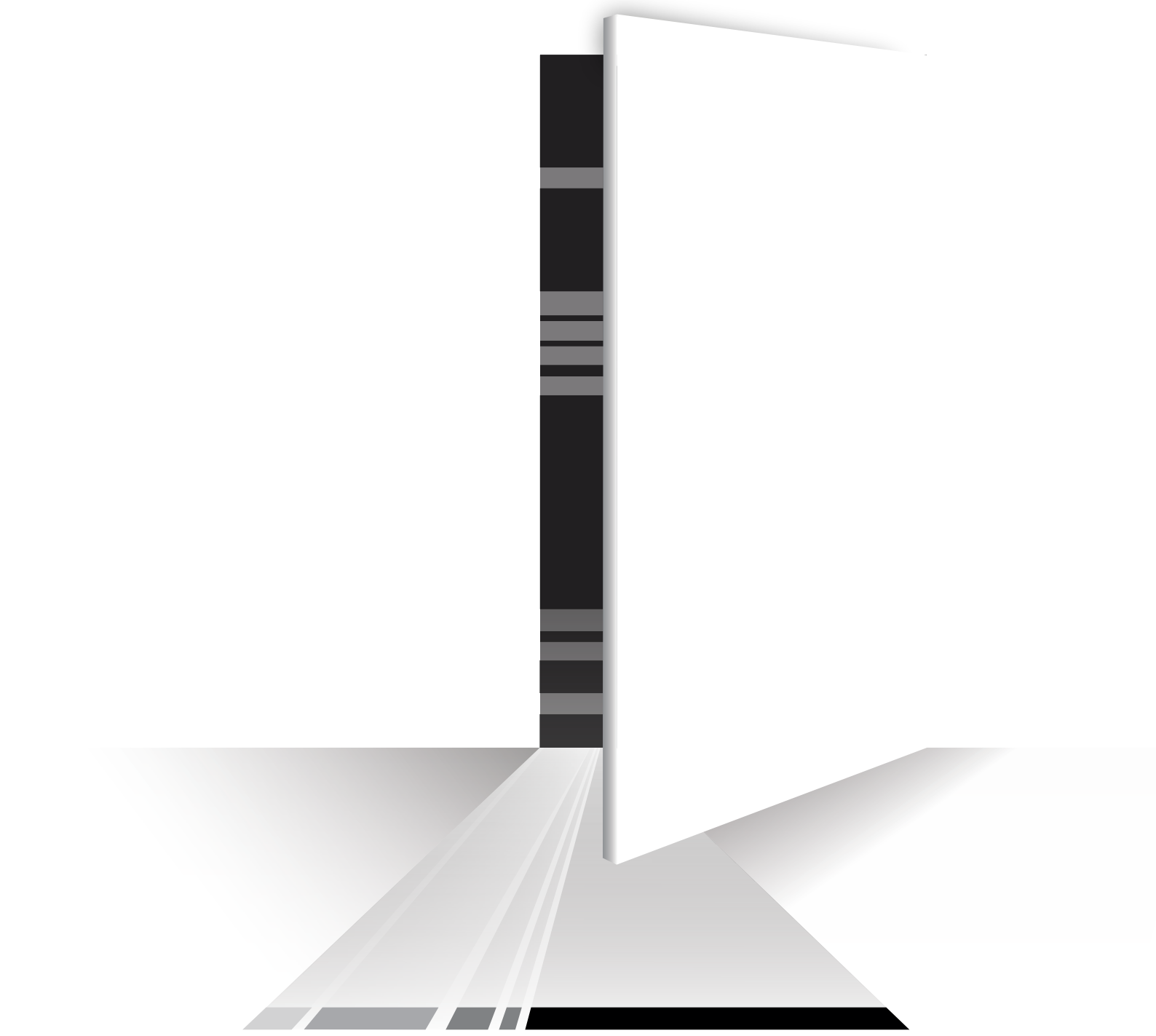
2024 Data Breach Investigations Report

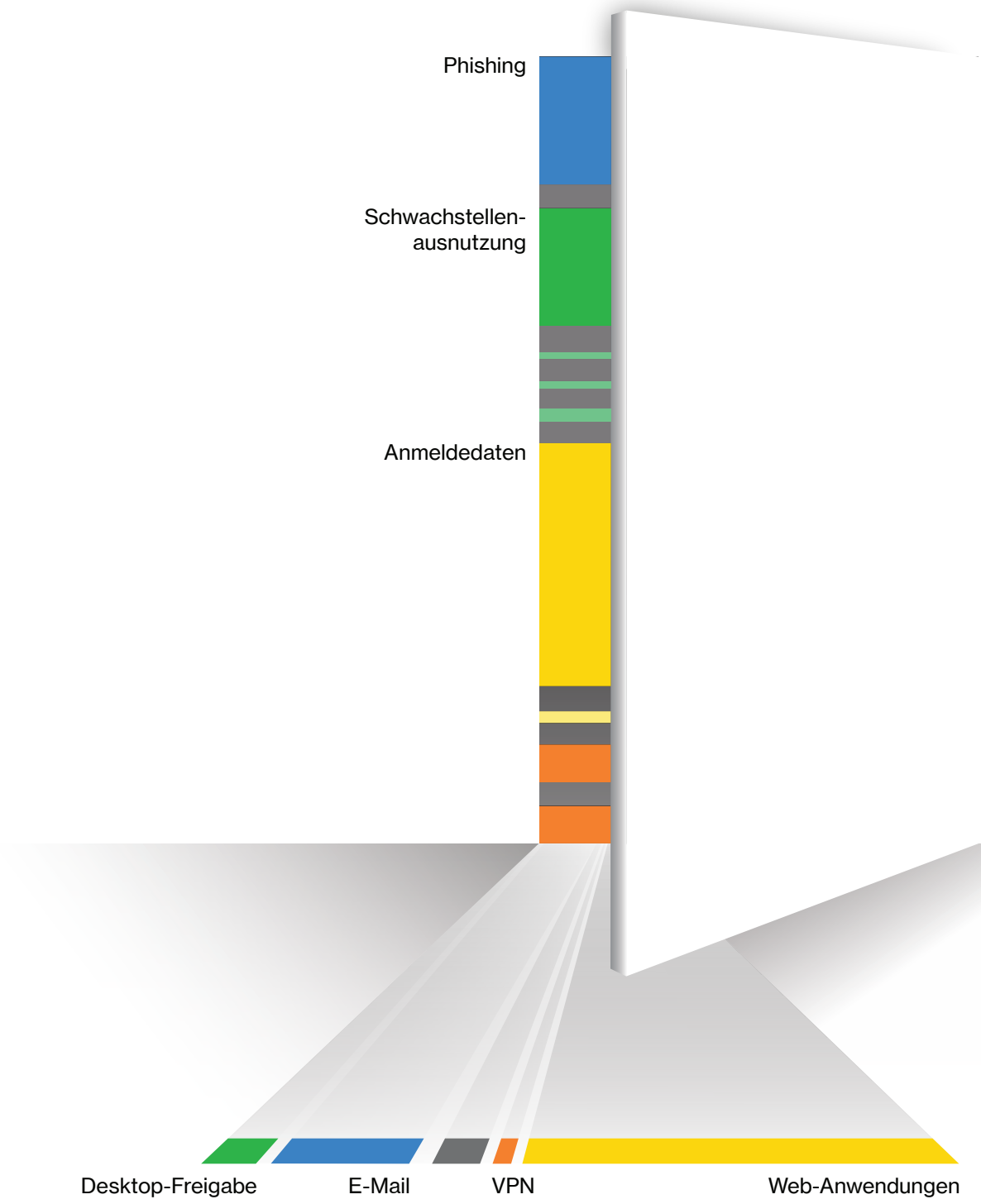
Kurzfassung



verizon business

Über die Titelseite

Im diesjährigen Bericht beschäftigen wir uns eingehender mit Angriffspfaden, um herauszufinden, mit welchen Kombinationen aus Aktionen und Vektoren Cyberkriminelle in der aktuellen Bedrohungslandschaft am häufigsten erfolgreich sind. Die einen Spalt weit geöffnete Tür auf der Titelseite soll die verschiedenen Wege repräsentieren, auf denen Angreifer in eine Infrastruktur gelangen können. Durch den Spalt sieht man ein Diagramm, das die relative Häufigkeit verschiedener Infiltrationsmethoden zeigt (Abbildung 7 im vollständigen Bericht enthält eine weniger kryptische Variante). Das aus der Türöffnung fallende Licht wird in ein Diagramm aufgefächert, das die relative Häufigkeit der Aktionsvektoren darstellt. Auf der Innenseite haben wir die beiden Verteilungen etwas weniger abstrakt und mit Beschriftung abgebildet. Wir hoffen, dass auch Sie ein bisschen Spaß an unserer künstlerischen Arbeit haben.


Phishing
Schwachstellen-
ausnutzung
Anmeldedaten
Desktop-Freigabe
E-Mail
VPN
Web-Anwendungen

Inhalt

Willkommen 5

Die Ergebnisse im Überblick/ Zusammenfassung 6

