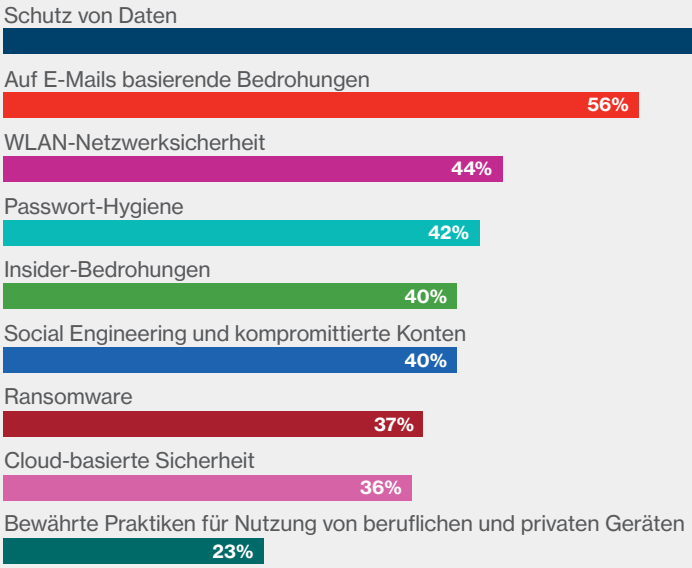
Neben technischen Lösungen und Kontrollen muss ein umfassendes Schulungsprogramm für das Personal das Herzstück der Cyberabwehr eines Unternehmens bilden.

Die IT-Sicherheitsschulungen sollten regelmäßig, umfassend und anpassungsfähig sein und eine Reihe von Themen abdecken – von den Motiven und Mechanismen hinter Cyber-Bedrohungen bis hin zur Frage, wie einfache Verhaltensfehler wie die Wiederverwendung von Passwörtern und unzureichende Datensicherheit die Wahrscheinlichkeit eines erfolgreichen Angriffs erhöhen können. Rund 82 Prozent der IT-Sicherheitsverantwortlichen geben an, dass sie aktuell ein fortlaufendes Schulungsprogramm zur Cybersicherheit für ihre Mitarbeiter durchführen.

Abbildung 6

Behandelte Themen im Rahmen der Mitarbeitersensibilisierung

Basis: 163 Unternehmen | Filter: Ja, wir haben laufende Sensibilisierungsprojekte



In mehr als zwei Drittel (68 Prozent) der Unternehmen wird Datensicherheit als Themenkomplex behandelt und bei 56 Prozent stehen E-Mail-basierte Bedrohungen als Thema auf dem Stundenplan. Da die E-Mail der Bedrohungsvektor Nummer eins ist, überrascht es, dass sie als Thema in den Awareness-Schulungen keine größere Rolle spielt.

Kein vollständiger Schutz ohne Security-Lösungen

Auch wenn Mitarbeiterschulungen und Sensibilisierungsmaßnahmen einen großen Nutzen für die IT-Sicherheit haben, sind technische Lösungen ein notwendiger Bestandteil jeder erfolgreichen IT-Sicherheitsstrategie. Dies gilt umso mehr, da Mitarbeiterschulungen dazu beitragen können, unvorsichtiges Verhalten zu minimieren, jedoch kaum etwas gegen die Bedrohung durch böswillige Insider ausrichten können. Hier müssen technische Lösungen zum Einsatz kommen, um einen potenziellen Datenverlust möglichst frühzeitig zu stoppen oder zu verhindern.

