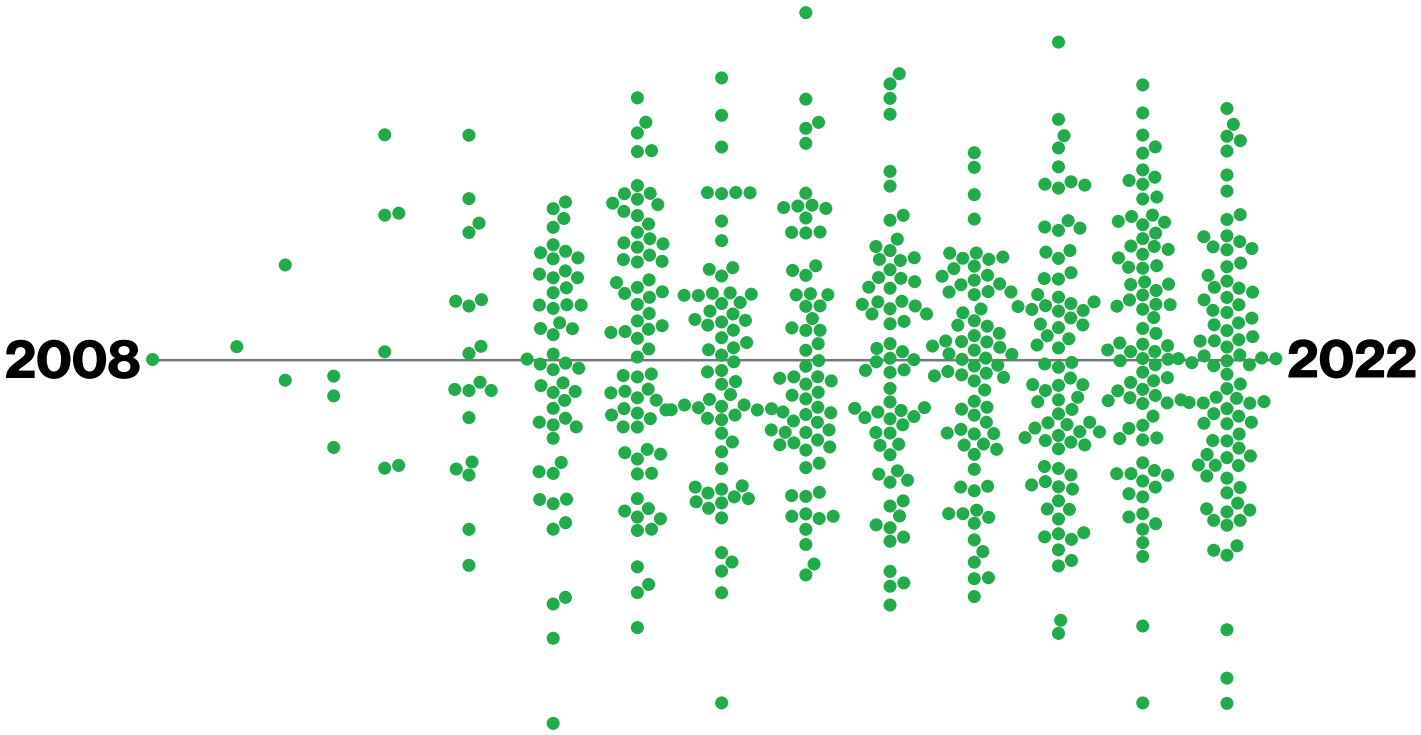
DBIR

2022 Data Breach Investigations Report

Executive Summary



Über die Titelseite

Unsere langjährigen Leser können sich vermutlich an die Titelseite unseres ersten Berichts im Jahr 2008 erinnern, auf der ein leerer Stuhl in einem Serverraum zu sehen war. Es sollte das Phänomen vermitteln, dass viele Unternehmen ihre Ressourcen und Daten nicht richtig pflegen. Die Titelseite von 2022 soll an diesen Bericht erinnern – sowohl aus Nostalgiegründen, als auch, um zu zeigen, dass viele Unternehmen weiterhin Schwierigkeiten haben, einen Überblick über ihre Mitarbeiter und Systeme zu behalten. Die Timeline mit dem Punktdiagramm (Jahresdarstellung) zeigt die Anzahl der global beteiligten Unternehmen und Organisationen, die uns im Laufe der vergangenen 15 Jahre unterstützt haben.

Inhaltsverzeichnis

Herzlich willkommen zur 15. Ausgabe des jährlich erscheinenden Verizon Data Breach Investigations Report

Seit 2018 präsentiert sich der DBIR als „Nachschlagewerk, das den Sicherheitsexperten moderner Unternehmen anhand praxisrelevanter Daten einen Überblick über gängige Bedrohungen durch kriminelle Hacker verschafft." In der aktuellen 15. Ausgabe setzen wir diese Tradition fort, indem wir Ihnen die Gefahren vorstellen, denen Ihr Unternehmen aktuell ausgesetzt ist. Außerdem legen wir mit Hilfe von Statistiken aus früheren Ausgaben dar, wie sich die Bedrohungslage in den letzten Jahren verändert hat.

Die vorliegenden Daten zeigen, dass das von vielerlei Herausforderungen geprägte letzte Jahr auch in Sachen Cyberkriminalität durchaus außergewöhnlich war. Finanziell motivierte Gruppen und skrupellose staatliche Hackerorganisationen traten in den zurückliegenden 12 Monaten so aggressiv wie selten zuvor auf und führten unter anderem massive, schlagzeilenträchtige Angriffe auf kritische Infrastrukturen und Lieferketten durch. Um diese Aktivitäten genau wie in den Vorjahren im Detail zu beleuchten, haben wir für den vorliegenden Bericht insgesamt 23.896 Vorfälle untersucht, von denen 5.212 als bestätigte Sicherheitsverletzungen gelten. Die entsprechenden Daten stammen zum einen aus dem Verizon Threat Research Advisory Center (VTRAC), zum anderen von 87 beteiligten Unternehmen und Organisationen aus aller Welt, ohne deren Unterstützung die Erstellung dieser Publikation nicht möglich gewesen wäre. Wir hoffen, dass Ihnen unser Bericht einen informativen Überblick über spartenübergreifende Risiken, die gängigsten Angriffsmethoden in Ihrer Branche sowie mögliche Maßnahmen zum Schutz Ihres Unternehmens und Ihrer Ressourcen bietet. Dabei versuchen wir in gewohnter Weise – wo immer dies möglich ist –, die Weiterentwicklung der Taktiken über die Jahre nachzuzeichnen, wie in Abbildung 1 und 2 dargestellt. Auf den folgenden Seiten finden Sie die wichtigsten Erkenntnisse aus dem diesjährigen DBIR in einer Kurzfassung, die Sie gern an Ihre Kollegen weiterleiten können. Zusätzlich ist der vollständige Bericht mit detaillierteren Angaben zu den aktuellen Bedrohungen zum Download verfügbar. Damit genug der einleitenden Worte: Lassen wir die Zahlen und Fakten sprechen.

