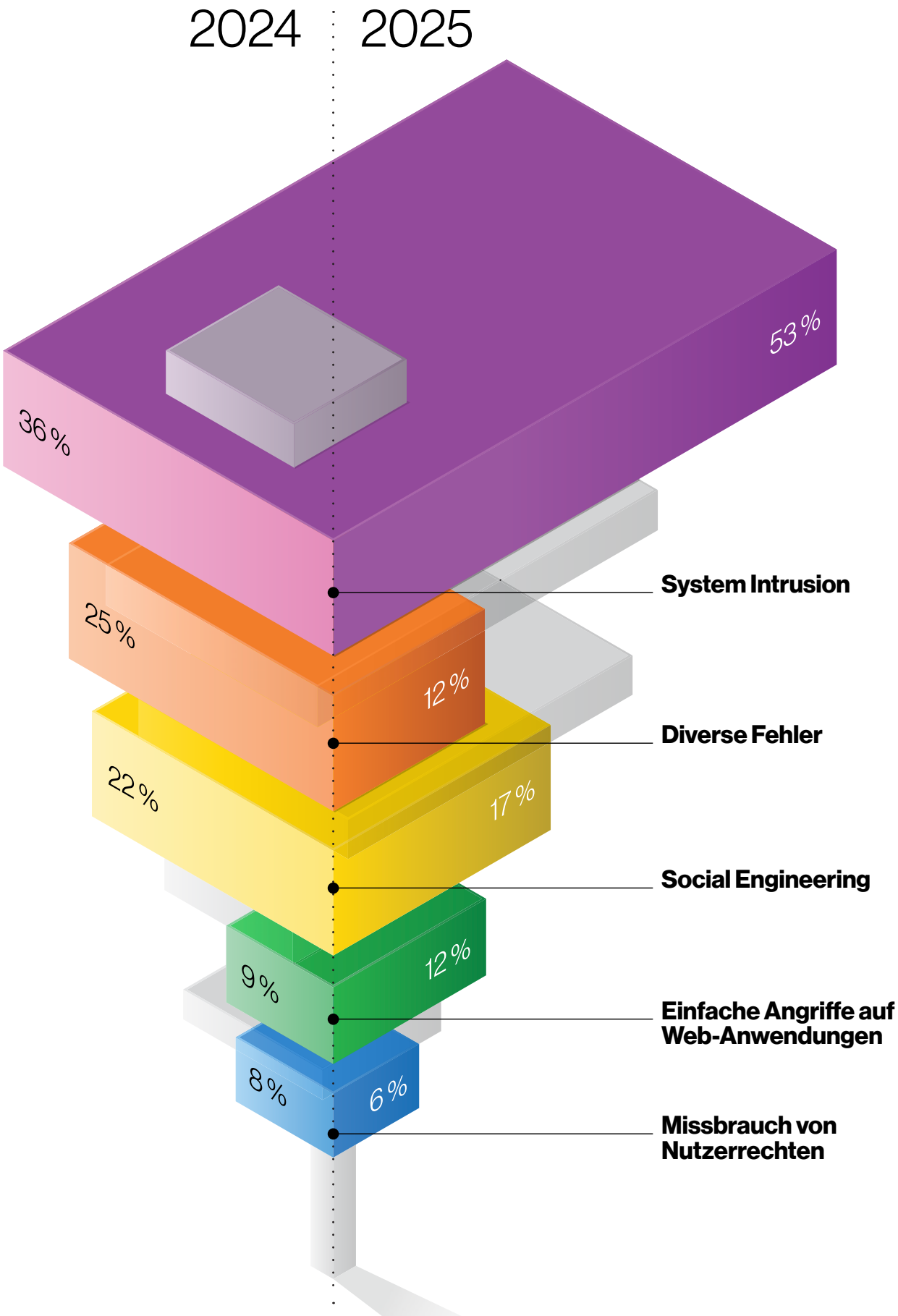
Data Breach Investigations Report 2025

Kurzfassung

verizon business


2024
2025
36 %
53 %
System Intrusion
25 %
12 %
Diverse Fehler
22 %
17 %
Social Engineering
9 %
12 %
Einfache Angriffe auf Web-Anwendungen
8 %
6 %
Missbrauch von Nutzerrechten

Über die Titelseite

Im diesjährigen Berichtszeitraum kamen Sicherheitsverletzungen unter Ausnutzung der Infrastrukturen von Dritten, die als Datentreuhänder fungieren oder das Fundament für kritische Betriebsprozesse bereitstellen, immer und immer wieder zur Sprache.

Da moderne Organisationen in immer höherem Maße auf die Services dieser Drittanbieter angewiesen sind, kommt die Entwicklung und Umsetzung effektiver Sicherheitsprogramme einem wahren Balanceakt gleich, der von unserem hervorragenden Designteam im Titelbild des vorliegenden Berichts auf einprägsame Weise veranschaulicht wird. Wenn Ihnen die in prekärer Position auf dem Kopf stehende Pyramidenform leichtes Unbehagen bereitet, gewinnen Sie einen ersten Eindruck davon, wie sich CISOs angesichts der aktuellen Sicherheitslage fühlen.

Entlang der Hochachse des Diagramms finden Sie die prominenten Angriffs- und Vorfallsmuster aus unserem Datensatz in aufsteigender Relevanz (wobei das Angriffsvolumen des vorherigen Jahres links von der Achse und das Angriffsvolumen des aktuellen Jahres rechts von der Achse aufgetragen ist). Auf der Innenseite des Titelblatts haben wir die beiden Verteilungen etwas weniger abstrakt und mit Beschriftung abgebildet.

Die sich daraus ergebende umgekehrte Pyramide mag zu kopflastig und instabil aussehen, um aufrecht stehenzubleiben. Dass sie dies dennoch tut, ist ein eindrucksvoller Beweis für die harte Arbeit und die koordinierten Bemühungen in der Branche. Mit intensiver Zusammenarbeit, einem hohen Maß an Organisation und einem regen Informationsaustausch können wir die Cybersicherheit aller nachhaltig stärken und vielleicht sogar hin und wieder eine Nacht lang beruhigt schlafen.

