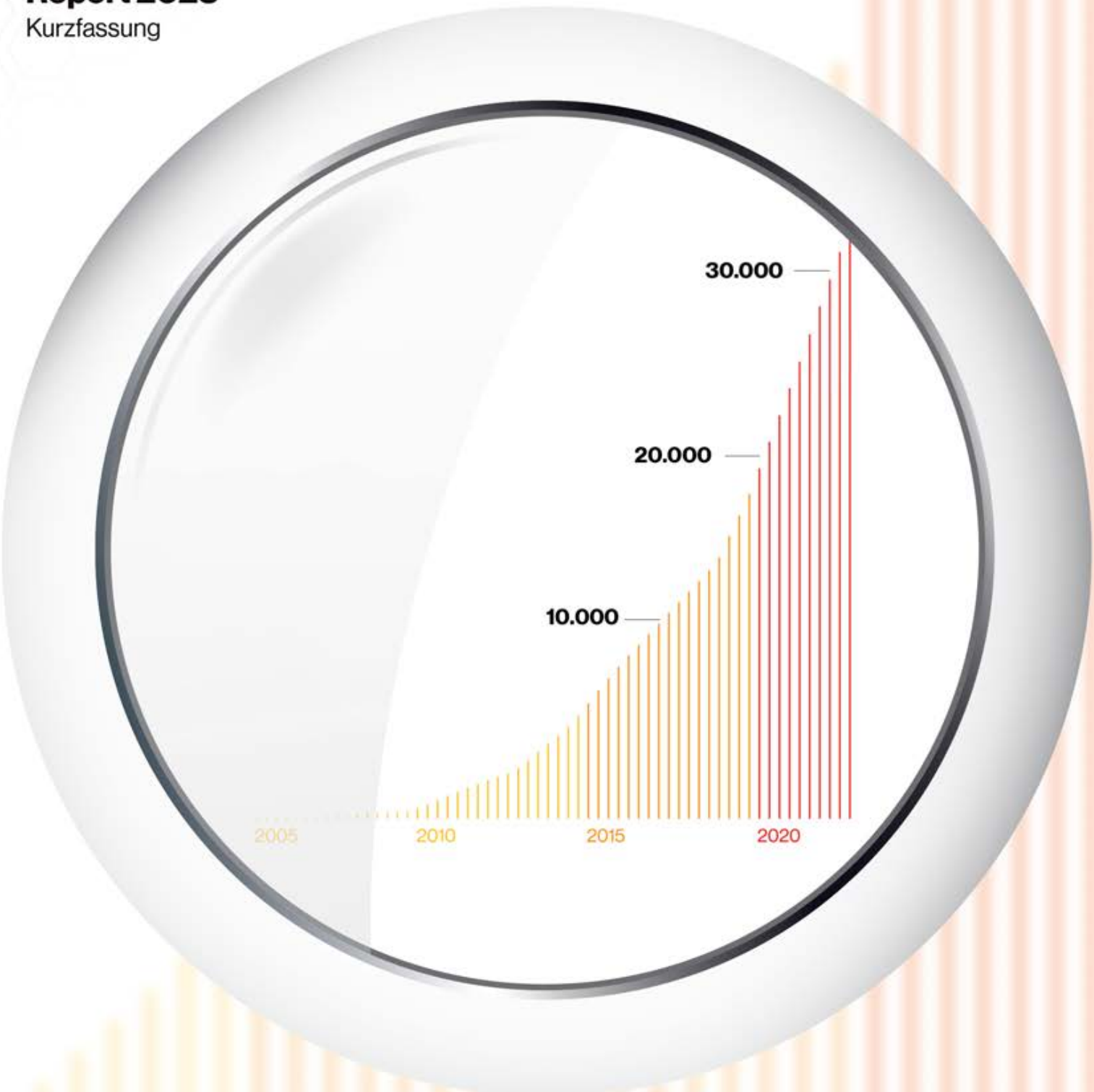
DBIR

Data Breach Investigations Report 2023

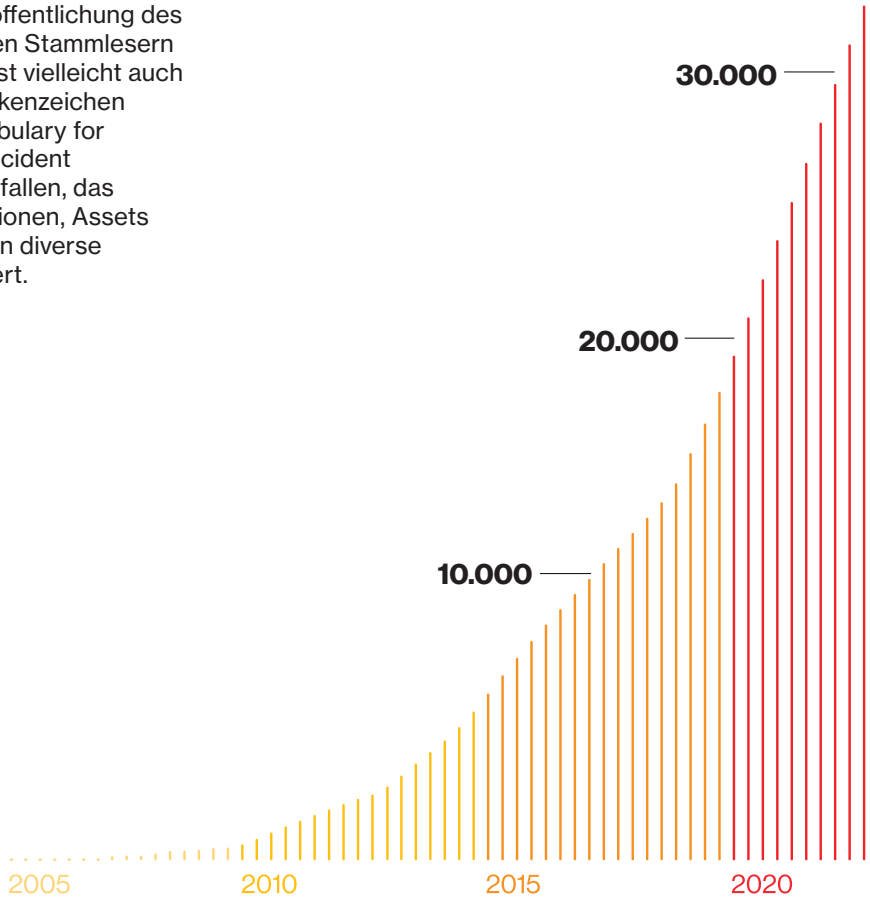
Kurzfassung



verizon

Über die Titelseite

Mit der Lupe auf der Titelseite wollen wir darauf hinweisen, dass unser Team seine Energie und seine Ressourcen im diesjährigen Berichtszeitraum wieder mehr auf den Kerndatensatz zu Angriffen konzentriert hat. Das vergrößerte Diagramm zeigt die Gesamtzahl der Angriffe in diesem Datensatz seit der Veröffentlichung des ersten Berichts. Unseren Stammlesern und Stammleserinnen ist vielleicht auch das wabenförmige Markenzeichen des Frameworks „Vocabulary for Event Recording and Incident Sharing“ (VERIS) aufgefallen, das die vier A (Akteure, Aktionen, Assets und Attribute) und deren diverse Auflistungen symbolisiert.



Inhaltsverzeichnis

Willkommensgruß

Hallo und herzlich willkommen zur 16. Ausgabe des jährlich erscheinenden Verizon Data Breach Investigations Report (DBIR).

Mit dem DBIR wollen wir Sicherheitsprofis eine detaillierte, datenbasierte Analyse echter Cyberangriffe und anderer Formen der Cyberkriminalität vorlegen und beschreiben, wie diese