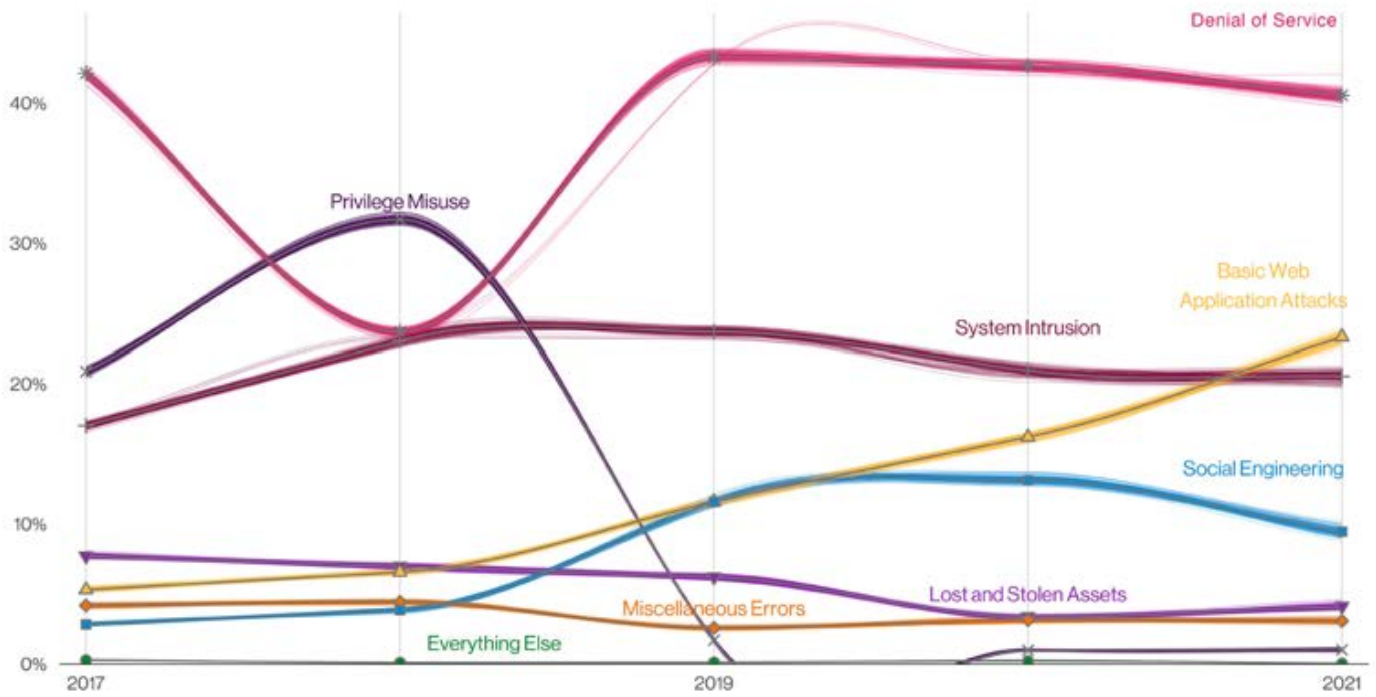


Abbildung 1: Vorfallsmuster im Laufe der Zeit

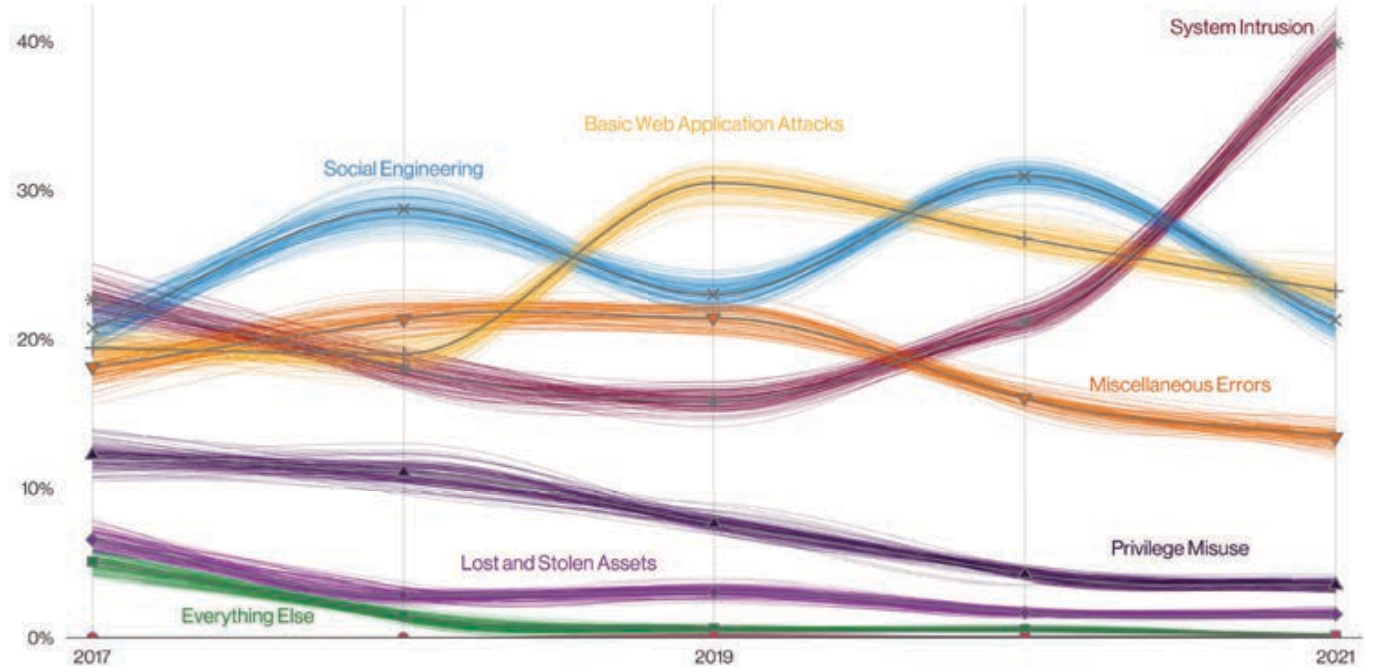


Abbildung 2: Muster der Sicherheitsverletzungen im Laufe der Zeit

Das Wichtigste in Kürze

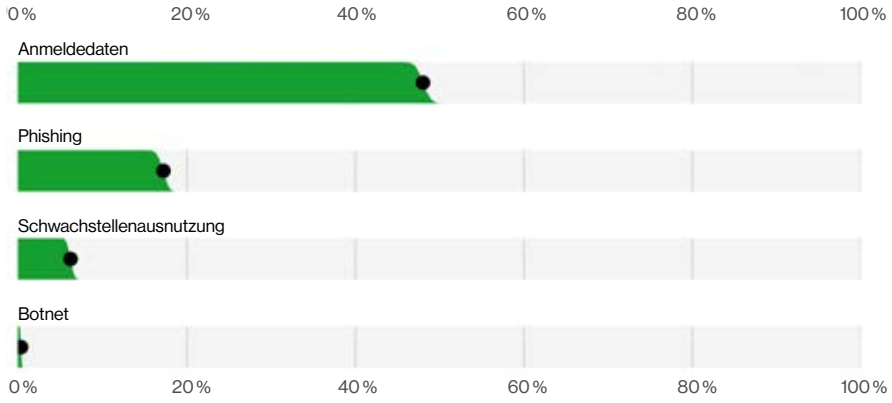


Abbildung 3: Anteil der Sicherheitsverstöße ohne Fehler oder Missbrauch (n=4.250)

Zu den vier gravierendsten Bedrohungen Ihrer IT-Infrastruktur zählen: der Missbrauch gestohlener Anmeldedaten, Phishing, die Ausnutzung vorhandener Schwachstellen und der Einsatz von Botnets. Da alle vier Gefahren in sämtlichen Abschnitten des DBIR eine prominente Rolle spielen, können Sie Ihr Unternehmen nur dann umfassend schützen, wenn Sie einen speziell darauf zugeschnittenen Sicherheitsplan implementieren.

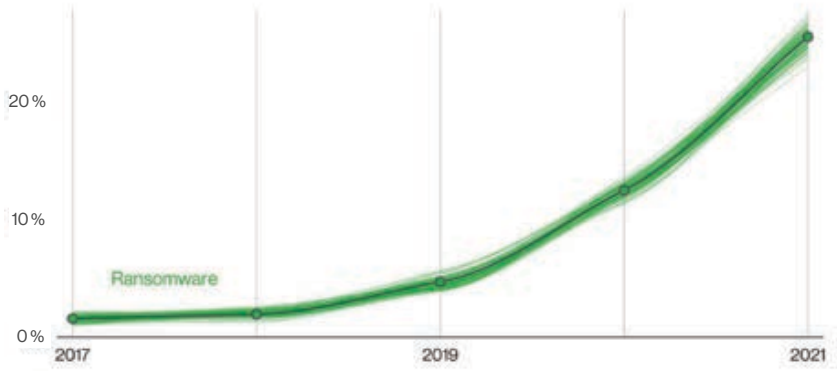


Abbildung 4: Nutzung von Ransomware bei Angriffen im Laufe der Zeit

Zugleich stieg die Zahl der Angriffe mit Ransomware um fast 13 Prozent (auf insgesamt 25 Prozent der Sicherheitsverletzungen) – und wuchs damit in einem Jahr so stark wie