Inhalt

Willkommensgruß 5

Die Ergebnisse im Überblick/ Zusammenfassung 6

Branchenspezifische Erkenntnisse 10

Bildungswesen 10

Finanz- und Versicherungsbranche 11

Gesundheitswesen 11

Fertigungsindustrie 12

Einzelhandel 12

Öffentlicher Sektor 13

Branchendaten auf einen Blick 14

Ergebnisse für spezifische Regionen 16

Halten Sie sich und Ihr Team auf dem Laufenden 18

Willkommensgruß

Hallo und herzlich willkommen zum Verizon Data Breach Investigations Report (DBIR) 2025

Wir freuen uns über Ihr Interesse an der mittlerweile 18. Ausgabe des DBIR. Auf den folgenden Seiten finden langjährige Leser und Neulinge fundierte Zahlen und Fakten zum aktuellen Stand der Cyberkriminalität. Außerdem erfahren Sie hier, mit welchen Bedrohungen Ihr Unternehmen wahrscheinlich konfrontiert sein wird, wer die Urheber dieser Angriffe sind und wie Sie sich davor schützen können.

Zu diesem Zweck hat das mit der Erstellung des DBIR beauftragte Team insgesamt 22.052 Vorfälle untersucht, von denen 12.195 als schwerwiegende Datensicherheitsverletzungen in Organisationen aller Größen und Sparten eingestuft wurden. Das ist die höchste Zahl an Sicherheitsverletzungen, die jemals für einen einzelnen Bericht analysiert wurden. Als Quelle dienten uns dabei zum einen die in den Einsatzberichten des Verizon Threat Research Advisory Center (VTRAC) dokumentierten Vorfälle und Sicherheitsverletzungen, zum anderen die großzügigen Beiträge von Experten aus aller Welt sowie öffentlich verfügbare Informationen über Sicherheitsvorfälle. Zusammengenommen ergibt sich so ein umfassendes Bild der Angriffe gegen Organisationen aus insgesamt 139 Ländern.

Obwohl die jeweilige Bedrohungslage in gewissem Maße von der Größe, der Branche und den Standorten einer Organisation abhängt, lassen sich aus unseren Datensätzen doch stets allgemeingültige Erkenntnisse gewinnen. Der DBIR 2025 ist da keine Ausnahme, da er eindrücklich die entscheidende Rolle belegt, die Drittunternehmen beim Zustandekommen von Sicherheitsverletzungen spielen.

Zwar ist bereits seit Längerem zu beobachten, dass bestimmte Software- und Serviceanbieter unabsichtlich zur Ausweitung der Angriffsfläche ihrer Kunden beitragen. In den letzten zwei bis drei Jahren hat sich dies jedoch von einer Serie gelegentlich auftretender Pannen (mit üblicherweise eher moderaten Konsequenzen) zu einem weit verbreiteten schleichenden Problem mit potenziell desaströsen Folgen entwickelt. Tatsächlich hat das Phänomen mittlerweile solche Ausmaße angenommen, dass es auch im Titelbild des diesjährigen Berichts deutlich sichtbar wird und auf den kommenden Seiten wiederholt Erwähnung findet.

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

Die Ergebnisse im Überblick/ Zusammenfassung

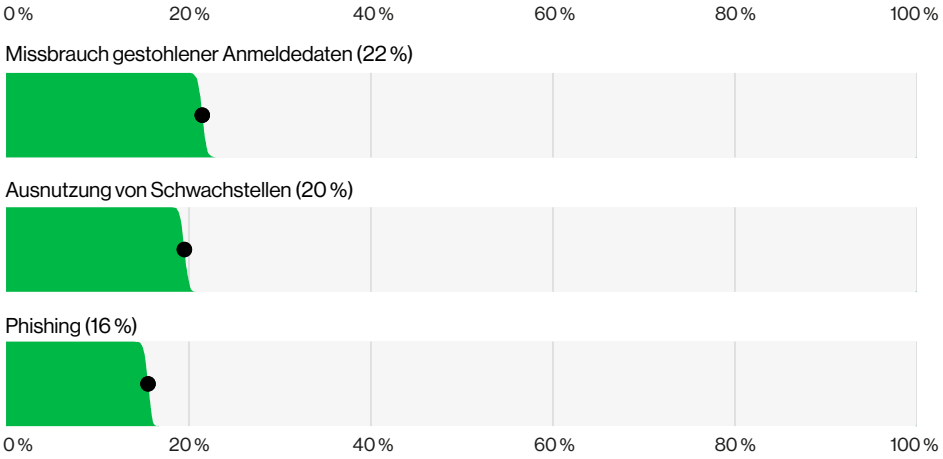


Abbildung 1: Bekannte Einfallstore bei Sicherheitsverletzungen ohne Fehler oder Missbrauch (n=9.891)

Die Ausnutzung bestehender Schwachstellen nahm auch in diesem Jahr weiter zu, bei 20 % der Vorfälle verschafften die Angreifer sich auf diesem Weg Zugang. Damit liegt diese Methode nur noch knapp hinter dem Missbrauch gestohlener Anmeldedaten, dem weiterhin meistgenutzten Angriffsvektor. Verglichen mit dem Bericht des Vorjahres ist die Ausnutzung vorhandener Schwachstellen um 34 % gestiegen, was teilweise auf Zero-Day-Angriffe auf Edge-Geräte und VPNs zurückzuführen ist. Im Zuge dieser Entwicklung hat sich die Zahl der Angriffe auf Edge- und VPN-Schwachstellen fast verachtfacht und ist von 3 % (im DBIR 2024) auf beeindruckende 22 % (im aktuellen Berichtszeitraum) gewachsen. Obwohl sich Unternehmen und Institutionen nach Kräften bemühen, die Sicherheitslücken ihrer Edge-Geräte zu schließen, zeigt unsere Analyse, dass im aktuellen Berichtszeitraum nur 54 % der Sicherheitslücken vollständig behoben wurden und dass dies im Median 32 Tage dauerte.