Branchenspezifische Erkenntnisse 9

Hotel- und Gaststättengewerbe 9

Bildungswesen 10

Finanz- und Versicherungsbranche 10

Gesundheitswesen 11

IT 11

Fertigung 12

Professional Services, technische und wissenschaftliche Dienstleistungen 12

Öffentliche Verwaltung 13

Einzelhandel 13

Ergebnisse für spezifische Regionen 14

Halten Sie sich und Ihr Team auf dem Laufenden 16

Willkommen

Vielen Dank für Ihr Interesse am Data Breach Investigations Report (DBIR) 2024.

Wir freuen uns, alten Freunden und neuen Lesern diese 17. Ausgabe unseres Berichts vorlegen zu dürfen. Wie immer geht es auch im diesjährigen DBIR um die verschiedenen Kategorien von Angreifern, deren Taktiken und die Ziele, auf die sie es abgesehen haben. Wir möchten uns gleich eingangs bedanken: bei den vielen talentierten Personen aus aller Welt, die schon seit Jahren großzügig und uneigennützig ihre Daten und Einblicke mit uns teilen, und bei unserem hauseigenen Dream Team, dem Verizon Threat Research Advisory Center (VTRAC). Ohne diese beiden Gruppen könnten wir nicht untersuchen und analysieren, welche Trends in der Cyberkriminalität für Unternehmen aller Größen und in allen Branchen und Weltregionen aktuell relevant sind.