über die gesamten vorherigen fünf Jahre. Angesichts dieses beunruhigenden Trends sollten Sie sich stets ins Gedächtnis rufen, dass Ransomware erst in Ihre Infrastruktur eingeschleust werden muss, um ihren erpresserischen Zweck erfüllen zu können. Wenn Sie also effektive Maßnahmen gegen die vier eingangs genannten Bedrohungen ergreifen, schließen Sie zugleich die gängigsten Einfallstore für Ransomware.

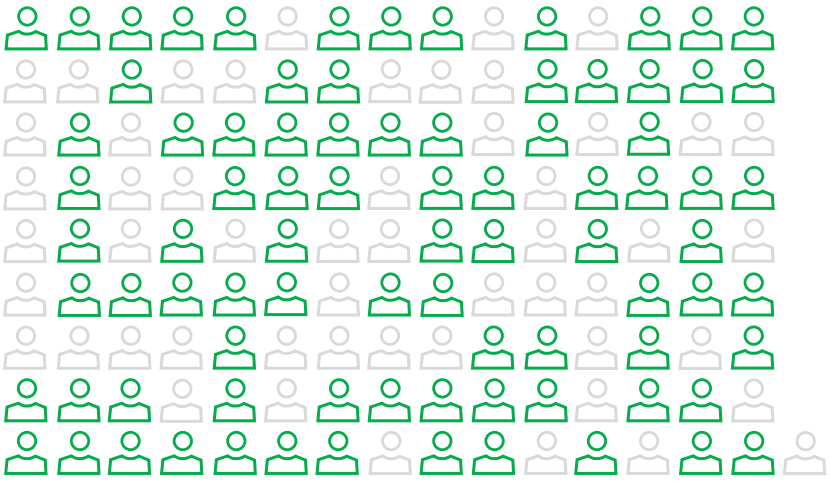


Abbildung 5: Partnerunternehmen als Angriffsvektor bei Systeminfiltrationen (n=3.403). Jedes Symbol steht für 25 Vorfälle.

Darüber hinaus hat sich 2021 gezeigt, dass schon die Infiltration einer einzelnen Lieferkette weitreichende Folgen haben kann. Lieferketten waren in 61 Prozent der Vorfälle betroffen. Ein Angriff auf Partnerunternehmen kann den Angreifern neue Handlungsspielräume eröffnen. Vor allem staatlich gesponsorte Gruppen entscheiden sich oft für eine solche Vorgehensweise und nutzen die Zugriffsrechte von Partnerunternehmen, um sich Zugang zur eigentlichen Zielumgebung zu verschaffen.

