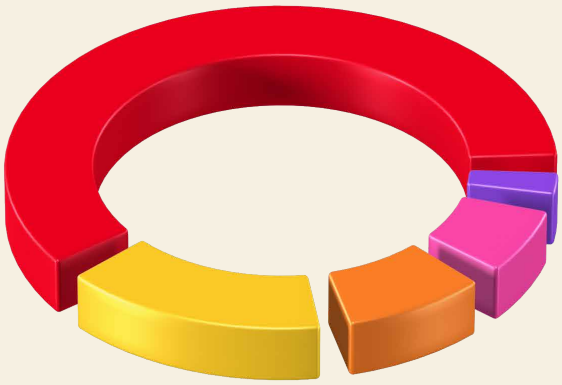
Data Breach Investigations Report 2026

Kurzfassung

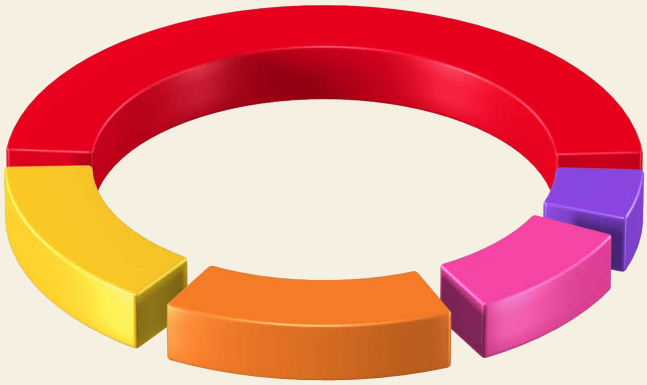
verizon business

2026



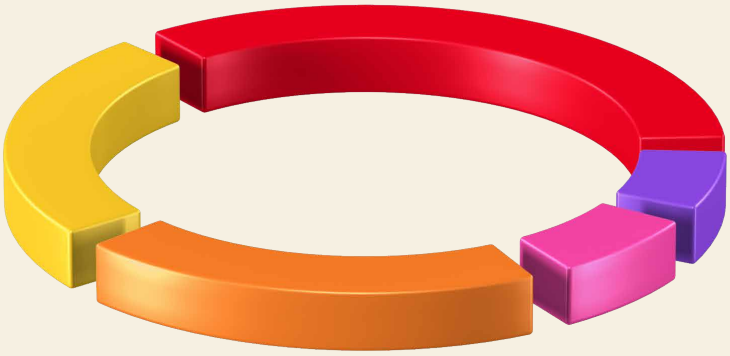
- **61 %** System Intrusion
- **17 %** Social Engineering
- **10 %** Einfache Angriffe auf Web-Anwendungen
- **8 %** Diverse Fehler
- **3 %** Missbrauch von Nutzerrechten

2025



- **53 %** System Intrusion
- **18 %** Einfache Angriffe auf Web-Anwendungen
- **17 %** Social Engineering
- **12 %** Diverse Fehler
- **7 %** Missbrauch von Nutzerrechten

2024



- **36 %** System Intrusion
- **25 %** Diverse Fehler
- **22 %** Social Engineering
- **9 %** Einfache Angriffe auf Web-Anwendungen
- **8 %** Missbrauch von Nutzerrechten

Über die Titelseite

Der Aphorismus „Die einzige Konstante ist der Wandel“ wird gemeinhin dem griechischen Philosophen Heraklit zugeschrieben. Auch wenn er aus historischer Sicht wohl keine praktischen Erfahrungen mit Cybersicherheit hatte, läge er mit dieser Einstellung in unserer Branche genau richtig. Die Bedrohungslandschaft entwickelt sich ständig weiter, und die Ausgabe 2026 des Data Breach Investigations Report (DBIR) macht deutlich, dass die Kernprinzipien der Cybersicherheit der einzige Weg sind, um diesen Veränderungen gewachsen zu sein. Ein wenig digitaler Stoizismus, wenn Sie so wollen.

Auf der Titelseite sehen Sie konzentrische Ringe, die unsere Daten für jedes Jahr symbolisieren. Sie schweben herab und landen schließlich auf dem Fundament unseres Wissens über Cybersicherheit. Diese Erfahrungswerte vertiefen unser Verständnis bei und stärken unsere Abwehrstrategien. Die einzelnen Segmente entsprechen den Vorfallkategorien der letzten vier Jahre.

Der oberste Ring stellt unseren Bericht für das Jahr 2026 dar, gefolgt von den Jahren 2025, 2024 und 2023. Der unterste Ring ist bereits fest im Fundament verankert.

Im Vergleich zum Vorjahr wurden mehr Zero-Day-Bedrohungen und kritische Schwachstellen beobachtet. KI-generierte Malware ist inzwischen weit verbreitet. Zudem wird im Vorfeld von Sicherheitsverletzungen zunehmend erfolgreich komplexes Social Engineering betrieben. Schneller, größer, riskanter – die Bedrohungslage verschärft sich. Dennoch sind die aktuellen Herausforderungen den meisten Sicherheitsteams bereits seit Langem bekannt. Die neue Welt der allgegenwärtigen Bedrohung erfordert mehr Fokus und Agilität, aber keine radikalen Kurswechsel. Gefragt ist eher Feinabstimmung als revolutionäre Umbrüche. Wenn wir weiterhin am selben Strang ziehen und das Gemeinwohl im Auge behalten, sind wir auch heute für die Zukunft gewappnet.

Übrigens nennt man diese Ringdiagramme auch Donut-Diagramme. Das nur nebenbei.

Inhalt

Willkommensgruß

Hallo und herzlich willkommen zum Verizon Data Breach Investigations Report (DBIR) 2026! Wir begrüßen unsere Stammleser und freuen uns über alle neuen Mitglieder der DBIR-Community. Schön, dass Sie unseren Ausführungen folgen.

In der 19. Ausgabe des Verizon DBIR haben wir mehr als 31.000 reale Sicherheitsvorfälle untersucht, darunter über 22.000 bestätigte Datensicherheitsverletzungen in Unternehmen aus 145 Ländern. Das ist die höchste Anzahl von Sicherheitsverletzungen, die wir je in einem einzelnen Bericht untersucht haben. Uns ist bewusst, dass wir diese Aussage nicht zum ersten Mal treffen. Sie ist jedoch nach wie vor zutreffend, denn die Zahl der untersuchten Fälle steigt von Jahr zu Jahr weiter an. Ob das nun gut oder schlecht ist, müssen Sie selbst entscheiden. Für die betroffenen Organisationen ist es sicherlich kein Grund zum Feiern, doch zur Erkennung neuer Bedrohungen für Ihr Unternehmen ist diese Entwicklung eindeutig von Vorteil.

Gäbe es ein Motto für diesen Bericht, so wäre es vermutlich „Dem Wandel zum Trotz standhaft bleiben“. Heutzutage würde wohl niemand bestreiten, dass alle Bereiche des modernen Lebens von einem stetig zunehmenden Wandel geprägt sind. Der vorliegende Bericht soll Unternehmen dabei unterstützen, den Veränderungen im Bereich der Cybersicherheit möglichst effektiv zu begegnen. Die präsentierten Daten stammen aus dem Zeitraum Oktober 2024 bis November 2025. Dennoch sind sich das DBIR-Team und Verizon zum Zeitpunkt der Veröffentlichung im Jahr 2026 der zunehmenden Auswirkungen und Möglichkeiten der KI-gestützten Schwachstellensuche und -ausnutzung absolut bewusst. Bei Vorliegen entsprechender Frühindikatoren werden wir auf diese Trends eingehen und unsere Prognosen abgeben.