in Unternehmen und Organisationen verschiedener Größenordnungen in unterschiedlichen Branchen und geografischen Regionen verlaufen. Wir hoffen, dass wir Ihnen damit Einblicke in die spezifischen Bedrohungen vermitteln können, die Ihnen in Ihrer Tätigkeit mit der größten Wahrscheinlichkeit begegnen werden, sodass Sie die effektivsten Gegenmaßnahmen vorbereiten können.

Wie in früheren Jahre ermitteln wir, welche Rückschlüsse sich aus unseren Daten über die Cyberkriminellen und deren Tools ziehen lassen. In diesem Jahr haben wir 16.312 Vorfälle untersucht, von denen 5.199 als bestätigte Sicherheitsverletzungen gelten. Die entsprechenden Daten stammen zum einen aus dem Verizon Threat Research Advisory Center (VTRAC), das in diesem Jahr 20 Jahre alt wird, und zum anderen von 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. Auf den folgenden Seiten finden Sie die wichtigsten Erkenntnisse aus dem diesjährigen DBIR in einer Kurzfassung, die Sie gern an Ihre Kollegen und Kolleginnen weiterleiten können. Zusätzlich ist der vollständige Bericht mit detaillierteren Angaben zu den aktuellen Bedrohungen zum Download verfügbar.