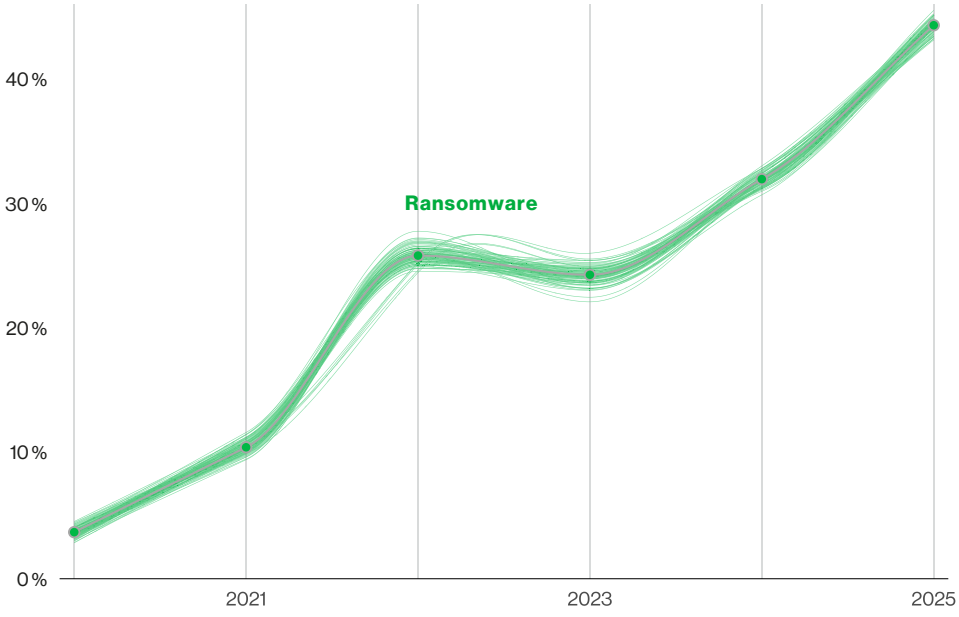


Abbildung 2: Ransomware-Einsatz bei Sicherheitsverletzungen im Zeitverlauf (n=10.747)

Die Zahl der Sicherheitsverletzungen, bei denen der Einsatz von Ransomware (mit und ohne begleitende Datenverschlüsselung) festgestellt wurde, ist ebenfalls stark angestiegen – von 32 % im DBIR 2024 auf 44 % im aktuellen Bericht. Dennoch gibt es in diesem Bereich auch eine gute Nachricht: Der Medianwert der an Ransomware-Gruppen gezahlten Lösegelder ist von 150.000 Dollar (im vorigen Berichtszeitraum) auf 115.000 Dollar gesunken. Eine mögliche Ursache dieses Rückgangs ist die Tatsache, dass 64 % der betroffenen Organisationen jegliche Zahlungen verweigerten, während dies vor zwei Jahren auf lediglich 50 % zutraf.

Zugleich ist festzustellen, dass kleinere Organisationen überproportional von Ransomware betroffen sind. Ransomware spielte bei 39 % der in Großunternehmen und bei 88 % der in KMU untersuchten Sicherheitsverstöße eine Rolle.

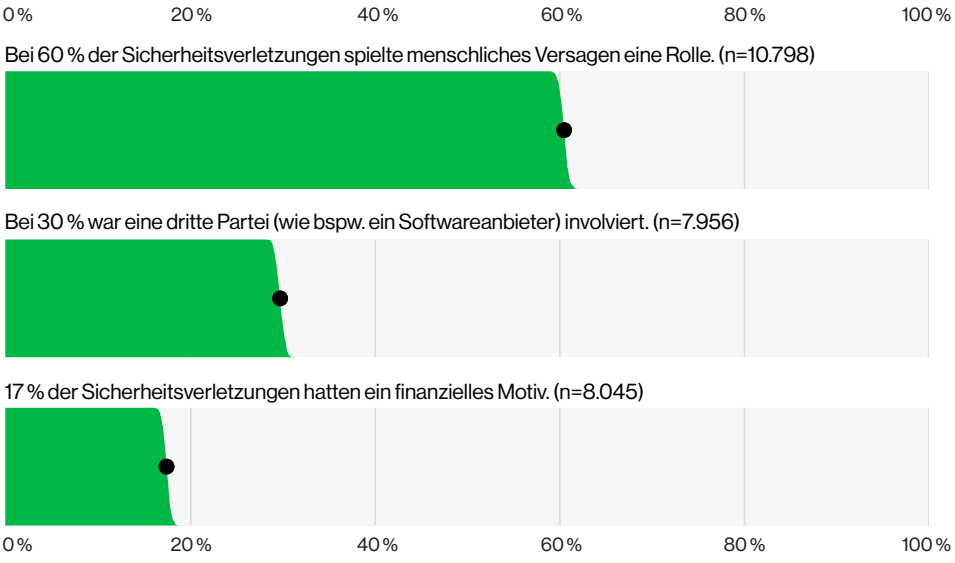


Abbildung 3: Einige wichtige Zahlen zu Sicherheitsvorfällen

Während der Faktor Mensch weiterhin bei etwa 60 % der untersuchten Vorfälle eine Rolle spielt, hat sich der Anteil der Sicherheitsverletzungen über Drittanbieter gegenüber dem vorigen Berichtszeitraum von 15 % auf 30 % verdoppelt.

Tatsächlich waren einige der aufsehenerregenden Vorfälle im DBIR 2025 nur möglich, weil dieselben Anmeldedaten in internen und in Drittanbieterumgebungen verwendet und dann dort abgegriffen und missbraucht wurden. In diesem Zusammenhang zeigen unsere Daten, dass der Medianwert für den Zeitaufwand zur Beseitigung von in GitHub-Repositorys offengelegten Betriebsgeheimnissen bei 94 Tagen liegt.