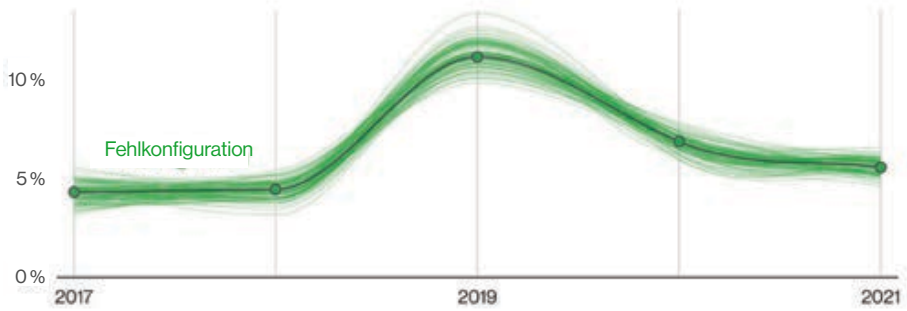


Abbildung 6: Fehlkonfigurationen bei Angriffen im Laufe der Zeit

Weiterhin von Bedeutung sind einfache Fahrlässigkeiten der Mitarbeiter, die für 14 Prozent der Sicherheitsverstöße verantwortlich sind, und falsch konfigurierte Datenspeicher in der Cloud. Die Verantwortlichen in den Unternehmen sollten keinesfalls davon ausgehen, dass ihre Belegschaft mittlerweile unfehlbar ist, nur weil dieses Muster 2021 im zweiten Jahr in Folge stagniert.

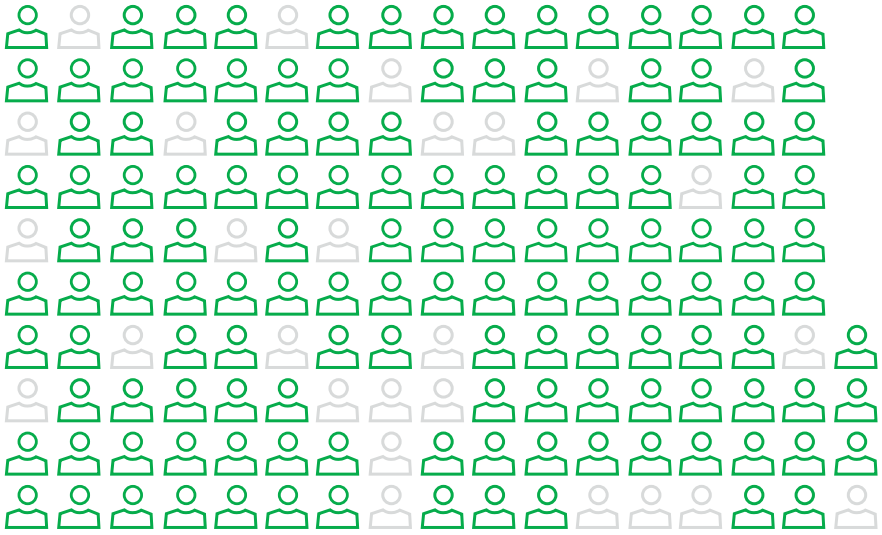


Abbildung 7: Der Faktor Mensch bei Sicherheitsverletzungen (n=4.110). Jedes Symbol repräsentiert 25 Sicherheitsverletzungen.

Und auch in anderer Hinsicht ist und bleibt der Faktor Mensch eine wichtige Größe: 82 % der Sicherheitsverletzungen dieses Jahres wurden durch menschliches Zutun ermöglicht. Gestohlene Anmeldedaten, erfolgreiches Phishing und verlorengegangene Geräte tragen immer wieder entscheidend zu Vorfällen und Datensicherheitsverletzungen bei.

Branchenspezifische Erkenntnisse

Obwohl Cyberkriminalität eine ernste Gefahr für Firmen aller Branchen und Größen darstellt, hängen Art und Häufigkeit der Angriffe bis zu einem gewissen Grad von der Beschäftigtenzahl, dem Geschäftsfeld und dem Standort Ihres Unternehmens ab. Deshalb benötigen Sie für eine effektive Cyberabwehr nicht nur einen Überblick über die allgemeine Bedrohungslage, sondern auch detaillierte Informationen über die für Sie relevanten Gefahren. Aus diesem Grund enthält der diesjährige Bericht wieder elf Spartenanalysen und – dieses Jahr neu – einen leicht verständlichen Abschnitt, der sich speziell an Kleinstunternehmen (mit zehn oder weniger Mitarbeitern) richtet. Und natürlich werfen wir gegen Ende einmal mehr einen Blick auf die in den verschiedenen Weltregionen dominanten Probleme. Wie immer orientieren wir uns bei den Spartenanalysen an der Brancheneinteilung des North American Industry Classification System (NAICS).

Hotel- und Gaststättengewerbe (NAICS 72)

Das Hotel- und Gaststättengewerbe verzeichnet seit 2016 einen stetigen Rückgang bei System Intrusion. Dennoch wird die Branche weiterhin von emailbasierten Malware-Kampagnen und dem unbefugten Zugriff auf Webanwendungen mithilfe gestohlener Anmeldedaten geplagt.

Absolute Häufigkeit	156 Vorfälle, davon 69 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	84 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, Denial-of-Service und einfache Angriffe auf Web-Anwedungen.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (90 %), Insider (10 %); alle Vorfälle: Externe Angreifer (95 %), Insider (5 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (91 %), Spionage (9 %); alle Vorfälle: Finanzielle Motive (64 %), Spionage (36 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (45 %), Personenbezogene Daten (45 %), Zahlungsdaten (41 %), Sonstige (18 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4)
Anhaltende Trends	Die Branche steht nach wie vor im Visier finanziell motivierter Krimineller, die es auf Zahlungsdaten und personenbezogene Daten abgesehen haben.

Medien und Unterhaltung (NAICS 71)

Die Spitzenplätze in dieser Branche belegen einmal mehr System Intrusion und einfache Angriffe auf Web-Anwendungen, die jedoch im Vergleich zum Vorjahr die Positionen getauscht haben. Sonstige Fehler findet sich unverändert auf Platz drei. Außerdem sind Denial-of-Service-Angriffe weiterhin ein gravierendes Problem, besonders im Bereich Glücksspiel.