Angriffs- und Vorfallsmuster im Zeitverlauf

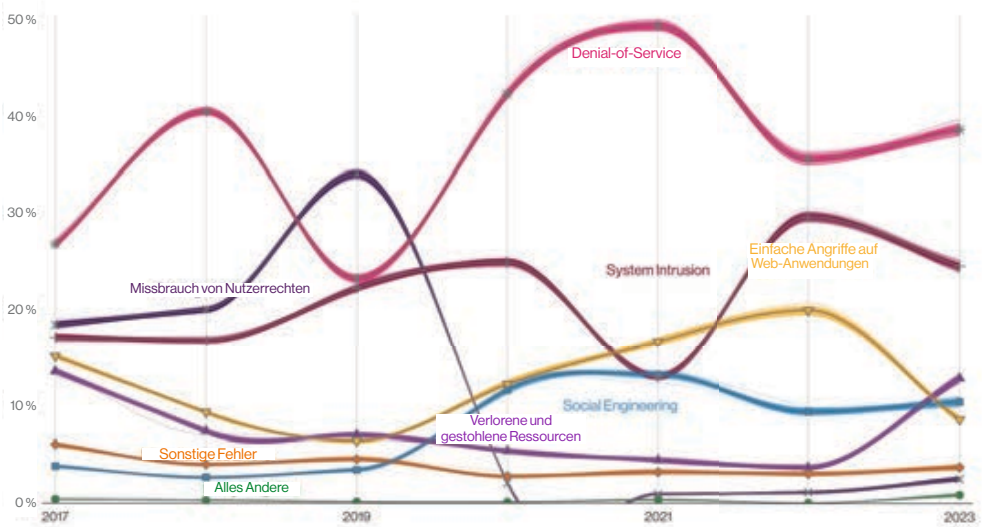


Abbildung 1: Vorfallskategorien im Zeitverlauf

Mitunter lohnt es sich, einen Blick zurückzuwerfen, um zu sehen, wie sich die Vorfallsverteilung von Jahr zu Jahr entwickelt. Abbildung 1 zeigt, dass die meisten Vorfälle – wie schon seit mehreren Jahren – in die Kategorie Denial-of-Service fallen.

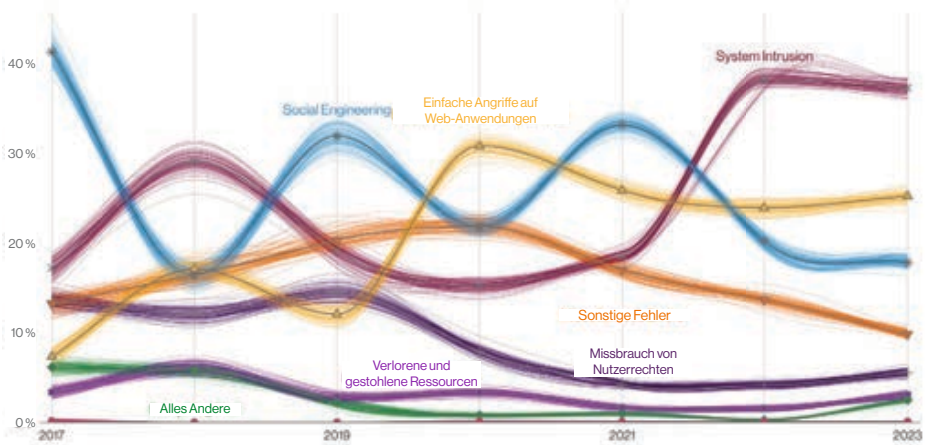
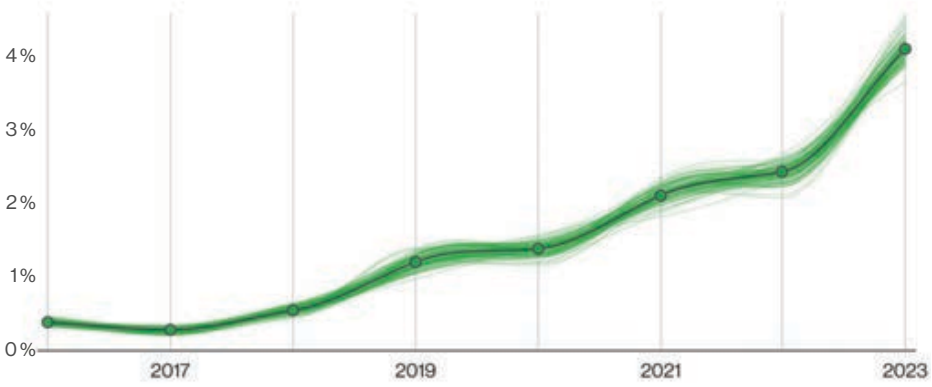


Abbildung 2: Muster der Sicherheitsverletzungen im Laufe der Zeit

Wenn wir uns hingegen auf Vorfälle mit belegten Datenverlusten beschränken, ergibt sich ein anderes Bild (Abbildung 2).

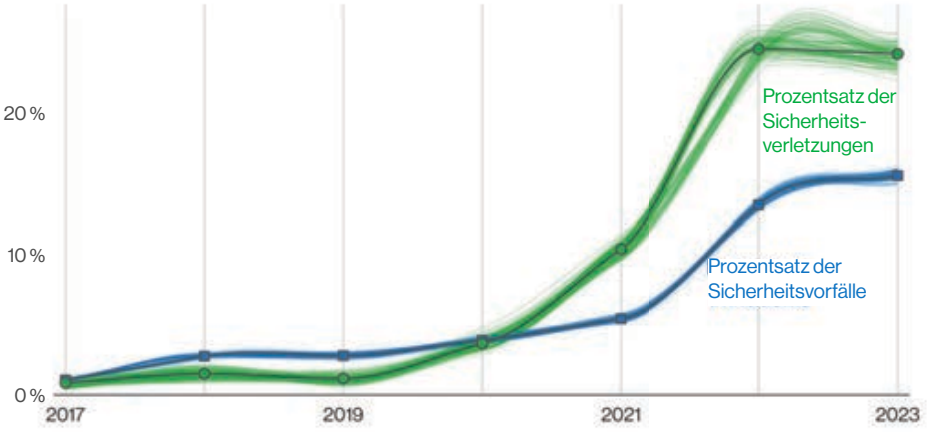
Vorfälle des Typs System Intrusion, die sich durch komplexere Angriffsverläufe auszeichnen, nehmen zu. Dabei handelt es sich meist um mehrstufige Angriffe, bei denen oft auch Ransomware eingesetzt wird. Doch wir greifen vor. Sehen wir uns zunächst einige der wichtigsten Untersuchungsergebnisse aus dem diesjährigen Bericht an.