Außerdem dokumentieren wir in unserer Analyse einen Zuwachs des Anteils der Spionageangriffe auf 17 %. Das ist jedoch zum Teil auf die veränderte Zusammensetzung der Gruppe der am DBIR beteiligten Organisationen zurückzuführen. Zugleich stellen wir fest, dass 70 % der betreffenden Sicherheitsverletzungen mit der Ausnutzung bestehender Schwachstellen begann, was das von ungepatchten Services ausgehende Risiko eindrucksvoll belegt. Interessanterweise betreiben staatlich gesponsorte Angreifergruppen jedoch nicht nur Spionage, sondern verfolgten in ca. 28 % aller Fälle auch finanzielle Ziele, um – wie in den Medien wiederholt spekuliert wird – die eigene Vergütung aufzustocken.

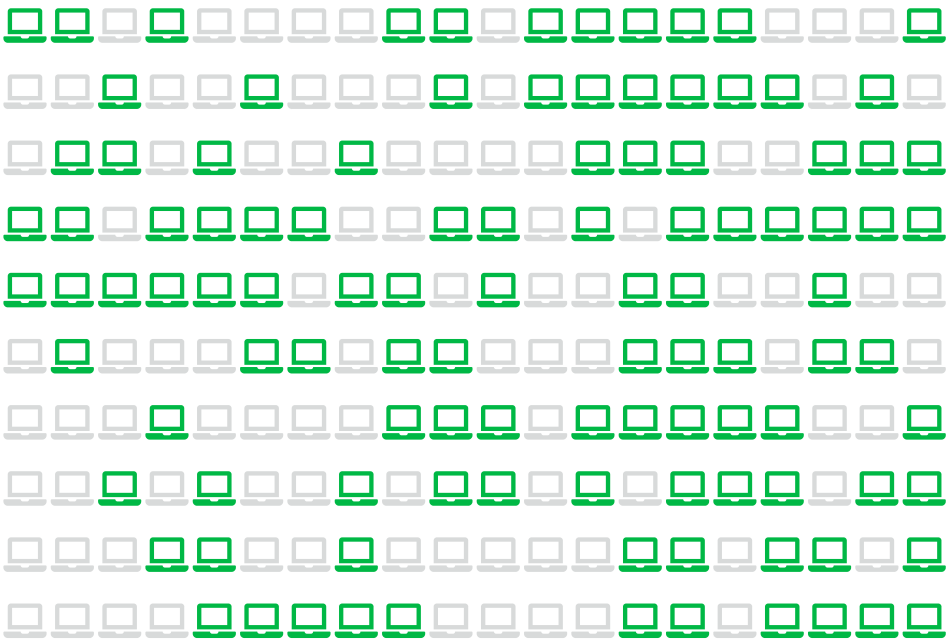


Abbildung 4: Anteil der nicht unternehmensseitig verwalteten Geräte mit Unternehmens-Anmeldedaten, die in Infostealer-Logs aufgeführt sind (jedes Symbol entspricht 0,5 %)

In puncto gestohlene Anmeldedaten hat unsere Untersuchung der im Darknet angebotenen Anmeldedaten-Logs der Infostealer-Malware ergeben, dass es sich bei 30 % der infiltrierten Systeme um von Unternehmen lizenzierte Geräte handelte. 46 % der infiltrierten Geräte, von denen Anmeldedaten für Unternehmenssysteme gestohlen wurden, erwiesen sich als nicht von der jeweils betroffenen Organisation verwaltete Geräte, auf denen sowohl persönliche als auch geschäftliche Anmeldedaten gespeichert waren. Aller Wahrscheinlichkeit nach waren dies BYOD-Geräte oder unternehmenseigene Geräte, die unter Missachtung der geltenden Richtlinien genutzt werden.

Indessen zeigt der Abgleich der von Kriminellen angebotenen Infostealer-Logs mit den 2024 von Ransomware-Gruppen angegriffenen Internetdomains, dass 54 % der infiltrierten Domains in den geleakten Anmeldedaten auftauchen (beispielsweise als URLs, zu denen die Anmeldedaten vorgeblich Zugriff gewähren). Zudem waren bei 40 % der betroffenen Personen Unternehmens-E-Mail-Adressen Teil der kompromittierten Anmeldedaten. Das legt den Schluss nahe, dass die Anmeldedaten für Ransomware-Attacken missbraucht wurden, was wiederum auf einen Access Broker als Eintrittsvektor hindeutet.

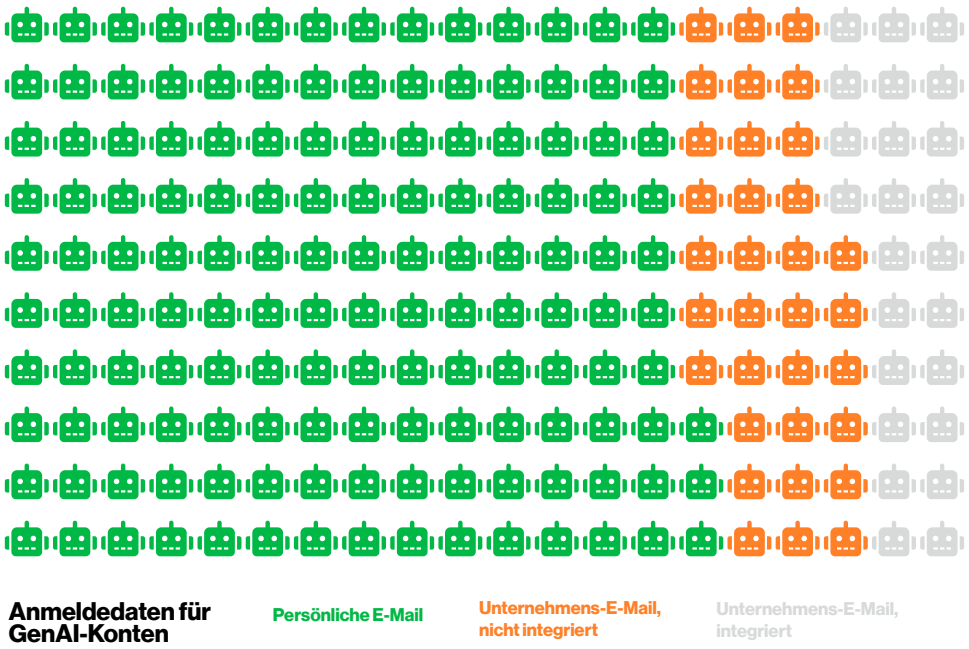


Abbildung 5: Aufschlüsselung der GenAI-Zugriffe nach Kontotyp (jedes Symbol entspricht einem Anteil von 0,5 %)

Anfang 2025 hat generative künstliche Intelligenz (GenAI) zwar immer noch nicht die Weltherrschaft übernommen, wohl aber einen Platz auf der Agenda von Cyberkriminellen gefunden – wie die Betreiber von KI-Plattformen bereit verschiedentlich meldeten. So zeigen etwa die Daten eines unserer Partner, dass sich die Anzahl schädlicher E-Mails mit synthetisch erzeugtem Text im Verlauf der letzten zwei Jahre verdoppelt hat.