Seit der Veröffentlichung des DBIR-Berichts 2025 haben wir bei einigen Ausprägungen der Cyberkriminalität signifikante Veränderungen beobachtet. In anderen Bereichen betrifft der Wandel eher die Geschwindigkeit und das Ausmaß als die Vorgehensweise selbst. Die Ausnutzung von Schwachstellen, die in mehreren Abschnitten des Berichts behandelt wird, ist inzwischen die häufigste Methode, mit der sich Angreifer Zugang zu den IT-Systemen eines Unternehmens verschaffen. Dies unterstreicht erneut die Bedeutung der korrekten Umsetzung grundlegender Sicherheitsmaßnahmen. Wie schon länger prognostiziert[1], setzen Bedrohungsakteure zunehmend auf generative KI, um sich in den verschiedenen Angriffsphasen unterstützen zu lassen. Dazu gehören die Auswahl von Zielen, die Ausbreitung in Systemen, die Schwachstellenanalyse und die Entwicklung von Malware und Tools zur Effizienzsteigerung. Auch bei unserem Lieblingsthema Social Engineering beobachten wir neue Entwicklungen. Angreifer nutzen vermehrt Sprachtools und andere mobile Strategien, um Menschen während der Arbeit zu überlisten.

Auf den folgenden Seiten finden Sie die wichtigsten Ergebnisse aus unserem Bericht, darunter auch Zahlen und Fakten zu Sicherheitsverletzungen in verschiedenen Branchen und Regionen. Diese Kurzfassung können Sie gern an Ihre Kollegen weiterleiten. Der vollständige Bericht mit detaillierteren Angaben zu aktuellen Bedrohungen steht auf Englisch zum Download bereit.

1. Damit sind Prognosen aus den beiden zuletzt erschienenen DBIR-Berichten gemeint, die weiter oben bereits erwähnt wurden.

Optimale Nutzung des Berichts

Für neue Leser:

Bevor Sie sich in den DBIR 2026 vertiefen, empfehlen wir Ihnen, diesen Abschnitt zu lesen. Der Bericht wird bereits seit einiger Zeit publiziert und uns ist bewusst, dass manche Formulierungen nicht selbsterklärend sind. Wir verwenden sehr spezielle Namenskonventionen, Begriffe und Definitionen und investieren viel Zeit, um die Konsistenz im gesamten Bericht sicherzustellen. Dieser Abschnitt soll Ihnen dabei helfen, sich mit der Sprache vertraut zu machen.
Als Stammleser des DBIR (herzlichen Dank!) können Sie gerne zum nächsten Abschnitt übergehen.

Was Sie erwartet

Der Data Breach Investigations Report (DBIR) ist eine jährlich durchgeführte Studie von Verizon, in der wir Analysen zu Sicherheitsvorfällen auf Basis anonymisierter Daten veröffentlichen. Diese Daten stammen von rund hundert Datenpartnern. Mithilfe des VERIS-Frameworks (Vocabulary for Event Recording and Incident Sharing, siehe Folgeseite) werden die Datenpunkte standardisiert. Dadurch entsteht eine praktikable Grundlage für die statistische Auswertung dieser Art von Daten. Aufgrund der Geheimhaltung rund um Sicherheitsvorfälle und der Komplexität von Abwehrmaßnahmen liegen uns oft nicht alle fallspezifischen Details vor.

Dieser Bericht zeichnet sich insbesondere durch seine breite Datenbasis aus. In anbieterspezifischen Publikationen finden sich oft fundierte und detaillierte Beschreibungen von intern durchgeführten Cyberuntersuchungen. Der vorliegende Bericht umfasst hingegen die unterschiedlichen Perspektiven mehrerer Datenpartner. Hierzu zählen große Incident-Response-Dienstleister, kleine IT-Forensik-Unternehmen, regionale und nationale Ermittlungsbehörden sowie Makler für Cyberversicherungen und Rückversicherer. Wir sind zuversichtlich, dass wir damit der Wahrheit über die tatsächliche Bedrohungslage ein gutes Stück näherkommen.

Ressourcen zum VERIS-Framework

Ihnen werden Begriffe wie „Bedrohungsakteure“, „Urheber der Bedrohung“, „Angriffsaktivität“ oder „Bedrohungsaktivität“ und „Variante“ begegnen. Sie stammen aus dem VERIS-Framework, das eine einheitliche und eindeutige Erfassung von Daten zu Sicherheitsvorfällen ermöglicht. Ihre Definitionen lauten wie folgt:

Urheber der Bedrohung/ Bedrohungsakteur/Akteur: Wer steckt dahinter? Womöglich ein externer Angreifer, der eine Phishing-Kampagne gestartet hat. Oder ein Mitarbeiter, der vertrauliche Dokumente im Fahrzeug zurückgelassen hat.

Angriffsaktivität: Mit welchen Taktiken wurde die Ressource angegriffen? VERIS unterteilt Sicherheitsvorfälle in sieben Hauptkategorien: Malware, Hacking, Social Engineering, Missbrauch, physischer Angriff, menschlicher Fehler und umweltbedingte Faktoren. Beispiele hierfür sind das Hacken eines Servers, das Einschleusen von Malware oder die Täuschung von Personen durch Social Engineering.

Variante: Genauere Unterkategorie, z. B. die Einstufung eines externen Angreifers als organisierte kriminelle Gruppe oder die Klassifizierung eines Hackerangriffs als SQL-Injection oder Brute-Force-Attacke.

Wir verwenden auch die Begriffe „Vektor“, „Motiv“ und „Kategorie“. In den einzelnen Abschnitten wird der Leser jeweils an die Bedeutung dieser Terminologie herangeführt.

Weiterführende Informationen:

- Unter github.com/vz-risk/veris (auf Englisch) finden Sie das JSON-Schema (JavaScript Object Notation) des Frameworks, Anwendungsbeispiele, Skripte, Aufzählungen und Zuordnungen zu den „Critical Security Controls“ des Center for Internet Security (CIS) sowie zum MITRE ATT&CK-Framework. Außerdem wird hier der VERIS-Styleguide bereitgestellt.

- Auf der benutzerfreundlichen Website verisframework.org (auf Englisch) finden Sie weitere Informationen zum Framework sowie diverse Beispiele und nützliche Aufzählungen.

Vorfall oder Verletzung

Für die Begriffe „Sicherheitsvorfall“ und „Sicherheitsverletzung“ gelten die folgenden Definitionen:

Sicherheitsvorfall: Ein negatives Ereignis, das die Integrität, Vertraulichkeit oder Verfügbarkeit von Daten gefährdet.

Sicherheitsverletzung: Ein Ereignis, das einen bestätigten (und nicht nur möglichen) Datenzugriff durch nicht autorisierte Personen zur Folge hat. Ein DDoS-Angriff (Distributed Denial of Service) wird in der Regel eher als Vorfall denn als Sicherheitsverletzung eingestuft, da hierbei nur selten Daten gestohlen werden. Wir sind uns jedoch bewusst, dass dies die Schwere des Angriffs nicht mindert.