Das Wichtigste in Kürze



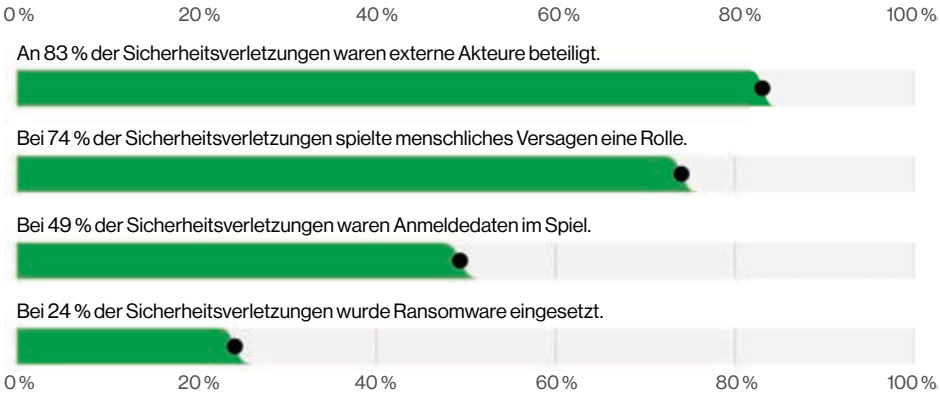
Social-Engineering-Angriffe sind oft sehr effektiv und für Cyberkriminelle äußerst lukrativ. Das ist vielleicht ein Grund dafür, dass sich die Anzahl der CEO-Fraud-Angriffe (die im wesentlichen eine Form von Pretexting sind) über alle Vorfälle hinweg fast verdoppelt hat (siehe Abbildung 3), sodass sie nun mehr als 50 % aller Social-Engineering-Vorfälle ausmachen.

Abbildung 3: Pretexting-Vorfälle im Zeitverlauf



Ransomware ist weiterhin eine der bei Angriffen meistgenutzten Methoden. Ihr Anteil am Gesamtvolumen ist zwar nicht gestiegen, hat sich aber auf dem hohen Niveau von 24 % gehalten. Ransomware wurde in Unternehmen und Institutionen aller Größenordnungen und in allen Branchen beobachtet.

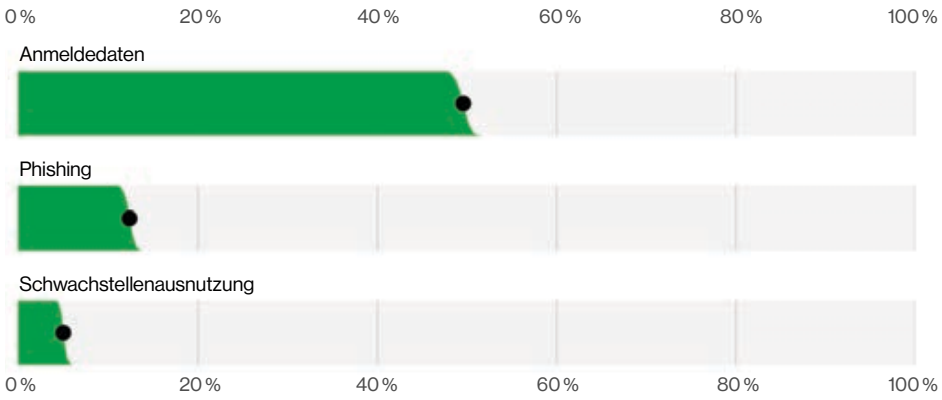
Abbildung 4: Ransomware-Aktionsvarianten im Zeitverlauf



Bei 74 % der Angriffe wurden menschliche Schwächen ausgenutzt, zum Beispiel in Form von Bedienfehlern, Missbrauch von Nutzerrechten, Nutzung gestohlener Anmeldedaten oder Social Engineering.