Zudem besteht die Gefahr, dass sensible Unternehmensdaten über GenAI-Plattformen geleakt werden, da 15 % der Mitarbeiter wenigstens alle 15 Tage über unternehmenseigene Geräte auf GenAI-Systeme zugreifen. Das ist umso bedenklicher, als in vielen Fällen nicht unternehmenseigene E-Mail-Adressen als Kennung für die betreffenden Konten verwendet werden (72 %) oder der Kontozugriff per Unternehmens-E-Mails ohne Integration der vorgeschriebenen Authentifizierungssysteme erfolgt (17 %).

Branchenspezifische Erkenntnisse

Wie bereits in der Einleitung erwähnt, haben unsere Experten für den Verizon Data Breach Investigations Report 2025 insgesamt 22.052 Vorfälle untersucht und 12.195 davon als schwerwiegende Sicherheitsverletzungen eingestuft. In diesem Abschnitt schlüsseln wir diese Vorfälle auf die einzelnen Branchen auf. Dabei zeigt sich (wie zu vermuten war), dass einige Bedrohungen in bestimmten Branchen häufig, in anderen hingegen nur selten auftreten. In vielen Fällen spiegeln die Unterschiede zwischen den in verschiedenen Branchen beobachteten Bedrohungen die Unterschiede zwischen den individuellen Angriffsflächen der untersuchten Organisationen wider.

So kann beispielsweise ein internationales Finanzinstitut mit anderen Bedrohungen konfrontiert sein als ein regionales Logistikunternehmen. Andererseits bestehen in vielen Fällen erstaunliche Überschneidungen zwischen den jeweiligen Bedrohungsprofilen. Denn letztlich achten die Urheber der Bedrohungen weniger auf die Größe, Branchenzugehörigkeit und Standorte einer Organisation, sondern gehen vor allem pragmatisch vor und stehlen einfach alles, was ihnen unter die Finger kommt. Abgesehen davon sollten Sie unbedingt weitere Einflussfaktoren (wie etwa die unterschiedlichen branchenspezifischen Meldepflichten, die daraus resultierende Aufmerksamkeit sowie die Gesamtzahl der pro Branche untersuchten Vorfälle) berücksichtigen, um die Inhalte dieses Abschnitts richtig zu interpretieren und die aktuelle Sicherheitslage in bestimmten Branchen akkurat einzuschätzen. Bitte beachten Sie außerdem, dass wir uns hier an der Brancheneinteilung des North American Industry Classification System (NAICS) orientieren.

Bildungswesen

(NAICS 61)

Absolute Häufigkeit	1.075 Vorfälle, davon 851 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Diverse Fehler und Social Engineering machten 80 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (62 %), Insider (38 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (88 %), Spionage (18 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (58 %), Interna (49 %), Sonstige Daten (35 %), Anmeldedaten (12 %)
Anhaltende Trends	System Intrusion, Diverse Fehler und Social Engineering sind die drei häufigsten Angriffs- und Vorfallsmuster – wie auch schon in den beiden zurückliegenden Jahren.
Zusammenfassung	Im Bildungswesen beobachten wir eine rückläufige Gesamtzahl an Vorfällen und Sicherheitsverletzungen, während die Zusammensetzung der erfassten Attacken in etwa der Verteilung der Vorjahre entspricht: System Intrusion ist weiterhin das häufigste Angriffsmuster in dieser Branche und die meisten Angriffe erfolgen aus finanziellen Motiven.

Finanz- und Versicherungsbranche

(NAICS 52)

Absolute Häufigkeit	3.336 Vorfälle, davon 927 mit bestätigten Datenlecks
Häufigste Angriffsmuster	74 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (78 %), Insider (22 %), Partner (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (90 %), Spionage (12 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (54 %), sonstige Daten (44 %), Interna (35 %), Anmeldedaten (22 %)
Anhaltende Trends	System Intrusion ist einmal mehr das häufigste Angriffsmuster, insbesondere als Begleiterscheinung komplexerer Angriffe. Positiv interpretiert könnte das daran liegen, dass Cyberkriminelle durch effektivere Sicherheitsmaßnahmen zu aufwendigeren Operationen gezwungen werden.
Zusammenfassung	Die Finanz- und Versicherungsbranche steht weiterhin primär im Visier finanziell motivierter Gruppen, die üblicherweise nicht wählerisch sind und alle verfügbaren Arten von Daten stehlen. Allerdings ist die Zahl der Spionage-Angriffe im diesjährigen Berichtszeitraum gestiegen.

Gesundheitswesen

(NAICS 62)

Absolute Häufigkeit	1.710 Vorfälle, davon 1.542 mit bestätigten Datenlecks
Häufigste Angriffsmuster	74 % der bestätigten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusions, Alles Andere und Diverse Fehler.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (67 %), Insider (30 %), Partner (4 %), mehrere Akteure (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (90 %), Spionage (16 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Gesundheitsdaten(45 %), personenbezogene Daten (40 %), Interna (32 %), sonstige Daten (24 %)
Anhaltende Trends	Die drei häufigsten Angriffs- und Vorfallsmuster sind dieselben wie im letzten Jahr, treten aber in leicht veränderter Rangfolge auf.
Zusammenfassung	Das Gesundheitswesen gehört weiterhin zu den wichtigsten Schauplätzen für Cyberangriffe, deren Gesamtzahl im diesjährigen Berichtszeitraum leicht gestiegen ist. Dabei hat „System Intrusion“ (einschließlich Ransomware) die Bedrohungen der Kategorie „Verschiedene Fehler“ vom Spitzenplatz der häufigsten Angriffs- und Vorfallsmuster verdrängt. Die steigende Zahl der Fälle von Spionage in der Branche ist besorgniserregend.