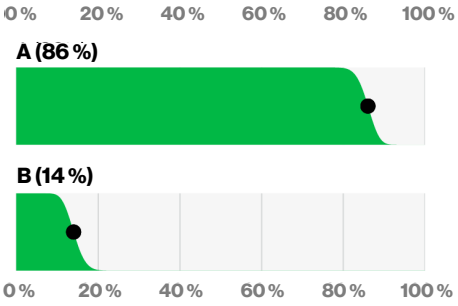


Abbildung 2: Beispielhaftes abgeschrägtes Balkendiagramm (n=230)

Branchenbezeichnungen

Wir nutzen das nordamerikanische Klassifizierungssystem NAICS, um die betroffenen Unternehmen und Institutionen einzelnen Branchen zuzuordnen. NAICS verwendet zur Klassifizierung zwei- bis sechsstellige Codes. Unsere Analysen finden in der

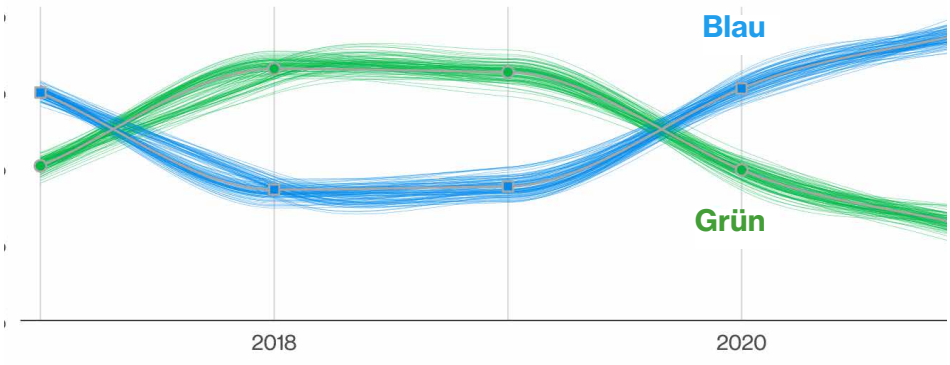


Abbildung 1: Beispielhaftes Spaghetti-Diagramm

Regel auf der zweistelligen Ebene statt, wobei wir die NAICS-Codes gemeinsam mit der Branchenbezeichnung nennen. Wenn ein Diagramm beispielsweise mit „Finanzwesen (NAICS 52)“ beschriftet ist, ist die 52 nicht als Wert zu verstehen. 52 ist der NAICS-Code für die Finanz- und Versicherungsbranche. In den Abbildungen wird zur besseren Übersichtlichkeit meist die Sammelbezeichnung „Finanzwesen” verwendet. Ausführliche Informationen über die Codes und das Klassifizierungssystem finden Sie unter: census.gov/naics.

Vertrauen in unsere Daten

Bereits seit dem DBIR 2019 macht eine schräge rechte Kante in unseren Balkendiagrammen deutlich, dass es in der Informationssicherheit keine absoluten Gewissheiten gibt. Trotz aller verfügbaren Daten können wir keine endgültigen Aussagen treffen. Anstatt jedoch zu kapitulieren und zu beklagen, dass mangels ausreichender Daten keine präzisen Messungen möglich sind (oder noch schlimmer, Fakten schlicht zu erfinden), machen wir uns an die Arbeit. Auch in diesem Jahr können Sie miterleben, wie wir uns mit den unsicheren Zahlen im Bericht auseinandersetzen.

Die Abbildungen 1, 2 und 3 zeigen beispielsweise mögliche Realitäten. Die inhärente Ungewissheit im Bereich der Cybersicherheit wird durch die Abschrägung des Balkendiagramms, die Linien im Spaghetti-Diagramm, die Punkte im Punktdiagramm und die Farben im Bilddiagramm jeweils auf eigene Weise vermittelt.

Das abgeschrägte Balkendiagramm ist unseren Stammlesern bereits bekannt. Die Abschrägung verdeutlicht die Unsicherheit eines Datenpunkts bei einem Konfidenzniveau von 95 % (ein gängiger Standardwert für statistische Tests). Einfach ausgedrückt: Wenn sich die schrägen Bereiche zweier oder mehrerer Balken überlappen, lässt sich nicht mit Sicherheit sagen, welcher

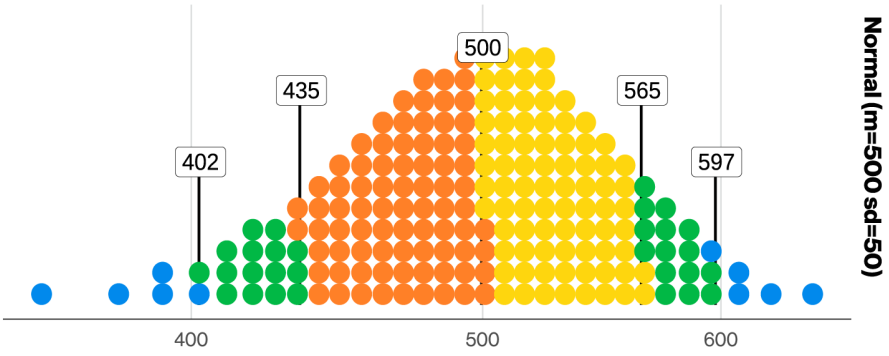


Abbildung 3: Beispielhaftes Punktdiagramm (n=10.000, jeder Punkt entspricht einem Ereignis)
Orange: untere Hälfte von 80 %, Gelb: obere Hälfte von 80 %, Grün: 80–95 %, Blau: Ausreißer, 95 % der Ereignisse: 402–597, 80 % der Ereignisse: 435–565, Median: 500

davon größer ist.

Ähnlich wie beim abgeschrägten Balkendiagramm sollen auch beim Spaghetti-Diagramm die möglichen Werte innerhalb des Konfidenzintervalls dargestellt werden. Da dieses Diagramm jedoch auch den Zeitfaktor berücksichtigt, ist es etwas komplexer. Die einzelnen Linien stellen jeweils eine Teilmenge aller möglichen Verbindungen zwischen den Punkten einer Beobachtung innerhalb des Konfidenzintervalls dar. Wie Sie sehen können, sind einige Linien stärker gestreut. Dies deutet auf ein breiteres Konfidenzintervall und eine kleinere Stichprobe hin.

Auch das Punktdiagramm feiert sein Comeback. Bitte beachten Sie, dass jeder Punkt eine bestimmte Anzahl der in der Bildunterschrift beschriebenen Ereignisse darstellt. Im Gegensatz zu Median oder Durchschnitt vermittelt diese Visualisierung ein viel besseres Verständnis für die Verteilung der Ereignisse auf einzelne Organisationen und stellt deutlich mehr Informationen bereit. Zudem haben wir mehr Farben und Beschriftungen verwendet, um die Diagramme informativer zu gestalten. Statistisch gesehen ist das Punktdiagramm nichts anderes als ein quantisiertes Dichtediagramm. Und ganz allgemein: Wer mag denn keine bunten Punkte?

Zentrale Themen und Ergebnisse

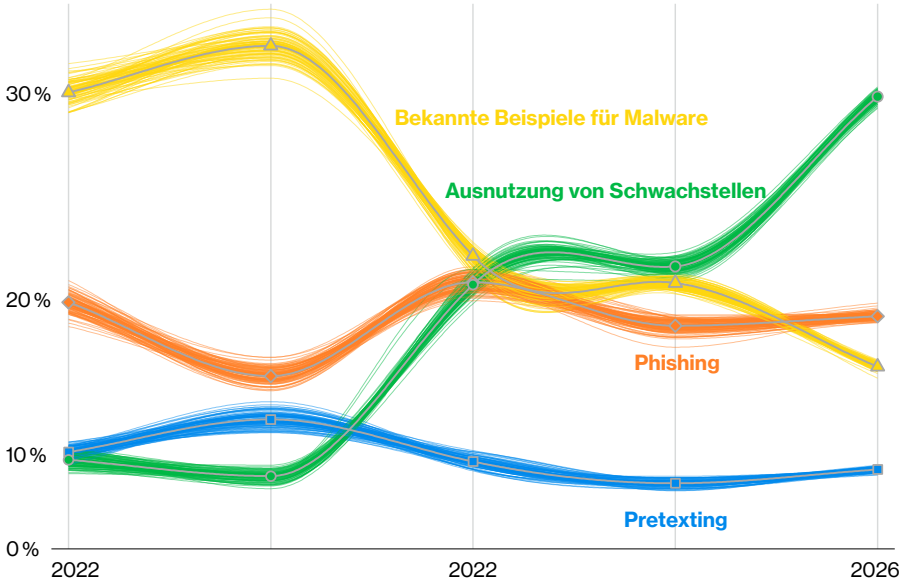


Abbildung 4: Bekannte Einfallstore bei Sicherheitsverletzungen ohne Fehler oder Missbrauch im Zeitverlauf (n=19.905 für 2026)

Die Ausnutzung von Schwachstellen nimmt zu

Die Ausnutzung vorhandener Schwachstellen ist inzwischen der häufigste Eintrittsvektor. Im diesjährigen Datenbestand stieg dieser Anteil auf 31 %, während der bisherige Spitzenreiter „Missbrauch von Zugangsdaten“ auf 13 % zurückging.