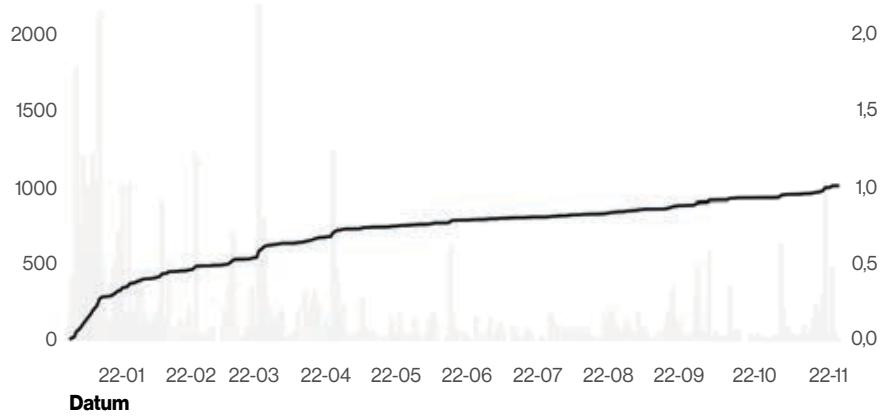
83 % der Angriffe wurde von Außenseitern verübt und finanzielle Bereicherung ist mit 95 % nach wie vor das weitaus häufigste Motiv.

Abbildung 5: Einige wichtige Zahlen



Gestohlene Anmeldedaten, Phishing und das Ausnutzen von Schwachstellen sind die drei Methoden, mit denen Angreifer sich am häufigsten Zugang zu fremden Umgebungen verschaffen.

Abbildung 6: Einige wichtige Ergebnisse zu Sicherheitsverstößen ohne Bedienfehler oder Missbrauch (n = 4.291)



Über 32 % aller 2022 beobachteten Log4j-Scans fanden in den ersten 30 Tagen nach der Veröffentlichung der Schwachstelle statt. (Die größte Anzahl wurde innerhalb der ersten 17 Tage beobachtet.)

Abbildung 7: Verteilung der Log4j-Scans im Verlauf des Jahres 2022

Log4j beschäftigte unsere an der Berichterstellung beteiligten Partner so sehr, dass bei 90 % der gemeldeten Vorfälle, die als Schwachstellenausbeutung klassifiziert wurden, „Log4j“ oder „CVE-2021-4428“ im Kommentar stand. Allerdings waren nur 20,6 % der Vorfälle mit Kommentaren versehen.

Abbildung 8: Anteil der identifizierten Exploit-Angriffe, bei denen Log4j ausgenutzt wurde (n = 394). Jedes Symbol steht für einen Vorfall.

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. Auch in diesem Jahr haben wir zehn Spartenanalysen erstellt.

Branchenbezeichnungen

Im Rahmen unserer DBIR-Berichte nutzen wir das nordamerikanische Branchenklassifizierungssystem NAICS, um die betroffenen Unternehmen und Institutionen Branchen zuzuordnen.

NAICS nutzt zwei- bis sechsstellige Codes, um Unternehmen und Organisationen zu klassifizieren. Unsere Analysen finden in der Regel auf der zweistelligen Ebene statt und wir nennen die NAICS-Codes gemeinsam mit der Branchenbezeichnung. Wenn ein Diagramm also beispielsweise mit „Öffentliche Verwaltung (NAICS 92)“ beschriftet ist, ist die 92 nicht als Wert zu verstehen. 92 ist der NAICS-Code für die öffentliche Verwaltung. Ausführliche Informationen über die Codes und das Klassifizierungssystem finden Sie unter: https://www.census.gov/naics/?58967?yearbck=2012

Hotel- und Gaststättengewerbe

(NAICS 72)

Absolute Häufigkeit	254 Vorfälle, davon 68 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering machten 90 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (93 %), Insider (9 %), Mehrere Akteure (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (100 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Zahlungsdaten (41 %), Anmeldedaten (38 %), Personenbezogene Daten (34 %), Sonstige (26 %)
Anhaltende Trends	Die drei häufigsten Angriffsmuster sind dieselben wie im vorigen Jahr, aber in veränderter Reihenfolge. Externe Angreifer versuchen weiterhin, die luktrativen Daten der Unternehmen dieser Branche zu stehlen.
Zusammen-fassung	Zahlungskartendaten sind weiterhin das bevorzugte Ziel in dieser Branche, wie zu erwarten war. Die Nutzung von RAM-Scrapern durch finanziell motivierte Angreifer bleibt eine konstante Gefahr.

Bildungswesen

(NAICS 61)

Absolute Häufigkeit	497 Vorfälle, davon 238 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, sonstige Fehler und Social Engineering machten 76 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (72 %), Insider (29 %), Mehrere Akteure (1 %), Partner (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (92 %), Spionage (8 %), Mutwille (1 %), Spaß (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (56 %), Anmeldedaten (40 %), Sonstige (25 %), Insider (20 %)
Anhaltende Trends	System Intrusions und sonstige Fehler gehörten wieder zu den drei häufigsten Angriffs- und Vorfallsmustern in dieser Branche. Auch das Verhältnis zwischen externen Angreifern und Insidern ist nahezu konstant geblieben.
Zusammenfassung	Einfache Angriffe auf Web-Anwendungen wurden von Social Engineering aus den Top-Drei verdrängt. Ransomware spielt in diesem Sektor weiterhin eine große Rolle.

