

# DBIR 2022: Medien und Unterhaltung

Überblick

(NAICS 71)

**Herzlich willkommen zum Überblick über Medien und Unterhaltung, Ihrer branchenspezifischen Kurzfassung der 15. Ausgabe des jährlich erscheinenden Verizon Data Breach Investigations Report (DBIR). Es ist kaum zu glauben, dass unser erster Bericht nun schon 15 Jahre zurückliegt.**

Seither untersuchen wir im DBIR, welche Arten von Cyberangriffen aktuell besonders häufig auftreten und wie Unternehmen sich vor ihnen schützen können. Dieses Jahr haben wir dazu 23.896 Vorfälle analysiert, darunter 215 aus der Medien- und Unterhaltungsbranche. Bei 96 dieser Vorfälle wurden den Angaben der Betroffenen zufolge Daten gestohlen. Diese und alle anderen in diesem Bericht präsentierten Zahlen 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 die gängigsten Angriffsmethoden in der Medien- und Unterhaltungsbranche sowie nützliche Informationen zur besseren Vorbereitung auf deren Abwehr vermittelt.

Im Folgenden finden Sie eine Übersicht über die für Ihre Branche relevantesten Untersuchungsergebnisse aus dem diesjährigen Bericht, die Sie gern an Ihre Kollegen weiterleiten

**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. Ausführliche Informationen über die Codes und das Klassifizierungssystem finden Sie unter: [census.gov/naics/?58967?yearbck=2012](https://census.gov/naics/?58967?yearbck=2012)**

können. Der vollständige Bericht ist (auf Englisch) unter [verizon.com/dbir](https://verizon.com/dbir) zum Download verfügbar und enthält eine detailliertere Beschreibung der Bedrohungslage im Jahr 2022.

---

## Angriffs- und Vorfalldmuster

Die Angriffs- und Vorfalldmuster wurden im DBIR 2014 als nützliche Typologie häufig auftretender Szenarien eingeführt. Im vergangenen Jahr haben wir sie überarbeitet und ihre Anzahl von neun auf acht reduziert, um Veränderungen in den Angriffsmethoden und der Bedrohungslage widerzuspiegeln.

Diese acht Muster wurden mithilfe eines eleganten maschinellen Lernverfahrens für das Clustering identifiziert und bilden komplexe Interaktionszusammenhänge sowie das Geschehen im Verlauf einer Sicherheitsverletzung besser ab. Dadurch eignen sie sich unter anderem als Grundlage für praktische Empfehlungen zur Prävention entsprechender Vorfälle.

---

## Social Engineering

**Psychologische Manipulation, die das Opfer zu einer Handlung verleiten soll, die grundlegende Datenschutzprinzipien verletzt**

Menschliche Fehler leisten noch immer 82 % aller Sicherheitsverstöße Vorschub, und ein großer Teil dieser Vorfälle entfällt auf dieses Angriffsmuster. Hinzu kommt, dass Angreifer sich mit Social Engineering nicht nur Zugang zu einer Umgebung verschaffen, sondern oft auch Malware einschleusen oder Zugangsdaten stehlen, um dann in einem zweiten Schritt noch mehr Schaden anzurichten. Das unterstreicht, wie wichtig die Sensibilisierung der Mitarbeiter für diese Gefahr ist.

- Bei 59 % der untersuchten Social-Engineering-Angriffe wurden Anmeldedaten gestohlen und bei 31 % wurden gestohlene Anmeldedaten genutzt. Bei Social-Engineering-Angriffen ist die Wahrscheinlichkeit, dass Anmeldedaten gestohlen werden, dreimal höher als bei den anderen Angriffs- und Vorfalldmustern.
- Phishing wird bei diesen Angriffen doppelt so häufig genutzt wie das sogenannte Pretexting, bei dem der Angreifer einen Vorwand schafft, um Kontakt zu seinem Opfer herzustellen.
- Finanzielle Bereicherung tritt bei Social-Engineering-Angriffen achtmal häufiger als Motiv auf als Spionage.

## Einfache Angriffe auf Web-Anwendungen

### Vorfälle, bei denen die Angreifer eine Web-Anwendung kapern und danach nur wenige weitere Schritte oder zusätzliche Aktionen durchführen

In den meisten Fällen missbrauchen sie dabei gestohlene Anmeldedaten, um sich Zugang zu den über das Internet erreichbaren Infrastrukturkomponenten eines Unternehmens (wie Webserver oder E-Mail-Server) zu verschaffen.