Absolute Häufigkeit	215 Vorfälle, davon 96 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	80 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und sonstige Fehler.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (74 %), Insider (26 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (97 %), Rache (3 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (66 %), Anmeldedaten (49 %), Sonstige (23 %), Gesundheitsdaten (15 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4)
Anhaltende Trends	Die in den Vorjahren dominanten Muster stehen auch in diesem Jahr wieder im Vordergrund – allerdings in leicht veränderter Reihenfolge. Bemerkenswert ist außerdem, dass in dieser Branche weiterhin Gesundheitsdaten gestohlen werden.

Bildungswesen (NAICS 61)

Die Bedrohungs- und Sicherheitslage in diesem Sektor entwickelt sich weitgehend analog zu den anderen Branchen. Insbesondere verzeichnet das Bildungswesen einen drastischen Anstieg der Zahl der Ransomware-Angriffe (die nun über 30 % aller bestätigen Sicherheitsverletzungen ausmachen). Außerdem müssen die Unternehmen aus dieser Branche dem Diebstahl von Anmeldedaten und Phishing vorbeugen, um die personenbezogenen Daten ihrer Mitarbeiter und Studierenden vor unbefugtem Zugriff schützen zu können.

Absolute Häufigkeit	1.241 Vorfälle, davon 282 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	80 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und sonstige Fehler.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (75 %), Insider (25 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (95 %), Spionage (5 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (63 %), Anmeldedaten (41 %), Sonstige (23 %), Interna (10 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4)
Anhaltende Trends	Die im Bildungswesen zu beobachtenden Hacker-Attacken zielen weiterhin vorwiegend auf externe Infrastrukturen ab und werden mehrheitlich von externen Angreifern mit finanziellen Motiven durchgeführt. Zugleich zählen Fehler der Mitarbeiter zu den wichtigsten Ursachen der in dieser Branche erfassten Sicherheitsverletzungen.

Finanz- und Versicherungsbranche (NAICS 52)

Banken und Versicherer waren auch in diesem Jahr wieder beliebte Ziele von finanziell motivierten Hackern, die für ihre Operationen oft Methoden aus dem Bereich Social Engineering (Phishing) sowie gestohlene Anmeldedaten und Malware bzw. Ransomware nutzen. Ein weiteres gängiges Vorfallsmuster in der Branche sind Falschzustellungen und andere sonstige Fehler – dieser Trend ist seit drei Jahren ungebrochen.

Absolute Häufigkeit	2.527 Vorfälle, davon 690 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	79 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und sonstige Fehler.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (73 %), Insider (27 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (95 %), Spionage (4 %), Rache (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (71 %), Anmeldedaten (40 %), Sonstige (27 %), Bankdaten (22 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4), Maßnahmen zur Stärkung der Datensicherheit (CSC 3)
Anhaltende Trends	System Intrusion, einfache Angriffe auf Web-Anwendungen und sonstige Fehler sind in weiten Teilen dieser Branche weiterhin vorherrschend, genau wie im vorangegangenen Jahr.

Gesundheitswesen (NAICS 62)

In dieser Branche haben einfache Angriffe auf Web-Anwendungen sonstige Fehler als häufigste Ursache von Cybersicherheitsverletzungen abgelöst. Dennoch stellen Fahrlässigkeiten der Mitarbeiter weiterhin ein gravierendes Problem dar.

Absolute Häufigkeit	849 Vorfälle, davon 571 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	76 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und sonstige Fehler.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (61 %), Insider (39 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (95 %), Spionage (4 %), Mutwille (1 %), Rache (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (58 %), Gesundheitsdaten (46 %), Anmeldedaten (29 %), Sonstige (29 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4), Zugangskontrolle (CSC 6)
Anhaltende Trends	Die drei in den Vorjahren dominanten Muster stehen auch in diesem Jahr wieder im Vordergrund – allerdings in leicht veränderter Reihenfolge. Zugleich stimmt die Verteilung der Urheber der erfassten Bedrohungen (bis auf die Nachkommastellen) exakt mit den Werten aus dem Vorjahr überein.

IT und TK-Beratung (NAICS 51)

Hier belegt System Intrusion in Bezug auf die bestätigen Sicherheitsverletzungen den diesjährigen Spitzenplatz, gefolgt von sonstigen Fehlern und einfachen Web-Applikationen. In der Gesamtheit aller Vorfälle weist jedoch Denial-of-Service weiterhin die größte Häufigkeit auf. Außerdem ist die Frequenz bei Malware in den letzten beiden Jahren merklich gestiegen, während die Zahl der von Mitarbeitern verschuldeten Fahrlässigkeiten seit dem Erreichen des Höchstwerts vor fünf Jahren rückläufig ist.

Absolute Häufigkeit	2.561 Vorfälle, davon 378 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	81 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und sonstige Fehler.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (76 %), Insider (24 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (78 %), Spionage (20 %), Ideologie (1 %), Rache (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (66 %), Sonstige (35 %), Anmeldedaten (27 %), Interna (17 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4), Zugangskontrolle (CSC 6)
Anhaltende Trends	Einfache Angriffe auf Web-Anwendungen und sonstige Fehler sind in weiten Teilen dieser Branche weiterhin vorherrschend, genau wie im vorangegangenen Jahr.

Fertigungsindustrie (NAICS 31-33)

Fertigungsbetriebe sind auch in diesem Jahr wieder häufig von Spionageoperationen betroffen, werden parallel jedoch auch verstärkt zum Ziel von DoS-Angriffen, Hacking mithilfe gestohlener Anmeldedaten und Ransomware.

Absolute Häufigkeit	2.337 Vorfälle, davon 338 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	88 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (88 %), Insider (12 %), Partner (1 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (88 %), Spionage (11 %), Rache (1 %), von untergeordneter Bedeutung (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (58 %), Anmeldedaten (40 %), Sonstige (36 %), Interna (14 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4)
Anhaltende Trends	In der Fertigungsindustrie zählen System Intrusion und einfache Angriffe auf Web-Applikationen weiterhin zu den dominanten Bedrohungsmustern.

Bergbau-, Öl- und Gasindustrie plus Versorgungsbetriebe (NAICS 21 u. 22)

Dieser Sektor ist mit ähnlichen Bedrohungen wie die anderen von uns untersuchten Branchen konfrontiert. Dementsprechend häufig ist der Diebstahl von Anmeldedaten und die Verschlüsselung von Unternehmensdaten mit Ransomware. Darüber hinaus sind Phishing und andere Social-Engineering-Angriffe weit verbreitet.