Jedes Jahr finden wir dabei sowohl innovative neue Angriffsmethoden als auch Variationen altbekannter Tricks, die immer noch erfolgreich sind. Von der Ausnutzung bekannter, weit verbreiteter Zero-Day-Sicherheitslücken wie in der Software MOVEit bis hin zu weit weniger spektakulären, aber dennoch unglaublich effektiven Taktiken wie Ransomware, Missbrauch gestohlener Anmeldedaten und Denial-of-Service (DoS) lassen Cyberkriminelle nichts unversucht, um zu beweisen, dass Verbrechen sich durchaus lohnen können.

Die sich ständig ändernde Cyberbedrohungslandschaft wirkt oft unübersichtlich und sogar beängstigend – besonders im vergangenen Jahr, denn da hatte die Cyberkriminalität Hochkonjunktur. Wir haben 30.458 Sicherheitsvorfälle in der Praxis analysiert – mehr als je zuvor – und 10.626 davon als Datenschutzverletzungen mit Opfern in 94 Ländern bestätigt. Auf den folgenden Seiten präsentieren wir einige der wichtigsten Ergebnisse des ausführlichen Berichts. Wir hoffen, dass diese interessant und nützlich für Sie sind.

Auf den folgenden Seiten finden Sie die wichtigsten Ergebnisse aus unserem Bericht, darunter auch Zahlen 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

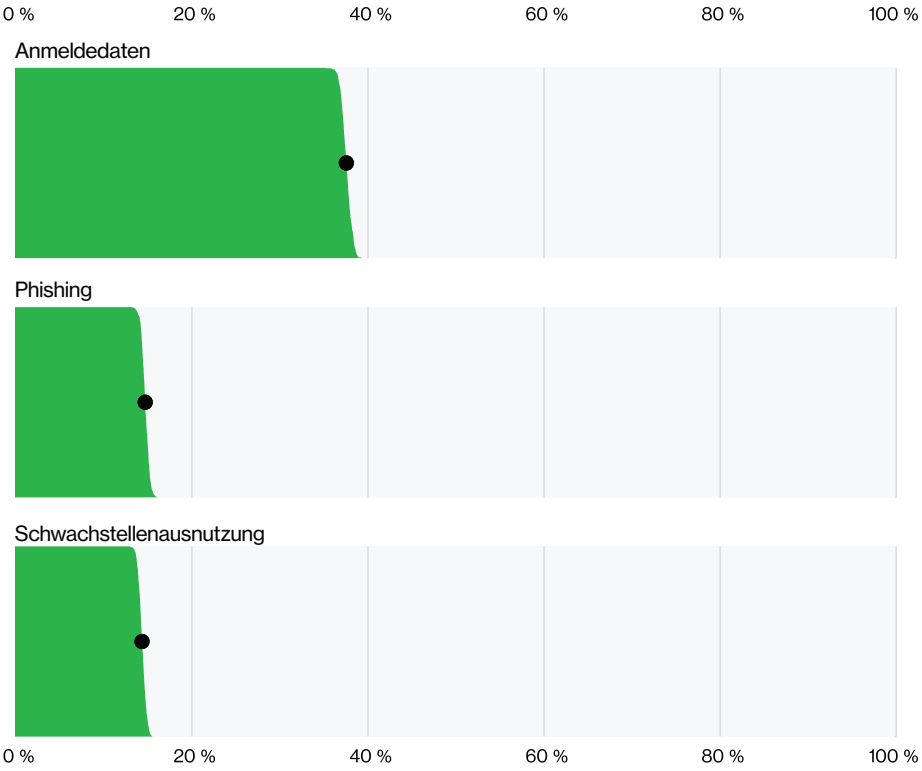


Abbildung 1: Anteil ausgewählter Infiltrationsmethoden an der Gesamtzahl der Sicherheitsverletzungen ohne Fehler oder Missbrauch seitens der Benutzer (n=6.963)

Unsere Analyse der Infiltrationsmethoden zeigt, dass der Anteil der Angriffe, bei denen Sicherheitslücken ausgenutzt wurden, sich gegenüber dem Vorjahr fast verdreifacht hat (Steigerung um 180 %). Das ist zu einem großen Teil auf Zero-Day-Sicherheitslücken wie in der Software MOVEit zurückzuführen, die von Cyberkriminellen ausgenutzt wurden, um über Web-Anwendungen in Umgebungen einzudringen und dann zumeist Ransomware- oder andere erpresserische Angriffe zu starten.