- Bei vier von fünf Angriffen auf Web-Anwendungen werden gestohlene Anmeldedaten verwendet. Dieses Ergebnis unterstreicht die Bedeutung strenger Passworrichtlinien.
- Einfache Angriffe auf Web-Anwendungen dienen mit viermal höherer Wahrscheinlichkeit Spionagezwecken als andere Angriffskategorien. Das lässt den Schluss zu, dass im staatlichen Auftrag handelnde Hacker bereitwillig auf komplexe Angriffe verzichten, wenn sie ihre Ziele mit einfacheren Methoden erreichen können.
- Im Kontext der einfachen Angriffe auf Web-Anwendungen ist der Missbrauch gestohlener Anmeldedaten sechsmal wahrscheinlicher als die Ausnutzung vorhandener Schwachstellen.

## System Intrusion

### Komplexe Angriffe, bei denen Malware und/oder Hacker-Methoden zur Einschleusung von Ransomware oder zur Realisierung anderer Zielsetzungen eingesetzt werden

Mit diesem Muster werden komplexe Angriffe beschrieben, die sich durch eine Kombination mehrerer Aktivitäten (wie Social Engineering, Malware und Hacking) auszeichnen. Angriffe über Lieferketten und Ransomware sind zwei Varianten dieses Musters, die in diesem Jahr stark gestiegen sind.

- 92 % der System Intrusions sind finanziell motiviert.
- Im Kontext von System Intrusions ist der Missbrauch gestohlener Anmeldedaten viermal wahrscheinlicher als die Ausnutzung vorhandener Schwachstellen.

## Diverse Fehler

### Vorfälle, bei denen die Sicherheit von Datenbeständen durch unbeabsichtigte Handlungen gefährdet wird Abhandlungskomponente Geräte gehören nicht zu dieser Kategorie, da sie bereits im Muster „Verlorene und gestohlene Ressourcen“ enthalten sind.

Die diesjährigen Daten zeigen, welche wichtige Rolle die Mitarbeiter spielen. Die beiden häufigsten Varianten „diverser Fehler“ sind Falschzustellungen und Fehlkonfigurationen. Fehlkonfigurationen werden häufig im Zusammenhang mit der Erkennungsmethode „Sicherheitsforscher“ genannt.

- Falsch konfigurierte Server, die infolge solcher Fehler über das Internet erreichbar sind, und der Versand von E-Mails an falsche Empfänger („Falschzustellungen“) machen 13 % aller Sicherheitsverstöße aus.

- Im Vorjahresvergleich sind externe Cloud-Speicher um 83 % seltener die Ursache für Sicherheitsverletzungen der Kategorie „diverse Fehler“. Das ist möglicherweise ein Hinweis auf die verstärkte Nutzung standardmäßig sicherer Technologien („Secure by Default“).
- 85 % der Sicherheitsverletzungen dieser Kategorie betreffen Server.

## Missbrauch von Nutzerrechten

### Sicherheitsvorfälle rund um die unbefugte oder böswillige Nutzung legitimer Zugriffsrechte

Die meisten Vorfälle dieser Art führen zu Datendiebstahl. Die Täter sind nach wie vor in der Regel finanziell motiviert und stehlen personenbezogene Daten, weil diese sich leicht zu Geld machen lassen.

- Im Vergleich zu allen anderen Kategorien sind von diesen Sicherheitsverletzungen mit dreimal höherer Wahrscheinlichkeit Dokumente betroffen.

## Verlorene und gestohlene Ressourcen

### Sicherheitsvorfälle, bei denen IT-Assets verloren gehen oder entwendet werden

Diebstahl ist in der Regel finanziell motiviert und wir gehen davon aus, dass auch IT-Ressourcen oft mit der Absicht gestohlen werden, sich am Weiterverkauf zu bereichern.

- Die von diesen Verbrechen betroffenen Daten sind (fast) haargenau dieselben wie im letzten Jahr. Während Diebstahl in der Regel von Außenstehenden begangen wird, sind für verlorene Assets natürlich Mitarbeiter verantwortlich.
- Die Täter gehören mit 14 Mal höherer Wahrscheinlichkeit keiner organisierten Gruppe an als bei anderen Vorfällen.