Absolute Häufigkeit	403 Vorfälle, davon 179 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	95 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (96 %), Insider (4 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (78 %), Spionage (22 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (73 %), Personenbezogene Daten (22 %), Interna (9 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Management von Nutzerkonten (CSC 5)
Anhaltende Trends	Die Branche steht nach wie vor im Visier finanziell motivierter Angreifer, verzeichnet jedoch auch eine signifikante Zahl von Spionageoperationen.

Anbieter qualifizierter, technischer und wissenschaftlicher Dienstleistungen (NAICS 54)

In diesem Sektor erweisen sich Denial-of-Service-Angriffe als großes Problem, da diese Attacken stets drastische Folgen haben, auch wenn sie nur selten mit Datenverlusten einhergehen. Den Spitzenplatz in der Rangliste der Vorfalls- und Angriffsmuster belegt jedoch auch in diesem Jahr wieder System Intrusion, während die Social-Engineering-Angriffe auf Platz drei abrutschen.

Absolute Häufigkeit	3.566 Vorfälle, davon 681 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	89 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (84 %), Insider (17 %), verschiedene (1 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (90 %), Spionage (10 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (56 %), Personenbezogene Daten (48 %), Sonstige (26 %), Interna (14 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4)
Anhaltende Trends	Zu den drei häufigsten Mustern in dieser Branche zählen einmal mehr System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering – allerdings in einer im Vergleich zum Vorjahr geänderten Reihenfolge.

Öffentliche Verwaltung (NAICS 92)

Im öffentlichen Sektor belegt System Intrusion in diesem Jahr den Spitzenplatz unter den Angriffs- und Vorfallsmustern. Zugleich ist mit Blick auf die gleichbleibend hohe Zahl der bestätigen Sicherheitsverletzungen durch eigene Mitarbeiter festzustellen, dass diese sieben Mal häufiger auf Fehler und Fahrlässigkeiten als auf böswilliges Handeln der Insider zurückzuführen sind.

Absolute Häufigkeit	2.792 Vorfälle, davon 537 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	81 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und sonstige Fehler.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (78 %), Insider (22 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (80 %), Spionage (18 %), Ideologie (1 %), Rache (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (46 %), Anmeldedaten (34 %), Sonstige (28 %), Interna (28 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Management von Nutzerkonten (CSC 5)
Anhaltende Trends	Sonstige Fehler zählen auch in diesem Jahr wieder zu den drei häufigsten Vorfallsmustern und halten damit ihre Position vom Vorjahr.

Einzelhandel (NAICS 44-45)

Einzelhändler sind überwiegend mit denselben Arten von Angriffen wie im letzten Jahr konfrontiert. Dazu zählen der Missbrauch gestohlener Anmeldedaten sowie Phishing und Ransomware.

Absolute Häufigkeit	629 Vorfälle, davon 241 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	84 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (87 %), Insider (13 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (98 %), Spionage (2 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (45 %), personenbezogene Daten (27 %), sonstige Daten (25 %), Zahlungsdaten (24 %)
Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Zugangskontrolle (CSC 6), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4)
Anhaltende Trends	Die Angriffe auf Einzelhändler gehen nach wie vor von verschiedenartigen Akteuren aus und basieren auf diversen Taktiken, darunter gängige Methoden wie Phishing oder die Infektion von Online-Zahlungsplattformen mit Malware zur Ausspähung von Kreditkartendaten.

Kleinstunternehmen

Wenn Cyberangriffe Schlagzeilen machen, ist meist ein bekannter Großkonzern betroffen. Das sollte jedoch nicht darüber hinwegtäuschen, dass kleine und kleinste Unternehmen ebenfalls lukrative Ziele für Kriminelle darstellen.

Viele Angreifer sind alles andere als wählerisch und nutzen jede sich bietende Gelegenheit gnadenlos aus. Die daraus resultierenden Vorfälle haben schon so manche kleinere Firma in den Konkurs getrieben. Deshalb sind auch Kleinstunternehmen (mit höchstens 10 Mitarbeitern) dringend aufgefordert, sich durch vorbeugende Maßnahmen zu schützen.

Aus unserem Datensatz geht hervor, dass die größte Bedrohung für diese Betriebe von Ransomware ausgeht. Dabei infizieren die Kriminellen die anvisierte IT-Infrastruktur mit einer bestimmten Art von Schadsoftware, die nach ihrer Aktivierung die Daten des betroffenen Unternehmens verschlüsselt und dann als Druckmittel zur Erpressung eines (oft recht hohen) Lösegelds für die Entschlüsselung dient. Die zweithäufigste Angriffsmethode in diesem Segment ist der Missbrauch gestohlener Anmeldedaten (bestehend aus Benutzername und Passwort). Um diese Daten zu erlangen, nutzen die Hacker zum einen die Brute-Force-Methode (bei der in rascher Folge eine Vielzahl von Kombinationen aus Buchstaben, Symbolen und Zahlen durchprobiert wird), zum anderen verschiedene Arten von Malware (weshalb eine aktuelle Antiviruslösung von großem Nutzen ist) sowie das sogenannte Credential Stuffing (bei dem erbeutete Anmeldedaten anderer Websites für den Zugriff auf Unternehmenskonten missbraucht werden). Ebenfalls gängig sind Phishing und andere Social-Engineering-Angriffe, bei denen die Kriminellen ihren Opfern unter Vorspiegelung falscher Tatsachen sensible Informationen entlocken.

Diese Kampagnen können täuschend echt wirken (und beispielsweise auf gefälschten Rechnungen eines bekannten Zulieferers mit geänderten Kontodaten basieren). Die entsprechenden Nachrichten werden meist per E-Mail zugestellt. Allerdings gibt es auch Fälle, in denen die Kriminellen ihre Opfer am Telefon von der Legitimität ihres „Anliegens“ überzeugen.

Wenn Sie im Detail erfahren möchten, wie Sie Ihr Unternehmen schützen und wen Sie im Verdachts- oder Ernstfall um Unterstützung bitten können, finden Sie im im Kapitel „Very Small Businesses“ der vollständigen Ausgabe des DBIR eine ausführliche Liste mit praktischen Empfehlungen.