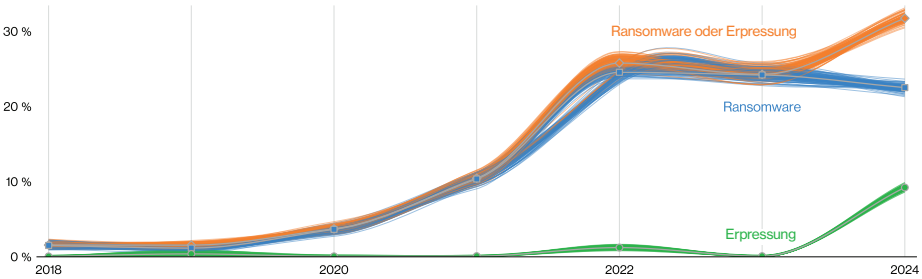


Abbildung 2: Anteil der Ransomware-Angriffe an der Gesamtzahl der Sicherheitsverletzungen im Zeitverlauf

Bei etwa einem Drittel aller Angriffe kam Ransomware oder eine andere Erpressungstaktik zum Einsatz. Reine Erpressungsangriffe haben im Verlauf des vergangenen Jahres zugenommen und sind nun ein Bestandteil von 9 % aller Sicherheitsvorfälle. Ransomware-Angreifer haben sich diese neueren Taktiken zu eigen gemacht, wodurch der Anteil der Ransomware-Angriffe auf 23 % gesunken ist. Wenn man beide Arten erpresserischer Angriffe zusammenzählt, ist ihr Anteil an der Gesamtzahl der Sicherheitsvorfälle jedoch stark gestiegen (auf nunmehr 32 %). Zudem stellt Ransomware in 92 % der untersuchten Branchen die größte Bedrohung dar.

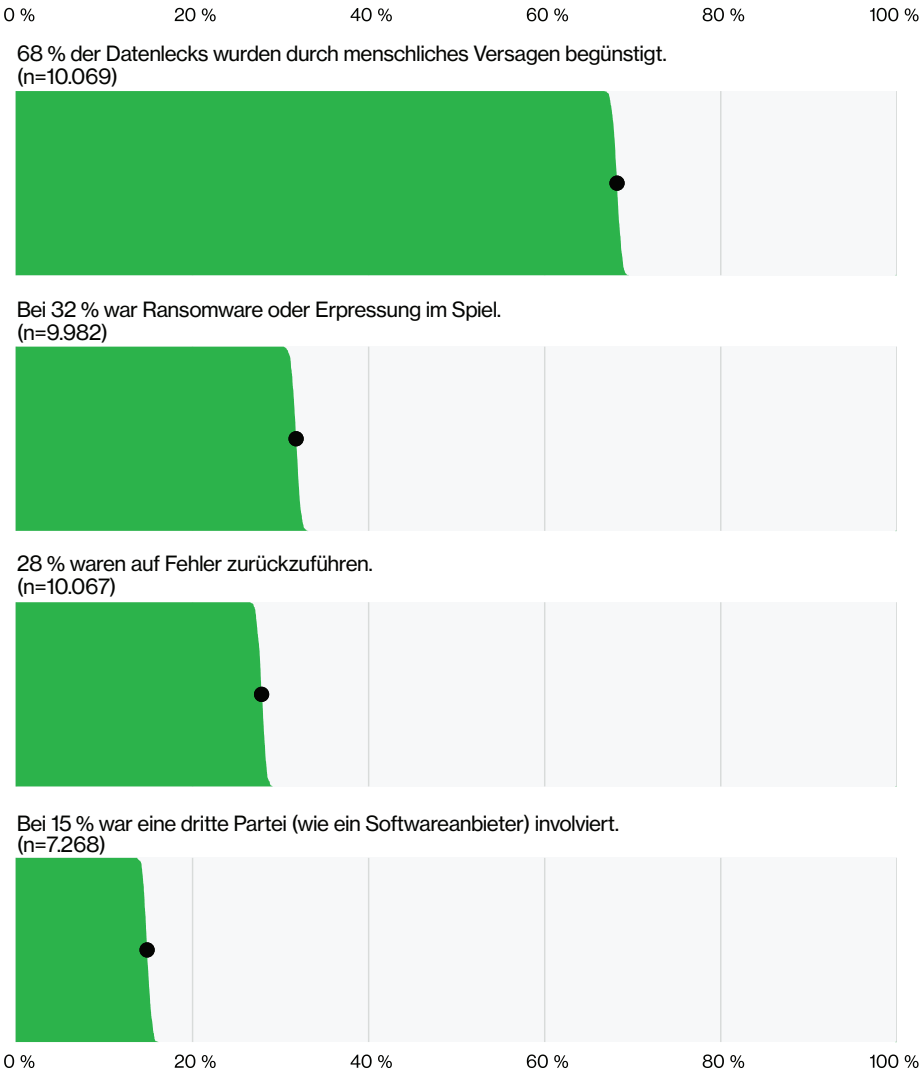


Abbildung 3: Einige wichtige Zahlen zu Sicherheitsvorfällen

Wir haben unsere Definition der Sicherheitsverletzungen, bei denen menschliches Fehlverhalten eine Rolle spielt, überarbeitet. Der böswillige Missbrauch von Nutzerrechten fällt nun nicht mehr in diese Kategorie, weil wir genauer als bisher messen wollen, was sich durch ein besseres Sicherheitsbewusstsein erreichen lässt. Menschliches Fehlverhalten spielte bei 68 % der für den diesjährigen DBIR analysierten Vorfälle eine Rolle, in etwa der gleiche Prozentsatz wie im Vorjahresbericht.