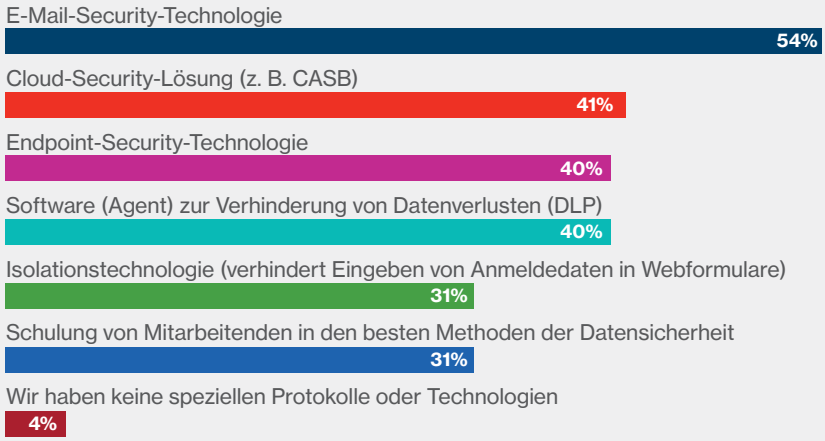
96%
96 Prozent der Unternehmen haben spezielle Protokolle oder Technologien zum Schutz vor Datenverlust

Die vorliegenden Ergebnisse zeigen deutlich, dass viele Organisationen nicht über angemessene technische Schutzmaßnahmen verfügen. Nur 54 Prozent der befragten Unternehmen nutzen eine E-Mail-Sicherheitstechnologie, mit der sich ein gewisser Teil der per E-Mail eingehenden Bedrohungen abwehren lässt. Noch schlechter sieht es bei Cloud-Lösungen aus. Nur 41 Prozent der Unternehmen verfügen über Sicherheitslösungen, die Cloud-basierte Infrastrukturen und Anwendungen schützen.

Abbildung 7

Das tun Unternehmen, um den Verlust von Unternehmensdaten zu bekämpfen

Basis: 200 Unternehmen



Die Situation lässt auch im Hinblick auf traditionellere Bedrohungen noch viel zu wünschen übrig. So setzen nur 40 Prozent der Unternehmen Technologien für die Endgerätesicherheit ein und nur der gleiche Prozentsatz verwendet Software zur Verhinderung von Datenverlusten (DLP). Da nur die Kombination von Schulungen und technischen Maßnahmen das Risiko von Cybervorfällen effektiv bekämpft, besteht in diesem Bereich akuter Nachholbedarf.

Weil IT-Systeme immer komplexer und die Methoden der Cyberkriminellen immer ausgefeilter werden, beginnt künstliche Intelligenz sich durchzusetzen, um den gestiegenen Risiken zu begegnen. Das gilt insbesondere im Bereich der proaktiven Sicherheitssoftware, wo Systeme auch aus Daten vergangener Vorfälle lernen und zukünftige Bedrohungen erkennen können. Allerdings gibt es noch reichlich zu tun, denn nur 59 Prozent der befragten IT-Sicherheitsverantwortlichen nutzen bereits Datenschutzlösungen, die künstliche Intelligenz und maschinelles Lernen einsetzen.

Fazit

Die moderne Bedrohungslandschaft entwickelt sich rasant weiter – mit größeren Angriffsflächen, mehr Zugangspunkten und immer raffinierteren Cyberangriffen. Unabhängig von der Art des Angriffs – E-Mail, Cloud-Anwendungen, Internet, soziale Medien – nutzen Cyberkriminelle den Faktor Mensch aus. Ob Hochstapler, die sich als vertrauenswürdige Kollegen ausgeben, oder immer überzeugendere Phishing-E-Mails mit bösartigen Links – es sind die Endanwender, die im Kampf gegen Cyberkriminelle an vorderster Front stehen.