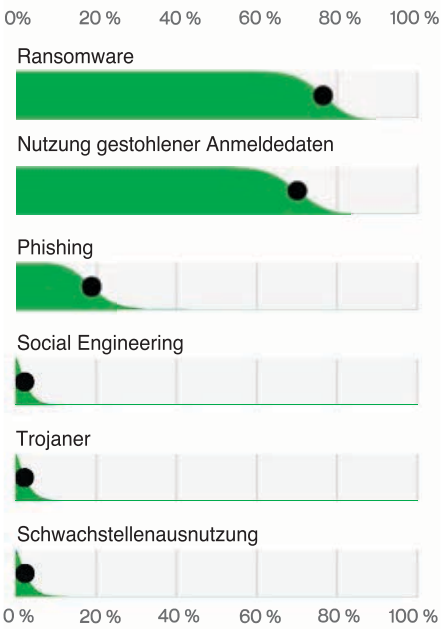


Abbildung 8: Bei Angriffen auf Unternehmen mit 1 bis 10 Mitarbeitern genutzte Methoden (n=61)

Ergebnisse für spezifische Regionen

In dieser Ausgabe des DBIR präsentieren wir zum dritten Mal regionsspezifische Vorfallsdaten und Erkenntnisse, um unsere Leser über weltweite Trends und Unterschiede in Sachen Cyberkriminalität zu informieren. Allerdings ist dabei (wie schon in den Vorjahren) zu beachten, dass Umfang und Detailgenauigkeit unserer regionalen Analysen von zahlreichen Faktoren abhängen, darunter die Präsenz der an der Berichterstellung beteiligten Partner, landesspezifische gesetzliche Meldevorgaben und die Arbeitsbelastung unserer Mitarbeiter.

Asien-Pazifik (APAC)

Asien-Pazifik verzeichnet eine große Zahl von Social-Engineering-Angriffen und Hackereinbrüchen, ist jedoch im Vergleich zu anderen Regionen in deutlich geringerem Maße von Ransomware betroffen.

Absolute Häufigkeit	4.114 Vorfälle, davon 283 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	98 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (98 %), Insider (2 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (54 %), Spionage (46 %), von untergeordneter Bedeutung (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (72 %), Interna (26 %), Betriebsgeheimnisse (18 %), Sonstige (11 %)
Anhaltende Trends	In der Region APAC dominieren weiterhin einfache Angriffe auf Web-Anwendungen sowie Social-Engineering-Angriffe.

Europa, Naher Osten und Afrika (EMEA)

Der deutliche Anstieg der Zahl der Social-Engineering-Angriffe in dieser Region unterstreicht die Notwendigkeit zur Implementierung entsprechender Kontrollen und Gegenmaßnahmen. Zugleich erweist sich der Diebstahl von Anmeldedaten als großes Problem, was unter anderem an der konstant hohen Zahl der einfachen Angriffe auf Web-Anwendungen ersichtlich wird.

Absolute Häufigkeit	1.093 Vorfälle, davon 307 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	97 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (97 %), Insider (3 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (79 %), Spionage (21 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (67 %), Interna (67 %), Betriebsgeheimnisse (20 %), Sonstige (18 %)
Anhaltende Trends	Die drei häufigsten Muster sind dieselben wie im Vorjahr, allerdings in geänderter Reihenfolge. Des Weiteren zeigt sich, dass die überwiegende Mehrzahl der Sicherheitsverletzungen in dieser Region durch externe Angreifer verursacht wird.

Nordamerika (NA)

In dieser Region belegen Systeminfiltrationen erstmals den Spitzenplatz unter den Angriffs- und Vorfallsmustern. Damit führt Social Engineering nicht länger die Rangliste der häufigsten Bedrohungen an, obwohl Phishing und verwandte Angriffe weiterhin ein großes Problem in Nordamerika darstellen. Außerdem werden viele hier ansässige Unternehmen nach wie vor zum Ziel einfacher Angriffe auf Web-Anwendungen.

Absolute Häufigkeit	4.504 Vorfälle, davon 1.638 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	90 Prozent der erfassten Sicherheitsverletzungen entfallen auf die Kategorien System Intrusion, einfache Angriffe auf Web-Anwendungen und Social Engineering.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (90 %), Insider (10 %), verschiedene (1 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (96 %), Spionage (3 %), Rache (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (66 %), Interna (21 %), Personenbezogene Daten (20 %), Sonstige (20 %)
Anhaltende Trends	Die drei häufigsten Muster sind dieselben wie im Vorjahr, allerdings in geänderter Reihenfolge. Des Weiteren zeigt sich, dass viele Sicherheitsverletzungen in dieser Region durch externe Angreifer verursacht werden.

Immer am Puls der Zeit

Das DBIR-Team arbeitet ständig an der Erweiterung und Verbesserung des zur Klassifizierung und Analyse von Sicherheitsvorfällen verwendeten VERIS-Frameworks (Vocabulary for Event Recording and Incident Sharing). Für den diesjährigen Bericht haben wir eine Darstellungweise entwickelt, die auf der MITRE ATT&CK Matrix und den Empfehlungen des Center for Internet Security basiert und Unternehmen die Entwicklung und Umsetzung eines datengestützten Cybersicherheitsprogramms erleichtern soll. Außerdem arbeiten wir gemeinsam mit anderen InfoSec-Spezialisten an Attack Flow – einem Projekt zur Erstellung eines neuen Datenformats, das die Beschreibung der verschiedenen Angriffsschritte erleichtert und standardisiert. Dadurch sind unsere Analysen aussagekräftiger und können von der Cybersicherheits-Community nutzbringend eingesetzt werden.

Best Practices

Auch in diesem Jahr bieten wir Ihnen konkrete Vorschläge für praktische Maßnahmen zur Stärkung der Sicherheit. Die im Folgenden aufgeführten Best Practices sind Ergebnis eines Abgleichs der im DBIR präsentierten Daten mit den vom Center for Internet Security empfohlenen Critical Security Controls (CSC) und unserer Ansicht nach für die meisten Unternehmen lohnenswert.

CSC 3 – Maßnahmen zur Stärkung der Datensicherheit

Hier geht es um die Implementierung von Prozessen und Technologien zur Identifizierung, Klassifizierung und sicheren Handhabung aller Arten von Unternehmensdaten. Durch entsprechende Maßnahmen können die Verantwortlichen verhindern, dass vertrauliche Daten versehentlich per E-Mail versendet oder infolge von Fehlkonfigurationen offengelegt werden.