Außerdem haben wir die Definition von Sicherheitsverletzungen, bei denen Dritte involviert sind, weiter gefasst. Diese Kategorie umfasst nun auch Vorfälle, bei denen die Infrastrukturen von Partnern betroffen sind, sowie direkte und indirekte Lieferkettenprobleme – wie zum Beispiel Vorfälle, die auf Schwachstellen in Drittanbietersoftware zurückzuführen sind. Kurz gesagt handelt es sich hier um Vorfälle, die man potenziell abschwächen oder vermeiden könnte, indem man Anbieter mit einer guten Sicherheitsbilanz auswählt. Der Anteil dieser Vorfälle liegt in diesem Jahr bei 15 %. Er ist im vergangenen Jahr also um 68 % gestiegen, hauptsächlich aufgrund der Ausnutzung von Zero-Day-Schwachstellen für Ransomware- und andere erpresserische Angriffe.

Der Anteil der von uns untersuchten Vorfälle, bei denen menschliche Fehler eine Rolle spielten, ist auf 28 % gestiegen. Das liegt zum Teil daran, dass wir in diesem Jahr erstmals Daten mehrerer Regulierungsgremien, an die Datenschutzverstöße gemeldet werden müssen, in unseren Datensatz einbezogen haben. Das bestätigt unsere Vermutung, dass Fehler in der Realität eine wichtigere Rolle spielen als in den Berichten, die man in den Medien und bei Incident-Response-Anbietern liest.

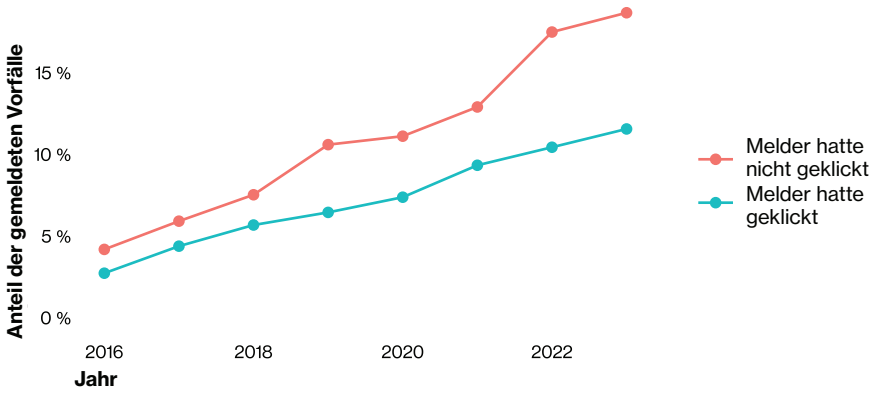


Abbildung 4: Anteil der gemeldeten Phishing-E-Mails nach Klick-Status

Die Melderate von Phishing-Versuchen steigt seit einigen Jahren an. Unsere Partner haben uns 2023 Daten aus Übungen zur Nutzersensibilisierung zur Verfügung gestellt, aus denen hervorgeht, dass 20 % der Nutzer, die bei einem Einsatz simulierte Phishing-E-Mails erhielten, diese meldeten. Auch 11 % der Nutzer, die auf die E-Mail geklickt hatten, meldeten das. Das ist eine gute Nachricht, denn die mittlere Zeit zwischen dem Öffnen einer E-Mail und dem Klicken auf einen schädlichen Link liegt bei 21 Sekunden und die mittlere Zeit zwischen dem Klicken und dem Eingeben von Daten bei 28 Sekunden. Das bedeutet: In weniger als 60 Sekunden fallen Nutzer auf Phishing-E-Mails herein und geben ihre Daten preis.

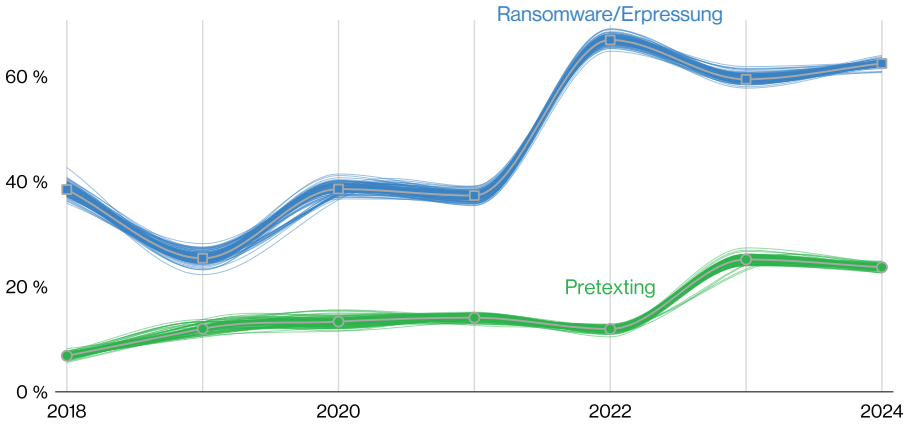


Abbildung 5: Ausgewählte finanziell motivierte Angreiferaktionen im Zeitverlauf

Finanziell motivierte Angreifer bleiben normalerweise bei den Angriffstechniken, die den größten Gewinn bringen.