Fokus auf den Faktor Mensch

Deshalb ist eine Strategie, die den Menschen in den Mittelpunkt stellt, ein Muss für Unternehmen. Organisationen müssen damit beginnen, die am stärksten gefährdeten Benutzer zu identifizieren, und sicherstellen, dass diesen das notwendige Wissen und die erforderlichen Tools an die Hand gegeben werden, um ihr Unternehmen zu schützen. Das bedeutet gezielte und anpassungsfähige Sicherheitsschulungen, die jedem Mitglied der Belegschaft klar machen, welche Rolle es bei der Preisgabe sensibler Daten und Informationen spielen kann. Aus technischer Sicht funktioniert mit dem Wegfall des traditionellen Netzwerkrands der alte Ansatz für Datensicherheit nicht mehr. Unternehmen müssen in Lösungen zum Schutz ihrer Informationen und gegen Insider-Risiken investieren, die den modernen Netzwerkrand schützen – vom Endpunkt bis zu Cloud-Anwendungen, E-Mails und dem Internet.

Moderne Lösungen als Schlüssel

Ein moderner Ansatz zum Schutz von Informationen muss das menschliche Verhalten berücksichtigen, ob im Büro, zu Hause oder unterwegs. Leider sind herkömmliche Lösungen für Data Loss Prevention (DLP) und gegen Insider-Risiken bei weitem nicht in der Lage, Vorfälle in Echtzeit oder unmittelbar nach deren Auftreten zu verhindern, zu erkennen und zu untersuchen. Unternehmen in Deutschland müssen einen neuen DLP-Ansatz verfolgen, der neue externe und interne Bedrohungen abwehrt, die auf ihr Unternehmen, ihre Mitarbeiter und ihre Daten abzielen. Ein moderner DLP-Ansatz verschafft Unternehmen mehr Transparenz und Kontext, ermöglicht schnellere und genauere Entscheidungen, spart Zeit und Verwaltungsaufwand und reduziert das Risiko von Datenverlust. Nicht zu vergessen sind Lösungen für das Insider Threat Management (ITM), die KI- und ML-Technologien einsetzen, um einen kontextbezogenen Einblick in die Art und Weise zu erhalten, wie Mitarbeiter auf die von ihnen erstellten Daten zugreifen.

Wenn Themen wie diese nicht auf angemessene Weise angegangen werden, bleiben deutsche Unternehmen anfällig für die wachsende Zahl von Cyberbedrohungen.

„Mit dem Verschwinden des traditionellen Netzwerkperimeters funktioniert die alte Art des Datenschutzes einfach nicht mehr; Unternehmen müssen in Lösungen zum Schutz von Informationen und vor Insider-Risiken investieren, die den modernen Netzwerkrand schützen - vom Endpunkt über Cloud-Apps und E-Mails bis zum Web.“

Bert Skaletski, Resident CISO für die EMEA-Region bei Proofpoint

Methodik

STUDIENINFOS

Im Rahmen der vorliegenden Studie wurden im August 2022 insgesamt 200 leitende IT- und Security-Verantwortliche aus deutschen Unternehmen hinsichtlich relevanter IT-Security-Themen befragt. Bei den Befragten handelt es sich um Beschäftigte, die maßgeblichen Einfluss an Entscheidungen rund um die IT-Sicherheitsstrategien haben oder an Entscheidungen oder Aktivitäten zur IT-Security beteiligt sind. Es wurden ausschließlich Teilnehmer aus Unternehmen der Branchen Industrie, Handel, Dienstleistung, Banken und Versicherungen sowie öffentliche Verwaltungen, Non-Profit, Gesundheits- und Sozialwesen mit mindestens 1.000 Beschäftigten berücksichtigt.

Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Abbildung 8

Branchen

Basis: 200 Unternehmen

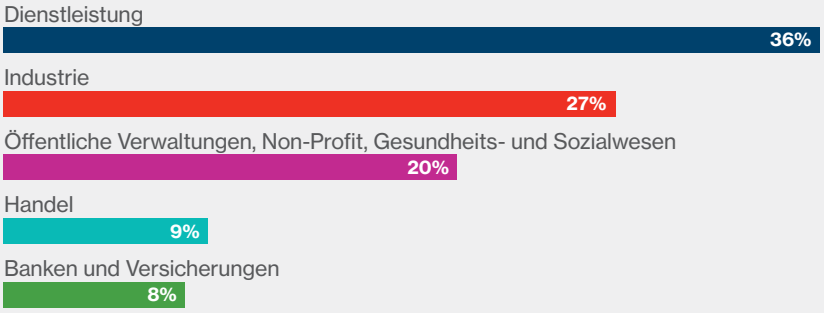


Abbildung 9

Mitarbeitergrößenklassen

Basis: 200 Unternehmen

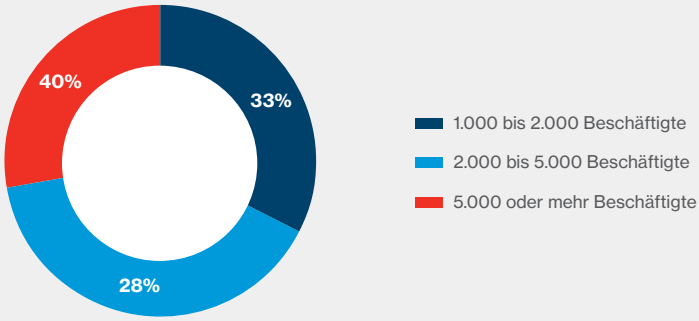
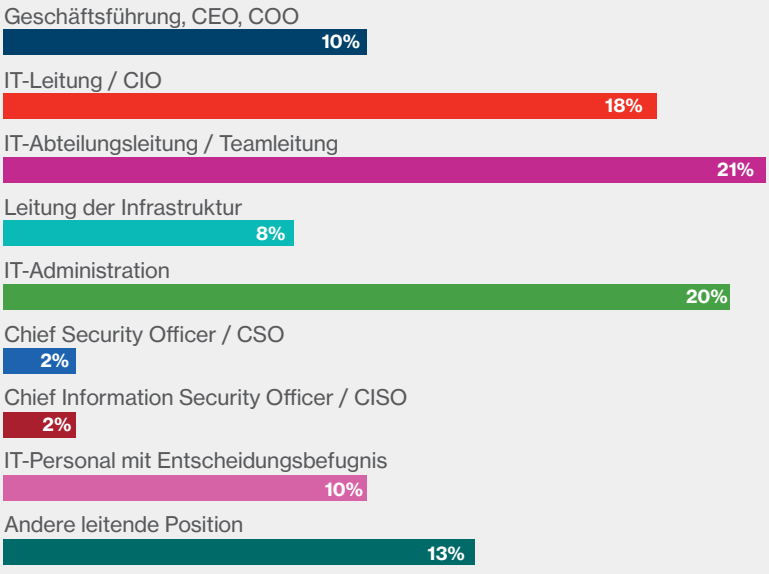


Abbildung 10

Position

Basis: 200 Unternehmen



Weitere Informationen

Kontakt für mehr Informationen

Ercan Hayvali
Analyst

Telefon: +49 561 8109 178
E-Mail: ercan.hayvali@techconsult.de

techconsult GmbH
Baunsbergstr. 37
D-34131 Kassel

Telefon: +49 561 8109 0
Fax.: +49 561 8109 101
Web: www.techconsult.de

Über techconsult GmbH

Die techconsult GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Sonstige Informationen

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

MEHR ERFAHREN

Mehr Informationen über Proofpoint auf **proofpoint.com/de**.

ÜBER PROOFPOINT

Proofpoint, Inc. ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter. Denn diese bedeuten für ein Unternehmen zugleich das größte Kapital aber auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Cybersecurity-Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und IT-Anwender in Unternehmen für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als 75 Prozent der Fortune-100-Unternehmen, verlassen sich auf Proofpoints Sicherheits- und Compliance-Lösungen, bei denen der Mensch im Mittelpunkt steht, um ihre wichtigsten Risiken bei der Nutzung von E-Mails, der Cloud, Social Media und dem Internet zu minimieren.