CSC 4 – Sichere Konfiguration der Unternehmensressourcen und -software

Hinter diesem Wortungetüm verbergen sich vielfältige Maßnahmen, die sicherstellen sollen, dass neu eingerichtete Lösungen nicht im Nachhinein um aufgesetzte Schutzmaßnahmen erweitert werden müssen, weil sie von Anfang an über integrierte Sicherheitsmechanismen verfügen. Die Umsetzung dieses Prinzips hilft bei der Vermeidung von manuellen Fehlern und daraus resultierenden Sicherheitsverletzungen und ermöglicht beispielsweise die Prävention von Datenlecks durch den Einsatz von Remote-Löschfunktionen auf verlorengegangenen Mobilgeräten.

CSC 5 – Management von Nutzerkonten

Diese Maßnahmen zielen vor allem auf eine effektivere Verwaltung des Zugriffs auf Nutzerkonten und die Vereitelung von Brute-Force- und Credential-Stuffing-Angriffen.

CSC 6 – Zugangskontrolle

Durch ein effektives Management der Rechte und Privilegien Ihrer Nutzer und die Implementierung von Multifaktor-Authentifizierungsverfahren können Sie wichtige Komponenten Ihrer Infrastruktur schützen und den Nutzen gestohlener Anmeldedaten (für die Angreifer) minimieren.

CSC 14 – Schulungen zur Steigerung des Sicherheitsbewusstseins

Sicherheitsschulungen haben eine lange Tradition und bedürfen daher keiner näheren Erklärung. In Anbetracht der auffallenden Häufigkeit fahrlässiger Verhaltensweisen und der hohen Virulenz von Social-Engineering-Angriffen kann kein Zweifel daran bestehen, dass eine Investition in entsprechende Trainingseinheiten entscheidend zum Schutz Ihres Unternehmens beiträgt.

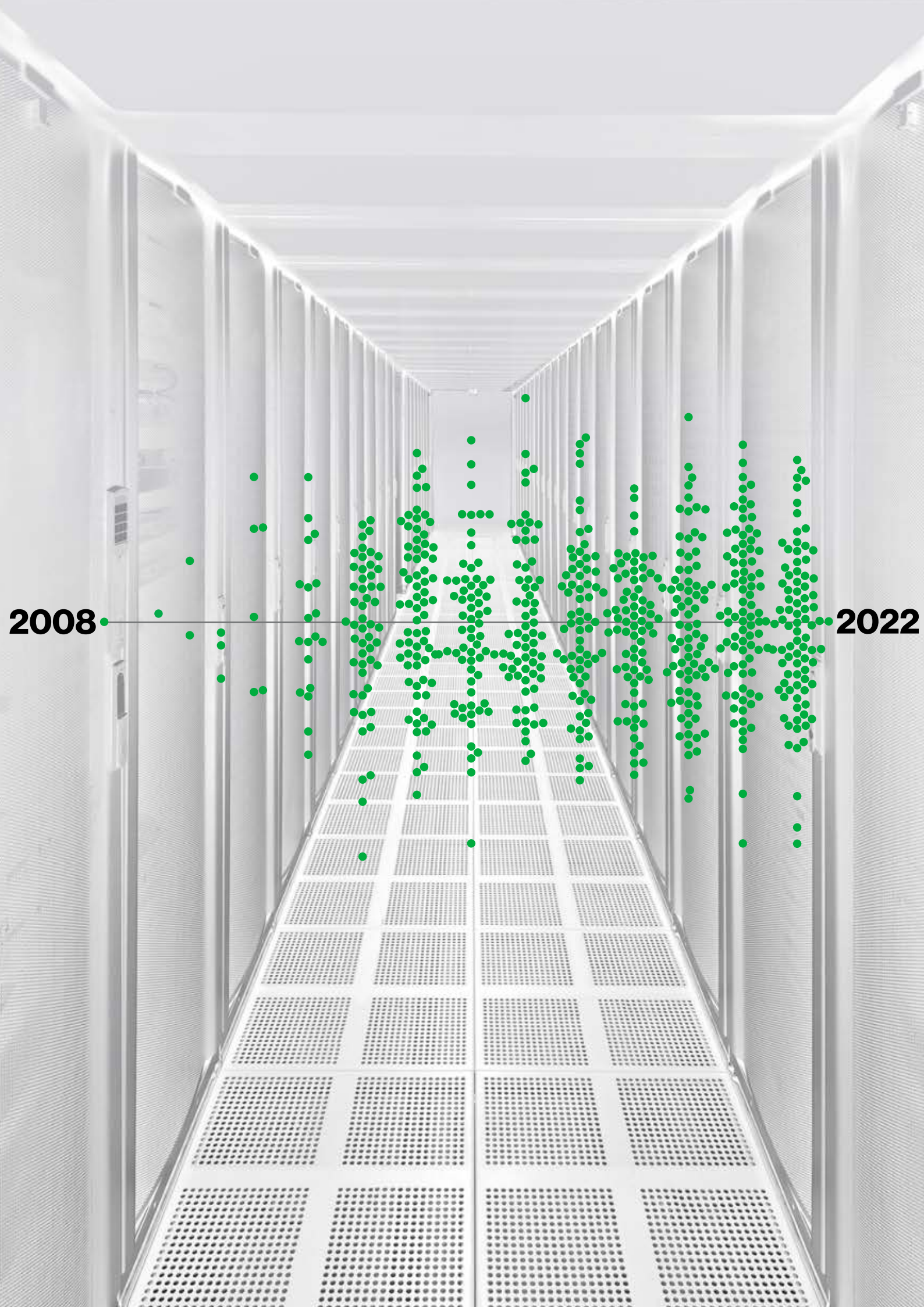
Halten Sie sich und Ihr Team auf dem Laufenden

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 alle Zahlen, Daten und Fakten, die für fundierte Maßnahmen zum Schutz Ihres Unternehmens und zur Stärkung des Sicherheitsbewusstseins Ihrer Mitarbeiter erforderlich sind.

Holen Sie sich den vollständigen DBIR 2022 unter https://www.verizon.com/business/de-de/resources/reports/dbir/.

Möchten Sie dazu beitragen, die Welt sicherer zu machen?

Der DBIR basiert auf Beiträgen von Dutzenden von Unternehmen und könnte mit Ihrer Beteiligung noch besser werden. Falls Sie interessiert sind oder 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)


2008
2022