In den letzten drei Jahren machten Ransomware- und andere erpresserische Angriffe fast zwei Drittel dieser Angriffe aus. (Der Anteil schwankte zwischen 59 % und 66 %.) 95 % der Angriffe mit einer Erpressungskomponente, die dem Internet Crime Complaint Center (IC3) des FBI gemeldet wurden, verursachten Verluste zwischen drei US-Dollar und 1.141.467 US-Dollar. Der Mittelwert lag bei 46.000 US-Dollar. Außerdem wissen wir von Beitragenden, die an Lösegeldverhandlungen beteiligt waren, dass das mittlere ursprünglich verlangte Lösegeld bei 1,34 % (und in 80 % der Fälle zwischen 0,13 % und 8,3 %) des Unternehmensumsatzes lag.

In den letzten beiden Jahren spielte Pretexting bei etwa einem Viertel (24 % bzw. 25 %) der finanziell motivierten Vorfälle eine Rolle – und gipfelte in den meisten Fällen in Business-E-Mail-Compromise (BEC). Der mittlere Transaktionsbetrag bei BEC lag in beiden Jahren bei 50.000 US-Dollar.

Branchen-spezifische Erkenntnisse

Wir haben bereits in früheren Berichten erwähnt, dass ein und dieselbe Angriffsform den Sicherheitsteams in einer Branche den Schlaf rauben kann, während sie für ihre Kollegen in anderen Sektoren kaum eine Rolle spielt. Der entscheidende Faktor ist die Angriffsfläche – der potenzielle Tatort für Cyberkriminalität aller Art. Zusammen mit einer ganzen Reihe anderer Aspekte, von den Eigenheiten einzelner Angreifergruppen über die in verschiedenen Branchen genutzten Technologie-Infrastrukturen und die von unterschiedlichen Unternehmen verarbeiteten und gespeicherten Daten bis hin zu der Art und Weise, wie diese Daten genutzt und abgerufen werden, formt die Angriffsfläche eine komplexe Kulisse aus Sicherheitsherausforderungen.

Bei einem Technologie-Giganten mit Hunderttausenden Mobilgeräten, auf denen unzählige verschiedene Apps installiert sind, wird diese auch als Risikoprofil bezeichnete Kulisse ganz anders aussehen als bei einer exklusiven Boutique, deren Kassensystem und/oder einfacher Online-Shop von den jeweiligen Anbietern unterstützt werden. Dementsprechend hängen auch die Bedrohungen, denen ein Unternehmen sich stellen muss, von der Branche, der Größe und ähnlichen Faktoren ab. Zudem haben auch die Anforderungen bezüglich der Meldung von Sicherheitsverstößen einen Einfluss darauf, was über die Sicherheitslage in einer Branche bekannt wird. In diesem Abschnitt schauen wir uns jede der neun Branchen, die wir für unseren Bericht untersucht haben, überblicksartig an. Die Klassifizierung der untersuchten Unternehmen basiert auch in diesem Jahr auf der Brancheneinteilung des North American Industry Classification System (NAICS).

Hotel- und Gaststättengewerbe

(NAICS 72)

Absolute Häufigkeit	220 Vorfälle, davon 106 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 92 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (92 %), Insider (9 %), verschiedene (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (100 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Anmeldedaten (50 %), personenbezogene Daten (28 %), Zahlungsdaten (19 %), Systemdaten (19 %), sonstige Daten (16 %)
Anhaltende Trends	Ransomware- und Social-Engineering-Angriffe stellen mit 35 % der Vorfälle weiterhin ein großes Problem in dieser Branche dar.
Zusammen-fassung	Social Engineering hat erheblich zugenommen und spielt nun bei 25 % der Sicherheitsverletzungen in diesem Sektor eine Rolle. Der Anteil der Vorfälle mit Pretexting hat sich gegenüber dem Vorjahreszeitraum mehr als verdoppelt und liegt nun bei 20 %.

Bildungswesen
(NAICS 61)

Absolute Häufigkeit	1.780 Vorfälle, davon 1.537 mit bestätigten Datenlecks
Häufigste Angriffsmuster	Bestätigte Sicherheitsverletzungen: System Intrusions, Social Engineering und diverse Fehler machten 90 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (68 %), Insider (32 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (98 %), Spionage (2 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (83 %), Interna (20 %), sonstige Daten (18 %), Anmeldedaten (9 %)
Anhaltende Trends	Die drei häufigsten Angriffs- und Vorfallsmuster sind dieselben wie im Vorjahr. Bei den meisten Vorfällen ging es externen Angreifern um den Diebstahl personenbezogener Daten.
Zusammenfassung	Diverse Fehler, die Insidern unterlaufen, und Erpressung durch externe Angreifer bestimmen in dieser Branche weiterhin das Bild.

Finanz- und Versicherungsbranche
(NAICS 52)

Absolute Häufigkeit	3.348 Vorfälle, davon 1.115 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, diverse Fehler und Social Engineering machten 78 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (69 %), Insider (31 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (95 %), Spionage (5 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (75 %), sonstige Daten (30 %), Bankdaten (27 %), Anmeldedaten (22 %)
Anhaltende Trends	Diverse Fehler, insbesondere Falschzustellungen, stellen eine anhaltende Herausforderung für diese Branche dar.
Zusammenfassung	System Intrusions haben diverse Fehler und einfache Angriffe auf Web-Anwendungen überholt und stellen in diesem Jahr die größte Bedrohung in der Finanz- und Versicherungsbranche dar. Das ist zumindest teilweise auf einen Trend hin zu komplexeren Angriffen, oft mit Social-Engineering-Komponenten, zurückzuführen. Detailliertere Informationen über die Lage in Europa, dem Nahen Osten und Afrika (EMEA) bestätigen, dass Ransomware-Angriffe in dieser Region weiterhin eine ernstzunehmende Gefahr darstellen.