Finanz- und Versicherungsbranche

(NAICS 52)

Absolute Häufigkeit	1.832 Vorfälle, davon 480 mit bestätigten Datenlecks
Vorherrschende Muster	Einfache Angriffe auf Web-Anwendungen, sonstige Fehler und System Intrusions machten 77 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (66 %), Insider (34 %), Mehrere Akteure (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (97 %), Spionage (3 %), Mutwille (1 %), Ideologische Motive (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (74 %), Anmeldedaten (38 %), Sonstige (30 %), Bankdaten (21 %)
Anhaltende Trends	Die drei häufigsten Muster sind dieselben wie im Vorjahr, allerdings in veränderter Reihenfolge. Personenbezogene Daten, die für Betrugsversuche aller Art nützlich sind, bleiben die am häufigsten gestohlene Datenart.
Zusammenfassung	Aus der Tatsache, dass einfache Angriffe auf Web-Anwendungen das häufigste Muster sind, lässt sich schließen, dass es Angreifern keine große Mühe bereitet, sich Zugang zu verschaffen. Gemeinsam mit der Menge der Falschzustellungen deutet dies darauf hin, dass bessere Kontrollen einen erheblichen Anteil der Angriffe in diesem Sektor verhindern könnten.

Gesundheitswesen

(NAICS 62)

Absolute Häufigkeit	525 Vorfälle, davon 436 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, einfache Angriffe auf Web-Anwendungen und sonstige Fehler machten 68 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (66 %), Insider (35 %), Mehrere Akteure (2 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (98 %), Spionage (2 %), Spaß (1 %), Ideologische Motive (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (67 %), Gesundheitsdaten (54 %), Anmeldedaten (36 %), Sonstige (17 %)
Anhaltende Trends	Die drei häufigsten Muster sind dieselben wie im Vorjahr, allerdings in veränderter Reihenfolge. Fehler durch Benutzer aus den eigenen Reihen sind in diesem Sektor nach wie vor eine große Herausforderung.
Zusammenfassung	Ransomware-Erpresser greifen diese Branche weiterhin an und stehlen dabei immer häufiger auch Daten. Fehler (insbesondere Falschzustellungen) treten nach wie vor häufig auf. Außerdem stellen auch Insiderbedrohungen eine nicht zu unterschätzende Gefahr dar.

IT und TK-Beratung

(NAICS 51)

Absolute Häufigkeit	2.110 Vorfälle, davon 384 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering machten 77 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (81 %), Insider (20 %), Mehrere Akteure (2 %), Partner (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (92 %), Spionage (8 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (51 %), Anmeldedaten (37 %), Sonstige (35 %), Insider (19 %)
Anhaltende Trends	System Intrusions sind weiterhin das häufigste Angriffsmuster in dieser Branche und finanzielle Motive die häufigste Angriffsursache.
Zusammenfassung	Der Anteil der Ausnutzung von Fehlern als Angriffs- und Vorfallsmuster ist seit mehreren Jahren rückläufig. In diesem Jahr wurden sie von Social Engineering aus den Top-Drei verdrängt. 70 % der Vorfälle im Sektor NAICS 51 sind Denial-of-Service-Angriffe.

Fertigung

(NAICS 31–33)

Absolute Häufigkeit	1.817 Vorfälle, davon 262 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 83 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (90 %), Insider (11 %), Mehrere Akteure (2 %), Partner (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (96 %), Spionage (4 %), Mutwille (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (60 %), Anmeldedaten (38 %), Sonstige (37 %), Insider (18 %)
Anhaltende Trends	Die drei häufigsten Muster sind dieselben wie im Vorjahr, allerdings in veränderter Reihenfolge. Finanziell motivierte externe Angreifer richten in dieser Branche weiterhin großen Schaden an.
Zusammenfassung	Hacking- und Malware-Aktivitäten liegen als häufigste Muster Kopf an Kopf. Social Engineering liegt weit abgeschlagen auf Platz drei, stellt aber trotzdem ebenfalls eine nicht zu unterschätzende Gefahr dar. Ein weiteres wichtiges Risiko für diesen Sektor sind Denial-of-Service-Angriffe auf die Infrastrukturen, die unter anderem das Einhalten von Terminen gefährden sollen.

Bergbau-, Öl- und Gasindustrie plus Versorgungsbetriebe

(NAICS 21 u. 22)

Absolute Häufigkeit	143 Vorfälle, davon 47 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, einfache Angriffe auf Web-Anwendungen und sonstige Fehler machten 81 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (80 %), Insider (20 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (63–93 %), Spionage (4–32 %), Rache (1–21 %), Ideologische Motive (0–15 %), Mutwille/Angst/Spaß/Sonstige/Folgeangriffe (je 0 %–7 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (50 %), Insider (33 %), Sonstige (26 %), Anmeldedaten (24 %)
Anhaltende Trends	System Intrusions und einfache Angriffe auf Web-Anwendungen sind in dieser Branche weiterhin besorgniserregend weit verbreitet.
Zusammenfassung	Ransomware wird bei etwa einem Drittel der Angriffe in diesem Sektor genutzt. Social Engineering verliert – entgegen dem allgemeinen Trend – in dieser Branche an Bedeutung.