2025 wurden lediglich 26 % der kritischen Schwachstellen aus dem offiziellen KEV-Katalog („Known Exploited Vulnerabilities“) der US-Behörde CISA von den betroffenen Unternehmen vollständig behoben. Im Vorjahr betrug dieser Wert noch 38 %.

Die mittlere Zeit bis zur vollständigen Behebung stieg auf 43 Tage an. Das sind fast zwei Wochen mehr als der Vorjahreswert von 32 Tagen. Im Durchschnitt mussten Unternehmen in diesem Jahr 50 % mehr kritische Schwachstellen beseitigen als im Vorjahr.

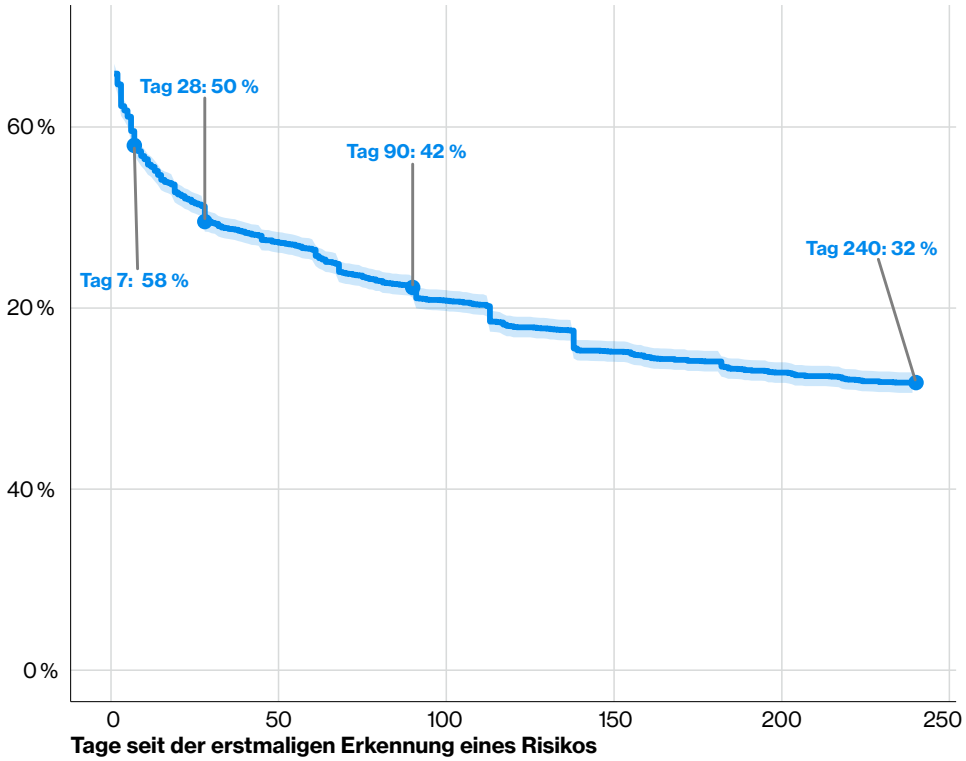


Abbildung 5: Ereigniszeitanalyse der Schwachstellenbehebung in cloudbasierten MFA-Diensten von Drittanbietern (n=7.513)

Bedrohungen durch Ransomware und Drittanbieter steigen weiter

Der Anteil der Ransomware-Angriffe ist im Vorjahresvergleich von 44 % auf 48 % gestiegen. Die Zahlungshäufigkeit ist jedoch zurückgegangen: 69 % der Opfer zahlten kein Lösegeld. Auch die mittlere Lösegeldsumme ist weiterhin rückläufig. Im aktuellen Datenbestand betrug sie 139.875 USD, im Vorjahr waren es noch 150.000 USD.

Mit der zunehmenden Nutzung von Diensten und Softwareprodukten Dritter steigt auch das damit verbundene Risiko. So ist die Zahl der drittanbieterbedingten Sicherheitsverletzungen im Vergleich zum Vorjahr um 60 % gestiegen und macht nun 48 % aller Sicherheitsverstöße aus.

Eine zeitbezogene Betrachtung der Instandhaltung externer Cloud-Umgebungen zeigt, dass nur 23 % der Drittanbieter eine fehlende oder unzureichend gesicherte Multi-Faktor-Authentifizierung vollständig korrigiert haben. 50 % aller erkannten Mängel wurden allerdings innerhalb eines Monats behoben.

Bei schwachen Passwörtern und falsch konfigurierten Berechtigungen dauerte es hingegen fast acht Monate, bis 50 % aller Probleme behoben wurden.

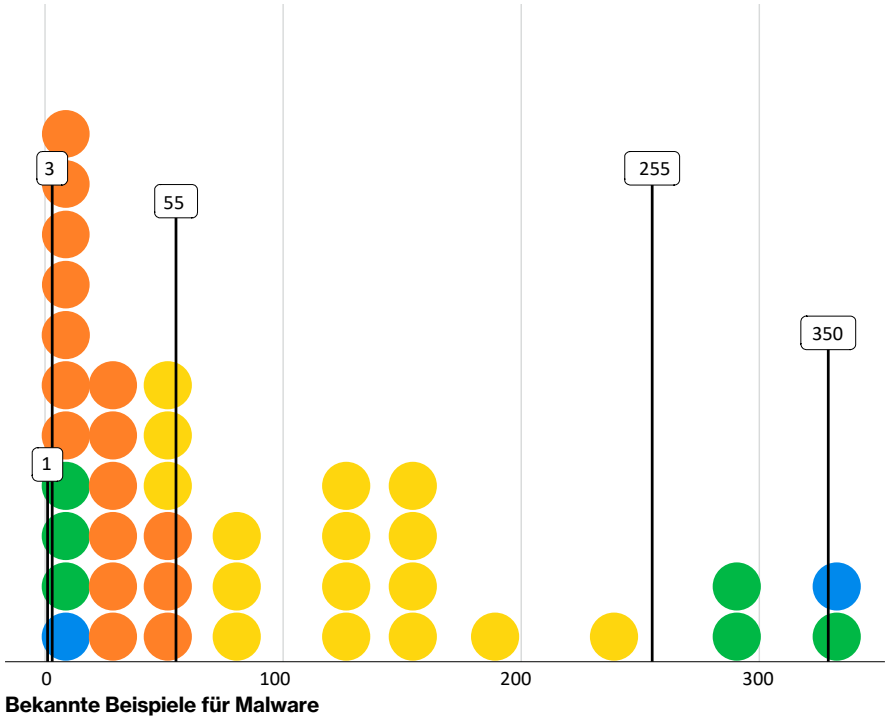


Abbildung 6: Verteilung bekannter Beispiele für Malware nach beobachteten ATT&CK-Techniken (n=9.897; jeder Kreis entspricht 247,43 Instanzen)

Neue Bedrohungen durch generative KI

In verschiedenen Angriffsphasen kommt nachweislich generative KI zum Einsatz, beispielsweise bei der Zielauswahl, dem Erstzugriff und der Entwicklung von Malware und anderer Tools. Im Median wurden 15 dokumentierte Techniken KI-gestützt analysiert oder eingesetzt, bei einigen Bedrohungsakteuren waren es sogar 40 bis 50.