Gesundheitswesen
(NAICS 62)

Absolute Häufigkeit	1.378 Vorfälle, davon 1.220 mit bestätigten Datenlecks
Häufigste Angriffsmuster	Diverse Fehler, der Missbrauch von Nutzerrechten und System Intrusions machten 83 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Insider (70 %), externe Angreifer (30 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (98 %), Spionage (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (75 %), Interna (51 %), sonstige Daten (25 %), Anmeldedaten (13 %)
Anhaltende Trends	System Intrusions gehören weiterhin zu den drei häufigsten Angriffsarten.
Zusammenfassung	Für das Gesundheitswesen weichen die Ergebnisse der diesjährigen Analyse deutlich von denen der letzten Jahre ab. Absichtlich durch Insider verursachte Datenlecks sind – nach einem stetigen Rückgang seit 2018 – stark gestiegen und zurück auf Platz zwei. Interessanterweise haben diese Insider es häufiger auf personenbezogene als auf medizinische Daten abgesehen.

IT
(NAICS 51)

Absolute Häufigkeit	1.367 Vorfälle, davon 602 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering machten 79 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (79 %), Insider (21 %), verschiedene (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (87 %), Spionage (14 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Sonstige Daten (46 %), personenbezogene Daten (45 %), Anmeldedaten (27 %), Interna (22 %)
Anhaltende Trends	Die drei häufigsten Angriffs- und Vorfallsmuster sind dieselben wie im Vorjahr, auch die Rangfolge hat sich nicht geändert. Das ist etwas überraschend, da unser Team für den diesjährigen Bericht deutlich mehr Sicherheitsverletzungen in diesem Sektor untersucht hat als für den Vorjahresbericht.
Zusammenfassung	Obwohl wir insgesamt mehr Vorfälle untersucht haben als im Vorjahr, gab es in dieser Branche erheblich weniger Sicherheitsverletzungen. Ransomware und die Nutzung gestohlener Anmeldedaten spielen bei System Intrusions weiterhin eine dominante Rolle. Bei den Social-Engineering-Angriffen ist der Anteil der Phishing-Angriffe leicht gesunken, während der der Pretexting-Vorfälle gestiegen ist. Außerdem spielt Spionage als Motiv eine etwas größere Rolle als im Vorjahr, was darauf hindeutet, dass das Interesse staatlich gesponserter Akteure an dieser Branche wächst – und dass stärkere Erkennungsmaßnahmen erforderlich sind.

Fertigungsindustrie

(NAICS 31–33)

Absolute Häufigkeit	2.305 Vorfälle, davon 849 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und diverse Fehler machten 83 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (73 %), Insider (27 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (97 %), Spionage (3 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (58 %), Sonstige (40 %), Anmeldedaten (28 %), Interna (25 %)
Anhaltende Trends	Zwei der drei häufigsten Angriffs- und Vorfallsmuster des Vorjahres sind auch dieses Jahr auf dem Podium. Die meisten Angriffe sind nach wie vor finanziell motiviert.
Zusammenfassung	In der Fertigung ist die Anzahl der durch Fehler begünstigten Sicherheitsverletzungen gestiegen. Auch die Installation von Malware durch Angreifer, die sich mit gestohlenen Anmeldedaten Zugang verschafft haben, tritt beunruhigend häufig auf.

Anbieter qualifizierter, technischer und wissenschaftlicher Dienstleistungen

(NAICS 54)

Absolute Häufigkeit	2.599 Vorfälle, davon 1.314 mit bestätigten Datenlecks
Häufigste Angriffsmuster	Social Engineering, System Intrusions und diverse Fehler machten 85 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (75 %), Insider (25 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (95 %), Spionage (6 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (40 %), Anmeldedaten (38 %), sonstige Daten (33 %), Interna (23 %)
Anhaltende Trends	Personenbezogene und Anmeldedaten sind weiterhin die am häufigsten betroffenen Datenarten in dieser Branche.
Zusammenfassung	Social Engineering spielt bei 40 % der Sicherheitsverletzungen eine Rolle und ist damit eine der größten Bedrohungen in dieser Branche. 20 % der Angriffe sind allein auf Pretexting zurückzuführen. Gleichzeitig ist der Anteil der durch Falschzustellung und andere Nutzerfehler verursachten Sicherheitsverstöße gestiegen.