## Denial-of-Service

### Angriffe auf Netzwerk- oder Anwendungsebene, die die Verfügbarkeit von Netzwerken und Systemen beeinträchtigen

Große Unternehmen werden doppelt so häufig mit Denial-of-Service-Attacken (DoS-Attacken) angegriffen wie mit den anderen Angriffs- und Vorfällen. Für viele sind sie kaum mehr als ein Ärgernis, doch einige sind so häufig betroffen, dass es ihr Geschäftsmodell beeinträchtigt.

## Alles Andere

### Dies ist keine echte „Kategorie“, sondern ein Sammelbecken für alle Vorfälle, die sich keinem der anderen Muster zuordnen lassen.

## Medien und Unterhaltung

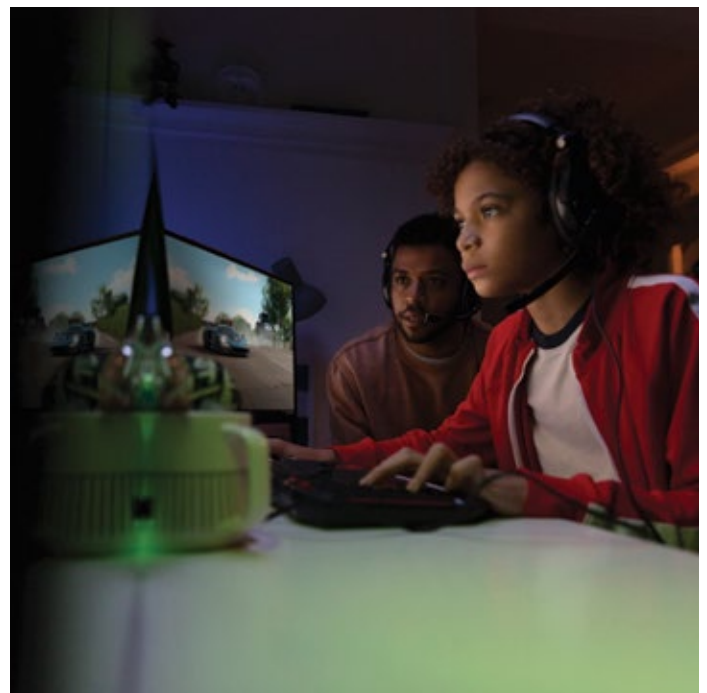
Die Spitzenplätze in dieser Branche belegen einmal mehr die Angriffs- und Vorfalldmuster System Intrusion und einfache Angriffe auf Web-Anwendungen, die jedoch im Vergleich zum Vorjahr die Positionen getauscht haben. „Diverse Fehler“ findet sich unverändert auf Platz drei. Außerdem sind Denial-of-Service-Angriffe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

Muster im Zeitverlauf	Fünjahres-trend	Dreijahres-trend	Vergleich mit anderen Branchen
<b>Einfache Angriffe auf Web-Anwendungen</b>	Unverändert	Unverändert	Unverändert
<b>System Intrusion</b>	Unverändert	Unverändert	Rückläufig
<b>Diverse Fehler</b>	Unverändert	Unverändert	Zunehmend

Die wichtigste Einkommensquelle der Medien- und Unterhaltungsbranche sind Live-Events wie Tanz-, Theater- oder Sportveranstaltungen. Das entscheidende Kriterium ist, dass sie nicht vorab aufgezeichnet und erst später ausgestrahlt werden. Außerdem gehört auch das Glücksspiel zu dieser Kategorie. Unter diesem NAICS-Code werden also sehr verschiedene Organisationen mit nahezu unvorstellbar diversen Angriffsflächen zusammengefasst. Viele haben jedoch gemeinsam, dass zumindest ein Teil ihrer Infrastruktur für kritische Funktionen auf das Internet angewiesen ist. Das können zum Beispiel der Kartenverkauf oder die Entgegennahme von Bestellungen (oder auch Wetten) sein. Eine Denial-of-Service-Attacke ist dort natürlich ein sehr ungern gesehener Gast. Nichtsdestotrotz sind DoS-Attacken geradezu Stammgäste in dieser Kategorie (insbesondere in der Glücksspielbranche der asiatisch-pazifischen Region) und machen 20 % der Vorfälle aus.