Anbieter qualifizierter, technischer und wissenschaftlicher Dienstleistungen

(NAICS 54)

Absolute Häufigkeit	1.398 Vorfälle, davon 423 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering machten 90 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (92 %), Insider (9 %), Mehrere Akteure (3 %), Partner (2 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (96 %), Spionage (4 %), Mutwille (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (57 %), Anmeldedaten (53 %), Sonstige (25 %), Insider (16 %)
Anhaltende Trends	System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering sind weiterhin die größten Bedrohungen in diesem Sektor.
Zusammenfassung	Obwohl die häufigsten Angriffs- und Vorfallsmuster sich nicht geändert haben, ist in dieser Branche ein Anstieg der Ransomware-Angriffe zu verzeichnen. Die wichtigsten Angriffsvektoren sind dabei die gleichen wie im vorigen Jahr.

Öffentliche Verwaltung

(NAICS 92)

Absolute Häufigkeit	3.273 Vorfälle, davon 584 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, verlorene und gestohlene Ressourcen sowie Social Engineering machten 76 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (85 %), Insider (30 %), Mehrere Akteure (16 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (68 %), Spionage (30 %), Ideologische Motive (2 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Personenbezogene Daten (38 %), Sonstige (35 %), Anmeldedaten (33 %), Insider (32 %)
Anhaltende Trends	Die Branche steht nach wie vor im Visier finanziell motivierter externer Angreifer, verzeichnet jedoch auch eine signifikante Zahl von Spionageoperationen durch ausländische Akteure, die wissen wollen, womit ihre Rivalen sich beschäftigen. Die am häufigsten gestohlene Datenart sind weiterhin personenbezogene Daten.
Zusammenfassung	Spionage spielt in diesem Sektor als Motiv nach wie eine größere Rolle als in allen anderen Branchen. Auch der Anteil der Sicherheitsverletzungen mit mehreren Akteuren ist hier besonders hoch. Eine Koalition aus externen Angreifern, Partnern und/oder Insidern, die gemeinsam Daten stehlen, ist keine besonders wünschenswerte Form der internationalen Zusammenarbeit.

Einzelhandel

(NAICS 44–45)

Absolute Häufigkeit	406 Vorfälle, davon 193 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 88 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (94 %), Insider (7 %), Mehrere Akteure (2 %), Partner (2 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (100 %), Spionage (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Zahlungsdaten (37 %), Anmeldedaten (35 %), Sonstige (32 %), Personenbezogene Daten (23 %)
Anhaltende Trends	Einzelhandelsunternehmen sind weiterhin ein lukratives Ziel für Cyberkriminelle, die Zahlungskartendaten stehlen wollen.
Zusammenfassung	Die drei häufigsten Angriffs- und Vorfallsmuster sind im Einzelhandel zwar dieselben wie in vielen anderen Sektoren, doch neben den überall beobachteten Bedrohungen wie Ransomware und einfachen Angriffen auf Web-Anwendungen spielt hier auch der Diebstahl von Zahlungskartendaten eine große Rolle.

Kleine und mittlere Unternehmen

In einigen früheren Berichten haben wir kleine und mittlere Unternehmen (KMU) mit Großkonzernen verglichen, um zu sehen, ob deren Angriffsflächen sich erheblich voneinander unterscheiden. Inzwischen nutzen KMUs und Großkonzerne zunehmend ähnliche Services und Infrastrukturen, wodurch ihre Angriffsflächen mehr Gemeinsamkeiten aufweisen als je zuvor. Infolgedessen hängen die Angriffsprofile nun weniger von der Unternehmensgröße ab. Es gibt jedoch nach wie vor große Unterschiede bei der Fähigkeit von Unternehmen zur Bedrohungsabwehr, da diese erheblich davon abhängt, welche Ressourcen im Ernstfall zur Verfügung stehen.

Deshalb haben wir in diesem Jahr beschlossen, auf den Ergebnissen unserer Zusammenarbeit mit MITRE zum Abgleich der Frameworks VERIS und ATT&CK aufzubauen und praxistaugliche Empfehlungen zur koordinierten Nutzung dieser Frameworks und der empfohlenen Abwehrmaßnahmen des Center for Internet Security Implementation Group (CIS Controls) für KMUs verschiedener Größen zu geben.

Die Frameworks kommen
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). Wir haben eine Darstellungsweise entwickelt, die auf der MITRE ATT&CK Matrix und den vom CIS veröffentlichten kritischen Sicherheitssystemen (Critical Security Controls) basiert und Unternehmen die Entwicklung und Umsetzung eines datengestützten Cybersicherheitsprogramms erleichtern soll.

Am 6. April 2023 wurde die zweite Version der VERIS/ATT&CK-Zuordnung veröffentlicht. Ausführlichere Informationen dazu finden Sie unter https://center-for-threat-informed-defense.github.io/attack_to_veris/. Vor dem Hintergrund der immer strengeren gesetzlichen Vorschriften zur Meldung von Datenlecks – bislang ohne ein allgemein akzeptiertes Format für diese Meldungen – kommt diese erneute Kooperation zum richtigen Zeitpunkt.