Fertigungsindustrie

(NAICS 31-33)

Absolute Häufigkeit	3.837 Vorfälle, davon 1.607 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und Einfache Angriffe auf Web-Anwendungen machten 85 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (86 %), Insider (14 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (87 %), Spionage (20 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (64 %), sonstige Daten (37 %), personenbezogene Daten (33 %), Anmeldedaten (22 %)
Anhaltende Trends	System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen sind weiterhin die drei häufigsten Angriffs- und Vorfallsmuster in der Branche, wobei das Gros der akuten Bedrohungen auf das Konto finanziell motivierter, externer Akteure geht.
Zusammenfassung	Im diesjährigen Berichtszeitraum erwies sich jede fünfte Sicherheitsverletzungen als Spionageangriff, während dieser Anteil im vorigen Jahr noch bei lediglich 3 % lag. Dabei waren Interna (wie sensible Pläne, Berichte und E-Mails) die bei Weitem am häufigsten betroffene Datenart. Bei mehr als 90 % der betroffenen Organisationen handelte es sich um KMU mit weniger als 1.000 Mitarbeitern.

Einzelhandel

(NAICS 44-45)

Absolute Häufigkeit	837 Vorfälle, davon 419 mit bestätigten Datenlecks
Häufigste Angriffsmuster	93 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (96 %), Insider (3 %), Partner (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (100 %), Spionage (9 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (65 %), sonstige Daten (30 %), Anmeldedaten (26 %), Zahlungsdaten (12 %)
Anhaltende Trends	Weder die Zusammensetzung noch die Rangfolge der drei häufigsten Angriffs- und Vorfallsmuster in dieser Branche haben sich im Vergleich zum Vorjahr verändert.
Zusammenfassung	In der Einzelhandelsbranche ist ein Zuwachs der Zahl der Cyberangriffe zu beobachten, wobei es die Kriminellen nicht mehr schwerpunkmäßig auf Zahlungskartendaten, sondern vielmehr auf einfacher verfügbare Datentypen abgesehen haben. Des Weiteren war im Vergleich zum letztjährigen Berichtszeitraum ein deutlicher Anstieg der Spionageangriffe zu verzeichnen. Die zuständigen Sicherheitsteams sollten sich auf raffiniertere, besser getarnte Bedrohungen vorbereiten.

Öffentlicher Sektor

(NAICS 92)

Absolute Häufigkeit	1.422 Vorfälle, davon 946 mit bestätigten Datenlecks
Häufigste Angriffsmuster	78 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Diverse Fehler und Einfache Angriffe auf Web-Anwendungen.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (67 %), Insider (33 %), Partner (1 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (76 %), Spionage (29 %), ideologische Motive (2 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (47 %), Interna (44 %), sonstige Daten (41 %), Betriebsgeheimnisse (17 %)
Anhaltende Trends	Die Branche steht weiterhin im Visier raffinierter Angreifer, die es auf die von staatlichen Behörden erhobenen Bürgerdaten abgesehen haben. Obwohl das Gros der Sicherheitsverletzungen auf das Konto externer Akteure geht, ist eine Vielzahl von Vorfällen auf fahrlässige Fehler von Behördenmitarbeitern und anderen Insidern zurückzuführen.
Zusammenfassung	Veränderungen in der Gruppe der an diesem Bericht beteiligten Organisationen haben dazu geführt, dass sich die Zahl der gemeldeten Vorfälle im diesjährigen Berichtszeitraum verringerte, während die Zahl der bestätigen Sicherheitsverletzungen auf dem Vorjahresniveau blieb. Das bedeutet, dass Behörden und andere staatliche Organisationen nach wie vor Ziel krimineller Angreifer sind. Dabei spielt Ransomware eine zentrale Rolle und tritt bei 30 % der Sicherheitsverletzungen auf sämtlichen Ebenen des öffentlichen Sektors in Erscheinung. Zudem stellen Falschzustellungen und andere menschliche Fehler weiterhin ein großes Problem dar.

Branchendaten auf einen Blick

Da wir hier nicht genug Platz, Zeit und in manchen Fällen auch nicht genug Daten haben, um alle Branchen im Detail zu betrachten, bietet die nachstehende Tabelle 1 überblickshafte Informationen zu allen Sparten, die wir im letzten Abschnitt nicht erwähnt haben.

Branche (NAICS)	Absolute Häufigkeit	Häufigste Angriffsmuster	Urheber der Bedrohungen (bestätigte Sicherheits-verletzungen)	Motive der Angreifer (bestätigte Sicherheits-verletzungen)	Betroffene Daten (bestätigte Sicherheits-verletzungen)
Landwirtschaft (11)	80 Vorfälle, davon 55 mit bestätigten Datenlecks	96 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering.	Externe Angreifer (96 %), Insider (4 %)	Finanzielle Motive (98 %), Spionage (33 %), ideologische Motive (2 %)	Interna (67 %), sonstige Daten (39 %), Betriebsgeheim-nisse (35 %)
Öffentliche Verwaltung (56)	153 Vorfälle, davon 145 mit bestätigten Datenlecks	97 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusions, Social Engineering und Diverse Fehler.	Externe Angreifer (95 %), Insider (3 %), Partner (2 %)	Finanzielle Motive (100 %)	Interna (83 %), Anmeldedaten (31 %), personenbezogene Daten (10 %), sonstige Daten (8 %)
Bauwesen (23)	307 Vorfälle, davon 252 mit bestätigten Datenlecks	96 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen.	Externe Angreifer (97 %), Insider (3 %)	Finanzielle Motive (77 %), Spionage (23 %)	Interna (77 %), Anmeldedaten (31 %), sonstige Daten (23 %), Betriebsgeheim-nisse (21 %)
Medien und Unterhaltung (71)	493 Vorfälle, davon 293 mit bestätigten Datenlecks	76 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Diverse Fehler.	Externe Angreifer (71 %), Insider (29 %)	Finanzielle Motive (97 %), Spionage (18 %), ideologische Motive (3 %), Spaß (1 %)	Personenbezogene Daten (58 %), sonstige Daten (39 %), Interna (32 %), Anmeldedaten (18 %)
IT und TK-Beratung (51)	1.589 Vorfälle, davon 784 mit bestätigten Datenlecks	82 % der erfassten Sicherheitsverlet-zungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering.	Externe Angreifer (83 %), Insider (17 %), Partner (1 %)	Finanzielle Motive (78 %), Spionage (36 %), ideologische Motive (1 %)	Sonstige (62 %), Interna (51 %), personenbezogene Daten (37 %), Betriebsgeheim-nisse (27 %)