Der Spitzenplatz der einfachen Angriffe auf Web-Anwendungen ist besorgniserregend, da die Angreifer hierfür kaum Vorkenntnisse benötigen. Bei System Intrusions müssen sie sich viel mehr anstrengen und setzen auch häufig Ransomware ein. Wie schon in früheren Jahren nutzen alle Angreifer sehr gern gestohlene Anmeldedaten, um sich als legitime Mitarbeiter auszugeben und unerkannt zu bleiben, bis sie ihr Ziel erreicht haben.

<b>Absolute Häufigkeit</b>	215 Vorfälle, davon 96 mit bestätigten Datenlecks
<b>Top-Muster</b>	Einfache Angriffe auf Web-Anwendungen, System Intrusions und Diverse Fehler: 80 % der bestätigten Sicherheitsverletzungen
<b>Urheber der Bedrohungen</b>	Bestätigte Sicherheitsverletzungen: Externe Angreifer (74 %), Insider (26 %)
<b>Motive der Angreifer</b>	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (97 %), Rache (3 %)
<b>Betroffene Daten</b>	Bestätigte Sicherheitsverletzungen: Personenbezogene Daten (66 %), Anmeldedaten (49 %), Sonstige (23 %), Gesundheitsdaten (15 %)
<b>Empfohlene Abwehrmaßnahmen (CIS Controls für IG1)</b>	Schulungen zur Steigerung des Sicherheitsbewusstseins (CSC 14), Sichere Konfiguration der Unternehmensressourcen und -software (CSC 4), Zugangskontrolle (CSC 6)
<b>Anhaltende Trends</b>	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.