In den meisten Fällen wurde KI zur Entwicklung von Malware und Tools für bekannte Angriffstechniken eingesetzt. Im Durchschnitt erfüllten 55 bekannte Malware-Varianten dieselben Funktionen.

Weniger als 2,5 % der beobachteten Instanzen KI-gestützter Malware involvierten ungewöhnliche Techniken, die jeweils nur einmal oder gar nicht dokumentiert sind.

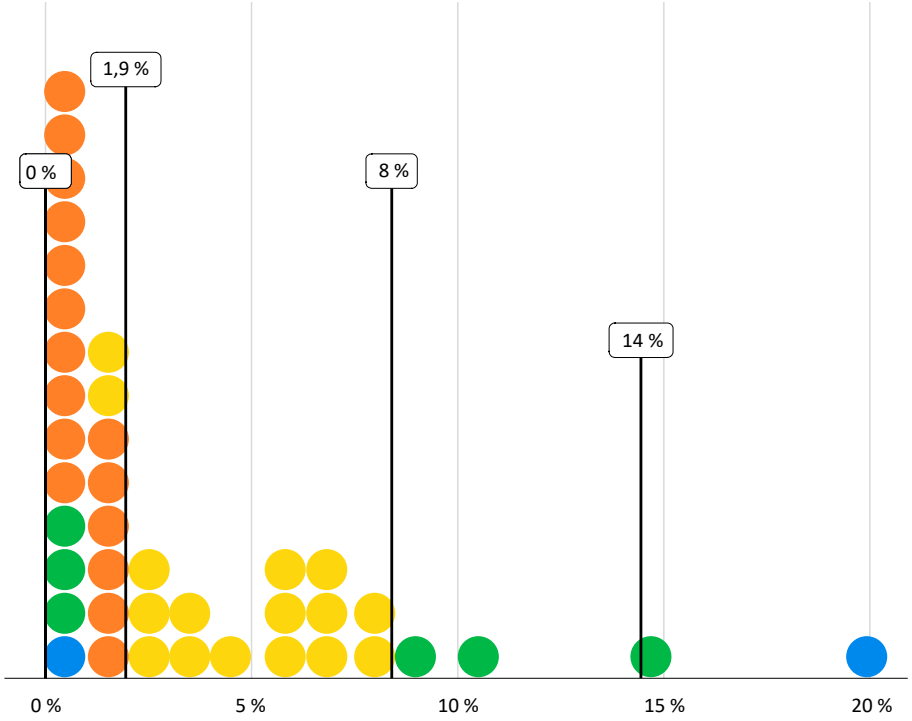


Abbildung 7: Verteilung der Erfolgsquote simulierter Social-Engineering-Kampagnen ohne E-Mail-Nutzung (n=35; jeder Kreis entspricht 0,88 Kampagnen)

Social Engineering über Mobilgeräte

Bei 62 % der Sicherheitsverletzungen spielte der Faktor Mensch eine Rolle. Dies stellt einen leichten Anstieg gegenüber dem Vorjahresanteil von 60 % dar. Mit 16 % war Social Engineering das dritthäufigste Muster.

Bei Phishing-Simulationen über mobile Angriffsvektoren wie Voice oder SMS ist die mittlere „Klickrate“ um 40 % höher als bei E-Mails.

Pretexting entwickelt sich zunehmend zu einem relevanten Eintrittsvektor für Ransomware und Erpressung. Während der Anteil von Phishing-Angriffen mit 16 % im Jahresvergleich unverändert blieb, machten Pretexting-Angriffe 6 % aller Sicherheitsverletzungen aus. Beim Pretexting bauen Angreifer durch erfundene Szenarien ein Vertrauensverhältnis zu Nutzern auf und verleiten diese zu Handlungen, die das Unternehmen unwissentlich gefährden. Dies geschieht häufig am Telefon, kann aber auch per E-Mail oder SMS erfolgen.

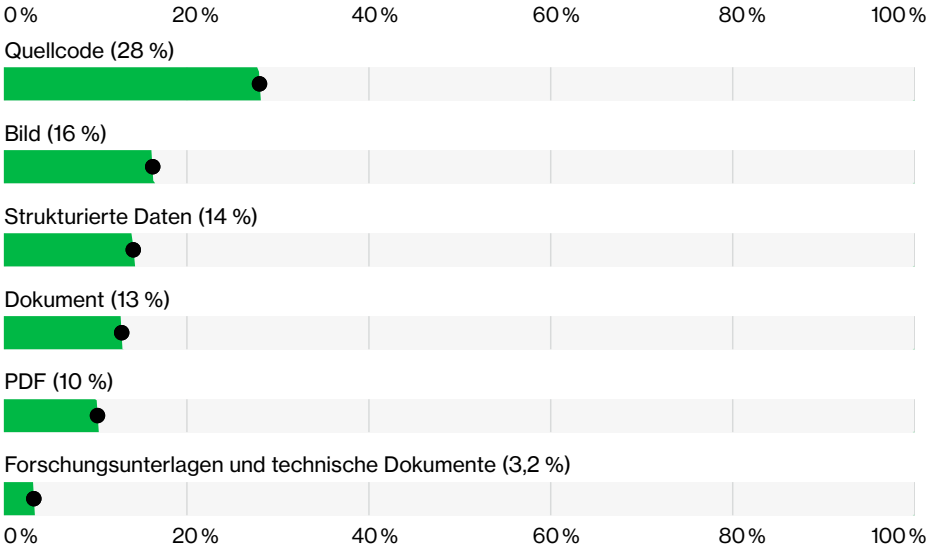


Abbildung 8: Ausgewählte Datentypen bei DLP-Vorfällen durch den Einsatz generativer KI-Tools (n=858.440)

Verstöße gegen Schatten-KI-Verbote und böswillige Insider

67 % der Nutzer verwenden private Konten auf Firmengeräten, um auf KI-Dienste zuzugreifen, darunter auch nicht genehmigte generative KI-Tools („Schatten-KI“). Dies entspricht einem leichten Rückgang gegenüber dem Vorjahr. Inzwischen nutzen allerdings 45 % der Beschäftigten ihre Firmengeräte regelmäßig, um auf genehmigte und nicht genehmigte KI-Dienste zuzugreifen. Im Vorjahr waren es lediglich 15 %.

Mittlerweile ist Schatten-KI die dritthäufigste Sicherheitsverletzung durch nicht-böswillige Insider, die in unseren DLP-Daten (Data Loss Prevention) für 2025 erfasst wurde. Dies entspricht einer Vervierfachung gegenüber dem Vorjahr.

Am häufigsten wurde Quellcode an generative KI-Modelle übergeben, dicht gefolgt von Bildern und anderen strukturierten Daten. In 3,2 % der Verstöße gegen DLP-Richtlinien wurde durch das Hochladen von Forschungsunterlagen und technischen Dokumenten in nicht genehmigte KI-Systeme geistiges Eigentum gefährdet.