	Kleine und mittlere Unternehmen (weniger als 1.000 Angestellte)	**Großunternehmen (mehr als 1.000 Angestellte)**
Absolute Häufigkeit	699 Vorfälle, davon 381 mit bestätigten Datenlecks	496 Vorfälle, davon 227 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 92 % der bestätigten Sicherheitsverletzungen aus.	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 85 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (94 %), Insider (7 %), Mehrere Akteure (2 %), Partner (1 %)	Bestätigte Sicherheitsverletzungen: Externe Angreifer (89 %), Insider (13 %), Mehrere Akteure (2 %), Partner (2 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (98 %), Spionage (1 %), Mutwille (1 %), Rache (1 %)	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (97 %), Spionage (3 %), Ideologische Motive (2 %), Mutwille (1 %), Spaß (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Anmeldedaten (54 %), Insider (37 %), Sonstige (22 %), Systemdaten (11 %)	Bestätigte Sicherheitsverletzungen: Insider (41 %), Anmeldedaten (37 %), Sonstige (30 %), Systemdaten (22 %)

Ergebnisse für spezifische Regionen

In dieser Ausgabe des DBIR präsentieren wir zum vierten Mal regionsspezifische Vorfallsdaten und Erkenntnisse, um unseren Lesern und Leserinnen eine – hoffentlich interessante und nützliche – breitere Perspektive der globalen Cyberkriminalität zu vermitteln. Wie schon in früheren Berichten müssen wir dabei allerdings auch dieses Jahr wieder darauf hinweisen, dass der Umfang und die Detailgenauigkeit unserer regionalen Analysen von vielen Faktoren abhängen, darunter von der Mitarbeit von Unternehmen in der Region, regionalen gesetzlichen Meldevorgaben und unseren eigenen Daten. Falls Ihre Region im Folgenden nicht erwähnt wird, nehmen Sie bitte Kontakt mit uns auf, um über eine mögliche Bereitstellung von Daten für zukünftige Berichte zu sprechen und fordern Sie Fachkollegen in Ihrer Region auf, dies ebenfalls zu tun. Nur so können wir die Qualität und geografische Abdeckung dieses Berichts Jahr für Jahr verbessern. Wenn Ihre Region hier nicht erwähnt wird, heißt das nicht, dass wir keinerlei Daten haben, sondern nur, dass wir nicht genug Vorfälle für eine statistisch relevante Analyse Ihrer Region untersuchen konnten.

Asien-Pazifik (APAC)

Absolute Häufigkeit	699 Vorfälle, davon 164 mit bestätigten Datenlecks
Vorherrschende Muster	Social Engineering, System Intrusions und einfache Angriffe auf Web-Anwendungen machten 93 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (92 %), Insider (9 %), Partner (2 %), Mehrere Akteure (2 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (61 %), Spionage (39 %), Mutwille (2 %), Rache (2 %), Folgeangriffe (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Insider (56 %), Betriebsgeheimnisse (42 %), Sonstige (33 %), Anmeldedaten (29 %)

Europa, Naher Osten und Afrika (EMEA)

Absolute Häufigkeit	2.557 Vorfälle, davon 637 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 97 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätige Sicherheitsverletzungen: Externe Angreifer (98 %), Insider (2 %), Mehrere Akteure (1 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (91 %), Spionage (8 %), Ideologische Motive (1 %), Spaß (1 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Anmeldedaten (53 %), Insider (37 %), Systemdaten (35 %), Sonstige (15 %)

Lateinamerika und Karibik (LAC)

Absolute Häufigkeit	535 Vorfälle, davon 65 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, Social Engineering und einfache Angriffe auf Web-Anwendungen machten 94 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (95 %), Insider (5 %), Partner (2 %), Mehrere Akteure (2 %)
Motive der Angreifer	Bestätige Sicherheitsverletzungen: Finanzielle Motive (93 %), Spionage (11 %), Ideologische Motive (2 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Systemdaten (55 %), Insider (32 %), Geheime/Vertrauliche Daten (23 %), Anmeldedaten (23 %), Sonstige (19 %)

Nordamerika (NA)

Absolute Häufigkeit	9.036 Vorfälle, davon 1.924 mit bestätigten Datenlecks
Vorherrschende Muster	System Intrusions, einfache Angriffe auf Web-Anwendungen und Social Engineering machten 85 % der bestätigten Sicherheitsverletzungen aus.
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (94 %), Insider (12 %), Mehrere Akteure (9 %), Partner (2 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (99 %), Spionage (1 %), Rache (1 %)
Betroffene Daten	Bestätige Sicherheitsverletzungen: Anmeldedaten (67 %), Insider (50 %), Personenbezogene Daten (38 %), Sonstige (24 %)

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.

Den vollständigen DBIR 2023 finden Sie unter verizon.com/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. Wir würden uns sehr über Ihre Beiträge zu zukünftigen Ausgaben des jährlich erscheinenden Verizon DBIR freuen. Der Anmeldeprozess ist klar und einfach. Bitte schicken Sie eine E-Mail an dbircontributor@verizon.com. Verbesserungsvorschläge können Sie per Tweet an @VZDIR schicken. Weitere Informationen über das Framework VERIS finden Sie unter verisframework.org.