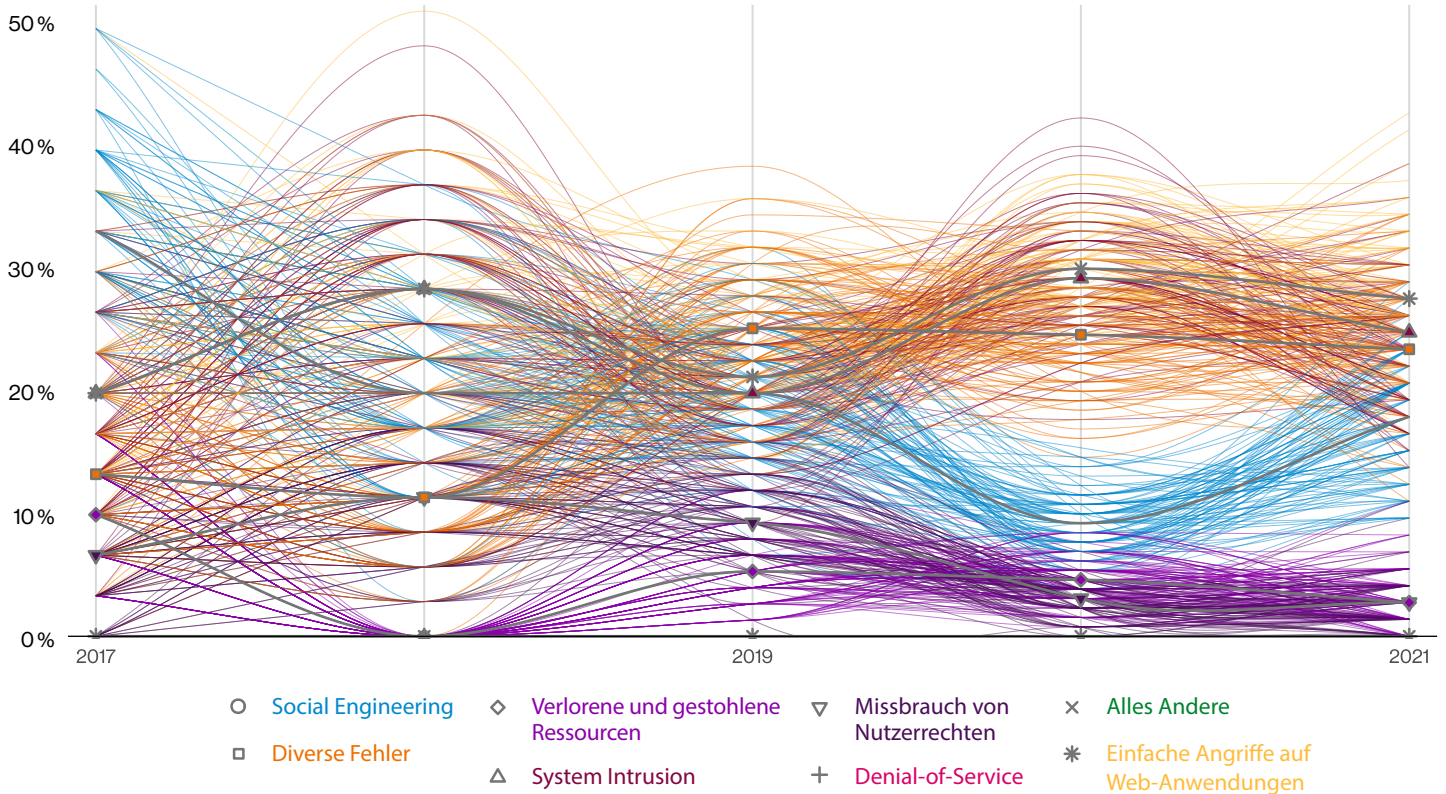


Abbildung 1: Relative Häufigkeit der Muster in der Medien- und Unterhaltungsbranche im Zeitverlauf

Bei Datendiebstählen wurden wieder vor allem personenbezogene und Anmeldedaten entwendet. Bei personenbezogenen Daten ist jedoch ein Rückgang gegenüber den 83 % vom vorigen Jahr zu verzeichnen. Seltsamerweise werden immer noch bei 15 % der Datendiebstähle Gesundheitsdaten erbeutet. Das ist besser als der Vorjahreswert (26 %), aber immer noch erstaunlich für eine Branche ohne Verbindung zum Gesundheitswesen. Vielleicht stammen diese Daten von Unternehmen, die eine Gesundheitsversicherung für ihre Mitarbeiter abgeschlossen haben und daher Daten dieser Art speichern müssen, oder aus Dateien über Entschädigungen für Arbeitsunfälle. Ein Teil der gestohlenen Patientenakten könnte auch von Sportmannschaften stammen, die ebenfalls unter diesen NAICS-Code fallen. Trotzdem hat uns dieses Ergebnis überrascht.

Diverse Fehler zählen auch in diesem Jahr wieder zu den drei häufigsten Vorfalldmustern (25 %) und halten damit ihre Position vom Vorjahr. Der häufigste dieser Fehler waren Fehlkonfigurationen (ca. 15 % der bestätigten Sicherheitsverletzungen). Die Branche scheint ein Problem gegen ein anderes ausgetauscht zu haben, denn Falschzustellungen (der häufigste Fehler 2021) sind erheblich zurückgegangen.

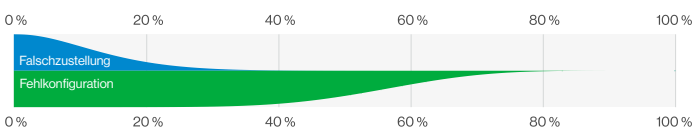


Abbildung 2: Anteil der Falschzustellungen und Fehlkonfigurationen bei Sicherheitsverstößen der Kategorie „Diverse Fehler“ (Medien und Unterhaltung, n=16)

### Vertrauen in unsere Daten

Seit dem DBIR 2019 weist die schräge rechte Kante der Balken in unseren Balkendiagrammen darauf hin, dass man in der Informationssicherheit nichts mit absoluter Gewissheit sagen kann.

Die Abschrägung zeigt das 95%-Konfidenzintervall an (den Standardwert für statistische Tests).

Spaghetti-Diagramme und die relativ neuen Piktogramm-Plots sollen die inhärente Ungewissheit auf ähnliche Weise abbilden, sind aber besser für eine einzige Proportion geeignet.

### Halten Sie sich und Ihr Team auf dem Laufenden

Um den aktuellen Bedrohungen in der Medien- und Unterhaltungsbranche 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.

Den vollständigen DBIR 2022 finden Sie unter <https://www.verizon.com/business/de-de/resources/reports/dbir/>.

Einzelheiten zum Netzwerk und Abdeckungskarten finden Sie unter <https://www.verizon.com/business/de-de>. © 2022 Verizon. FL5491022