Branchenspezifische Erkenntnisse

Wie schon in der Einleitung erwähnt, haben wir in diesem Jahr mehr als 22.000 bestätigte Datensicherheitsverletzungen analysiert. Das ist mit Abstand die größte Anzahl, die wir je in einem einzelnen Bericht untersucht haben. Im folgenden Abschnitt werden diese Vorfälle nach Branchen aufgeschlüsselt. Aufgrund der unterschiedlichen Angriffsflächen in den einzelnen Sektoren sind auch die wichtigsten Bedrohungen branchenspezifisch ausgeprägt.

Beim Lesen dieses Abschnitts sollten Sie einige Punkte beachten. Etwaige branchenspezifische Unterschiede sind auf mehrere Faktoren zurückzuführen. Dazu zählen abweichende Aufsichts- und Meldepflichten sowie das damit verbundene Ausmaß externer Kontrollen. Zudem standen uns je nach Branche unterschiedlich große Datensamples zur Verfügung. Bitte berücksichtigen Sie diese und weitere Aspekte, wenn Sie einzelne Sektoren miteinander vergleichen.

In diesem Abschnitt suchen viele Leser nach konkreten Ergebnissen für ihre Branche. Bitte achten Sie dabei auf die wichtigsten Angriffsmuster in Ihrem Bereich. Einen genaueren Überblick über einzelne Sektoren und Muster finden Sie in den entsprechenden Abschnitten des vollständigen Berichts. Dort erfahren Sie alles Wissenswerte über Cyberangriffe, vor denen Sie sich mit hoher Wahrscheinlichkeit schützen müssen.

Bildungswesen

(NAICS 61)

Der Bildungssektor ist vor allem von finanziell motivierten Angriffen von außen betroffen. Diese erfolgen durch die Einschleusung von Ransomware, die Ausnutzung vorhandener Schwachstellen sowie den Missbrauch zahlreicher gestohlener Anmeldedaten.

Absolute Häufigkeit	1.302 Vorfälle, davon 1.252 mit bestätigten Datenlecks
Häufigste Angriffsmuster	83 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Diverse Fehler
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (78 %), Insider (22 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (78 %), Spionage (21 %), Ideologische Motive (2 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (64 %), Personenbezogene Daten (41 %), Sonstige (26 %), Betriebsgeheimnisse (19 %)
Aufschlüsselung der Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (34 %), Phishing (22 %), Missbrauch von Zugangsdaten (8 %)
Weitere Kennzahlen	Faktor Mensch (68 %), Dritte (40 %)
Anhaltende Trends	Wie in den beiden Vorjahren sind auch dieses Jahr die Muster System Intrusion, Social Engineering und Diverse Fehler am häufigsten vertreten

Finanz- und Versicherungs-branche

(NAICS 52)

Die Branche ist nach wie vor ein bevorzugtes Ziel für finanziell motivierte Angriffe von außen. Zu den größten Bedrohungen zählen System Intrusions durch Ransomware, Phishing, die Ausnutzung vorhandener Schwachstellen und der Missbrauch gestohlener Anmeldedaten. Menschliches Versagen und Risiken durch Dritte sind nach wie vor wesentliche Einflussfaktoren.

Absolute Häufigkeit	3.809 Vorfälle, davon 1.300 mit bestätigten Datenlecks
Häufigste Angriffsmuster	81 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Alles Andere
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (88 %), Insider (12 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (98 %), Spionage (3 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (53 %), Personenbezogene Daten (43 %), Sonstige (28 %), Anmeldedaten (26 %)
Aufschlüsselung der Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (22 %), Phishing (20 %), Missbrauch von Zugangsdaten (15 %)
Weitere Kennzahlen	Faktor Mensch (65 %), Dritte (34 %)
Anhaltende Trends	Seit 2022 ist System Intrusion das am häufigsten beobachtete Angriffsmuster. Die Angreifer handeln dabei vor allem aus finanziellen Motiven

Gesundheitswesen

(NAICS 62)

Einrichtungen des Gesundheitswesens sind von einer Mischung aus System Intrusions durch Ransomware und wiederholtem menschlichen Versagen betroffen. Die finanziell motivierten Angriffe von außen erfolgen unter Ausnutzung vorhandener Schwachstellen, mittels Phishing und durch den Missbrauch gestohlener Zugangsdaten. Mitarbeiterfehler und Fehlkonfigurationen sind nach wie vor eine häufige Ursache für Sicherheitsverletzungen.

Absolute Häufigkeit	1.492 Vorfälle, davon 1.438 mit bestätigten Datenlecks
Häufigste Angriffsmuster	81 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Diverse Fehler und Social Engineering
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (81 %), Insider (19 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (99 %), Spionage (2 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (65 %), Personenbezogene Daten (37 %), Anmeldedaten (25 %), Sonstige (19 %)
Aufschlüsselung der Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (20 %), Phishing (14 %), Missbrauch von Zugangsdaten (11 %)
Weitere Kennzahlen	Bestätigte Sicherheitsverletzungen: Faktor Mensch (54 %), Dritte (32 %)
Anhaltende Trends	Seit Beginn unserer Erfassung zählt die Kategorien Diverse Fehler zu den häufigsten Mustern in dieser Branche. System Intrusion steht zum zweiten Mal in Folge an erster Stelle

Fertigungsindustrie

(NAICS 31–33)

Die kontinuierlich wachsende Zahl der Sicherheitsverletzungen in diesem Sektor ist hauptsächlich auf Ransomware-Angriffe zurückzuführen.

Absolute Häufigkeit	3.627 Vorfälle, davon 2.713 mit bestätigten Datenlecks
Häufigste Angriffsmuster	91 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (95 %), Insider (5 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (87 %), Spionage (15 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (81 %), Anmeldedaten (26 %), Sonstige (22 %), Personenbezogene Daten (17 %)
Aufschlüsselung der Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (38 %), Phishing (13 %), Missbrauch von Zugangsdaten (11 %)
Weitere Kennzahlen	Bestätigte Sicherheitsverletzungen: Dritte (61 %), Faktor Mensch (56 %)
Anhaltende Trends	In der Fertigungsindustrie sind die wichtigsten Muster dieselben wie im Vorjahr. Die meisten Bedrohungsakteure handeln aus finanziellen Motiven

Öffentliche Verwaltung

(NAICS 92)

Verwaltungsbehörden werden vor allem von finanziell motivierten Kriminellen und staatlich gesponserten Akteuren angegriffen. Daher ist die Häufigkeit der Kategorie „System Intrusions durch Ausnutzung von Schwachstellen und durch Ransomware“ auffällig hoch. Darüber hinaus ist der Sektor von einer ungewöhnlich hohen Anzahl interner Vorfälle betroffen, die auf diverse Fehler zurückzuführen sind. Dazu gehören insbesondere Falschzustellungen aufgrund des massenhaften Korrespondenzaufkommens und vorsätzlicher Datenmissbrauch.

Absolute Häufigkeit	3.634 Vorfälle, davon 2.410 mit bestätigten Datenlecks
Häufigste Angriffsmuster	80 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Diverse Fehler und Missbrauch von Nutzerrechten
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (56 %), Insider (44 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (69 %), Spionage (33 %), Ideologische Motive (2 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (50 %), Interna (39 %), Sonstige (37 %), Betriebsgeheimnisse (30 %)
Aufschlüsselung der Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (40 %), Phishing (20 %), Missbrauch von Zugangsdaten (8 %)
Weitere Kennzahlen	Faktor Mensch (69 %), Dritte (36 %)
Anhaltende Trends	In diesem Sektor stehen die gleichen Angriffsmuster an erster und zweiter Stelle wie im Vorjahr. Lediglich das dritthäufigste Muster „Einfache Angriffe auf Web-Anwendungen” wurde durch „Missbrauch von Nutzerrechten” abgelöst. Der Anteil externer Angriffe blieb im Jahresvergleich unverändert

Einzelhandel

(NAICS 44–45)

Einzelhändler sind häufig Angriffen von außen ausgesetzt, in deren Vorfeld Schwachstellen ausgenutzt, Zugangsdaten gestohlen oder Phishing-Kampagnen durchgeführt werden. Diese Aktivitäten führen oft zu Ransomware-Angriffen und Datendiebstahl. Dabei werden zunehmend Systeme von Drittanbietern sowie interne Unternehmensdaten ins Visier genommen.