Tabelle 1: Daten zu betroffenen Branchen ohne eigenen Abschnitt

Branche (NAICS)	Absolute Häufigkeit	Häufigste Angriffsmuster	Urheber der Bedrohungen (bestätigte Sicherheits-verletzungen)	Motive der Angreifer (bestätigte Sicherheits-verletzungen)	Betroffene Daten (bestätigte Sicherheits-verletzungen)
Management (55)	113 Vorfälle, davon 107 mit bestätigten Datenlecks	99 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Missbrauch von Nutzerrechten.	Externe Angreifer (97 %), Partner (2 %), Insider (1 %)	Finanzielle Motive (99 %), Spionage (1 %)	Interna (95 %), Anmel-dedaten (33 %), Ge-sundheitsdaten (1 %), personenbezogene Daten (1 %), Systemdaten (1 %)
Bergbau (21)	64 Vorfälle, davon 52 mit bestätigten Datenlecks	96 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen.	Externe Angreifer (98 %), Insider (6 %), Mehrere Akteure (4 %)	Finanzielle Motive (100 %), Spionage (3 %), Rache (3 %)	Interna (59 %), Anmeldedaten (43 %), Systemdaten (20 %), sonstige Daten (18 %)
Sonstige Dienstleister (81)	683 Vorfälle, davon 583 mit bestätigten Datenlecks	79 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Diverse Fehler.	Externe Angreifer (68 %), Insider (33 %)	Finanzielle Motive (69 %), Spionage (31 %)	Personenbezogene Daten (57 %), Interna (48 %), sonstige Daten (44 %), Betriebsgeheim-nisse (18 %)
Professionen (54)	2.549 Vorfälle, davon 1.147 mit bestätigten Datenlecks	91 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen.	Externe Angreifer (93 %), Insider (7 %), Partner (1 %)	Finanzielle Motive (88 %), Spionage (17 %)	Interna (70 %), sonstige Daten (25 %), Anmeldedaten (24 %), Personenbezogene Daten (24 %)
Immobilien-branche (53)	339 Vorfälle, davon 320 mit bestätigten Datenlecks	84 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Diverse Fehler.	Externe Angreifer (64 %), Insider (36 %)	Finanzielle Motive (100 %)	Personenbezogene Daten (70 %), Interna (40 %), sonstige Daten (27 %), Bankdaten (17 %)
Transportwesen (48–49)	361 Vorfälle, davon 248 mit bestätigten Datenlecks	91 % der erfassten Sicherheitsverlet-zungen entfallen auf die Kategorien System Intrusion, Einfache Angriffe auf Web-Anwendungen und Social Engineering.	Externe Angreifer (94 %), Insider (7 %), mehrere Akteure (2 %), Partner (1 %)	Finanzielle Motive (98 %), Spionage (16 %), ideologische Motive (1 %)	Interna (67 %), sonstige Daten (25 %), Anmeldedaten (22 %), personenbezogene Daten (20 %)
Versorgungsunter-nehmen (22)	358 Vorfälle, davon 213 mit bestätigten Datenlecks	92 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Einfache Angriffe auf Web-Anwendungen.	Externe Angreifer (92 %), Insider (8 %), mehrere Akteure (1 %)	Finanzielle Motive (70 %), Spionage (66 %), Rache (1 %)	Interna (80 %), Betriebsgeheim-nisse (61 %), sonstige Daten (42 %)
Großhandel (42)	330 Vorfälle, davon 319 mit bestätigten Datenlecks	98 % der Sicherheits-verletzungen entfallen auf die Kategorien System Intrusion, Social Engineering und Missbrauch von Nutzerrechten.	Externe Angreifer (97 %), Insider (3 %)	Finanzielle Motive (100 %)	Interna (93 %), Anmeldedaten (24 %), sonstige Daten (3 %), personenbezogene Daten (3 %), Systemdaten (3 %)

Tabelle 1: Daten zu betroffenen Branchen ohne eigenes Kapitel (Fortsetzung)

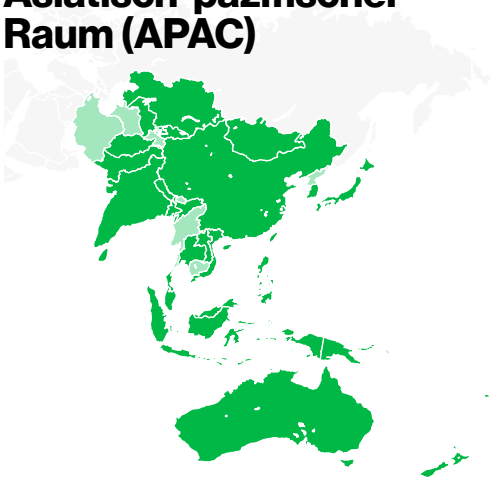
Ergebnisse für spezifische Regionen

Unsere Experten werden oft gefragt, wie sich die Aktivitäten der Cyberkriminellen von Region zu Region unterscheiden (oder ähneln). Deshalb schlüsseln wir das weltweite Geschehen in diesem Abschnitt nach Makroregionen auf. Dabei werden unsere Einblicke in die jeweilige Sicherheitslage unter anderem durch regionsspezifische Offenlegungspflichten, die in unseren Datenbeständen enthaltenen Angaben sowie die geografischen Tätigkeitsbereiche der an diesem Bericht beteiligten Organisationen beeinflusst. Ungeachtet dessen hoffen wir, dass diese globale Perspektive nützlich und informativ für Sie ist.