Öffentliche Verwaltung

(NAICS 92)

Absolute Häufigkeit	12.217 Vorfälle, davon 1.085 mit bestätigten Datenlecks
Häufigste Angriffsmuster	Diverse Fehler, System Intrusions und Social Engineering machten 78 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Insider (59 %), externe Angreifer (41 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (71 %), Spionage (29 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (72 %), Interna (37 %), sonstige Daten (31 %), Anmeldedaten (17 %)
Anhaltende Trends	System Intrusions und Social Engineering sind nach wie vor die beiden häufigsten Angriffsarten in diesem Sektor.
Zusammenfassung	Diverse Fehler, insbesondere Falschzustellungen, haben stark zugenommen und sind nun die führende Ursache von Sicherheitsverletzungen in dieser Branche – was einmal mehr unterstreicht, wie weit verbreitet und gefährlich menschliche Fehler sind. System Intrusions und Social Engineering liegen nun auf Platz zwei und drei. Ein Nebeneffekt der zahlreichen durch diverse Fehler verursachten Vorfälle – und ein gutes Beispiel für die potenziellen Konsequenzen von Achtlosigkeit – ist die Tatsache, dass Insider für deutlich mehr als die Hälfte der Sicherheitsverletzungen verantwortlich waren.

Einzelhandel

(NAICS 44–45)

Absolute Häufigkeit	725 Vorfälle, davon 369 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 92 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (96 %), Insider (4 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (99 %), Spionage (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Anmeldedaten (38 %), sonstige Daten (31 %), Zahlungsdaten (25 %), Systemdaten (20 %)
Anhaltende Trends	Die drei häufigsten Angriffs- und Vorfallsmuster sind dieselben wie im Vorjahr, auch die Rangfolge hat sich nicht geändert. Finanziell motivierte Angreifer sind nach wie vor die weitaus größte Gefahr in dieser Branche.
Zusammenfassung	Während in dieser Branche in vergangenen Jahren hauptsächlich Zahlungskartendaten gestohlen wurden, waren Angreifer in diesem Jahr noch stärker an Anmeldedaten interessiert. Bei Social-Engineering-Angriffen hat das Pretexting (auf Kosten von Phishing) zugenommen. Denial-of-Service-Angriffe bleiben im Einzelhandel weiterhin ein Problem, da sie sich unmittelbar auf den Kundendienst und den Absatz auswirken.

Ergebnisse für spezifische Regionen

Auch im DBIR 2024 haben wir die Vorfälle und Datenlecks in unserem Datensatz nach Weltregionen unterteilt und aus dieser Perspektive analysiert. Wir hoffen, dass wir unseren Lesern damit eine kurze und übersichtliche Zusammenfassung der Cybersicherheitstrends in den verschiedenen Regionen geben und zugleich hervorheben können, welche Unterschiede und welche Gemeinsamkeiten es zwischen den Regionen gibt. Dabei müssen wir (wie schon in den Vorjahren) jedoch darauf hinweisen, dass Umfang und Detailgenauigkeit unserer regionalen Analysen von zahlreichen Faktoren abhängen (Beitragende in der Region, landesspezifische gesetzliche Meldevorgaben, Arbeitsbelastung unserer Mitarbeitenden usw.), und daher nicht für alle Regionen gleich sind. Wir hoffen, dass Sie, unsere Leser, diese geografische Perspektive nützlich und interessant finden.

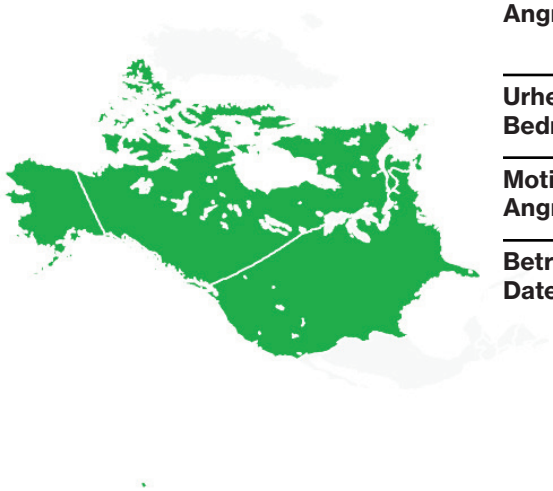
Asien-Pazifik (APAC)

Absolute Häufigkeit	2.130 Vorfälle, davon 523 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 95 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (98 %), Insider (2 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (75 %), Spionage (25 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Anmeldedaten (69 %), Interna (37 %), Betriebsgeheimnisse (24 %), sonstige Daten (17 %)

Europa, Naher Osten und Afrika (EMEA)

Absolute Häufigkeit	8.302 Vorfälle, davon 6.005 mit bestätigten Datenlecks
Häufigste Angriffsmuster	Diverse Fehler, System Intrusions und Social Engineering machten 87 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (51 %), Insider (49 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (94 %), Spionage (6 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (64 %), sonstige Daten (36 %), Interna (33 %), Anmeldedaten (20 %)

Nordamerika (NA)



Absolute Häufigkeit	16.619 Vorfälle, davon 1.877 mit bestätigten Datenlecks
Häufigste Angriffsmuster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 91 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (93 %), Insider (8 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (97 %), Spionage (4 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (50 %), Anmeldedaten (26 %), Interna (19 %), sonstige Daten (16 %)

Halten Sie sich und Ihr Team auf dem Laufenden.

Um den 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 Zahlen, Daten und Fakten für fundiertere Entscheidungen zum Schutz Ihres Unternehmens.

Den vollständigen DBIR 2024 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 oder per Tweet an @VZDBIR erreichen. Außerdem sollten Sie nicht versäumen, die GitHub-Seite zu unserem VERIS-Framework zu besuchen: https://github.com/vz-risk/veris (auf Englisch).

verizon business