Absolute Häufigkeit	997 Vorfälle, davon 806 mit bestätigten Datenlecks
Häufigste Angriffsmuster	95 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (99 %), Insider (1 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (85 %), Spionage (19 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (84 %), Anmeldedaten (26 %), Betriebsgeheimnisse (20 %), Sonstige (14 %)
Aufschlüsselung der Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (42 %), Missbrauch von Zugangsdaten (14 %), Phishing (9 %)
Weitere Kennzahlen	Bestätigte Sicherheitsverletzungen: Dritte (68 %), Faktor Mensch (58 %)
Anhaltende Trends	Die drei häufigsten Angriffsmuster sind zwar dieselben geblieben, ihre Rangfolge hat sich jedoch verändert. Diese Muster werden seit Langem beobachtet, ihre Positionierung ändert sich jedoch von Jahr zu Jahr

Kleine und mittlere Unternehmen

Kleinbetriebe sind überproportional häufig von Ransomware betroffen. Oft müssen sie sich vor den gleichen Bedrohungen schützen wie andere Sektoren und Unternehmen, verfügen jedoch zumeist über weniger Ressourcen zur Abwehr.

Absolute Häufigkeit	7.256 Vorfälle, davon 7.152 mit bestätigten Datenlecks
Häufigste Angriffsmuster	100 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (100 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (100 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (97 %), Anmeldedaten (31 %), Systemdaten (1 %), Sonstige (1 %)
Aufschlüsselung der Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (26 %), Missbrauch von Zugangsdaten (13 %), Phishing (9 %)
Weitere Kennzahlen	Bestätigte Sicherheitsverletzungen: Dritte (55 %), Faktor Mensch (45 %)
Anhaltende Trends	Zu den Hauptursachen für Sicherheitsverletzungen in kleinen und mittleren Unternehmen zählen nach wie vor System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering

Branchendaten auf einen Blick

Da uns sowohl der Platz als auch die Zeit fehlen und wir zudem nicht über ausreichende Daten verfügen, um jede Branche im Detail zu betrachten, bietet die folgende Tabelle einen Überblick über alle Sparten, die im vorherigen Abschnitt nicht behandelt wurden.

Branche (NAICS)	Absolute Häufigkeit	Häufigste Angriffsmuster	Urheber der Bedrohungen (bestätigte Sicherheitsverletzungen)	Motive der Akteure (bestätigte Sicherheitsverletzungen)	Betroffene Daten (bestätigte Sicherheitsverletzungen)
Landwirtschaft (11)	223 Vorfälle, davon 219 mit bestätigten Datenlecks	91 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering	Externe Angreifer (100 %)	Finanzielle Motive (71 %), Spionage (29 %), Ideologische Motive (1 %)	Interna (70 %), Sonstige (43 %), Betriebsgeheimnisse (36 %)
Öffentliche Verwaltung (56)	422 Vorfälle, davon 419 mit bestätigten Datenlecks	98 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen	Externe Angreifer (99 %), Insider (1 %)	Finanzielle Motive (100 %)	Interna (96 %), Anmeldedaten (28 %), Sonstige (2 %), Systemdaten (2 %)
Bauwesen (23)	843 Vorfälle, davon 828 mit bestätigten Datenlecks	95 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen	Externe Angreifer (99 %), Insider (1 %)	Finanzielle Motive (97 %), Spionage (5 %)	Interna (86 %), Anmeldedaten (34 %), Sonstige (13 %), Betriebsgeheimnisse (6 %)
Medien und Unterhaltung (71)	587 Vorfälle, davon 483 mit bestätigten Datenlecks	82 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Alles Andere	Externe Angreifer (86 %), Insider (14 %)	Finanzielle Motive (89 %), Spionage (20 %), Ideologische Motive (1 %)	Interna (54 %), Personenbezogene Daten (45 %), Sonstige (31 %), Betriebsgeheimnisse (20 %)
IT und TK-Beratung (51)	1.703 Vorfälle, davon 1.099 mit bestätigten Datenlecks	79 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Alles Andere	Externe Angreifer (89 %), Insider (11 %), Mehrere Akteure (1 %)	Finanzielle Motive (84 %), Spionage (16 %), Ideologische Motive (2 %)	Interna (52 %), Personenbezogene Daten (39 %), Sonstige (31 %), Anmeldedaten (24 %)

Tabelle 1: Daten zu betroffenen Branchen ohne eigenen Abschnitt

Branche (NAICS)	Absolute Häufigkeit	Häufigste Angriffsmuster	Urheber der Bedrohungen (bestätigte Sicherheitsverletzungen)	Motive der Akteure (bestätigte Sicherheitsverletzungen)	Betroffene Daten (bestätigte Sicherheitsverletzungen)
Management (55)	103 Vorfälle, davon 101 mit bestätigten Datenlecks	98 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen	Externe Angreifer (100 %)	Finanzielle Motive (100 %)	Interna (96 %), Anmeldedaten (35 %), Multifaktor-Zugangsdaten (3 %), Sonstige (2 %)
Bergbau (21)	72 Vorfälle, davon 70 mit bestätigten Datenlecks	96 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Alles Andere und Einfache Angriffe auf Web-Anwendungen	Externe Angreifer (100 %)	Finanzielle Motive (97 %), Spionage (1 %), Ideologische Motive (1 %)	Interna (74 %), Anmeldedaten (31 %), Personenbezogene Daten (17 %), Sonstige (9 %)
Sonstige Dienstleister (81)	900 Vorfälle, davon 885 mit bestätigten Datenlecks	85 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Diverse Fehler	Externe Angreifer (81 %), Insider (19 %)	Finanzielle Motive (78 %), Spionage (23 %)	Interna (66 %), Personenbezogene Daten (38 %), Sonstige (28 %), Betriebsgeheimnisse (20 %)
Professionen (54)	3.578 Vorfälle, davon 2.558 mit bestätigten Datenlecks	91 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen	Externe Angreifer (97 %), Insider (3 %)	Finanzielle Motive (96 %), Spionage (5 %)	Interna (80 %), Anmeldedaten (31 %), Personenbezogene Daten (14 %), Sonstige (11 %)
Immobilienbranche (53)	505 Vorfälle, davon 499 mit bestätigten Datenlecks	85 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Diverse Fehler	Externe Angreifer (79 %), Insider (22 %)	Finanzielle Motive (100 %)	Interna (63 %), Personenbezogene Daten (43 %), Anmeldedaten (24 %), Sonstige (16 %)
Transportwesen (48–49)	689 Vorfälle, davon 652 mit bestätigten Datenlecks	89 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Alles Andere	Externe Angreifer (99 %), Insider (1 %)	Finanzielle Motive (89 %), Spionage (15 %), Ideologische Motive (1 %)	Interna (84 %), Anmeldedaten (27 %), Betriebsgeheimnisse (16 %), Sonstige (14 %)
Versorgungsunternehmen (22)	638 Vorfälle, davon 597 mit bestätigten Datenlecks	94 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering	Externe Angreifer (97 %), Insider (3 %)	Spionage (71 %), Finanzielle Motive (36 %)	Interna (85 %), Betriebsgeheimnisse (68 %), Sonstige (21 %)
Großhandel (42)	1.057 Vorfälle, davon 1.048 mit bestätigten Datenlecks	99 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering	Externe Angreifer (100 %)	Finanzielle Motive (100 %)	Interna (98 %), Anmeldedaten (29 %)