Wenn Sie dazu beitragen möchten, dass Ihre Region an dieser Stelle in Zukunft besser repräsentiert wird, können Sie sich gern als freiwilliger Datenpartner melden und Ihre Zulieferer und Kunden ebenfalls dazu ermutigen. Nehmen Sie einfach Kontakt mit uns auf.

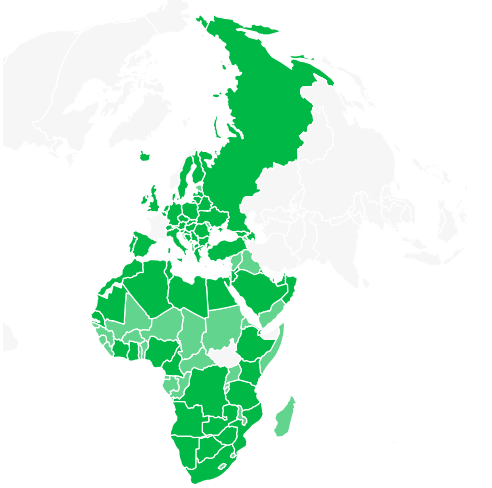
Durch Daten repräsentierte Länder Nicht durch Daten repräsentierte Länder

Asiatisch-pazifischer Raum (APAC)



Absolute Häufigkeit	2.687 Vorfälle, davon 1.374 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und Einfache Angriffe auf Web-Anwendungen machten 97 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (99 %), Insider (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (83 %), Spionage (34 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (78 %), sonstige Daten (41 %), Betriebsgeheimnisse (33 %)

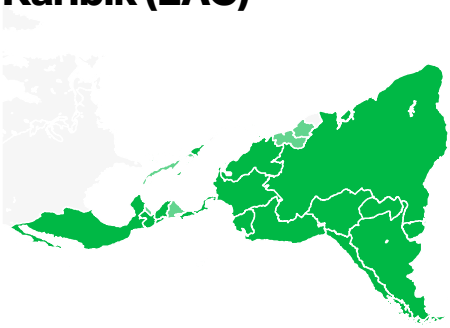
Europa, Naher Osten und Afrika (EMEA)



Absolute Häufigkeit	9.062 Vorfälle, davon 5.321 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und Diverse Fehler machten 89 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (71 %), Insider (29 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (87 %), Spionage (18 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (62 %), personenbezogene Daten (49 %), sonstige Daten (37 %), Betriebsgeheimnisse (13 %)

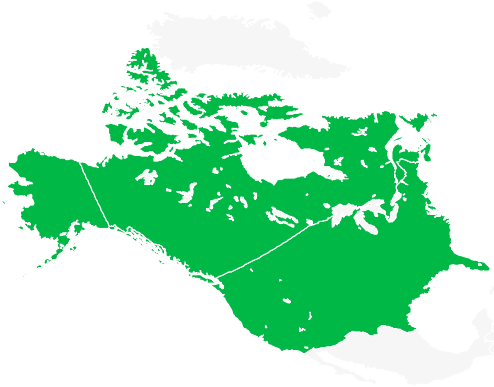
Durch Daten repräsentierte Länder Nicht durch Daten repräsentierte Länder

Lateinamerika und Karibik (LAC)



Absolute Häufigkeit	657 Vorfälle, davon 413 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und Einfache Angriffe auf Web-Anwendungen machten 99 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (100 %), Insider (1 %), mehrere Akteure (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (84 %), Spionage (27 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (97 %), Betriebsgeheimnisse (27 %), sonstige Daten (24 %)

Nordamerika (NA)



Absolute Häufigkeit	6.361 Vorfälle, davon 2.867 mit bestätigten Datenlecks
Häufigste Angriffsmuster	90 % der bestätigten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusions, Alles Andere und Social Engineering.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (91 %), Insider (5 %), Partner (5 %), mehrere Akteure (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (95 %), Spionage (9 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Interna (49 %), Gesundheitsdaten (35 %), Anmeldedaten (23 %), sonstige Daten (17 %)

Halten Sie sich und Ihr Team auf dem Laufenden

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

Deshalb bietet Ihnen die vollständige Ausgabe des DBIR einen detaillierten, praxisrelevanten Überblick über die Ziele, Methoden und Aktivitäten der Angreifer. Holen Sie sich alle Zahlen, Daten und Fakten, die für fundierte Maßnahmen zum Schutz Ihres Unternehmens und zur Stärkung des Sicherheitsbewusstseins Ihrer Mitarbeiter erforderlich sind.

Den vollständigen DBIR 2025 finden Sie unter verizon.com/dbir.

Möchten Sie dazu beitragen, die Cybersicherheit weltweit zu stärken?

Für alle Organisationen, die Daten zu Vorfällen oder zur Sicherheit allgemein erfassen und bereit sind, diese für zukünftige Ausgaben des jährlich erscheinenden Verizon DBIR mit uns zu teilen, haben wir einen klaren und einfachen Anmeldeprozess. Falls das (wie wir sehr hoffen) auch auf Sie zutrifft, schicken Sie bitte eine E-Mail an dbircontributor@verizon.com.

Falls Sie uns Verbesserungsvorschläge für den nächsten DBIR unterbreiten möchten, können Sie uns unter der E-Mail-Adresse dbir@verizon.com erreichen oder eine Nachricht an Verizon Business (oder einen der beteiligten Autoren) senden. Außerdem sollten Sie nicht versäumen, die GitHub-Seite zu unserem VERIS-Framework zu besuchen: https://github.com/vz-risk/veris (auf Englisch).