Tabelle 1: Daten zu betroffenen Branchen ohne eigenen Abschnitt (Fortsetzung)

Ergebnisse für spezifische Regionen

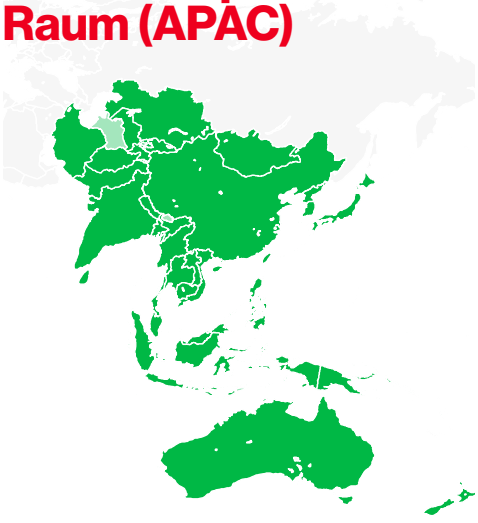
In diesem Abschnitt schlüsseln wir unsere Erkenntnisse nach Makroregionen auf, um aufzuzeigen, inwiefern sich die Trends in den einzelnen Regionen ähneln bzw. unterscheiden.

Unsere Einblicke in die jeweilige Sicherheitslage hängen von verschiedenen Faktoren ab. Dazu zählen die regional geltenden Offenlegungspflichten, die verfügbaren Daten und die Standorte unserer Datenpartner. Wenn Sie der Meinung sind, dass Ihre Region auf den folgenden Seiten unterrepräsentiert ist, können Sie uns gerne kontaktieren und selbst Daten beisteuern. Wir freuen uns, wenn Sie auch andere Unternehmen aus Ihrer Region dazu anregen.

Durch Daten repräsentierte Länder

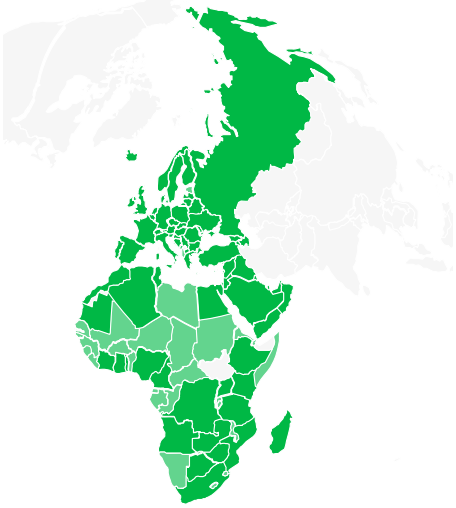
Nicht durch Daten repräsentierte Länder

Asiatisch-pazifischer Raum (APAC)



Absolute Häufigkeit	5.229 Vorfälle, davon 2.855 mit bestätigten Datenlecks
Häufigste Angriffsmuster	97 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (99 %), Insider (1 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (70 %), Spionage (36 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (70 %), Anmeldedaten (36 %), Sonstige (35 %), Betriebsgeheimnisse (30 %)
Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (42 %), Missbrauch von Zugangsdaten (25 %), Phishing (15 %)
Sonstiges	Bestätigte Sicherheitsverletzungen: Dritte (69 %), Faktor Mensch (71 %)

Europa, Naher Osten und Afrika (EMEA)

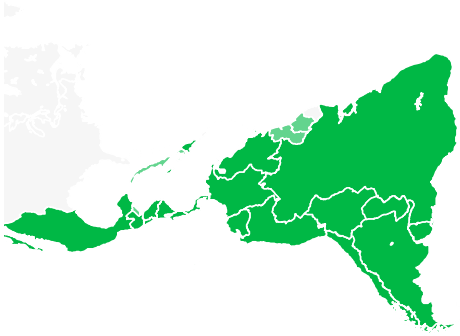


Absolute Häufigkeit	8.245 Vorfälle, davon 6.060 mit bestätigten Datenlecks
Häufigste Angriffsmuster	92 % der Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Diverse Fehler
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (80 %), Insider (20 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (76 %), Spionage (27 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (73 %), Sonstige (49 %), Personenbezogene Daten (34 %), Betriebsgeheimnisse (24 %)
Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (47 %), Phishing (28 %), Missbrauch von Zugangsdaten (6 %)
Sonstiges	Bestätigte Sicherheitsverletzungen: Dritte (54 %), Faktor Mensch (70 %)

Durch Daten repräsentierte Länder

Nicht durch Daten repräsentierte Länder

Lateinamerika und Karibik (LAC)



Absolute Häufigkeit	813 Vorfälle, davon 718 mit bestätigten Datenlecks
Häufigste Angriffsmuster	98 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (99 %), Insider (1 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (90 %), Spionage (11 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (93 %), Anmeldedaten (23 %), Betriebsgeheimnisse (24 %), Sonstige (3 %)
Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (44 %), Phishing (20 %), Missbrauch von Zugangsdaten (5 %)
Sonstiges	Bestätigte Sicherheitsverletzungen: Dritte (74 %), Faktor Mensch (57 %)

Nordamerika (NA)

Absolute Häufigkeit	12.371 Vorfälle, davon 8.426 mit bestätigten Datenlecks
Häufigste Angriffsmuster	87 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (88 %), Insider (12 %)
Motive der Akteure	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (98 %), Spionage (3 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (77 %), Anmeldedaten (36 %), Personenbezogene Daten (9 %), Sonstige (8 %)
Eintrittsvektoren	Bestätigte Sicherheitsverletzungen: Ausnutzung vorhandener Schwachstellen (30 %), Missbrauch von Zugangsdaten (20 %), Phishing (12 %)
Sonstiges	Bestätigte Sicherheitsverletzungen: Dritte (43 %), Faktor Mensch (59 %)

Bleiben Sie auf dem Laufenden und gewappnet

Um den aktuellen Bedrohungen die Stirn bieten zu können, benötigen Sie zuverlässige Informationen.

Deshalb bietet Ihnen die vollständige Ausgabe des DBIR einen detaillierten und praxisrelevanten Überblick über die Ziele, Methoden und Aktivitäten der Akteure. Holen Sie sich alle Zahlen, Daten und Fakten, die Sie für fundierte Schutzmaßnahmen und zur Stärkung des Sicherheitsbewusstseins Ihrer Mitarbeiter benötigen.

Den vollständigen DBIR 2026 finden Sie unter verizon.com/dbir.

Möchten Sie dazu beitragen, die Cybersicherheit weltweit zu stärken?

Falls Ihr Unternehmen Daten zu IT-Vorfällen oder zur Sicherheit allgemein erfasst, würden wir uns sehr freuen, wenn Sie als Daten- oder Forschungspartner am jährlichen DBIR-Bericht von Verizon mitwirken. Der Ablauf ist sehr einfach. Schreiben Sie uns dazu eine E-Mail an dbircontributor@verizon.com. Wir besprechen dann die Einzelheiten und klären gemeinsam, wie Sie sich an der Forschung für den DBIR beteiligen können.

Wir freuen uns über Feedback und Verbesserungsvorschläge zum DBIR. Schreiben Sie dazu bitte an dbir@verizon.com. Sie können sich auch über LinkedIn an Verizon Business oder die Autoren wenden. Besuchen Sie außerdem die GitHub-Seite zu unserem VERIS-Framework unter github.com/vz-risk/veris (auf Englisch).